

# Fortinet, Inc.

## FortiMail-4000A™

### Anti-spam Effectiveness and Feature Comparison vs. IronPort Systems C350 E-mail Security Appliance



## Test Summary

**Premise:** E-mail security appliances designed to thwart phishing attacks, viruses and spam must be able to deliver exceptionally high rates of spam blockage combined with low levels of “false positives” and “false negatives” to be effective. Those E-mail security products should have a robust set of features that make them easy to deploy, configure and offer a simple licensing model for enterprises and service providers.

Fortinet, Inc. commissioned The Tolly Group to measure the effectiveness of the company’s FortiMail-4000A™ multi-layered E-mail security appliance at blocking spam and virus messages.

Tolly Group engineers tested the performance of the FortiMail-4000A against an IronPort Systems C350 E-mail Security Appliance. In accordance with The Tolly Group’s Fair Testing Charter, IronPort was invited to review the test methodology, offer suggestions for optimal configuration of its product and comment on its results.

Engineers measured the percentage of spam blocked, the number of “false positives,” “false negatives” and virus messages detected per product. Engineers also validated a number of E-mail security features and deployment flexibility.

Tests were conducted in November 2007.

### Test Highlights

- ▶ Blocks 99.91% of more than 28,000 inbound messages containing spam
- ▶ Demonstrates flexible deployment of transparent, server, and gateway modes
- ▶ Offers in-house developed anti-virus and anti-spam security updates with no per-user licensing

### Features Verified on FortiMail-4000A and IronPort C350

Feature/Function	FortiMail-4000A	IronPort C350
	Supported / Not Supported	Supported / Not Supported
No per-user anti-spam license fee		
No third-party anti-virus licensing		
Graylist anti-spam filtering		
Transparent mode deployment		
Server mode deployment		
Gateway mode deployment		
Per-mailbox policy		
Configurable SMTP policy		

Source: The Tolly Group, November 2007

Figure 1

## Executive Summary

Tests show that the Fortinet FortiMail-4000A is as accurate at blocking spam as IronPort Systems C350 E-mail Security Appliance and is equally adept at combatting “false negatives” and “false positives.”

Service providers and enterprise network architects can benefit from adoption and deployment of integrated tools that offer protection from E-mail abuse. Fortinet’s FortiMail-4000A integrates support for anti-spam, anti-virus, malware prevention and E-mail policy enforcement into a single product.

This test focuses on FortiMail-4000A’s anti-spam/anti-virus effectiveness, particularly when compared to the IronPort C350 Mail Security Appliance.

FortiMail-4000A accurately detected 28,726 spam messages and 4 virus messages, while the IronPort C350 detected 26,544 spam and zero virus messages.

### FEATURE VERIFICATION

The Tolly Group examined a variety of features and functions available on both the FortiMail-4000A and the IronPort C350 appliance. (See Figure 1.)

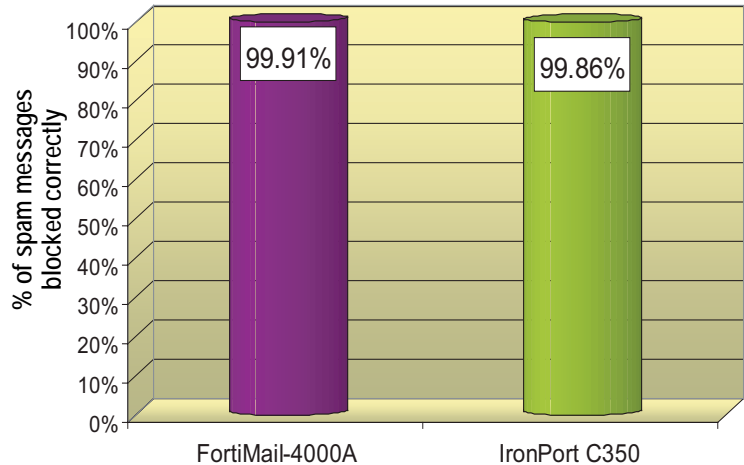
### LICENSING MODELS

Engineers examined the license fee associated with both products. With the FortiMail-4000A, engineers verified that users pay a single license fee for anti-spam and anti-virus, which covers all users in a network. By contrast, IronPort charges-users a licensing fee for anti-spam and anti-virus on a per-mailbox basis.

