



Spam Filter

Technical Note

<i>Spam Filter Technical Note</i>	
Document Version:	2
Publication Date:	9 July 2004
Description:	This document describes how to configure the FortiGate Spam Filter.
Product	FortiGate Antivirus Firewalls v2.80 MR2

Fortinet Inc.

No part of this publication including text, examples, diagrams or illustrations may be reproduced, transmitted, or translated in any form or by any means, electronic, mechanical, manual, optical or otherwise, for any purpose, without prior written permission of Fortinet Inc.

Spam Filter Technical Note

FortiGate Antivirus Firewall v2.80 MR2

9 July 2004

Trademarks

Products mentioned in this document are trademarks or registered trademarks of their respective holders.

Regulatory Compliance

FCC Class A Part 15 CSA/CUS

For technical support, please visit <http://www.fortinet.com>.

Send information about errors or omissions in this document or any Fortinet technical documentation to techdoc@fortinet.com.

Table of Contents

FortiGate spam filtering techniques	5
IP address	7
RBL & ORDBL	8
Email address	9
MIME headers.....	11
Banned word.....	12
Using Perl regular expressions	15
Configuring spam filtering in a protection profile.....	17
Spam filtering options	17
Creating a protection profile that uses spam filtering.....	18
Configuring logging and alert email	18
Spam log messages	19
Configuring replacement messages.....	22

Spam is such a prevalent and damaging force on corporate networks that many companies devote multiple products and people to spam protection in an attempt to stem the bandwidth-stealing tide. FortiGate Antivirus Firewalls provide spam protection using a variety of techniques, all easily configured and adapted by the administrator or a managed security service provider.

Spam filters are configured globally in the FortiGate unit but can be enabled separately in each firewall protection profile. See the *FortiGate Administration Guide* for protection profile and firewall policy details and procedures.

Administrators can monitor spam events through log messages and alert email.

Blocked email messages are replaced by a standard warning message from the FortiGate unit. These replacement messages can be customized by the administrator.

This document describes:

- [FortiGate spam filtering techniques](#)
- [Configuring spam filtering in a protection profile](#)
- [Configuring logging and alert email](#)
- [Configuring logging and alert email](#)

FortiGate spam filtering techniques

Incoming email is passed through the spam filters in sequence, with each filter passing the email to the next if no matches or problems are found. When a match or problem is found the FortiGate unit will tag, pass, or discard (SMTP only) the email according to the settings in the protection profile.

FortiGate firewalls filter spam using the following techniques in the following order:

- IP address black and white lists
- Real-time Blackhole Lists and Open Relay Database Lists
- HELO DNS lookup
- Email address black and white lists
- Return email DNS check
- MIME header blocking
- Content filtering using words, phrases, wildcards, and regular expressions

[Table 1](#) describes each FortiGate spam filtering technique and provides a link to the relevant configuration procedure.

Table 1: FortiGate spam filtering techniques

Spam Filtering Technique	Description	Configuration
IP Address	<p>Also known as a black and white list. This list is compiled by the administrator.</p> <p>The FortiGate unit uses the IP address list to filter incoming email. The FortiGate unit compares the IP address of the sender to the list in sequence. If a match is found, the corresponding action is taken. Action can be mark as spam, clear, or reject. If no match is found, the email is passed to the next spam filter.</p>	See "IP address" on page 7.
RBL & ORDBL	<p>Using Real-time Blackhole Lists (RBLs) and Open Relay Database Lists (ORDBLs) is an effective way to tag or reject spam as it enters your system. These lists act as domain name servers that match the domain of incoming email to a list of IP addresses known to send spam or allow spam to pass through. RBLs keep track of reported spam source addresses and ORDBLs keep track of unsecured third party SMTP servers, known as open relays, which some spammers use to send unsolicited bulk email.</p> <p>The FortiGate unit compares the IP address or domain name of the sender to any database lists you configure in sequence. If a match is found, the corresponding action is taken. If no match is found, the email is passed to the next spam filter.</p>	See "RBL & ORDBL" on page 8.
HELO DNS lookup	After receiving the HELO command (which contains the domain name) from the SMTP client, the FortiGate unit does a reverse lookup of the domain name against the IP address of the sender.	See "Spam filtering options" on page 17.
Email Address	<p>Another form of black and white list. The email address list is also compiled by the administrator.</p> <p>The FortiGate unit uses the email address list to filter incoming email. The FortiGate unit compares the email address or domain of the sender to the list in sequence. If a match is found, the corresponding action is taken. Action can be mark as spam, clear, or reject. If no match is found, the email is passed to the next spam filter.</p>	See "Email address" on page 9.
Return email DNS check	The FortiGate unit checks that the return email domain name has an MX or A record in the DNS server.	See "Spam filtering options" on page 17.
MIME Headers	<p>Administrators can use the MIME headers list to mark email from certain bulk mail programs or with certain types of content that are common in spam messages. You can choose to mark the email as spam or clear for each header you configure.</p> <p>The FortiGate unit compares the MIME header key-value pair of incoming email to the list pair in sequence. If a match is found, the corresponding action is taken. If no match is found, the email is passed to the next spam filter.</p>	See "MIME headers" on page 11.
Banned word	<p>Also known as content or lexical analysis. Control spam by blocking email containing specific words or patterns.</p> <p>The FortiGate unit searches for banned words in email messages. If a match is found, the corresponding action is taken. If no match is found, the email is passed to the recipient.</p>	See "Banned word" on page 12.

