



FortiGuard-Antispam Service FAQ

Product Marketing Product FAQ

Version 1.00
7 February 2005

© Copyright 2005 Fortinet Inc. All rights reserved.

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.

Trademarks

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

FortiGuard-Antispam Service FAQ

Fortinet's new FortiGuard-Antispam Service is designed to help reduce the amount of spam email that is targeting companies of all sizes. The FortiGuard-Antispam Service is a fully managed service provided by Fortinet and provides a "dual pass" scanning technology to increase spam detection rates standard Real-Time Blackhole List (RBL) services that have been steadily losing ground against the latest spam techniques.

Q: What is the new FortiGuard-Antispam Service and why is it important?

A: FortiGuard-Antispam is a new fee based antispam service that extends the capabilities of today's RBL services. An RBL service only looks at the sending SMTP server's IP Address and compares it with a list of well-known spammer IP Addresses. Many free or low cost RBL services often contain outdated information which leads to false positives, false negatives and low spam detection rates. FortiGuard-Antispam utilizes Fortinet's own spam probes that are located around the world to attract spam email. This information is continuously updated into FortiGuard-Antispam to ensure accurate spammer lists and improves spam detection rates.

In addition to spammer IP Address comparisons, FortiGuard-Antispam extends its spam detection functionality with Universal Resource Identifier (URI) Scanning. URI Scanning looks deep into each email message to scan for well-known spam content such as spam URL links. As spammers get more creative and use infected PC's to deliver spam, RBL services using only IP Address lookups will become less effective. To improve performance over standard RBL services, FortiGuard-Antispam offers caching to accelerate database lookups. FortiGuard-Antispam can be enabled on FortiGate or FortiMail platforms.

Q: What is required to run the FortiGuard-Antispam Service?

A: FortiGuard-Antispam is a fully managed service that is maintained by Fortinet's Response Team around the world. There are two components that make up the FortiGuard-Antispam service – an agent that runs on the FortiGate or FortiMail platforms and the managed AntiSpam Content Database that resides on the FortiGuard-Antispam servers located throughout the Internet. The agent running on the FortiGate or FortiMail platforms communicate with the FortiGuard-Antispam servers and forwards IP Address and URI information to the FortiGuard-Antispam servers for spam checking.

The FortiGuard-Antispam servers contain the latest information on known spammers and URI spam content. The FortiGuard-Antispam server rates the information sent by the FortiGuard-Antispam agents and returns the results to the FortiGate or FortiMail units. Aside from enabling the service on the FortiGate or FortiMail device, there are no other resources required by the customer. FortiGuard-Antispam can help eliminate the daily maintenance routines associated with maintaining black/white lists, reviewing and fixing RBL inaccuracies and so forth - freeing up valuable time for email administrators.

Q: Which versions of FortiOS and FortiMail will support the FortiGuard-Antispam Service?

A: FortiGuard-Antispam will be supported on all current FortiGate platforms and will be enabled with the FortiOS MR releases. MR6 supports the IP Address Lookup technology and FortiOS MR8 will support the URI Scanning technology. On FortiMail platforms, FortiGuard-Antispam will be supported with the v1.2 release in early Q2 2005.

Q: How can customers enable the FortiGuard-Antispam Service?

A: FortiGuard-Antispam can be implemented in one of two ways.

1. It can be enabled as a service on all current models of the FortiGate Antivirus Firewall products running FortiOS MR6 or later.
2. It can be implemented as a service on Fortinet's dedicated FortiMail Secure Messaging platforms running FortiMail v1.2 or later (available Q2 2005).

For FortiGate customers, enabling FortiGuard-Antispam at the perimeter where the FortiGate unit is installed can dramatically help reduce the amount of "obvious spam". This helps reduce the amount of

spam messages entering through the firewall, flooding email servers or antispam gateways, and can help push off costly upgrades to email servers that are running out of resources processing spam messages.

FortiMail customers who would like to centralize all antispam functions into one platform can enable the FortiGuard-Antispam service to create a layered antispam solution on a single dedicated antispam device. For customers looking for better antispam performance and additional antispam technology to supplement existing antispam solutions, FortiGuard-Antispam provides a cost effective solution with guaranteed improvements.

Q: What is the best way to take advantage of the FortiGuard-Antispam Service?

A: Fortinet has made it very simple for customers to enable the FortiGuard-Antispam Service. A free 30 day trial is available on all FortiGate AntiVirus Firewall platforms running FortiOS v2.8 MR6 and later. Customers can turn on the FortiGuard-Antispam service and customize their AntiSpam policies to either Tag or Drop the spam messages identified by FortiGuard-Antispam. To keep the service operational after the 30 day trial, simply purchase the FortiGuard-Antispam service for the FortiGate model and register the FortiGuard-Antispam product to enable the annual license.