### ANTI-VIRUS LICENSING

Engineers examined the licensing

**Spam Detection Percentage of FortiMail-4000A vs. IronPort C350 Appliance**  
Based on 28,751 and 26,581 Live Corporate Spam Messages Received\*



\* NOTE: Both devices were tested in a 24-hour period from 6:00 p.m. to 6:00 p.m. FortiMail was tested from October 31st through November 1st. IronPort was tested from November 5th through November 6th.

Source: The Tolly Group, November 2007

Figure 2

**Spam Processing Analysis of Fortinet FortiMail-4000A versus IronPort C350**

Category	FortiMail-4000A	IronPort C350
<b>Inbound Messages Tested*</b>	29,187	27,280
Total Spam	28,751	26,581
Spam Blocked Correctly	28,726	26,544
<b>Spam Detection Percentage</b>	99.91%	99.86%
False Negatives (Spam missed)	31 out of 28,751	37 out of 26,581
False Positives (Classified as SPAM but not actually spam)	6 out of 1,984 quarantined messages	0 out of 261 quarantined messages
<b>Legitimate Messages</b>	426 out of 29,187	699 out of 27,280
<b>Virus Messages Detected</b>	4 out of 29,187	0 out of 27,280

\* NOTE: For the test, E-mail messages were collected for a 24-hour period for each platform. The FortiMail-4000A was tested from October 31st through November 1st (from 6:00 p.m. to 6:00 p.m.). For the IronPort C350, testing occurred from November 5th through November 6th (from 6:00 p.m. to 6:00 p.m.). The traffic included real-world Tolly Group corporate E-mail messages.

Source: The Tolly Group, November 2007

Figure 3

options available for each product's anti-virus capabilities.

For the FortiMail-4000A, engineers verified that the product uses its own in-house anti-virus engine. By contrast, the IronPort C350 uses either a Sophos anti-virus engine or a McAfee anti-virus engine. That means users must purchase a license for each device to support these third-party anti-virus products.

#### GRAYLIST FILTERING

Engineers verified that the FortiMail-4000A supports Graylist anti-spam filtering which temporarily rejects the suspected message until the originating server resends the message to the destination. In the case of the IronPort C350, the system did not support this feature at the time of testing.

In the case of the IronPort C350, the system did not support Graylisting as used by many standard anti-spam systems. Nevertheless, the IronPort system does include a policy feature that slows down the rate of incoming suspected messages to the network instead of temporarily rejecting them.

#### TRANSPARENT MODE DEPLOYMENT

The Tolly Group examined that inline mode, or transparent mode, is supported by the FortiMail-4000A but not by the C350 appliance. Transparent mode is used to perform spam filtering and anti-virus scanning without modifying the MX records and network topology in the existing infrastructure.

#### SERVER MODE DEPLOYMENT

The Tolly Group examined that server mode deployment is supported by the FortiMail-4000A but not by the C350 appliance. Server mode enables the FortiMail-4000A to act as an E-mail server in the network to provide anti-spam and anti-virus filtering, along with E-mail services.

#### GATEWAY MODE DEPLOYMENT

The Tolly Group's hands-on evaluation shows that both the FortiMail-4000A and IronPort C350 support gateway mode deployment. This enables either device to act as a gateway in front of backend E-mail servers to filter incoming messages for viruses and spam.

#### POLICY MANAGEMENT

The Tolly Group also verified that both the FortiMail-4000A and the IronPort C350 provide policy control on a per-mailbox basis, as well as on a domain basis.

#### SMTP POLICY CONFIGURATION

The FortiMail-4000A supports configurable SMTP filters based upon policy attributes. This enables administrators to set incoming session rates and administer policy filtering. The IronPort C350 also offers SMTP policy configuration.