IP address

You can enter an IP address and mask in two formats:

- x.x.x.x/x.x.x.x, for example 62.128.69.100/255.255.255.0
- x.x.x.x/x, for example 62.128.69.100/24

This section describes:

- [IP address list](#)
- [IP address options](#)
- [Configuring the IP address list](#)

IP address list

You can configure the FortiGate unit to filter email from specific IP addresses. You can designate an action for each IP address as clear, spam, or reject. You can filter single IP addresses, or a range of addresses at the network level by configuring an address and mask.

Figure 1: Sample IP address list

IP Address / Mask	Action	Icons
219.161.10.0/24	Spam	Icons for Create, Edit, Delete
64.59.0.0/16	Spam	Icons for Create, Edit, Delete
63.200.172.0/24	Clear	Icons for Create, Edit, Delete
69.0.0.0/8	Reject	Icons for Create, Edit, Delete

IP address options

IP address list has the following icons and features:

- Create New** Select Create New to add an IP address to the IP address list.
The Page up, Page down, and Remove all entries icons.
- IP address/Mask** This column displays the current list of IP addresses.
- Action** This column displays the action to take on email from the configured IP address. Actions are:
Mark as Spam to apply the spam action configured in the protection profile, Mark as Clear to let the email pass to the next filter, or Mark as Reject (SMTP only) to immediately drop the connection.
The Delete and Edit/View icons.

Configuring the IP address list

To add an IP address to the IP address list

- 1 Go to **Spam Filter > IP Address**.
- 2 Select Create New.

Figure 2: Adding an IP address



- 3 Enter the IP address/mask you want to add.
- 4 If required, select before or after another IP address in the list to place the new IP address in the correct position.
- 5 Select the action to take on email from the IP address.
- 6 Select OK.

RBL & ORDBL

There are several free and subscription servers available that provide reliable access to continually updated RBLs and ORDBLs. Check with the service you are using to confirm the correct domain name for connecting to the server.

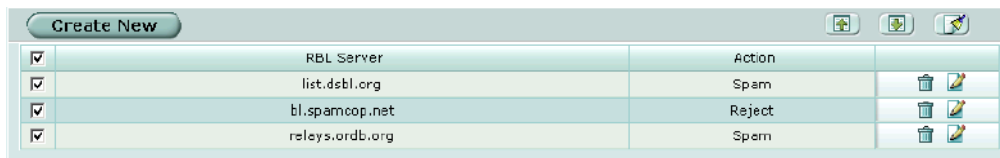
This section describes:

- [RBL & ORDBL list](#)
- [RBL and ORDBL options](#)
- [Configuring the RBL & ORDBL list](#)

RBL & ORDBL list

You can configure the FortiGate unit to filter email by accessing RBL or ORDBL servers. You can designate an action for a match by each server as spam or reject.

