FortiGuard Antispam

Frequently Asked Questions

FORTINET

Q: What is FortiGuard Antispam?

A: FortiGuard Antispam Subscription Service (FortiGuard Antispam) is the core of the Fortinet antispam solution. FortiGuard Antispam consists of FortiGate, FortiMail, and/or FortiClient as the service delivery unit, combined with FortiGuard servers in the FortiGuard Service Distribution Network to provide constant signature updates. FortiGuard Antispam provides global filters, while the service delivery units complete the antispam solution with local filters.

Q: What technologies are used to detect spam in the FortiGuard Antispam solution?

A: Fortinet takes a comprehensive and multi-layer approach, using a number of filtering techniques to detect and filter spam:

Global filters – Through the FortiGuard Service Distribution Network, FortiGuard Antispam Service is powered by two databases, FortiIP and FortiSig, providing the spam data that result in global filters. FortiIP is a sender IP reputation database. FortiSig is a spam signature database. These global filters are constantly updated and enable Fortinet FortiGate, FortiClient and FortiMail products to detect and filter most spam delivered over the Internet.

Customized filters – Various customized spam filters are provided to compliment the Fortinet Antispam solution on the service delivery units: FortiGate, FortiClient and FortiMail. These customized filters range from banned words filters, local white and black lists of sender email address, heuristic rules, to highly sophisticated techniques such as Bayesian training in FortiMail. See the documentation of respective products for more information.

Dedicated Service Team – To complete the Fortinet Antispam solution and provide our customers with “Best in Class” Antispam solutions, our dedicated service team of engineers and analysts is committed to respond to and resolve any False Positive report or other spam identification related issues within 24 hours. This includes monitoring and analysis of the latest spam techniques, continuously updating the FortiGuard Antispam databases, as well as development of new spam filters.

FortiIP – Sender IP reputation database
Most spam is presently sent from mis-configured or malware-infected hosts. The FortiGuard Antispam Service maintains a global IP reputation database where the reputation of each IP is built and maintained based on multiple properties relating to an IP address gathered from various sources. The properties of an IP address include its Who-is information, geographical location, its service provider, whether it is an open relay or hijacked host, etc. One of the key properties used to maintain the reputation is the email volume from this sender, as gathered from our FortiGuard Antispam Service network. By comparing a sender's recent email volume with its historical pattern, FortiGuard Antispam Service updates each IP's reputation in real-time, resulting in a highly effective sender IP address filter.

FortiSig is a spam signature database containing three types of signatures: FortiSig1 - FortiSig3:

FortiSig1 – Spamvertised URLs
About 90% of spam has one or more URLs in the message body. These URLs link one to spammers' website promoting their products and services. In the case of phishing spam, the embedded URLs direct the recipient to a fake institution's website in order to collect private information. FortiGuard Antispam Service collects spam samples through our FortiGuard Antispam Service network composed of spam traps, along with spam sample submissions from our customers and partners. The URLs are then extracted from the spam samples and sent through a rigorous testing process before being added the FortiSig database. The URLs are then subject to the continuous aging process where obsolete entries are removed.

FortiSig2 – Spamvertised Email Addresses
Similar to the spamvertised URLs, lots of spam have an email address in the message body that

prompts one to contact the spammers. By extracting these email addresses from the spam sample, these spamvertised email addresses provide another powerful global filter to identify and filter spam.

FortiSig3 – Spam Object Checksums
Introduced in FortiOS 3.0, FortiSig3 was added to counterattack hard-to-detect spam messages that do not contain elements tracked by FortiSig1 or FortiSig2 databases. Using a proprietary algorithm, objects in spam are identified and a checksum is calculated for each object. The object can be part of the message body or an attachment. The checksum is then added into the FortiSig3 database, providing another highly effective global filter with virtually no False Positives.

For the latest technology overview, please see
http://www.fortinet.com/FortiGuardCenter/antispam/antispam_info.html#spamtech.

Q: What is the Fortinet definition of "spam"?
A: Most recipients easily agree on certain email messages as being spam, such as the never-ending mail relating to erectile dysfunction and Nigerian scams. In contrast, some recipients may consider all advertisements and newsletters as spam while other recipients may consider newsletters as legitimate email.

