FortiGate® UTM User Guide

FortiOS™ 4.0 MR1
Introduction .......................................................................................................................... 9
Before you begin .................................................................................................................... 9
How this guide is organized ............................................................................................... 9
Document conventions ....................................................................................................... 10
IP addresses .......................................................................................................................... 10
Cautions, Notes and Tips .................................................................................................... 10
Typographical conventions ............................................................................................... 11
CLI command syntax ......................................................................................................... 12
Registering your Fortinet product ..................................................................................... 13
Fortinet products End User License Agreement .............................................................. 13
Customer service and technical support .......................................................................... 13
Training .................................................................................................................................. 13
Fortinet documentation .................................................................................................... 14
Tools and Documentation CD ............................................................................................ 14
Fortinet Knowledge Base .................................................................................................. 14
Comments on Fortinet technical documentation ............................................................. 14
UTM overview .................................................................................................................... 15
UTM components ................................................................................................................ 15
AntiVirus .................................................................................................................................. 15
Intrusion Protection System (IPS) ...................................................................................... 15
Anomaly protection (DoS policies) .................................................................................... 16
One-armed IDS (sniffer policies) ...................................................................................... 16
Web filtering ......................................................................................................................... 16
Email filtering ....................................................................................................................... 16
Data Leak Prevention (DLP) .............................................................................................. 16
Application Control (for example, IM and P2P) ............................................................... 16
Protection profiles ................................................................................................................. 17
SSL content scanning and inspection .............................................................................. 17
Setting up certificates to avoid client warnings ............................................................... 18
SSL content scanning and inspection settings ............................................................... 20
Network defence ................................................................................................................ 23
Monitoring ............................................................................................................................ 23
Blocking external probes ................................................................................................... 23
Address sweeps .................................................................................................................... 23
Port scans ............................................................................................................................. 24
Probes using IP traffic options ....................................................................................... 24
Evasion techniques ............................................................................................................. 24
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Defending against DoS attacks</td>
<td>26</td>
</tr>
<tr>
<td>The “three-way handshake”</td>
<td>26</td>
</tr>
<tr>
<td>SYN flood</td>
<td>27</td>
</tr>
<tr>
<td>SYN spoofing</td>
<td>28</td>
</tr>
<tr>
<td>DDoS SYN flood</td>
<td>28</td>
</tr>
<tr>
<td>Configuring the SYN threshold to prevent SYN floods</td>
<td>29</td>
</tr>
<tr>
<td>SYN proxy</td>
<td>29</td>
</tr>
<tr>
<td>Other flood types</td>
<td>29</td>
</tr>
<tr>
<td>Traffic inspection</td>
<td>29</td>
</tr>
<tr>
<td>IPS signatures</td>
<td>30</td>
</tr>
<tr>
<td>Suspicious traffic attributes</td>
<td>30</td>
</tr>
<tr>
<td>DoS policies</td>
<td>30</td>
</tr>
<tr>
<td>Application control</td>
<td>31</td>
</tr>
<tr>
<td>Content inspection and filtering</td>
<td>31</td>
</tr>
<tr>
<td>AntiVirus</td>
<td>31</td>
</tr>
<tr>
<td>FortiGuard Web Filtering</td>
<td>32</td>
</tr>
<tr>
<td>Email filter</td>
<td>32</td>
</tr>
<tr>
<td>DLP</td>
<td>32</td>
</tr>
<tr>
<td>AntiVirus</td>
<td>35</td>
</tr>
<tr>
<td>Antivirus concepts</td>
<td>35</td>
</tr>
<tr>
<td>Antivirus scanning order</td>
<td>35</td>
</tr>
<tr>
<td>Antivirus techniques</td>
<td>37</td>
</tr>
<tr>
<td>FortiGuard Antivirus</td>
<td>38</td>
</tr>
<tr>
<td>Enable antivirus scanning</td>
<td>38</td>
</tr>
<tr>
<td>Enable the file quarantine</td>
<td>38</td>
</tr>
<tr>
<td>Viewing antivirus database information</td>
<td>38</td>
</tr>
<tr>
<td>General configuration steps</td>
<td>39</td>
</tr>
<tr>
<td>Configuring the file quarantine</td>
<td>39</td>
</tr>
<tr>
<td>Enabling the extended virus database</td>
<td>40</td>
</tr>
<tr>
<td>Enabling quarantine in protection profiles</td>
<td>40</td>
</tr>
<tr>
<td>Adding the protection profile to a policy</td>
<td>40</td>
</tr>
<tr>
<td>Viewing quarantined files</td>
<td>41</td>
</tr>
<tr>
<td>Downloading quarantined files</td>
<td>41</td>
</tr>
<tr>
<td>Enable file filtering</td>
<td>41</td>
</tr>
<tr>
<td>General configuration steps</td>
<td>42</td>
</tr>
<tr>
<td>Creating a file filter list</td>
<td>42</td>
</tr>
<tr>
<td>Creating a file pattern</td>
<td>42</td>
</tr>
<tr>
<td>Creating a file type</td>
<td>42</td>
</tr>
<tr>
<td>Enable file filtering</td>
<td>43</td>
</tr>
<tr>
<td>Enable grayware scanning</td>
<td>43</td>
</tr>
<tr>
<td>Testing your antivirus configuration</td>
<td>44</td>
</tr>
</tbody>
</table>
AntiVirus example......................................................................................................... 44
Protecting your network against malicious email attachments.............................. 44

Email filter.................................................................................................................... 47

Email filtering concepts ............................................................................................ 47
  Email filter techniques ......................................................................................... 47
  Order of spam filtering ...................................................................................... 48

Enable email filtering ............................................................................................... 49
  Enabling FortiGuard IP address checking ............................................................. 50
  Enabling FortiGuard URL checking .................................................................... 50
  Enabling FortiGuard email checksum checking.................................................... 51
  Enabling FortiGuard spam submission .................................................................. 51
  Enabling IP address black/white list checking ....................................................... 51
  Enabling HELO DNS lookup ................................................................................ 53
  Enabling email address black/white list checking ............................................... 53
  Enabling return email DNS checking .................................................................. 55
  Enabling banned word checking ......................................................................... 55
  How content is evaluated ..................................................................................... 55

Configure the spam action ....................................................................................... 58

Configure the tag location ....................................................................................... 58

Configure the tag format ......................................................................................... 59

Email filter example ................................................................................................ 59
  Blocking email from a user .................................................................................. 59

Intrusion protection .................................................................................................. 61

IPS concepts ............................................................................................................. 61
  Anomaly-based defense ....................................................................................... 61
  Signature-based defense ...................................................................................... 61

Enable IPS scanning ................................................................................................ 63
  General configuration steps ................................................................................ 63
  Creating an IPS sensor ......................................................................................... 63
  Creating an IPS filter ........................................................................................... 64
  Updating predefined IPS signatures ..................................................................... 64
  Creating an IPS signature override ..................................................................... 64
  Creating a custom IPS signature ........................................................................ 65
  Custom signature syntax and keywords .............................................................. 65

Configure protocol decoders .................................................................................. 74

Enable packet logging ............................................................................................. 74

IPS examples ............................................................................................................ 75
  Using IPS to protect your web server ................................................................. 75
  Custom signature to block access to example.com ............................................. 77
  Custom signature to block the SMTP “vrfy” command ..................................... 79
# Web filtering

- **Web filtering concepts** ................................................................. 81
  - Different ways of controlling access ........................................... 83
  - Order of web filtering .............................................................. 83

- **Web content filter** ........................................................................ 83
  - General configuration steps ................................................... 84
  - Creating a web filter content list ............................................ 84
  - Configuring a web content filter list ....................................... 84
  - How content is evaluated ....................................................... 85
  - Enabling the web content filter and setting the content threshold 86

- **URL filter** ......................................................................................... 86
  - General configuration steps ................................................... 87
  - Creating a URL filter list ....................................................... 87
  - Configuring a URL filter list ................................................ 87

- **Web filtering example** ............................................................... 88
  - School district ........................................................................... 88

# FortiGuard Web Filtering

- **Before you begin** ........................................................................ 93

- **FortiGuard Web Filtering and your FortiGate unit** ................... 93
  - Order of Web Filtering .......................................................... 94

- **Enable FortiGuard Web Filtering** ............................................. 94
  - General configuration steps ................................................... 94
  - Configuring FortiGuard Web Filtering settings .................... 95
  - Configuring the FortiGuard Web Filtering categories .......... 96
  - Configuring the FortiGuard Web Filtering classifications .... 97

- **Add or change FortiGuard Web Filtering ratings** ................... 97

- **Create FortiGuard Web Filtering overrides** ............................. 98
  - Understanding administrative and user overrides ................. 98

- **Customize categories and ratings** ............................................ 99
  - Creating local categories ..................................................... 99
  - Customizing site ratings ....................................................... 99

- **FortiGuard Web Filtering example** ........................................ 100
  - School district ........................................................................ 100

# Data leak prevention

- **Data leak prevention concepts** ................................................ 101
  - DLP sensor ............................................................................. 101
  - DLP rule ................................................................................ 101
  - DLP compound rule ............................................................. 102
Introduction

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

The FortiGate UTM Guide describes the Unified Threat Management (UTM) features available on your FortiGate unit, including antivirus, intrusion prevention system (IPS), anomaly protection, 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 chapter contains the following topics:

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

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. Currently, the models include: 110C, 111C, 310B, 602B, 3016B, 3600A, 3810A, 5005FA2, 5001A.

How this guide is organized

This document contains the following chapters:

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

DoS overview: 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 filtering and FortiGuard Web Filtering: The first of these chapters describes basic web filtering concepts, the order in which the FortiGate unit performs web filtering, and configuration. The second chapter describes enhanced features of the subscription-based FortiGuard Web Filtering service and explains how to configure them. We recommend reading both chapters 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.