Figure 3: Sample RBL & ORDBL list



RBL and ORDBL options

RBL & ORDBL list has the following icons and features:

- Create New** Select Create New to add a server to the RBL & ORDBL list.
The Page up, Page down, and Remove all entries icons.
- RBL Server** The current list of servers. Select the check box to enable all the RBL and ORDBL servers in the list

Action The action to take on email matched by the RBLs and ORDBLs. Actions are: Mark as Spam to apply the spam action configured in the protection profile, or Mark as Reject (SMTP only) to immediately drop the connection.


The Delete and Edit/View icons.

Configuring the RBL & ORDBL list

To add a server to the RBL & ORDBL list

- 1 Go to **Spam Filter > RBL & ORDBL**.
- 2 Select Create New.

Figure 4: Adding an RBL or ORDBL server



- 3 Enter the domain name of the RBL or ORDBL server you want to add.
- 4 Select the action to take on email matched by the server.
- 5 Select Enable.
- 6 Select OK.

Email address

You can use Perl regular expressions or wildcards to add email address patterns to the list. See the [“Using Perl regular expressions” on page 15](#) for information about using regular expressions.

This section describes:

- [Email address list](#)
- [Email address options](#)
- [Configuring the email address list](#)

Email address list

The FortiGate unit can filter email from specific senders or all email from a domain (such as sample.net). You can designate the action to take for each email address as clear or spam.

Figure 5: Sample email address list

E-mail Address	Pattern Type	Action	
loser@spammer\,com	Regular Expression	Spam	
sample.*	Wildcard	Spam	
*@fortnet.com	Wildcard	Clear	

Email address options

Email address list has the following icons and features:

- Create New** Select Create New to add an email address to the email address list.
The Page up, Page down, and Remove all entries icons.
- Email address** This column displays the current list of email addresses.
- Pattern Type** This column displays the pattern type used in the email address entry.
Choose from wildcard or regular expression.
- Action** This column displays the action to take on email from the configured address. Actions are: Mark as Spam to apply the spam action configured in the protection profile, or Mark as Clear to let the email pass to the next filter.
The Delete and Edit/View icons.

Configuring the email address list

To add an email address or domain to the list

- 1 Go to **Spam Filter > E-mail Address**.
- 2 Select Create New.

Figure 6: Adding an email address

- 3 Enter the email address or pattern you want to add.
- 4 Select a pattern type for the list entry.
- 5 If required, select before or after another email address in the list to place the new email address in the correct position.
- 6 Select the action to take on email from the configured address or domain.
- 7 Select OK.

MIME headers

MIME (Multipurpose Internet Mail Extensions) headers are added to email to describe content type and content encoding, such as the type of text in the email body or the program that generated the email. Some examples of MIME headers include:

- X-mailer: outgluck
- X-Distribution: bulk
- Content_Type: text/html
- Content_Type: image/jpg

The first part of the MIME header is called the header key, or just header. The second part is called the value. Spammers will often insert comments into header values or leave them blank. These malformed headers can fool some spam and virus filters.

You can use Perl regular expressions or wildcards to add MIME header patterns to the list. See the [“Using Perl regular expressions” on page 15](#) for information about using regular expressions.



Note: MIME header entries are case sensitive.

This section describes:

- [MIME headers list](#)
- [MIME headers options](#)
- [Configuring the MIME headers list](#)

MIME headers list

You can configure the FortiGate unit to filter email with specific MIME header key-value pairs. You can designate an action for each MIME header as clear or spam.

Figure 7: Sample MIME headers list

Header	Value	Pattern Type	Action	
X-UIDL	*	Wildcard	Spam	
X-Distribution	bulk	Wildcard	Spam	
Content_Type	image/jpg	Wildcard	Spam	
Content-Type	text/plain	Wildcard	Clear	
X-Mailer	outgluck	wildcard	Spam	

MIME headers options

MIME headers list has the following icons and features:

- Create New** Select Create New to add a MIME header to the MIME headers list. The Page up, Page down, and Remove all entries icons.
- Header** This column displays the current list of MIME headers (keys).
- Value** This column displays the current list of MIME header values for each key.


Pattern Type	The pattern type used in the MIME header list entry. Choose from wildcard or regular expression.
Action	This column displays the action to take on email with the configured MIME header. Actions are: Mark as Spam to apply the spam action configured in the protection profile, Mark as Clear to let the email pass to the next filter, or Mark as Reject (SMTP only) to immediately drop the connection. The Delete and Edit/View icons.