Fortinet uses the industry standard definition of spam as being "Unsolicited Bulk Email (UBE)". Unsolicited means that the recipient has not granted verifiable permission for the email to be sent and the sender has no discernible relationship with any or all of the recipients. Bulk means the email is sent as part of a larger collection of messages, all having relatively identical content.

An email is considered spam if both Unsolicited and Bulk. Unsolicited email can be non-spam email, such as first contact inquiries, job inquiries and sales inquiries. Bulk email can also be non-spam email, such as subscribed newsletters, customer communications and discussion lists. The message content is generally irrelevant in determining whether an email is spam, though most are commercial in nature. Some spam fraudulently promotes penny stocks in the classic pump-and-dump scheme. Other spam promotes religious beliefs, further illustrating that spam identification by content is not generally reliable.

An email message is spam if the recipient's personal identity and context are irrelevant because the message is equally applicable to many other potential recipients, and the recipient has not verifiably granted deliberate, explicit, and revocable permission for it to be sent.

Q: How is the performance of an antispam service measured?
A: There are three major criteria in measuring the performance of an antispam service:

Catch Rate -- The percentage of spam identified out of all email in a collection. Given 1,000 messages, the Catch Rate is 90% if there are 700 spam messages and 300 clean messages with 630 spam messages being caught out of the 700 spam messages.

False Positive Rate – The percentage of clean email identified as spam out of all clean messages. Given 1,000 messages, the False Positive Rate is 0.3% if there are 700 spam and 300 legitimate messages with 1 clean message being inaccurately identified as spam out of the 300 legitimate messages.

Some vendors in the industry use the percentage of clean email identified as spam out of all email as their False Positive Rate, which can be misleading. This definition does not consider the number of clean messages in a collection of email. The False Positive Rate by this definition is 0.1% for the example above. The False Positive Rate by this definition will be 0.1% even if there are 999 spam messages in a collection of 1000 emails. The 1 clean message can be identified as spam and yield the same result.

Maintenance overhead – The amount of time required to achieve the above Catch Rate and False Positive Rate on the part of end users and/or network administrators.

The perfect antispam solution would have 100% Catch Rate, 0% False Positive Rate, and zero maintenance overhead.

Evaluating the effectiveness of an antispam solution is not simple, even with the well-defined metrics including Catch Rates and False Positive Rates. There is still a subjective element in determining whether a message is in fact spam, and the results may vary depending on the email collection used in a test.

Q: What is the performance of the FortiGuard Antispam solution?

A: We put FortiGate to the test, side by side with two other antispam vendor products: BrightMail and Barracuda. To minimize the variance that may result from the email collection used, we used real email messages as the test sample from a number of real-life email accounts over an extended period of time.

Each week, 4,000 email messages are randomly picked from tens of thousands of emails from these accounts. The 4,000 email messages are first manually reviewed by trained spam analysts. Each message is marked as spam or clean based on their training. To minimize the subjective element, messages are excluded from the test sample if there is no sufficient information to determine it is either spam or clean or if its legitimacy is debatable, including:

- Email messages that are detected as a virus will not be counted as test samples
- Email messages with empty body will not be counted in the test sample
- Newsletters, and any messages that are hard to classify as "spam" or "clean", will not be counted as test samples, except if they are big companies or companies with good reputations, in which case they will be treated as "clean"

The remaining messages are then transmitted over a cross-scanning pipeline of Antispam appliances/servers. Each appliance/server is configured to tag the subject line if the message is detected as spam. The products used in the test are:

- **FortiGate 400 with FortiOS 3.0** – as a transparent firewall, FortiGuard Antispam Service enabled only without any customer filters configured on the unit.
- **FortiGate 400 with FortiOS 2.8** – as a transparent firewall, FortiGuard Antispam Service enabled only without any customer filters configured on the unit.
- **FortiMail 400 version 2.80** – configured as an email server with FortiGuard Antispam Service enabled, heuristic rules and Bayesian training enabled.
- **BrightMail 6.0** – configured as a gateway, with reputation and all services enabled with live update, all filters enabled with default scoring.
- **Barracuda Spam Firewall 200** – with all services enabled including Bayesian training and Intent Analysis.

Once the messages come out of the pipeline, the numbers of spam and clean messages caught by each appliance/server are counted to calculate the Catch Rate and False Positive Rate for each.