#### SPAM BLOCKAGE

Engineers measured the ability of FortiMail-4000A and the competitive product tested to detect incoming spam with accuracy and to correctly block spam messages. (See Figure 2.)

Tests show that out of 28,751 spam-based and virus-laden messages received, the FortiMail-4000A correctly blocked 28,726 (99.91%) of the spam messages. Both devices were tested with live E-mail messages to ensure that reputation and session-based blocking functioned correctly.

The IronPort C350 handled 26,581 total inbound spam and virus messages, and detected 26,544 of those as spam. It correctly blocked 99.86% of the spam messages. (See Figure 3.)

This demonstrates that the FortiMail-4000A is as accurate and effective at blocking spam as the IronPort C350.

Fortinet,  
Inc.



FortiMail-  
4000A

E-mail Anti-spam  
Effectiveness

#### Product Specifications

*Vendor-supplied information not necessarily verified by The Tolly Group*

Fortinet, Inc.  
FortiMail-4000A

#### Hardware

- 12 hot-swappable disk drives
- Hardware RAID support (RAID 0, 1, 5, 10, 50)
- Redundant hot-swappable power supplies
- Four 10/100/1000 Base-T interfaces
- Up to 3,000 E-mail domains
- Recommended for up to 35,000 users

#### Features

- Multi-layered E-mail security: anti-spam, anti-virus, anti-phishing, anti-malware
- Inbound/outbound filtering
- Anti-spam filters include:
  - Global sender IP reputation
  - Local sender reputation
  - IP-based policies
  - SMTP protocol and session filters
  - Image analysis
  - Bayesian filtering
  - PDF file scanning
  - Dynamic heuristic rules filters
  - Deep header scanning
- Complete anti-virus scanning
- Real-time anti-virus updates
- Optimized for up to 400,000 messages per hour
- Multi-tiered admin domains

#### For more information contact:

Fortinet, Inc.  
1090 Kifer Road  
Sunnyvale, CA 94086  
Phone: (408) 235-7700  
Fax: (408) 235-7737  
<http://www.fortinet.com>

### “FALSE NEGATIVES”

When an anti-spam product misses incoming spam E-mails, treating them as “legitimate,” the product generates “false negatives.”

With 28,751 spam messages sent,

engineers found 31 false negatives on the FortiMail-4000A, generating a false negative rate of 0.11%. In the case of the IronPort C350, with 26,581 of total spam messages, engineers located 37 false negatives that yielded a false negative rate of 0.14%.

### “FALSE POSITIVES”

When an anti-spam product incorrectly identifies legitimate incoming E-mails as “spam” and then blocks those messages, the product generates “false positives.”