Configuring the MIME headers list

To add a MIME header to the list

- 1 Go to **Spam Filter > MIME headers**.
- 2 Select Create New.

Figure 8: Adding a MIME header



- 3 Enter the MIME header key.
- 4 Enter the MIME header value.
- 5 Select a pattern type for the list entry.
- 6 Select the action to take on email with that MIME header key-value.
- 7 Select OK.

Banned word

You can use Perl regular expressions or wildcards to add banned word patterns to the list. See the [“Using Perl regular expressions” on page 15](#) for information about using regular expressions.



Note: Perl regular expression patterns are case sensitive for Spam Filter banned words. To make a word or phrase case insensitive, use the regular expression `/i`. For example, `/bad language/i` will block all instances of `bad language` regardless of case. Wildcard patterns are not case sensitive.

This section describes:

- [Banned word list](#)
- [Banned word options](#)
- [Configuring the banned word list](#)

Banned word list

You can add one or more banned words to sort email containing those words in the email subject, body, or both.

Words can be designated as spam or clear. Banned words can be one word or a phrase up to 127 characters long.

If you enter a single word, the FortiGate unit blocks all email that contain that word. If you enter a phrase, the FortiGate unit blocks all email containing the exact phrase.

Figure 9: Sample banned word List

Pattern	Pattern Type	Language	Where	Action
all new	Wildcard	Western	Subject	Spam
act now	Wildcard	Western	Body	Spam
free credit report	Wildcard	Western	All	Spam
Fortinet	Wildcard	Japanese	All	Clear
porn	wildcard	Western	All	Spam

Banned word options

Banned word has the following icons and features:

- Create new** Select Create New to add a word or phrase to the banned word list.
The Page up, Page down, and Remove all entries icons.
- Pattern** This column displays the current list of banned words. Select the check box to enable all the banned words in the list.
- Pattern Type** The pattern type used in the banned word list entry. Choose from wildcard or regular expression.
- Language** This column displays the character set to which the banned word belongs: Simplified Chinese, Traditional Chinese, French, Japanese, Korean, Thai, or Western.
- Where** This column displays the location which the FortiGate unit searches for the banned word: subject, body, or all.
- Action** This column displays the action to take on email with a banned word. Actions are: Mark as Spam to apply the spam action configured in the protection profile, or Mark as Clear to let the email pass to the next filter.
The Delete and Edit/View icons.

When you select Create New or Edit you can configure the following settings for the banned word.

Figure 10: Adding a banned word



- Pattern** Enter the word or phrase you want to include in the banned word list.
- Pattern Type** Select the pattern type for the banned word. Choose from wildcard or regular expression.
- Language** Select the character set for the banned word. Choose from: Chinese Simplified, Chinese Traditional, French, Japanese, Korean, Thai, or Western.
- Where** Select the location to search for the banned word. Choose from: subject, body, or all.
- Action** The action to take on email containing a banned word. Actions are: Mark as Spam to apply the spam action configured in the protection profile, or Mark as Clear to let the email pass to the next filter.
- Enable** Select to enable screening for the banned word.

Configuring the banned word list

To add or edit a banned word

- 1 Go to **Spam Filter > Banned Word**.
- 2 Select Create New to add a banned word or select Edit for the banned word you want to modify.
- 3 Enter the word or phrase.
If you enter a single word, the FortiGate unit blocks all email containing that word. If you enter a phrase, the FortiGate unit blocks all email containing any word in the phrase. If you contain the phrase in quotation marks, the FortiGate unit blocks all email containing the exact phrase.
Banned word entries can be Perl compatible regular expressions. See the [“Using Perl regular expressions” on page 15](#) for information about using regular expressions.
- 4 Select the language (character set).
- 5 Select the location.
- 6 Select the action to take on email containing the banned word.
- 7 Select Enable.
- 8 Select OK.

Using Perl regular expressions

Email address list, MIME headers list, and banned word list entries can include wildcards or Perl regular expressions.

See <http://www.perldoc.com/perl5.8.0/pod/perlre.html> for detailed information about using Perl regular expressions.