Cautions, Notes and Tips

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

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

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

**Tip:** Highlights useful additional information, often tailored to your workplace activity.
## Typographical conventions

Fortinet documentation uses the following typographical conventions:

<table>
<thead>
<tr>
<th>Convention</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Button, menu, text box,</td>
<td>From <em>Minimum log level</em>, select <em>Notification</em>.</td>
</tr>
<tr>
<td>field, or check box label</td>
<td></td>
</tr>
<tr>
<td>CLI input*</td>
<td><code>config system dns</code></td>
</tr>
<tr>
<td></td>
<td><code>set primary &lt;address_ipv4&gt;</code></td>
</tr>
<tr>
<td></td>
<td><code>end</code></td>
</tr>
<tr>
<td>CLI output</td>
<td><code>FGT-602803030703 # get system settings</code></td>
</tr>
<tr>
<td></td>
<td><code>comments : (null)</code></td>
</tr>
<tr>
<td></td>
<td><code>opmode : nat</code></td>
</tr>
<tr>
<td>Emphasis</td>
<td>HTTP connections are <em>not</em> secure and can be intercepted by a third</td>
</tr>
<tr>
<td></td>
<td>party.</td>
</tr>
<tr>
<td>File content</td>
<td><code>&lt;HTML&gt;&lt;HEAD&gt;&lt;TITLE&gt;Firewall Authentication&lt;/TITLE&gt;&lt;/HEAD&gt;</code></td>
</tr>
<tr>
<td></td>
<td><code>&lt;BODY&gt;&lt;H4&gt;You must authenticate to use this service.&lt;/H4&gt;</code></td>
</tr>
<tr>
<td>Keyboard entry</td>
<td>Type a name for the remote VPN peer or client, such as <code>Central_Office_1</code>.</td>
</tr>
<tr>
<td>Navigation</td>
<td>Go to <code>VPN &gt; IPSEC &gt; Auto Key (IKE)</code>.</td>
</tr>
<tr>
<td>Publication</td>
<td>For details, see the <em>FortiGate Administration Guide</em>.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Links typically go to the most recent version. To access earlier releases, go to <a href="http://docs.fortinet.com/">http://docs.fortinet.com/</a>. This link appears at the bottom of each page of this document.</td>
</tr>
</tbody>
</table>

* For conventions used to represent command syntax, see “CLI command syntax” on page 12.
# CLI command syntax

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

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

For more information, see the [FortiGate CLI Reference](http://docs.fortinet.com/).

<table>
<thead>
<tr>
<th>Table 2: Command syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Convention</strong></td>
</tr>
</tbody>
</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` |
| Angle brackets `< >` | A word constrained by data type. 
  To define acceptable input, the angled brackets contain a descriptive name followed by an underscore (`_`) and suffix that indicates the valid data type. For example: 
  
  `<retries_int>`
  indicates that you should enter a number of retries, such as 5. 
  
  Data types include:
  
  - `<xxx_name>`: A name referring to another part of the configuration, such as `policy_A`. 
  - `<xxx_index>`: An index number referring to another part of the configuration, such as 0 for the first static route. 
  - `<xxx_pattern>`: A regular expression or word with wild cards that matches possible variations, such as `*@example.com` to match all email addresses ending in `@example.com`. 
  - `<xxx_fqdn>`: A fully qualified domain name (FQDN), such as `mail.example.com`. 
  - `<xxx_email>`: An email address, such as `admin@mail.example.com`. 
  - `<xxx_ipv4>`: An IPv4 address, such as `192.168.1.99`. 
  - `<xxx_ipv4range>`: An IPv4 address range. 
  - `<xxx_v4mask>`: A dotted decimal IPv4 netmask, such as `255.255.255.0`. 
  - `<xxx_ipv4mask>`: A dotted decimal IPv4 address and netmask separated by a space, such as `192.168.1.99 255.255.255.0`. 
  - `<xxx_ipv4/mask>`: A dotted decimal IPv4 address and CIDR notation netmask separated by a slash, such as `192.168.1.99/24`. 
  - `<xxx_ipv6>`: An IPv6 address. 
  - `<xxx_v6mask>`: A dotted decimal IPv6 netmask. 
  - `<xxx_ipv6mask>`: A dotted decimal IPv6 address and netmask separated by a space. 
  - `<xxx_str>`: A string of characters that is **not** another data type, such as `P@ssw0rd`. Strings containing spaces or special characters must be surrounded in quotes or use escape sequences. 
  - `<xxx_int>`: An integer number that is **not** another data type, such as 15 for the number of minutes. |
| Curly braces `{ }` | A word or series of words that is constrained to a set of options delimited by either vertical bars or spaces. You must enter at least one of the options, unless the set of options is surrounded by square brackets `[]`. |
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, http://support.fortinet.com. Many Fortinet customer services, such as firmware updates, technical support, and FortiGuard Antivirus and other FortiGuard services, require product registration. For more information, see the Fortinet Knowledge Base article Registration Frequently Asked Questions.

Fortinet products End User License Agreement

See the Fortinet products End User License Agreement.

Customer service and technical support

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

To learn about the technical support services that Fortinet provides, visit the Fortinet Technical Support web site at http://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 Fortinet technical support requirements for support issues.

Training

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

Table 2: Command syntax

| Options delimited by vertical bars | Mutually exclusive options. For example: {enable | disable} indicates that you must enter either enable or disable, but must not enter both. |
|-----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| Options delimited by spaces       | Non-mutually exclusive options. For example: {http https ping snmp ssh telnet} indicates that you may enter all or a subset of those options, in any order, in a space-delimited list, such as: ping https ssh |
|                                   | Note: To change the options, you must re-type the entire list. For example, to add snmp to the previous example, you would type: ping https snmp ssh |
|                                   | If the option adds to or subtracts from the existing list of options, instead of replacing it, or if the list is comma-delimited, the exception will be noted. |
Fortinet documentation

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

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

Tools and Documentation CD

The documentation for your product is available on the Fortinet Tools and Documentation CD shipped with your product. The documents on this CD are current at shipping time. For the most current versions of Fortinet documentation, visit the Fortinet Technical Documentation web site, http://docs.fortinet.com.

Fortinet Knowledge Base

The Fortinet Knowledge Base provides additional Fortinet technical documentation, such as troubleshooting and how-to articles, examples, FAQs, technical notes, a glossary, and more. Visit the Fortinet Knowledge Base at http://kb.fortinet.com.

Comments on Fortinet technical documentation

Please send information about any errors or omissions in this or any Fortinet technical document to techdoc@fortinet.com.
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 chapter:

- UTM components
- Protection profiles
- SSL content scanning and inspection

UTM components

AntiVirus

Your FortiGate unit stores a virus signature database that can identify more than 15,000 individual viruses. FortiGate models that support the extended virus database are able to identify more than 200,000 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 applied to a protection 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.
Protection profiles

A protection profile is a group of settings that you can apply to one or more firewall policies. Most UTM features are enabled in protection profiles.

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

You can use protection profiles to enable:

- antivirus protection
- web filtering
- FortiGuard Web Filtering
- email filtering
- IPS
- DLP
- dashboard statistics
- application control
- logging for traffic which violates the protection profile.

All of these features are enabled within the protection profile, and some include configuration options within the protection profile as well.

SSL content scanning and inspection

If your FortiGate model is 80C/CM, 82C, 110C, 111C, 310B, 602B, 3016B, 3600A, 3810A, 5005FA2, or 5005A, it supports SSL content scanning and inspection, and you can apply antivirus scanning, web filtering, FortiGuard web filtering, and email filtering. 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
- re-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**.

![Figure 2: Importing a signing CA certificate for SSL content scanning and inspection](image)

7. Select **OK**.

   The CA certificate is added to the **Local Certificates** list. In this example the signing CA certificate name is Example_CA. This name comes from the certificate file and key file name. If you want the certificate to have a different name, change these file names.