Below are the accumulated results over the a 13-week period ending Nov 1, 2006:

Product	Total Email	Spam Msgs	Total Clean	Spam Identified	False Positives	Catch Rate	False Positive Rate	False Positive Rate (2)
FortiOS 3.0	49,127	35,476	13,651	32,799	60	92.5%	0.44%	0.12%
FortiOS 2.8	49,127	35,476	13,651	31,740	49	89.5%	0.36%	0.10%
FortiMail 2.8	49,127	35,476	13,651	33,769	71	95.2%	0.52%	0.14%
BrightMail	49,127	35,476	13,651	33,700	56	95.0%	0.41%	0.11%
Barracuda	49,127	35,476	13,651	33,162	95	93.5%	0.70%	0.19%

Table 1 - Catch Rate and False Positive Rate of Antispam Products

The percentage of spam is 72% (35,476 / 49,127) of all messages, just about average in terms of spam volume worldwide. As a reference the "False Positive Rate (2)" in the table above shows the percentage of clean messages caught as spam of all messages, which some vendors use to claim lower False Positive Rates.

FortiMail 2.8 led in Catch Rate while it ranked fourth place in False Positives. Compared to BrightMail, it had a slightly higher Catch Rate, and higher False Positive Rate. Barracuda offers the average Catch Rate with a significantly higher False Positive Rate. Both versions of FortiOS offer reasonable Catch Rates at around 90% with a low False Positive Rate. As expected, FortiOS 3.0 delivers slightly higher Catch Rates because of its additional technique, FortiSig3 (Spam Object Checksums).

Note: FortiOS/FortiGate is a gateway-based solution. It relies exclusively on global filters offered by the FortiGuard Antispam Service with zero maintenance overhead. FortiMail, BrightMail and Barracuda are server-based solutions. They use many more techniques that are resource intensive and not feasible in a gateway product like the FortiGate. Considering these facts, FortiGuard Antispam Service delivered by FortiGate/FortiOS offers a highly effective, compelling antispam solution.

Q: How do I report an uncaught spam email?

A: If you identify uncaught spam, please forward them as "attachments" to submitspam@fortinet.com. It is very important that uncaught spam is forwarded as an attachment. Different email clients require different processes.

For details, see:
http://www.fortinet.com/FortiGuardCenter/antispam/antispam_info.html#submitspam.

Any other messages forwarded or sent to this address are ignored. False Positive or other antispam issues should be submitted to removespam@fortinet.com or contact_antispam@fortinet.com.

Q: What happens to the uncaught spam that is submitted to Fortinet?

A: All spam submitted to submitspam@fortinet.com is subjected to an automated process of analysis and signature mining, and added to the Fortinet spam archive. Generally we do not respond to these spam submissions due to the large volume. There is no guarantee that a spam submitted to us will be caught after we process it. There can be many reasons why this "same" spam continues to go into end user's inbox undetected. These are two common problems:

- The spam was not submitted as an attachment, or missing critical parts resulting in no signature being generated from the sample.
- The perceived "same" message is actually a different spam message from one previously submitted. This typically happens in the case of image spam where each image is manipulated with noise.

Q: How do I report a False Positive?

A: All False Positives (clean email falsely detected as spam) should be submitted to removespam@fortinet.com.

For full instructions, see:
http://www.fortinet.com/FortiGuardCenter/antispam/antispam_info.html#submitfp.

Q: What happens to the False Positive sample submitted?

A: All False Positives are subject to a manual analysis and processing by our spam analyst, generally within 24 hours. If a False Positive signature is found in the signature database, it will be removed so that the message will no longer be detected as spam. A notification email will be automatically sent to the submitter at the email address submitted.

Q: How do I contact the FortiGuard Antispam team?

A: For antispam issues to the FortiGuard Antispam subscription service, you can either email to contact_antispam@fortinet.com, or submit your requests on the Web: http://www.fortinet.com/FortiGuardCenter/contactus/contactus.html.

For product-specific issues with FortiOS, FortiClient and FortiMail, including antispam issues that are product specific, please contact the Technical Support.

See https://support.fortinet.com/Login/UserLogin.aspx.

FAQ121-1106-R2