Regular expression vs. wildcard match pattern

In Perl regular expressions, the '.' character refers to any single character. It is similar to the '?' character in wildcard match pattern. As a result:

- fortinet.com not only matches fortinet.com but also matches fortinetacom, fortinetbcom, fortinetccom and so on.

To match a special character such as '.' and '*' use the escape character '\'. For example:

- To mach fortinet.com, the regular expression should be: fortinet\.com

In Perl regular expressions, '*' means match 0 or more times of the character before it, not 0 or more times of any character. For example:

- forti*.com matches fortiiii.com but does not match fortinet.com

To match any character 0 or more times, use '.*' where '.' means any character and the '*' means 0 or more times. For example, the wildcard match pattern forti*.com should therefore be fort.*\.com.

Word boundary

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

Case sensitivity

Regular expression pattern matching is case sensitive in the Web and Spam filters. To make a word or phrase case insensitive, use the regular expression /i For example, /bad language/i will block all instances of "bad language" regardless of case.

Table 2: Perl regular expression formats

Expression	Matches
abc	abc (that exact character sequence, but anywhere in the string)
^abc	abc at the beginning of the string
abc\$	abc at the end of the string
a b	either of a and b
^abc abc\$	the string abc at the beginning or at the end of the string
ab{2,4}c	an a followed by two, three or four b's followed by a c
ab{2,}c	an a followed by at least two b's followed by a c

Table 2: Perl regular expression formats

<code>ab*c</code>	an a followed by any number (zero or more) of b's followed by a c
<code>ab+c</code>	an a followed by one or more b's followed by a c
<code>ab?c</code>	an a followed by an optional b followed by a c; that is, either abc or ac
<code>a.c</code>	an a followed by any single character (not newline) followed by a c
<code>a\.c</code>	a.c exactly
<code>[abc]</code>	any one of a, b and c
<code>[Aa]bc</code>	either of Abc and abc
<code>[abc]+</code>	any (nonempty) string of a's, b's and c's (such as a, abba, acbabacaaa)
<code>[^abc]+</code>	any (nonempty) string which does not contain any of a, b and c (such as defg)
<code>\d\d</code>	any two decimal digits, such as 42; same as <code>\d{2}</code>
<code>/i</code>	makes the pattern case insensitive. For example, <code>/bad language/i</code> blocks any instance of <code>bad language</code> regardless of case.
<code>\w+</code>	a "word": a nonempty sequence of alphanumeric characters and low lines (underscores), such as <code>foo</code> and <code>12bar8</code> and <code>foo_1</code>
<code>100\s*mk</code>	the strings <code>100</code> and <code>mk</code> optionally separated by any amount of white space (spaces, tabs, newlines)
<code>abc\b</code>	<code>abc</code> when followed by a word boundary (e.g. in <code>abc!</code> but not in <code>abcd</code>)
<code>perl\b</code>	<code>perl</code> when not followed by a word boundary (e.g. in <code>perlert</code> but not in <code>perl stuff</code>)
<code>\x</code>	tells the regular expression parser to ignore white space that is neither backslashed nor within a character class. You can use this to break up your regular expression into (slightly) more readable parts.
<code>/x</code>	used to add regexps within other text. If the first character in a pattern is forward slash '/', the '/' is treated as the delimiter. The pattern must contain a second '/'. The pattern between '/' will be taken as a regexp, and anything after the second '/' will be parsed as a list of regexp options ('i', 'x', etc). An error occurs if the second '/' is missing. In regular expressions, the leading and trailing space is treated as part of the regular expression.

Examples

To block any word in a phrase

```
/block|any|word/
```

To block purposely misspelled words

Spammers often insert other characters between the letters of a word to fool spam blocking software.

```
/^.*v.*i.*a.*g.*r.*a.*$/i
```

```
/cr[eéèêë] [\+\-\*=<>\.\,;!\?%&S@\^°\$\£€\{\}\|\|\_01]dit/i
```

To block common spam phrases

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

```
/work from home/i
```

```
/you're already approved/i
```

```
/special [\+\-\*=<>\.\,;!\?%&~#S@\^°\$\£€\{\}\|\|\_1]offer/i
```

Configuring spam filtering in a protection profile

Spam filtering can be combined with other FortiGate features – antivirus, web filtering, web category filtering, and the Intrusion Protection System (IPS) – to create protection profiles. Protection profiles are then added to individual user groups and then to firewall policies, or added directly to firewall policies.