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 3: SSL content scanning and inspection settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
<th>References</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>
<td>For more information about predefined services, see the FortiGate Administration Guide.</td>
</tr>
</tbody>
</table>
| Protocol recognition  | The TCP port numbers that the FortiGate unit inspects for HTTPS, IMAPS, POP3S, and SMTPS. Go to Firewall > Protection Profile. Add or edit a protection profile and configure Protocol Recognition for HTTPS, IMAPS, POP3S, and SMTPS. Using protocol recognition you can also configure the FortiGate unit to just 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. 
**Note:** You must set HTTPS Content Filtering Mode to Deep Scan before you can configure most SSL settings in the protection profile. | For more information about protocol recognition, see the FortiGate Administration Guide. |
| Antivirus              | Antivirus options including virus scanning and file filtering for HTTPS, IMAPS, POP3S, and SMTPS. Go to Firewall > Protection Profile. Add or edit a protection profile and configure Anti-Virus for HTTPS, IMAPS, POP3S, and SMTPS. | For more information, see “AntiVirus” on page 35.                                                                                      |
| Antivirus quarantine   | Antivirus quarantine options to quarantine files in HTTPS, IMAPS, POP3S, and SMTPS sessions. Go to UTM > AntiVirus > Quarantine. You can quarantine infected files, suspicious files, and blocked files found in IMAPS, POP3S, and SMTPS sessions. You can also quarantine infected files and suspicious files found in HTTPS sessions. | For more information, see “Enable the file quarantine” on page 38.                                                                    |
| Web filtering          | Web filtering options for HTTPS:  
  - Web Content Filter  
  - Web URL Filter  
  - ActiveX Filter (CLI only)  
  - Cookie Filter (CLI only)  
  - Java Applet Filter (CLI only)  
  - Web Resume Download Block  
  - Block invalid URLs  
  Go to Firewall > Protection Profile. Add or edit a protection profile and configure Web Filtering for HTTPS. | For more information, see “Web filtering” on page 81. For more information about the CLI-only options, see the FortiGate CLI Reference. |
<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>FortiGuard Web Filtering</td>
<td>FortiGuard Web Filtering options for HTTPS:</td>
<td>For more information, see &quot;Enable FortiGuard Web Filtering&quot; on page 94.</td>
</tr>
<tr>
<td></td>
<td>• Enable FortiGuard Web Filtering</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enable FortiGuard Web Filtering Overrides</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Provide details for blocked HTTP 4xx and 5xx errors</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Rate images by URL (blocked images will be replaced with blanks)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Allow websites when a rating error occurs</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Strict Blocking</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Rate URLs by domain and IP address</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Go to Firewall &gt; Protection Profile. Add or edit a protection profile and</td>
<td></td>
</tr>
<tr>
<td></td>
<td>configure Web Filtering &gt; FortiGuard Web Filtering for HTTPS.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Email filtering</td>
<td>Email filtering options for IMAPS, POP3S, and SMTPS:</td>
<td>For more information, see &quot;Email filter&quot; on page 47.</td>
</tr>
<tr>
<td></td>
<td>• FortiGuard Email Filtering (or Antispam) IP address check, URL check,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>E-mail checksum check, and Spam submission</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• IP address BWL check</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• E-mail address BWL check</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Return e-mail DNS check</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Banned word check</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Spam Action</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Tag Location</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Tag Format</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Go to Firewall &gt; Protection Profile. Add or edit a protection profile and</td>
<td></td>
</tr>
<tr>
<td></td>
<td>configure Email Filtering for IMAPS, POP3S, and SMTPS.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data Leak</td>
<td>DLP for HTTPS, IMAPS, POP3S, and SMTPS. To apply DLP, follow the steps</td>
<td>For more information, see &quot;Enable data leak prevention&quot; on page 102.</td>
</tr>
<tr>
<td>Prevention</td>
<td>below:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Go to UTM &gt; Data Leak Prevention &gt; Rule to add DLP rules. For HTTPS,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>add an HTTP rule and select HTTPS POST and HTTPS GET. For IMAPS, POP3S,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SMTPS, add an Email rule and select IMAPS, POP3S, and SMTPS.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Go to UTM &gt; Data Leak Prevention &gt; Sensor, create a new DLP sensor or</td>
<td></td>
</tr>
<tr>
<td></td>
<td>edit an existing one and then add the DLP rules to a DLP sensor.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Go to Firewall &gt; Protection Profile. Add or edit a protection profile</td>
<td></td>
</tr>
<tr>
<td></td>
<td>and use Data Leak Prevention Sensor to add the DLP sensor to a protection</td>
<td></td>
</tr>
<tr>
<td></td>
<td>profile. Note: In a protection profile, if you set Protocol Recognition &gt;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>HTTPS Content Filtering Mode to URL Filtering, DLP rules cannot inspect</td>
<td></td>
</tr>
<tr>
<td></td>
<td>HTTPS. Set this option to Deep Scan.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Go to Firewall &gt; Policy and add the protection profile to a firewall</td>
<td></td>
</tr>
<tr>
<td></td>
<td>policy.</td>
<td></td>
</tr>
<tr>
<td>DLP archiving</td>
<td>DLP archiving for HTTPS, IMAPS, POP3S, and SMTPS. Add DLP Rules for the</td>
<td></td>
</tr>
<tr>
<td></td>
<td>protocol to be archived.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 3: SSL content scanning and inspection settings
### Table 3: SSL content scanning and inspection settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>Displaying DLP meta-information on the system dashboard</td>
<td>DLP archive information on the Log and Archive Statistics widget on the system dashboard for HTTPS, IMAPS, POP3S, and SMTPS. Go to Firewall &gt; Protection Profile. Add or edit a protection profile and open Data Leak Prevention Sensor. For Data Leak Prevention Sensor, select the check box and then the sensor. For Display content meta-information on the system dashboard, select HTTPS, IMAPS, POP3S, and SMTPS as required. These options display meta-information on the Statistics dashboard widget.</td>
<td>For more information about DLP meta-information, see the FortiGate Administration Guide.</td>
</tr>
<tr>
<td>Archive SPAM email</td>
<td>DLP archiving of email tagged as spam by FortiGate Email Filtering in IMAPS, POP3S, and SMTPS sessions. Archive SPAMed emails to FortiAnalyzer/FortiGuard is available only if you have configured logging to a FortiAnalyzer unit or to the FortiGuard Analysis and Management Service. Go to Firewall &gt; Protection Profile. Add or edit a protection profile and open Data Leak Prevention Sensor. For Archive SPAMed emails to FortiAnalyzer/FortiGuard, select IMAPS, POP3S, and SMTPS as required.</td>
<td></td>
</tr>
</tbody>
</table>
Network defence

This chapter 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're not specifically targeted at your network.

The following topics are included in this chapter:

- 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.

### 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.

Table 4: 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/%99%103%105%46%98%105%110%47">http://www.example.com/%99%103%105%46%98%105%110%47</a>;</td>
</tr>
<tr>
<td>URL encoding</td>
<td><a href="http://www.example.com/%34%37%39%3B%42%34%39%34%3F">http://www.example.com/%34%37%39%3B%42%34%39%34%3F</a></td>
</tr>
<tr>
<td>ANSI encoding</td>
<td><a href="http://www.example.com/%u0063%u0067%u0069%u002E%u0062%u0066/%25">http://www.example.com/%u0063%u0067%u0069%u002E%u0062%u0066/%</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>

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.

**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 cannot 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

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.

Figure 6: Multiple attackers launch a distributed SYN flood

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 defense 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 `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, the FortiGate unit takes the configured action against the excess incomplete connections.

For more information, see “Creating and configuring a DoS sensor” on page 119. For recommendations on how to configure DoS policies, see “DoS policy recommendations” on page 30.

SYN proxy

FortiGate units that support Fortinet security processing modules offer a third action for the `tcp_syn_flood` threshold when a module is installed. Instead of Block and Pass, you can choose to Proxy the incomplete connections that exceed the threshold value. Although the SYN proxy is not a true proxy, it is more efficient and performs better than a true proxy. 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 and use a “best effect” algorithm to determine whether the connection attempt is legitimate or a SYN flood attack. Legitimate connections are passed while attacks are blocked.

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 section 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 116.

• 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 section 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 built-in-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 protection profile, enable IP address check in FortiGuard Email Filtering under 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 Post Block option in the protection profile.
- While DLP can detect sensitive data, it’s 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 chapter describes how to configure the antivirus options. From a protection 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.

If you enable virtual domains (VDOMs) on the Fortinet unit, most antivirus options are configured separately for each virtual domain. However, the file quarantine, the virus list and the grayware list are part of the global configuration. Only administrators with global access can configure and manage the file quarantine, view the virus list, and configure the grayware list.

The following topics are included in this chapter:

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

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.

Antivirus scanning order

The antivirus scanning function includes various modules and engines that perform separate tasks. The Fortinet unit performs antivirus processing in the following order:

- file size
- file pattern
- file type
- virus scan
- grayware
- heuristics.
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 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.

Figure 7 illustrates the antivirus scanning order. The first check for oversized files/email is to determine whether the file exceeds the configured size threshold. The second such 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. The AV 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
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, is to cover 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 setting the Oversized File/Email option under Firewall > Protection Profile > Antivirus to Block.

File pattern

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

File type

Once a file passes the file pattern scan, 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. If the file is not a blocked type, the next level of protection is applied.

Virus scan

If the file passes the file type scan, the FortiGate unit applies a virus scan to it. The virus definitions are keep up-to-date through the FortiGuard Distribution Network (FDN). The list is updated on a regular basis, so you do not have to wait for a firmware upgrade. For more information, see “FortiGuard Antivirus” on page 38.

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 43.

Heuristics

After an incoming file has passed the grayware scan, it is subjected to the heuristics scan. The Fortinet 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.
**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 DNSBL, through the FDN. The FortiGuard Center web site also provides the FortiGuard Antivirus virus and attack encyclopedia.

The connection between the Fortinet unit and FortiGuard Center is configured in System > Maintenance > FortiGuard. For more information, see the FortiGate Administration Guide.

---

**Enable antivirus scanning**

Antivirus scanning is enabled in the protection profile. Once it is enabled, all the firewall policies using that protection profile will have the traffic they control scanned according to your settings.

**To enable antivirus scanning**

1. Go to Firewall > Protection Profile.
2. Select the *Edit* icon of the protection profile for which you want to enable antivirus scanning.
3. Expand the *Anti-Virus* section.
4. In the row labeled *Virus Scan*, select the check boxes associated with the traffic you want scanned for viruses.
5. Select *OK*.

---

**Enable the file quarantine**

You can quarantine blocked and infected files if you have a Fortinet unit with a local disk, a FortiGate unit with a single width AMC slot containing a FortiGate-ASM-S08 module, or a FortiGate-ASM-SAS module. 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.

Fortinet 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.

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

  If your FortiGate unit supports extended virus database definitions, the database version and date it was last updated will be displayed in the Extended set field.
• **Virus Database:** Go to UTM > AntiVirus > Virus Database. This page shows the version number, number of included signatures, and a description of the antivirus database.

If your FortiGate unit supports extended virus database definitions, the version number and description of the extended virus database is also displayed.

**General configuration steps**

The following steps provide an overview of the file quarantine configuration. For best results, follow the procedures in the order given. You should have already enabled the protocols you require in a protection profile; otherwise quarantine will not work. Also, 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. If your FortiGate unit supports the extended virus database definitions, go to UTM > AntiVirus > Virus Database to enable the extended database.
3. Go to Firewall > Protection Profile and expand Anti-Virus to enable Quarantine for required protocols in the protection profiles. The Quarantine option only appears if your FortiGate unit has a local disk, an AMC slot containing a FortiGate-ASM-S08 or FortiGate-ASM-SAS module, or if your FortiGate unit is configured to use a FortiAnalyzer unit to quarantine files.
4. If you have not previously done so, go to Firewall > Policy and add the protection 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 Age Limit field, enter the number of hours quarantined files will be saved. Files older than the specified number of hours are deleted.
4. In the Max Filesize to Quarantine field, enter the maximum file size to quarantine, in megabytes. Files that exceed this limit are not quarantined.
5. Select OK.
Enabling the extended virus database

If your FortiGate unit supports extended virus database definitions, you can use them in addition to the regular virus database. The viruses in the regular virus database are also included in the extended virus database.

In most circumstances, the regular virus database provides sufficient protection. Viruses known to be active are included in the regular virus database. Only viruses that have become very rare or have stopped infecting hosts entirely are included in the extended virus database.

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.

Enable the extended antivirus database

1. Go to UTM > AntiVirus > Virus Database.
2. Select Extended Virus Database.
3. Select Apply.

Enabling quarantine in protection profiles

After configuring quarantine, you need to enable it for required protocols in the protection profiles. This option is available only if your FortiGate unit has a local disk, an AMC slot containing a FortiGate-ASM-S08 or FortiGate-ASM-SAS module, or if your FortiGate unit is configured to use a FortiAnalyzer unit to quarantine files.