Q: What if customers already have other antispam solutions enabled in their email architecture. How can FortiGuard-Antispam help these customers?

A: FortiGuard-Antispam was designed to be extremely flexible with respect to how it can be integrated with existing antispam solutions. Being a fully managed service, FortiGuard-Antispam can be enabled to augment any other existing antispam technology and help reduce the amount of spam at the perimeter. Using FortiGate's Transparent Mode capabilities, customers can quickly enable FortiGuard-Antispam on their FortiGate Antivirus Firewalls to scan all SMTP mail messages coming into their email servers and add an additional layer of spam checking without making any other change to their infrastructure.

Strategically, adding FortiGuard-Antispam can create a diversified antispam solution and increase performance of existing email servers. With the most obvious spam messages blocked at the perimeter using FortiGuard-Antispam, network traffic to and from the email server(s) is reduced and less CPU, disk, and memory resources are spent processing spam messages on the email servers which results in improved email system performance.

FortiGuard-Antispam adds an extra antispam check to any existing antispam solution, whether it's Fortinet's FortiMail technology or any other type of antispam technology. By having a dual pass capability, FortiGuard-Antispam offers better spam detection rates over static content filtering and RBL services relying solely on source IP Addresses of SMTP servers.

Q: How difficult is it to enable the FortiGuard-Antispam Service?

A: Fortinet has designed FortiGuard-Antispam's installation routine to be fast and easy with literally no maintenance overhead. To enable the service, customers simply perform the following procedure:

- Enable the FortiGuard-Antispam service from the Spam Filter Web Menu by checking the two FortiGuard-Antispam option check boxes (Enable and Caching)
- Enable FortiGuard-Antispam Checking on the firewall protection profile associated with the interface that mail is being received on
- Select the Spam Action to either Discard or Tag spam messages

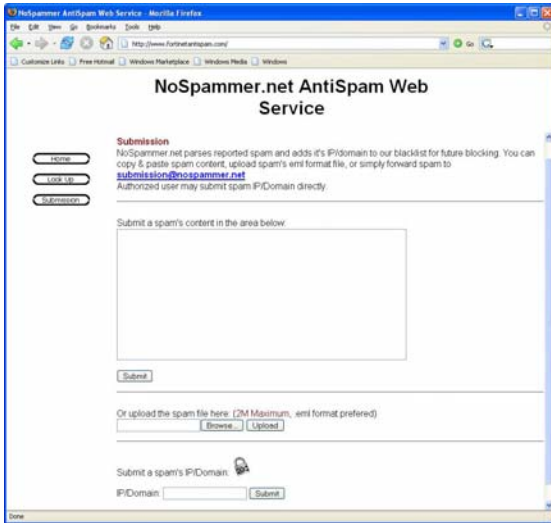
Turning FortiGuard-Antispam on is this simple. Less than a few minutes to fully enable and configure and with just a few mouse clicks.

Q: How can customers evaluate the effectiveness of FortiGuard-Antispam?

A: With the FortiOS v2.8 MR8 release, customers can use statistic commands located in the CLI interface to retrieve performance and historical statistics. FortiGuard-Antispam statistics show customers just how much spam was stopped or tagged at the perimeter and how many spam messages were good email messages verses obvious spam messages.

Q: How can customers use FortiGuard-Antispam to see if a specific domain is a known spammer domain or remove domains from the FortiGuard-Antispam Content Database?

A: As part of the FortiGuard-Antispam service, a Web site is provided for customers to search for known spam sites, report spam domains and abusers, and ask to be removed from the FortiGuard-Antispam List. To protect against spammers asking to be removed from the list, the removal requests will be reviewed by Fortinet engineers on a case-by-case bases.



Q: What is the licensing scheme for the FortiGuard-Antispam Service?

A: Like all Fortinet products, FortiGuard-Antispam is licensed on a per unit basis. There are no per user licenses like other popular email protection solutions and this can significantly reduce the total cost of the entire antispam solution - helping lower Total Cost of Ownership (TCO) and provide rapid Return-on-Investment (ROI).

A free 30 day trial makes it easy for customers to evaluate the FortiGuard-Antispam service on their existing FortiGate and FortiMail units. By purchasing and registering an annual or multi-year subscription, the service is extended past the 30 day free trial period. For FortiGate customers, this service is an optional component with a nominal fee. For FortiMail customers, FortiGuard-Antispam is included in the annual support cost beginning with FortiMail v1.2.

Please contact Fortinet Sales for pricing information.