Spam filtering options

Figure 11: Protection profile spam filtering options

Spam Filtering			
	IMAP	POP3	SMTP
IP address BWL check			<input checked="" type="checkbox"/>
RBL & ORDBL check	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
HELO DNS lookup			<input checked="" type="checkbox"/>
E-mail address BWL check	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Return e-mail DNS check	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
MIME headers check	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Banned word check	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Spam Action	tagged	tagged	discard
Append to:	<input checked="" type="radio"/> subject <input type="radio"/> MIME	<input checked="" type="radio"/> subject <input type="radio"/> MIME	<input checked="" type="radio"/> subject <input type="radio"/> MIME
Append with:	spam?	spam?	

The following options are available for spam filtering through the protection profile.

IP address BWL check	Black/white list check. Enable or disable checking incoming IP addresses against the configured spam filter IP address list. (SMTP only.)
RBL & ORDBL check	Enable or disable checking traffic against configured Real-time Blackhole List and Open Relay Database List servers.
HELO DNS lookup	Enable or disable looking up the source domain name (from the SMTP HELO command) in the Domain Name Server.
E-mail address BWL check	Enable or disable checking incoming email addresses against the configured spam filter email address list.
Return e-mail DNS check	Enable or disable checking that the domain specified in the reply-to or from address has an A or MX record.
MIME headers check	Enable or disable checking source MIME headers against the configured spam filter MIME header list.
Banned word check	Enable or disable checking source email against the configured spam filter banned word list.
Spam Action	Choose an action to take on email identified as spam. Choose from pass or tagged for IMAP and POP3 traffic, and pass, tagged, or discard for SMTP traffic. You can tag email by appending a custom word or phrase to the subject or inserting a MIME header and value into the email header. Note: Choosing to tag spam email messages automatically disables splice.
Append to	Choose to append the tag to the subject or MIME header of the email identified as spam.
Append with	Enter a word or phrase (tag) to append to email identified as spam. The maximum length is 63 characters.



Note: Some popular email clients cannot filter messages based on the MIME header. Check your email client features before deciding how to tag spam.

Creating a protection profile that uses spam filtering

- 1 Go to **Firewall > Protection Profile**.
- 2 Select **Create New**.
- 3 Enter a name for the protection profile.
- 4 Expand the **Spam Filtering** option list.
- 5 Enable any features you have configured in the **Spam Filter**.
- 6 Select any additional spam blocking features you want to use.
- 7 Select **tagged** as the **Spam Action** for **IMAP** and **POP3** and select **tagged** or **discard** for **SMTP**.
- 8 Configure any other required protection profile options.
- 9 Select **OK**.

The protection profile can now be added to any firewall policies that require it. The protection profile can also be added to user groups and the user groups added to firewall policies that use authentication.

Adding protection profiles to firewall policies

Adding a protection profile to a firewall policy applies the profile settings, including spam filtering, to traffic matching that policy.

Adding protection profiles to user groups

When creating a user group, you can also select a protection profile that applies to that group. Then, when you configure a firewall policy that includes user authentication, you select one or more user groups to authenticate. Each user group you select for authentication in the firewall policy can have a different protection profile, and therefore different Spam Filtering settings, applied to it.

Configuring logging and alert email

The FortiGate unit can record log messages to a variety of locations. Administrators can also receive alert email notifying them of specific events.


The FortiGate unit categorizes spam log messages by traffic type. You can enable logging and alert email for spam detected in IMAP, POP3, and SMTP traffic.

Figure 12: Spam log filter options

Log Filter						
	Check All	Syslog	WebTrends	Memory	Fortilog	Alert E-mail
▶ Traffic Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
▶ Event Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
▶ Anti-virus Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
▶ Web Filter Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
▶ Attack Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
▼ Spam Filter Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
SMTP	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
POP3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
IMAP	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
▶ Content Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Apply

To configure logging and alert email for spam events

- 1 Go to **Log&Report > Log Config > Log Setting**.
 - 2 Select and configure the settings for any logging locations you want to use.
 - 3 Select Apply.
 - 4 Go to **Log&Report > Log Config > Alert Email**.
 - 5 Select and configure authentication if required and enter the email addresses that will receive the alert email.
 - 6 Enter the time interval to wait before sending alert email for each logging severity level.
-  **Note:** If more than one log message is collected before an interval is reached, the messages are combined and sent out as one alert email.
- 7 Select Apply.
 - 8 Go to **Log&Report > Log Config > Log Filter**.
 - 9 Enable the appropriate traffic types for each log location and for alert email under the Spam Filter Log option.
 - 10 Select Apply.