To enable quarantine in a protection profile

1. Go to Firewall > Protection Profile.
2. Select the Edit icon of the protection profile to which you want to apply the quarantine configuration.
3. To enable quarantine for SSL protocols, set HTTPS Content Filtering Mode to Deep Scan in the Protocol Recognition part of the protection profile.
4. Expand the Anti-Virus section.
5. If you have not previously done so, select the protocols for the different options that you require. Quarantine will not work unless at least one is selected in the protection profile.
6. In the Quarantine row, select the protocols to which you want to apply the quarantine.
7. Select OK.

If you want to configure the FortiGate unit to use a FortiAnalyzer unit instead, see the FortiGate Administration Guide.

Adding the protection profile to a policy

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

To add the protection 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 For Protection Profile, select the protection profile that contains the quarantine configuration.
4 Configure other settings that you may require.
5 Select OK.

For more information about firewall policies, see the FortiGate Administration Guide.

**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**

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 42.

- **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:
Enable file filtering

- **Block**: the file will be blocked and a replacement messages will be sent to the user. If both file filter and virus scan are enabled, the Fortinet 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 Fortinet unit also writes a message to the virus log and sends an alert email message if configured to do so.

**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 protection profile.

**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 the **Edit** icon of the file filter list to which you will add the file pattern.
3. Select **Create New**.
4. Select **File Name Pattern** as the **Filter Type**.
5. 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.
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**.

**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.

Enable file filtering

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

To enable file filtering
1. Go to Firewall > Protection Profile.
2. Select Create New to add a protection profile or select the Edit icon of an existing one for which you want to enable file filtering.
3. Expand the Anti-Virus section.
4. In the row labeled File Filter, select the check boxes associated with the traffic you want scanned for files.
5. 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.
6. Select OK.

You also need to add the protection profile to a firewall policy for all settings to take effect. For more information about firewall policies, see the FortiGate Administration Guide.

Enable grayware scanning

Grayware programs are unsolicited commercial 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 ends.

To allow the FortiGate unit to scan for known grayware executable 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 38.

To enable grayware detection
1. Go to UTM > AntiVirus > Virus Database.
2. Select Enable Grayware Detection.

With grayware detection enabled, the FortiGate unit will also scan for grayware any time it checks for viruses.
Testing your antivirus configuration

You’ve configured your FortiGate unit to stop viruses, but you’d like to confirm your settings are correct. Even if you have a virus, it would be dangerous to use. 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 protection 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 example

The following example provides a sample antivirus configuration scenario for a fictitious company. All the steps, up to and including creating a protection profile, are provided. To complete the configuration, the protection profile needs to be selected in a firewall policy. Firewall policies vary depending on a company’s email configuration and are not covered in this example. For more information, see the FortiGate Administration Guide.

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 protection 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 protection profile and then select the protection profile in firewall policies that control email traffic.

To enable antivirus scanning in the protection profile

1. Go to Firewall > Protection Profile.
2. Select Create New to add a new protection profile, or select the Edit icon of an existing protection profile.
3. Expand the Protocol Recognition section and select Deep Scan.
   This will make SSL content scanning options available for configuration.
4. Expand the Anti-Virus section of the protection profile.
5. Select the Virus Scan check box for HTTP to scan web traffic for viruses and select the HTTPS check box to scan encrypted web traffic.
6. Select the Virus Scan check box for IMAP, POP3, and SMTP to scan all email protocols for viruses and select the IMAPS, POP3S, and SMTPS check boxes to scan encrypted email traffic.
7 Select OK to save the protection 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.
   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 protection profile and select the list.

Enabling file filtering
1 Go to Firewall > Protection Profile.
2 Select the Edit icon of the protection profile in which you already enabled virus scanning.
3 Expand the Anti-Virus section.
4 Select the File Filter check box for IMAP, POP3, and SMTP to scan all email protocols for viruses and select the IMAPS, POP3S, and SMTPS check boxes to scan encrypted email traffic.
5 At the end of the File Filter row, select the file filter list you created.
6 Select OK.
To complete the example, you also need to add the protection profile to a firewall policy for all settings to take effect. For more information, see the FortiGate Administration Guide.
Email filter

This chapter 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.

If you enable virtual domains (VDOMs), email filtering is configured separately for each virtual domain.

The following topics are included:
- Email filtering concepts
- Enable email filtering
- Configure the spam action
- Configure the tag location
- Configure the tag format
- Email filter example

Email filtering 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 protection 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.
Email filtering concepts

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 protection 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 sip 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.

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 protection 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 protection 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 filtering

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 Firewall > Protection Profile.
2. Select the Edit icon of the protection profile in which you want to enable email traffic inspection.
3. Expand the Email Filtering section.
4. 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.
5. 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 Firewall > Protection Profile.
2. Select the Edit icon of the protection profile in which you want to enable FortiGuard IP address checking.
3. Expand the Email Filtering section.
4. 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.
5. Select OK.

Select the edited protection 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 protection 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 Firewall > Protection Profile.
2. Select the Edit icon of the protection profile in which you want to enable FortiGuard URL checking.
3. Expand the Email Filtering section.
4. 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.
5. Select OK.

Select the edited protection 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 protection 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 Firewall > Protection Profile.
2. Select the Edit icon of the protection profile in which you want to enable FortiGuard checksum checking.
3. Expand the Email Filtering section.
4. 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.
5. Select OK.

Select the edited protection 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 protection 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 Firewall > Protection Profile.
2. Select the Edit icon of the protection profile in which you want to enable FortiGuard spam submission.
3. Expand the Email Filtering section.
4. 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.
5. Select OK.

Select the edited protection 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 protection 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 protection 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 sections 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 52.
Creating an IP address black/white list

Before you can enable IP address black/white list spam filtering in the protection 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 protection 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 Edit icon of the list to which you want to add an address.
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 Spam: Messages from clients with matching IP addresses will be treated as spam, subject to the action configured in the applicable protection profile. For more information, see “Configure the spam action” on page 58.
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 Firewall > Protection Profile.
2. Select the Edit icon of the protection profile in which you want to enable IP address black/white list checking.
3. Expand the Email Filtering section.
4 The IP address BWL check row has check boxes for each email traffic type. Select the types of traffic you want scanned.

5 Select the IP address black/white list to use from the drop-down list at the end of the row.

6 Select OK.

Select the edited protection 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 protection 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 submitted 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 Firewall > Protection Profile.
2 Select the Edit icon of the protection profile in which you want to enable HELO DNS lookup.
3 Expand the Email Filtering section.
4 The HELO DNS lookup row has a check box for the SMTP traffic type. Select the check box to enable HELO DNS lookup.
5 Select OK.

Select the edited protection 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 protection 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 protection 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 sections 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 the email address black/white list checking” on page 54.

Creating an email address black/white list

Before you can enable email address black/white list spam filtering in the protection 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 contains 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 on the email address black/white list specified in the active protection profile, it performs the action specified for the address.

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 protection profile. For more information, see “Configure the spam action” on page 58.
   • 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 the 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 Firewall > Protection Profile.
2 Select the Edit icon of the protection profile in which you want to enable email address black/white list checking.
3 Expand the Email Filtering section.
4 The E-mail address BWL check row has check boxes for each email traffic type. Select the types of traffic you want scanned.
5 Select the email address black/white list to use from the drop-down list at the end of the row.
6 Select OK.
Select the edited protection 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 protection 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 Firewall > Protection Profile.
2. Select the Edit icon of the protection profile in which you want to enable return email DNS checking.
3. Expand the Email Filtering section.
4. The Return e-mail DNS check row has check boxes for each email traffic type. Select the types of traffic you want checked.
5. Select OK.

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 protection profile. If the total score of the banned word discovered in the email message exceeds the threshold value set in the protection 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 sections 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 the banned word checking” on page 57.

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 protection 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 protection 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 protection profile, it totals the scores of the banned words in the email message. If the total is higher than the threshold set in the protection 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".
   - Regular expressions use Perl regular expression syntax. See http://perldoc.perl.org/perlretut.html for detailed information about using Perl regular expressions.
6. In the Language field, select the language.
7. Select where the FortiGate unit will check for the banned word. The options are the message body, the 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 protection 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 the 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 Firewall > Protection Profile.
2. Select the Edit icon of the protection profile in which you want to enable banned word checking.
3. Expand the Email Filtering section.
4. The Banned word check row has check boxes for each email traffic type. Select the types of traffic you want scanned.
5. Select the banned word list to use from the drop-down list at the end of the row.
6. 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.
7. Select OK.

Select the edited protection 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 protection 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 protection 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 Firewall > Protection Profile.
2. Select the Edit icon of the protection profile in which you want to configure the spam action.
3. Expand the Email Filtering section.
4. 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 58 and “Configure the tag format” on page 59.
5. Select OK.

Select the edited protection 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 protection 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 Firewall > Protection Profile.
2. Select the Edit icon of the protection profile in which you want to configure the tag location action.
3. Expand the Email Filtering section.
4 The Tag Location row has two options for each traffic type. Select the tag location you want for each traffic type:
   - **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.

5 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 Firewall > Protection Profile.
2. Select the Edit icon of the protection profile in which you want to configure the tag format.
3. Expand the Email Filtering section.
4. 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.
5. Select OK.

### Email filter example

**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 protection profile.
To enable Email Filter

1. Go to Firewall > Protection Profile.
2. Select the Edit icon of the protection profile that is used by the firewall policies handling email traffic.
3. Expand the Email Filtering section.
4. Select the check boxes labeled IMAP, POP3, and SMTP in the row immediately below the Email Filtering heading.
5. In the row E-mail address BLW check, select all three check boxes.
6. At the end of the E-mail address BLW check row, select the email address list you created in the previous procedure.
7. In the row Tag Location, select Subject for all three mail protocols.
8. In the row Tag Format, enter SPAM: in all three fields.
9. 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 each protection profile.

This chapter 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. For details, see the FortiGate Administration Guide.

The following topics are included:

- IPS concepts
- Enable IPS scanning
- Configure protocol decoders
- Enable 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. For details and configuration instructions regarding the DoS feature, see “DoS policy” on page 119.

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; 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 FortiGate 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, however. 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 and select the edit icon of the IPS sensor containing the filters you want to view.

Protection profile and firewall policy

To use an IPS sensor, you must enable IPS in a protection profile and select the IPS sensor. Then, in the policy handling the traffic that you want scanned, you must enable protection profiles and then select the protection profile in which you specified the IPS sensor.
Interface policy
Typically, IPS sensors are specified in a protection profile, but there is another way to use them. You can use the CLI to apply an IPS sensor directly to an interface-based policy.