Spam log messages

Spam log messages can be recorded to a location and can also be sent in alert email according to the configured options.

The following log messages are generated when email messages are blocked by a component of the spam filter.

Message ID: 80000 (SMTP)
83000 (POP3)
86000 (IMAP)

Severity: Notification

Message: src=<ip_address> dst=<ip_address> src_int=<interface_name>
dst_int=<interface_name> service=SMTP | POP3 | IMAP status=detected
msg="from ip is in ip blacklist"

Meaning: The email message from the specified source was blocked because the source IP address is marked as spam by the IP address list.

Action: None

Message ID: 80001 (SMTP)
83001 (POP3)
86001 (IMAP)

Severity: Notification

Message: src=<ip_address> dst=<ip_address> src_int=<interface_name>
dst_int=<interface_name> service=SMTP | POP3 | IMAP status=detected
msg="from ip is in rbl/ordbl"

Meaning: The email message from the specified source was blocked because the source IP address is on an RBL or an ORDBL.

Action: None

Message ID: 80002 (SMTP)
83002 (POP3)
86002 (IMAP)

Severity: Notification

Message: src=<ip_address> dst=<ip_address> src_int=<interface_name>
dst_int=<interface_name> service=SMTP | POP3 | IMAP status=detected
msg="smtp helo/ehlo domain name DNS check failed."

Meaning: The email message from the specified source was blocked because the source domain name in the SMTP HELO command did not match the Domain Name Server.

Action: None

Message ID: 80003 (SMTP)
83003 (POP3)
86003 (IMAP)

Severity: Notification

Message: src=<ip_address> dst=<ip_address> src_int=<interface_name>
dst_int=<interface_name> service=SMTP | POP3 | IMAP status=detected
msg="from email address is in email blacklist."

Meaning: The email message from the specified source was blocked because the source email address is marked as spam by the email address list.

Action: None

Message ID: 80004 (SMTP)
83004 (POP3)
86004 (IMAP)

Severity: Notification

Message: src=<ip_address> dst=<ip_address> src_int=<interface_name>
dst_int=<interface_name> service=SMTP | POP3 | IMAP status=detected
msg="the email contains banned header"

Meaning: The email message from the specified source was blocked because the MIME header contains a value marked as spam by the MIME headers list.

Action: None

Message ID: 80005 (SMTP)
83005 (POP3)
86005 (IMAP)

Severity: Notification

Message: src=<ip_address> dst=<ip_address> src_int=<interface_name>
dst_int=<interface_name> service=SMTP | POP3 | IMAP status=detected
msg="smtp helo/ehlo domain name DNS check failed."

Meaning: The email message from the specified source was blocked because the domain name of the reply-to or from address does not have an A or MX record on the DNS server.

Action: None

Message ID: 80006 (SMTP)
83006 (POP3)
86006 (IMAP)

Severity: Notification

Message: src=<ip_address> dst=<ip_address> src_int=<interface_name>
dst_int=<interface_name> service=SMTP | POP3 | IMAP status=detected
msg="The email contains banned word(s)."

Meaning: The email message from the specified source was blocked because it contains a word from the banned word list.

Action: None

Configuring replacement messages

Spam found in IMAP and POP3 traffic can only be tagged or passed according to the settings in the protection profile. Spam found in SMTP traffic can be tagged, passed, or discarded according to the settings in the protection profile. Discarded SMTP messages are replaced by a standard warning message from the FortiGate unit.

Replacement messages state the reason the email message was blocked. For example, if an email message is received from an IP address blocked by the IP address list, the message will read:

Mail from this IP address is not allowed and has been blocked.

To change a replacement message

- 1 Go to **System > Config > Replacement Messages**.
- 2 Expand the Spam replacement message list.
- 3 Select the Edit icon for the message you want to change.
- 4 Edit the message and select OK.