Enable IPS scanning
Enabling IPS scanning involves three 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 protection profile specifies what sort of processing is applied to network traffic. Antivirus scanning, web filtering, and IPS scanning are examples of the types of processing that can be applied to network traffic.
- 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 protection profile, the protection profile is selected in the 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 protection profile or create a new one.
4. In the protection profile, enable IPS Sensor and select the IPS sensor.
5. Select a firewall policy or create a new one.
6. In the firewall policy, select the Protection Profile check box and select the protection profile.

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

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. For more information, see “Creating an IPS sensor” on page 63.
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. For detailed descriptions of each setting, see the FortiGate Administration Guide.
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.
Intrusion protection

Enable IPS scanning

Note: Before an override can affect network traffic, you must add it to a filter, and you must select the filter in a protection profile applied to a 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 63.

To create an IPS signature override
1. Go to UTM > Intrusion Protection > IPS Sensor.
2. Select the Edit icon of the IPS sensor to which you want to add the override. For more information, see “Creating an IPS sensor” on page 63.
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 packet logging” on page 74.
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” on page 65.
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 sections.

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 sections.

Table 5 shows the valid characters and basic structure. For details about each keyword and its associated values, see “Custom signature keywords” on page 66.

Table 5: 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 66 for tables of supported keywords.</td>
</tr>
<tr>
<td>VALUE</td>
<td>Double quotes (&quot;) 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 6: Information keywords

<table>
<thead>
<tr>
<th>Keyword and value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--attack_id &lt;id_int&gt;;</td>
<td>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;</td>
</tr>
<tr>
<td>--name &lt;name_str&gt;;</td>
<td>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 &quot;Buffer_Overflow&quot;;</td>
</tr>
</tbody>
</table>
### Table 7: Session keywords

<table>
<thead>
<tr>
<th>Keyword and value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--flow {from_client</td>
<td>Specify the traffic direction and state to be inspected. They can be used for all IP traffic.</td>
</tr>
<tr>
<td>from_server</td>
<td>Example:</td>
</tr>
<tr>
<td>bi_direction };</td>
<td>--src_port 41523; --flow bi_direction;</td>
</tr>
<tr>
<td></td>
<td>The signature checks traffic to and from port 41523.</td>
</tr>
<tr>
<td></td>
<td>Previous FortiOS versions used to_client and to_server values. These are now deprecated, but still function for backwards compatibility.</td>
</tr>
</tbody>
</table>

| --service {HTTP | Specify the protocol type to be inspected. |
| TELNET | This keyword allows you to specify the traffic type by protocol rather than by port. If the decoder has the capability to identify the protocol on any port, the signature can be used to detect the attack no matter what port the service is running on. Currently, HTTP, SIP, SSL, and SSH protocols can be identified on any port based on the content. |
| FTP | |
| DNS | |
| SMTP | |
| POP3 | |
| IMAP | |
| RADIUS | |
| LDAP | |
| MSSQL | |
| RPC | |
| SIP | |
| H323 | |
| NBSS | |
| DCERPC | |
| SSH | |
| SSL | |

### Table 8: 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.</td>
</tr>
<tr>
<td>&lt;bytes_to_convert&gt;,</td>
<td>The available keyword options include:</td>
</tr>
<tr>
<td>&lt;offset&gt;[, relative]</td>
<td>• &lt;bytes_to_convert&gt;: The number of bytes to examine from the packet.</td>
</tr>
<tr>
<td>[, big] [, little]</td>
<td>• &lt;offset&gt;: The number of bytes into the payload to start processing.</td>
</tr>
<tr>
<td>[, string] [, hex] [, dec]</td>
<td>• relative: Use an offset relative to last pattern match.</td>
</tr>
<tr>
<td>[, oct] [, align];</td>
<td>• big: Process the data as big endian (default).</td>
</tr>
<tr>
<td></td>
<td>• little: Process the data as little endian.</td>
</tr>
<tr>
<td></td>
<td>• string: The data is a string in the packet.</td>
</tr>
<tr>
<td></td>
<td>• hex: The converted string data is represented in hexadecimal notation.</td>
</tr>
<tr>
<td></td>
<td>• dec: The converted string data is represented in decimal notation.</td>
</tr>
<tr>
<td></td>
<td>• oct: The converted string data is represented in octal notation.</td>
</tr>
<tr>
<td></td>
<td>• align: Round up the number of converted bytes to the next 32-bit boundary.</td>
</tr>
</tbody>
</table>
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.

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.

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.

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.
Intrusion protection

Enable IPS scanning

---

**Table 8: 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:  
  ```bash  
  --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:  
  ```bash  
  --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.

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.

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.

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 9: IP header keywords

<table>
<thead>
<tr>
<th>Keyword and Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--dst_addr [!]&lt;ipv4&gt;;</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. Example: <code>dst_addr [172.20.0.0/16, 10.1.0.0/16, 192.168.0.0/16]</code></td>
</tr>
<tr>
<td>--ip_id &lt;field_int&gt;;</td>
<td>Check the IP ID field for the specified value.</td>
</tr>
</tbody>
</table>
| --ip_option {rr | eol | nop | ts | sec | lsrr | ssrr | satid | any}; | Use the `ip_option` keyword to check various IP option settings. The available options include:  
  • `rr`: Check if IP RR (record route) option is present.  
  • `eol`: Check if IP EOL (end of list) option is present.  
  • `nop`: Check if IP NOP (no op) option is present.  
  • `ts`: Check if IP TS (time stamp) option is present.  
  • `sec`: Check if IP SEC (IP security) option is present.  
  • `lsrr`: Check if IP LSRR (loose source routing) option is present.  
  • `ssrr`: Check if IP SSRR (strict source routing) option is present.  
  • `satid`: Check if IP SATID (stream identifier) option is present.  
  • `any`: Check if IP any option is present. |
| --ip_tos <field_int>; | Check the IP TOS field for the specified value. |
| --ip_ttl [< | >] <ttl_int>; | Check the IP time-to-live value against the specified value. Optionally, you can check for an IP time-to-live greater-than (>) or less-than (<) the specified value with the appropriate symbol. |
| --protocol {<protocol_int> | tcp | udp | icmp}; | Check the IP protocol header. Example:  
  --protocol tcp; |
| --src_addr [!]<ipv4>; | Use the `src_addr` 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. Example: `src_addr 192.168.13.0/24` |
## Table 10: 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 acknowledgement 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. |
| --seq <seq_int>;  | Check for the specified TCP sequence number. |
| --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 `0x`.  
  To have the FortiGate search for the absence of the specified window size, add an exclamation mark (!) before the window size. |
### Table 11: UDP header keywords

<table>
<thead>
<tr>
<th>Keyword and Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--dst_port [!] {&lt;port_int&gt;</td>
<td>1:&lt;port_int&gt;</td>
</tr>
<tr>
<td></td>
<td>• &lt;port_int&gt; is a single port.</td>
</tr>
<tr>
<td></td>
<td>• #:&lt;port_int&gt; includes the specified port and all lower numbered ports.</td>
</tr>
<tr>
<td></td>
<td>• &lt;port_int&gt;: includes the specified port and all higher numbered ports.</td>
</tr>
<tr>
<td></td>
<td>• &lt;port_int&gt;:&lt;port_int&gt; includes the two specified ports and all ports in between.</td>
</tr>
<tr>
<td>--src_port [!] {&lt;port_int&gt;</td>
<td>1:&lt;port_int&gt;</td>
</tr>
<tr>
<td></td>
<td>• &lt;port_int&gt; is a single port.</td>
</tr>
<tr>
<td></td>
<td>• #:&lt;port_int&gt; includes the specified port and all lower numbered ports.</td>
</tr>
<tr>
<td></td>
<td>• &lt;port_int&gt;: includes the specified port and all higher numbered ports.</td>
</tr>
<tr>
<td></td>
<td>• &lt;port_int&gt;:&lt;port_int&gt; includes the two specified ports and all ports in between.</td>
</tr>
</tbody>
</table>

### Table 12: 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 13: 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>&lt;&lt;size_int&gt;</td>
</tr>
<tr>
<td></td>
<td>• &lt;size_int&gt; is a particular packet size.</td>
</tr>
<tr>
<td></td>
<td>• &lt;&lt;size_int&gt; is a packet smaller than the specified size.</td>
</tr>
<tr>
<td></td>
<td>• &gt;&gt;size_int&gt; is a packet larger than the specified size.</td>
</tr>
<tr>
<td></td>
<td>• &lt;size_int&gt;&lt;size_int&gt; is a packet within the range between the specified sizes.</td>
</tr>
<tr>
<td>--data_at &lt;offset_int&gt;[, relative];</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>--rpc_num &lt;app_int&gt;[, &lt;ver_int&gt;</td>
<td>*][, &lt;proc_int&gt;</td>
</tr>
<tr>
<td>--same_ip;</td>
<td>Check that the source and the destination have the same IP addresses.</td>
</tr>
</tbody>
</table>
Configure 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. For more details about this command, see the FortiGate CLI Reference.

Enable packet logging

Packet logging saves the network packets containing 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. This option is not available in IPS sensors or filters because enabling packet logging on a large number of signatures could produce an amount of data that is too large to use. Packet logging is designed as a focused diagnostic tool.

You can use a number of CLI commands to further configure packet logging. When logging to memory, the packet-log-memory command defines the maximum amount of memory used to store logged packets. This command only takes effect when logging to memory.

Since only the packet containing the signature is sometimes not sufficient to troubleshoot a problem, the packet-log-history command allows you to specify how many packets are captured when an IPS signature is found in a packet. If the value is set to larger than 1, the packet containing the signature is saved in the packet log, as well as those preceding it, with the total number of logged packets equaling the value. For example, if packet-log-history is set to 7, the FortiGate unit will save the packet containing the IPS signature and the six before it.

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

To enable packet logging for a signature

1. Create either a pre-defined override or a custom override in an IPS sensor. For more information, see “Creating an IPS signature override” on page 64.
2. Before saving the override, select Packet Log.
3 Select the IPS sensor in the protection profile applied to the firewall policy that allows
the network traffic the FortiGate unit will examine for the signature. For more
information, see the FortiGate Administration Guide.

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

To view and save logged packets
1 Go to Log&Report > Log Access.
2 Depending on where the logs are configured to be stored, select the appropriate tab:

<table>
<thead>
<tr>
<th>Memory</th>
<th>Select if logs are stored in the FortiGate unit memory.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disk</td>
<td>Select if the FortiGate unit has an internal hard disk and logs are stored there.</td>
</tr>
<tr>
<td>Remote</td>
<td>Select if logs are sent to a FortiAnalyzer unit or to the FortiGuard Analysis and Management Service.</td>
</tr>
</tbody>
</table>

3 Select the Attack Log log type.
4 Select the Packet Log icon of the log entry you want to view.
The IPS Packet Log Viewer window appears.
5 Select the packet to view the packet in binary and ASCII. Each table row represents a captured packet.
6 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.

IPS examples

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 8, 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 policy to allow access to the web server from the Internet using the virtual IP.
- a protection profile applied to the web server policy to scan for viruses.

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

**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 Edit icon of the web_server IPS sensor.
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 Edit icon of the web_server IPS sensor.
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 protection profile.

To edit the protection profile

1. Go to Firewall > Protection Profile and select the Edit icon of the protection profile that the web server uses.
2. Expand the IPS section.
3. Select the IPS Sensor check box and select the web_server sensor.

Since the protection profile is specified in the firewall policy controlling the web server traffic, the IPS sensor you selected in the protection profile will examine the web server traffic for matches to the signatures it contains.

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 65.

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 until to ignore all traffic originating 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; )

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 65.

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.

```c
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.

```c
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.

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

This chapter 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 threats from Internet content. 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 chapter describes the Web Content Filter and URL Filter functions. For information on FortiGuard Web Filtering, see “FortiGuard Web Filtering” on page 93.

The following topics are included in this chapter:

- Web filtering concepts
- Web content filter
- URL filter
- Web filtering example

Web filtering 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. It is estimated that 80% of all personal computers are infected with spyware. 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 section. 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 exempt
2. URL block
3. web pattern block
4. FortiGuard Web Filtering
5. web content filter
6. web script filter
7. antivirus scanning.

Note: The first two, the URL exempt and URL block filters, allow you to decide what action to take for specific addresses. For example, if you want to exclude www.example.com from being scanned, you can add it to the URL exempt list. Then no web filtering or virus scanning will be taken for this web site.

If you have blocked a pattern but want certain users to have access to URLs within that pattern, you can use the Override within the FortiGuard web filter. This will allow you to specify which users have access to which blocked URLs and how long they have that access. For example, 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 Filtering” on page 93.

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 protection 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 protection profile specifies what sort of processing is applied to the network traffic accepted by a firewall. Antivirus scanning, web filtering, and IPS scanning are examples of the types of processing.

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 protection 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 protection 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 Protection Profile and select the appropriate protection profile from the list. For more information about firewall policies, see the FortiGate Administration Guide.

Creating a web filter content list

You can create multiple content lists and then select the best one for each protection 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, forti*.com will match fortiii.com but not fortinet.com or fortiice.com. The symbol "*" represents "i" in this case, appearing any number of times. For more information, see the FortiGate Administration Guide for information about Perl regular expressions.

The maximum number of banned words in the list is 5000.

**To add a web content pattern**

1. Go to UTM > Web Filter > Web Content Filter.
2. Select the Edit icon of the web content filter list.
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 85.
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."

| Table 14: Banned Pattern Rules |
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 Firewall > Protection Profile.
2. Select Create New to add a new protection profile or select Edit to modify an existing one.
3. Select the Web Filtering expand arrow.
4. Select Web Content Filter.
5. Select the web content list.
6. Enter the threshold for the web content filter.
7. 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 web site. For example, www.example.com or 192.168.144.155 controls access to all pages at this web site.
- Enter a top-level URL followed by the path and file name to control access to a single page on a web site. For example, www.example.com/news.html or 192.168.144.155/news.html controls access to the news page on this web site.
- To control access to all pages with a URL that ends with example.com, add example.com to the filter list. For example, adding example.com controls access to www.example.com, mail.example.com, www.finance.example.com, and so on.
- Control access to all URLs that match patterns 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 are not scanned for viruses. If users on the network download files through the FortiGate unit from a trusted web site, add the URL of this web site to the URL filter list with an action to exempt it so the FortiGate unit does not virus scan files downloaded from this URL.

**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 protection profile or create a new one.
4. In the protection profile, expand the web filter section.
5. 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 Protection Profile and select the appropriate protection profile from the list. For more information about firewall policies, see the *FortiGate Administration Guide*.

**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 the Edit icon of an existing list.

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:
   
   - **Block**: Access to all sites matching the pattern www.example*.com will be denied.
   
   - **Exempt**: All further checking of the site including AV scanning will be stopped. For example, if you have created a filter that blocks www.example*.com, you can add a filter that exempts www.example.com.
   
   - **Allow**: An allow match exits the URL filter list and checks the other web filters.

7. Select Enable.

8. Select OK.

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 protection 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 Edit icon of the Student Web Content List.
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 Edit icon of the Teacher Web Content List.
3 Select the Edit icon of example from the Pattern list.
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 Edit icon of Student URL List.
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 the Edit icon of Teachers URL List.
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 protection profile must be created for the students and the teachers.

To create a protection profile for the students
1. Go to Firewall > Protection Profile.
2. Select Create New.
3. Enter Students as the Profile Name.
4. Enter optional comments to identify the profile.
5. Expand the Web Filtering category.
6. Enable Web Content Filter and select Student Web Content List from the drop-down list.
7. Enable Web URL Filter and select Student URL List from the drop-down list.
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 **Protection Profile**.
4 Select **Students** from the drop-down list.
5 Enter optional comments.
6 Configure other settings that you may require. For more information, see the *FortiGate Administration Guide*.
7 Select **OK**.

**To create a protection profile for the teachers**
1 Go to **Firewall > Protection Profile**.
2 Select **Create New**.
3 Enter **Teachers** as the **Profile Name**.
4 Enter optional comments to identify the profile.
5 Expand the **Web Filtering** category.
6 Enable **Web Content Filter** and select **Teacher Web Content List** from the list.
7 Enable **Web URL Filter** and select **Teacher URL List** from the list.
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 **Protection Profile**.
4 Select **Teachers** from the drop-down list.
5 Enter optional comments.
6 Select **OK**.
FortiGuard Web Filtering

This chapter describes FortiGuard Web Filtering for HTTP and HTTPS traffic.

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

FortiGuard Web Filtering 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 users can allow, block, or monitor. Categories may be added or updated as the Internet evolves. To make configuration simpler, users can also choose to allow, block, or monitor entire groups of categories. Blocked pages are replaced with a message indicating that the page is not accessible according to the Internet usage policy.

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

The following topics are discussed in this chapter:

- Before you begin
- FortiGuard Web Filtering and your FortiGate unit
- Enable FortiGuard Web Filtering
- Add or change FortiGuard Web Filtering ratings
- Create FortiGuard Web Filtering overrides
- Customize categories and ratings
- FortiGuard Web Filtering example

Before you begin

Before you follow the instructions in this chapter, you should have a FortiGuard Web Filtering 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 filtering concepts” on page 81.

FortiGuard Web Filtering and your FortiGate unit

When FortiGuard Web Filtering is enabled in a protection profile, the setting is applied to all firewall policies that use this protection 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

FortiGuard Web Filtering is one of a number of web filtering features available on your FortiGate unit. The web filtering options that you configure before FortiGuard Web Filtering may change the way it operates. For more information, see “Web filtering” on page 81. For example, if you allow the category that example.org belongs to in FortiGuard Web Filtering, but add example.org to the URL block list, users will not be able to view example.org because URL block occurs before FortiGuard Web Filtering.

Web filters are applied in a specific order:
1. URL exempt
2. URL block
3. web pattern block
4. FortiGuard Web Filtering
5. web content block
6. web script filter
7. antivirus scanning.

Note: The first two, the URL exempt and URL block filters, will allow you to decide what action to take for specific addresses. For example, if you want to exclude www.example.com from being scanned, you can add it to the URL exempt list. Then no web filtering or virus scanning will be taken to this web site.

If you have blocked a pattern but want certain users to have access to URLs within that pattern, you can use the Override within the FortiGuard web filter. This will allow you to specify which users have access to which blocked URLs and how long they have that access. For example, 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 before the FortiGate unit will grant access to the blocked URL.

Enable FortiGuard Web Filtering

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

General configuration steps
1. Go to Firewall > Protection Profile.
2. Select the Edit icon of the protection profile in which you want to enable FortiGuard Web Filtering, or select Create New to add a new protection profile.
3. Expand the 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 protection profile.
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 Protection Profile and select the appropriate protection profile from the list. For more information about firewall policies, see the FortiGate Administration Guide.

Configuring FortiGuard Web Filtering settings

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

To configure FortiGuard Web Filtering settings

1. Go to Firewall > Protection Profile.
2. Select the Edit icon of the protection profile in which you want to enable FortiGuard Web Filtering, or select Create New to add a new protection profile.
3. Expand the Web Filtering section.
4. Under the FortiGuard Web Filtering heading, select one or both of the HTTP and HTTPS check boxes in the row labeled Enable FortiGuard Web Filtering to enable FortiGuard Web Filtering for HTTP and HTTPS web traffic.
   At least one of these check boxes must be selected, for FortiGuard Web Filtering to function for the protocol. Other web filtering features, such as web content filter and URL filter, will function as configured, however.
5. Select Enable 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 Filtering overrides" on page 98.
6. Enable Provide details for blocked HTTP 4xx and 5xx errors 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.
   Note: To use this option for HTTPS, scroll up to Protocol Recognition and select Deep Scan, then return to this option and select the HTTPS check box.
7. Enable Rate images by URL (blocked images will be replaced with blanks) to have the FortiGate unit block or allow individual images that have been rated by FortiGuard.
   Blocked images are replaced on the originating web pages with blank place-holders. Rated image file types include GIF, JPEG, PNG, BMP, and TIFF.
   Note: To use this option for HTTPS, scroll up to Protocol Recognition and select Deep Scan, then return to this option and select the HTTPS check box.
8. Enable Allow websites when a rating error occurs to allow access to web pages that return a rating error from the web filtering 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.
9 The **Strict Blocking** 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.

10 Enable **Rate URLs by domain and IP address** to have the FortiGate unit request the rating of the site by URL and IP address separately, providing additional security against attempts to bypass FortiGuard Web Filtering.

**Note:** FortiGuard Web Filtering ratings for IP addresses are not updated as quickly as ratings for URLs. This can sometimes cause the FortiGate unit to block sites that should be blocked, or to block sites that should be allowed.

11 Enable **Block HTTP redirects by rating** to block HTTP redirects.

Many web sites use HTTP redirects legitimately; however, 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.

12 Select OK to save your changes to the protection profile.

### Configuring the FortiGuard Web Filtering categories

Categories are a means to describe the content of web sites. FortiGuard Web Filtering divides the web into dozens of categories in eight category groups. Every rated URL and IP address has at least one category assigned to it.

**To configure the FortiGuard Web Filtering categories**

1 Go to **Firewall > Protection Profile**.

2 Select the **Edit** icon of the protection profile in which you want to configure the FortiGuard Web Filtering categories, or select **Create New** to add a new protection profile.

3 Expand the **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 98.

Before you can allow an override, you must create it (see “Create FortiGuard Web Filtering overrides” on page 98) and then select **Enable FortiGuard Web Filtering Overrides** in the protection profile.
Select OK.

**Configuring the FortiGuard Web Filtering 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 Filtering classifications**

1. Go to Firewall > Protection Profile.
2. Select the Edit icon of the protection profile in which you want to configure the FortiGuard Web Filtering categories, or select Create New to add a new protection profile.
3. Expand the Web Filtering section.
   Under the FortiGuard Web Filtering heading, the classifications are listed in a 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 Filtering overrides” on page 98.
8. Select OK.

**Add or change FortiGuard Web Filtering 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 filtering 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.
Create FortiGuard Web Filtering overrides

You can configure FortiGuard Web Filtering 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. You can 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 the Edit icon for Administrative Overrides.
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.
   - A 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’ve included in a user group. Using the User Group selection, choose the user group. For more information about users and user groups, see the FortiGate Administration Guide.
   - 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 visible 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 Filtering rating categories are general enough that virtually any web site can be accurately categorized in one of them. The rigid structure of the categories can create complications, however. You might decide to block the *Web-based Email* category, but what if your company uses one web-based email provider? Local categories and local ratings allow you to assign sites to any category you choose. You can even create new categories. These settings only apply to your FortiGate unit however. The changes you make are not sent to the FortiGuard Web Filtering Service.

**Creating local categories**

Categories are labels that describe web site content. Creating your own category allows you to customize how the FortiGuard Web Filtering service works.

Local categories appear in the protection profile FortiGuard Web Filtering category list under the *Local Categories* category group. Local categories are empty when created. To populate local categories with web sites, see “Customizing site ratings” on page 99.

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.
FortiGuard Web Filtering example

FortiGuard Web Filtering can provide more powerful filtering to your network because you can use it to block millions of sites by blocking the categories they belong to.

School district

Continuing with the example in the Web filtering chapter, you can use FortiGuard Web Filtering to protect students from inappropriate material. For the first part of this example, see “Web filtering example” on page 88.

To enable FortiGuard Web Filtering

1. Go to Firewall > Protection Profile.
2. Select the Edit icon of the protection profile named Students.
3. Expand the Web Filtering section.
4. In the Enable FortiGuard Web Filtering row, select both the HTTP and HTTPS options.
5. Select OK.

The Students protection profile has FortiGuard Web Filtering 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 Firewall > Protection Profile.
2. Select the Edit icon of the protection profile named Students.
3. Expand the Web Filtering section.
4. In the category table, select Block for these categories: Potentially Liable, Controversial, and Potentially Non-productive.
5. Select OK to save the protection 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 and/or logged or archived 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 protection profile.

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 chapter describes how to configure the DLP settings.

If you enable virtual domains (VDOMs) on the FortiGate unit, you need to configure data leak prevention separately for each virtual domain.

The following topics are included:

- Data leak prevention concepts
- Enable data leak prevention
- DLP example

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 protection profile and select the DLP sensor to use. Once you do this, the traffic matching any firewall policy that the protection profile uses will have DLP enabled. The traffic 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 ([0-6]\d\d\d[-][0-6]\d\d\d\d{-2}][-\-]\d\d\d\d{-4}).

DLP rules allow you to specify various conditions depending on the type of traffic for which the rule is created. Table 15 lists the available conditions by traffic type.
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 with a subject that has 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 match 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 a protection profile.

The protection profile should be attached to a firewall policy that controls the intended traffic. For more information about protection profiles and firewall policies, see the FortiGate Administration Guide.

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:

```
([0-6]\d{2}|7([0-6]\d|7[0-2]))[ \-]?\d{2}[ \-]\d{4}
```

Rather than having to list every possible Social Security Number, this regular expression describes the structure of a Social Security Number. The FortiGate unit easily recognizes 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 17.
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 rule to apply to HTTPS get traffic, HTTPS post traffic, or both traffic types.

**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.

**SIP, SIMPLE, SCCP**
When you select the *Session Control* protocol, you can configure the rule to apply to any or all of the session control protocols (SIP, SIMPLE, and SCCP).

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 &quot;From:&quot; 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>Rule Type</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transfer size</td>
<td>Check the total size of the information transfer.</td>
<td>Email, HTTP, FTP, NNTP, IM</td>
</tr>
<tr>
<td>URL</td>
<td>Search for the specified URL in HTTP traffic.</td>
<td>HTTP</td>
</tr>
<tr>
<td>User group</td>
<td>Search for traffic from any user in the specified user group.</td>
<td>Email, HTTP, FTP, NNTP, IM</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 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 attribute. When this attribute is discovered in network traffic, the rule is activated.

Compound rules allow you to group individual rules to specify far more detailed activation conditions. Each included rule is configured with a single attribute, but every attribute must be detected before the rule is activated.

If you add individual rules to a compound rule, and add the compound rule to the sensor, the conditions in both rules have to be present in network traffic to activate the compound rule. If only one condition is present, the message passes the compound rule being 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.

| All-Email, All-FTP, All-HTTP, All-IM, All-NNTP | These rules will detect all traffic of the specified type. |
| Email-AmEx, Email-Canada-SIN, Email-US-SSN, Email-Visa-Mastercard | These four rules detect American Express numbers, Canadian Social Insurance Numbers, U.S. Social Security Numbers, or Visa and Mastercard numbers within the message bodies of SMTP, POP3, and IMAP email traffic. |
| HTTP-AmEx, HTTP-Canada-SIN, HTTP-US-SSN, HTTP-Visa-Mastercard | These four rules detect American Express numbers, Canadian Social Insurance Numbers, U.S. Social Security Numbers, or Visa and Mastercard numbers within the POST command in HTTP traffic. The HTTP POST is used to send information to a web server. As written, these rules are designed to detect data the user is sending to web servers. This rule does not detect the data retrieved with the HTTP GET command, which is used to retrieve web pages. |
| Large-Attachment | This rule detects files larger than 5MB attached to SMTP, POP3, and IMAP email messages. |
| Large-FTP-Put | This rule detects files larger than 5MB sent using the FTP PUT protocol. Files received using FTP GET are not examined. |
| Large-HTTP-Post | This rule detects files larger than 5MB sent using the HTTP POST protocol. Files received using HTTP GET are not examined. |
Creating a DLP sensor

DLP sensors are collections of DLP rules and DLP compound rules. Once a DLP sensor is configured, it can be selected in a protection profile. Any traffic handled by the policy in which the protection profile is selected will enforce 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. 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 Edit icon of the DLP sensor to which you want to add the rule.
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:

   - **None**: 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.
   - **Block**: 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.
   - **Exempt**: The exempt action prevents any DLP sensors from taking action on matching traffic. This action overrides the action assigned to any other matching sensors.
   - **Ban**: 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.
Data leak prevention Enable data leak prevention

Ban Sender 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.

Quarantine IP 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.

Quarantine Interface 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.

Ban, Ban Sender, Quarantine IP, and Quarantine Interface provide functionality similar to NAC quarantine. However, these DLP options cause DLP to block users and IP addresses at the application layer while NAC quarantine blocks IP addresses and interfaces at the network layer.

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.

Tip: To view or modify the replacement message text, go to System > Config > Replacement Message. For more information, see the FortiGate Administration Guide.

5 Select how traffic matching the rule will be handled.

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.

<table>
<thead>
<tr>
<th>Sensor</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content_Archive</td>
<td>All non-encrypted email, FTP, HTTP, IM, and NNTP traffic is archived to a FortiAnalyzer unit or the FortiGuard Analysis &amp; Management Service. Traffic is only archived. No blocking or quarantine is performed. If you have a FortiGate unit that supports SSL content scanning and inspection, you can modify this sensor to archive encrypted traffic as well.</td>
</tr>
<tr>
<td>Content_Summary</td>
<td>A summary of all non-encrypted email, FTP, HTTP, IM, and NNTP traffic is saved to a FortiAnalyzer unit or the FortiGuard Analysis &amp; Management Service. No blocking or quarantine is performed. If you have a FortiGate unit that supports SSL content scanning and inspection, you can modify this sensor to archive a summary of encrypted traffic as well.</td>
</tr>
<tr>
<td>Credit-Card</td>
<td>The number formats used by American Express, Visa, and Mastercard credit cards are detected in HTTP and email traffic. As provided, the sensor is configured not to archive matching traffic and an action of None is set. Configure the action and archive options that you require.</td>
</tr>
<tr>
<td>Large-File</td>
<td>Files larger than 5MB will be detected if attached to email messages or if send using HTTP or FTP. As provided, the sensor is configured not to archive matching traffic and an action of None is set. Configure the action and archive options that you require.</td>
</tr>
<tr>
<td>SSN-Sensor</td>
<td>The number formats used by U.S. Social Security and Canadian Social Insurance numbers are detected in email and HTTP traffic. As provided, the sensor is configured not to archive matching traffic and an action of None is set. Configure the action and archive options that you require.</td>
</tr>
</tbody>
</table>

DLP example

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 a protection profile. To complete the example, you need to make sure that the protection profile is added to a firewall policy that controls email traffic; however this example does not describe this. For more information, see the FortiGate Administration Guide.

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 Create New to add a rule to the sensor.
7. Set the Action to None.
8. Set Member type to Compound rule.
9. Select the President + subject rule.
10. Select OK.

With the DLP sensor ready for use, you need to select it in the protection profile.

To select the DLP sensor in the protection profile
1. Go to Firewall > Protection Profile.
2. Select the Edit icon of the protection profile attached to the firewall policy that controls email traffic.
3. Expand the Data Leak Prevention Sensor section.
4. Select the Data Leak Prevention Sensor check box and select the president DLP sensor from the drop-down list.
5. Select OK to save the protection profile.

With the DLP sensor specified in the correct protection profile, 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 protection profiles applied to the network traffic you need to monitor.

This chapter 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 chapter:

- Application control concepts
- Enable application control
- Application considerations
- Application control example

Application control concepts

You can control network traffic by the source or destination address, or by the port, the quantity or similar attributes of the traffic itself. 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 comes with 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 list of applications that application control can detect by adding applications to the FortiGuard Application Control Database. Because intrusion protection protocol decoders are used for application control, the application control database is part of the FortiGuard Intrusion Protection System Database and both of these databases have the same version number.

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 application control in a protection profile and select the application list you created.
4. Enable protection profile use in a firewall policy and select the protection profile in which you specified the application control list.

The protection profile settings will apply to all network traffic controlled by the policy, including application control and the application control list you configured.

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 > Black/White 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, containing no applications. Without applications, the application control list will not work.

Adding applications to an application control list

Once you have created an application control list, you need to need to define the applications that you want to control.

To add applications to an application control list

1. Go to UTM > Application Control > Black/White List.
2. Select the Edit icon of the application control list to which you want to add the application.
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 limits the options available in the Application selection. If you want to have 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 prevent all traffic from the application from flowing through the FortiGate unit.
- **Pass** allows the application traffic to flow normally through the FortiGate unit.

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 if traffic from the application is detected.

9 Some IM and VoIP applications have additional options:

**IM Options (for example AIM)**
- **Block Login** Select to prevent users from logging in to the selected IM system.
- **Block File Transfers** Select to prevent the sending and receiving of files using the selected IM system.
- **Block Audio** Select to prevent audio communication using the selected IM system.
- **Inspect Non-standard Port** Select to allow the FortiGate unit to examine non-standard ports for the IM client traffic.
- **Display DLP meta-information on the system dashboard** Select to include meta-information detected for the IM system on the FortiGate unit dashboard.

**VoIP Options (for example SCCP, SIP)**
- **Limit Call Setup** Enter the maximum number of calls each client can set up per minute.
- **Limit REGISTER request** Enter the maximum number of register requests per second allowed for the firewall policy.
- **Limit INVITE request** Enter the maximum number of invite requests per second allowed for the firewall policy.
- **Enable Logging of Violations** Select to enable logging of violations.

**Other Options**
- **Command** Some traffic types include a command option. Specify a command that appears in the traffic that you want to block or pass.
  
  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.

- **Method** 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.
  
  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.
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 both UDP and 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 example**

**No Instant Messaging**

Instant messaging use is not permitted at Example.com 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 > Black/White List*.
2. Select *Create New*.
3. In the *Name* field, enter *no IM* for the application control list name.
4. Select *OK* to create the new list.
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 > Protection Profile.
2 Select the Edit icon of the protection profile specified in the outgoing policy.
3 Expand the Application Control section.
4 Select the Application Black/White List check box.
5 Select the no IM list from the drop-down list.
6 Select OK to save the protection profile.

No IM use will be allowed by any firewall policies using the protection profile with the no IM application control list.
DoS policy

Denial of Service (DoS) policies are primarily used to apply DoS sensors to network traffic based on the FortiGate interface it is leaving or 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 chapter 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 chapter:

- 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 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 defence 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, see “DoS concepts” on page 23.

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 Edit icon of the DoS sensor you want to configure.
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>
Enabling DoS Policies

Steps to Enable DoS Policies:

1. Go to **Firewall > Policy > DoS Policy** and select **Create New**.
2. For **Source Interface/Zone**, select the interface to which the DoS policy will apply.
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**.

Options for DoS Sensors:

- **icmp_src_session**: If the number of concurrent ICMP connections from one source IP address exceeds the configured threshold value, the action is executed.
- **icmp_dst_session**: If the number of concurrent ICMP connections to one destination IP address exceeds the configured threshold value, the action is executed.

4. Select **Enable** to have the FortiGate unit examine traffic for the anomaly.
5. Select **Logging** to create an entry in the IPS 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** the incomplete connections that exceed the threshold value. When the tcp_syn_flood threshold action is set to **Proxy**, incomplete TCP connections are allowed as normal as long as the configured threshold is not exceeded. If the threshold is exceeded, the FortiGate unit will intercept incoming SYN packets and use a “best effect” algorithm to determine whether the connection attempt is legitimate or a SYN flood attack. A legitimate connection is allowed while an attack is blocked.

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 to which the DoS policy will apply.
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 protection profiles, 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 protection profile.

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 attack - best practices overview" on page 26, 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 chapter 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 chapter:

- Sniffer policy concepts
- Before you begin
- Enable one-arm sniffing

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 9 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.
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 10: 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 124. 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 124. 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.
**Enable one-arm sniffing**

**Sniffer policy**

### 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 **Edit** icon of the 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.

3. 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.

4. Select **OK**.

### 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. For more information, see "Designating a sniffer interface" on page 126.

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 required 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 required 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 required 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.
Index

Symbols

_email, 12
_fqdn, 12
_index, 12
_int, 12
_ipv4, 12
_ipv4/mask, 12
_ipv4mask, 12
_ipv6, 12
_ipv6mask, 12
_name, 12
_pattern, 12
_str, 12
_v4mask, 12
_v6mask, 12

A

allow
  pattern, 41
anomaly protection
  DoS, 16
antispm, see email filtering and FortiGuard, AntiSpam
antivirus, 35
  concepts, 35
  enabling scanning, 38
  example, 44
  file filtering, 15
  FortiAnalyzer, 15
  HTTPS, IMAPS, POP3S, SMTPS, 20
  scanning order, 35
antivirus quarantine
  HTTPS, IMAPS, POP3S, SMTPS, 20
application control, 16
archive SPAM email
  IMAPS, POP3S, SMTPS, 22

B

black list, 16
block
  pattern, 41

C

CA certificate, 18
  certificate
    key size, 18
    SSL, 18
CIDR, 12
  concepts
    antivirus, 35
    web filtering, 16
content scanning
  SSL, 17
custom signature
  adding, 65

D

data leak prevention (DLP), see DLP
  deep scan, 20
  DLP archive
    displaying on dashboard, 22
  DLP archiving
    HTTPS, IMAPS, POP3S, SMTPS, 21
DoS
  anomaly protection, 16
dotted decimal, 12

E

EICAR, 44
email filtering
  IMAPS, POP3S, SMTPS, 21
email filtering, see also FortiGuard, AntiSpam, 16
extended virus database, 40

F

file filtering, 41
  antivirus, 15
  enabling, 43
  general configuration steps, 42
file pattern, 35, 37, 41
  creating, 42
file quarantine
  configuring, 39
  general configuration steps, 39
file size, 35, 37
file type, 35, 37, 41
  creating, 42
firewall policy, 17, 40
FortiAnalyzer
  antivirus, 15
  quarantine, 38
FortiGate-ASM-S08 module, 38
FortiGate-ASM-SAS module, 38
FortiGuard
  AntiSpam, 16
  Antivirus, 38
  Web Filtering, 16, 21
    HTTPS, 21
FortiGuard Center, 38
FortiGuard, Distribution Network, 37
fully qualified domain name (FQDN), 12
Index

G

general configuration steps
  file filtering, 42
  file quarantine, 39
grayware, 35, 37
  scanning, 43

H

heuristics, 35, 37
HTTPS
  antivirus, 20
  antivirus quarantine, 20
  data leak prevention, 21
  DLP archiving, 21
  FortiGuard Web Filtering, 21
  protocol recognition, 20
  web filtering, 20

I

IDS
  one-armed IDS, 16
IM, 16
IMAPS
  antivirus, 20
  antivirus quarantine, 20
  archive SPAM email, 22
  data leak prevention, 21
  DLP archiving, 21
  email filtering, 21
  predefined firewall services, 20
  protocol recognition, 20
index number, 12
inspection
  SSL, 17
intrusion detection system, see IDS
intrusion prevention system, see IPS
intrusion protection system, see IPS
IPS
  adding custom signatures, 65
  overview, 15

K

key size
  certificate, 18

O

one-armed IDS, 16

P

P2P, 16
pattern, 12, 41
  allow, 41
  block, 41
  creating, 42
policy
  adding a protection profile, 40

POP3S
  antivirus, 20
  antivirus quarantine, 20
  archive SPAM email, 22
  data leak prevention, 21
  DLP archiving, 21
  email filtering, 21
  predefined firewall services, 20
  protocol recognition, 20
predefined firewall services
  IMAPS, POP3S, SMTPS, 20
protection profile, 17
  adding to a policy, 40
  quarantine, 40
protocol recognition
  HTTPS, IMAPS, POP3S, SMTPS, 20

Q

quarantine, 38
  protection profile, 40

R

regular expression, 12

S

scanning order
  antivirus, 35
signature
  adding custom IPS signatures, 65
SMTPS
  antivirus, 20
  antivirus quarantine, 20
  archive SPAM email, 22
  data leak prevention, 21
  DLP archiving, 21
  email filtering, 21
  predefined firewall services, 20
  protocol recognition, 20
sniffer policies, 16
SSL
  antivirus, 20
  antivirus quarantine, 20
  archive SPAM email, 22
  certificate, 18
  content inspection, 17
  content scanning, 17
  data leak prevention, 21
  DLP archiving, 21
  email filtering, 21
  example, 44
  FortiGuard Web Filtering, 21
  HTTPS, 21
  inspection, 17
  predefined firewall services, 20
  protocol recognition, 20
  settings, all, 20
  supported FortiGate models, 17
  web filtering, 20
string, 12
U
Unified Threat Management, see UTM
URL filtering, 16
UTM
  overview, 15
V
value parse error, 12

virus database, 38, 40
virus scan, 35, 37

W
web content filtering, 16
web filtering, 16
  HTTPS, 20
wild cards, 12
wildcard, 41