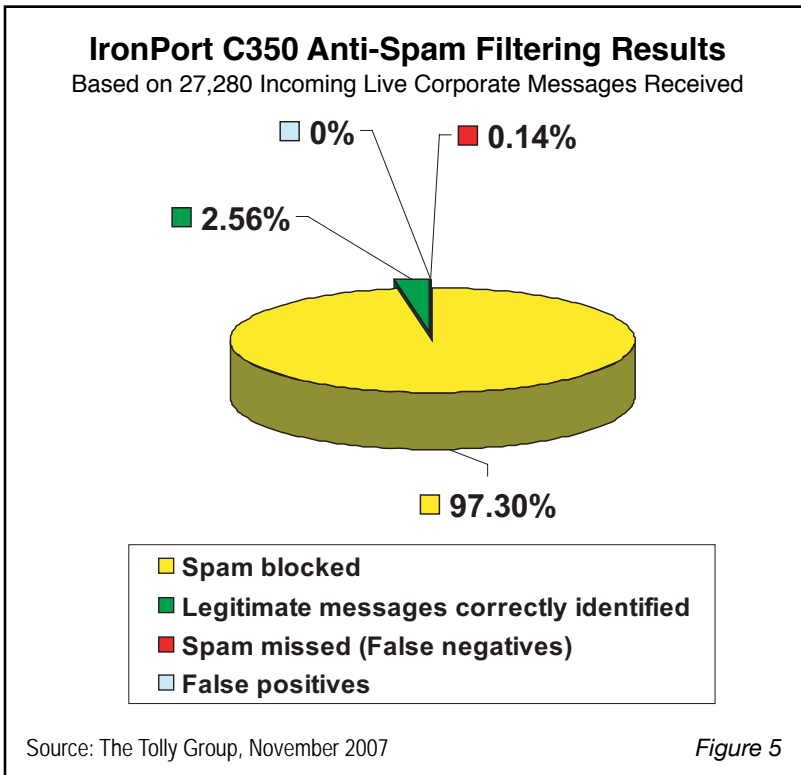
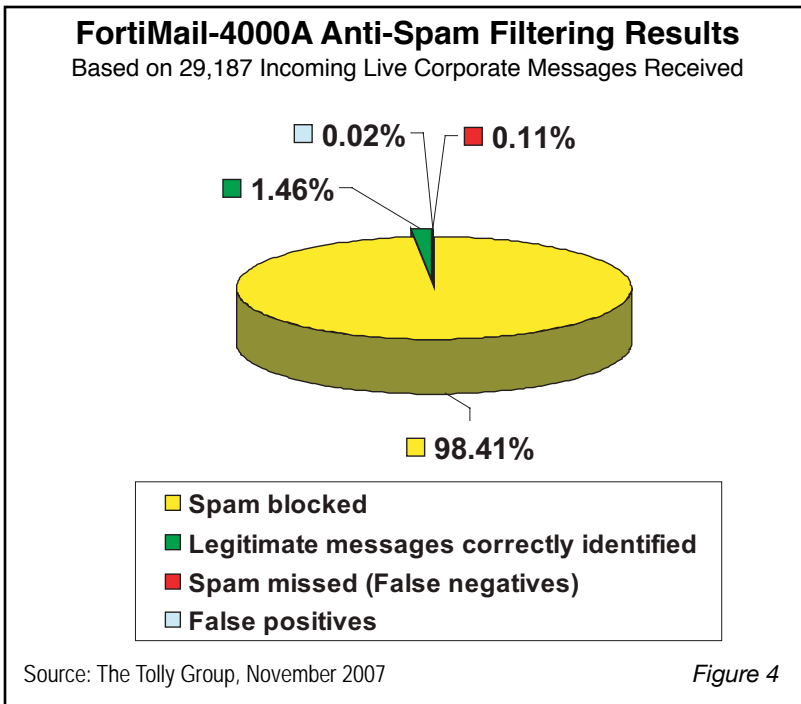
For the FortiMail-4000A and IronPort C350, engineers identified six and zero “false positives,” out of 1,984 quarantined messages and 261 quarantined messages, respectively for each platform. (See Figures 4 and 5.)

Both the FortiMail-4000A and the IronPort C350 utilize their own databases to determine if the sending IP address is reputable. Based on that information, the products can block the vast majority of spam messages at the connection level without incurring the overhead of actually receiving the message and passing it on to the next level of spam detection.

Given that these reputation databases are being updated constantly (according to the vendors), it is unlikely that “false positives” are being generated based on a company being black-listed in error. For the purpose of this test, all spam blocked at the connection level was considered as accurately blocked spam. The decision was made because it is impractical to conduct reverse DNS lookup and analysis on some 50,000+ spam messages blocked at the connection level.

### METHODOLOGY & CONFIGURATION

Tolly Group engineers tested Fortinet’s FortiMail-4000A E-mail security platform version (3.00 Build 143, 071019) equipped with four 10/100/1000 Ethernet ports and 3 TB (Terabytes) of storage capacity, against an IronPort C350 E-mail security appliance version (5.5.0-430) equipped with two Broadcom Gigabit Base-T ports and one Intel 10/100 Base-T Ethernet port, one Intel Xeon processor and 35 GB (Gigabytes) of storage



capacity, plus 45 GB for queue capacity and reporting data, respectively.

Tolly Group engineers tested both platforms with a live E-mail stream of messages in order to test each device capabilities and behavior when they are deployed in a live network. This way, all inbound messages were kept intact without modifying sender information and/or SMTP session state.

**TEST BED CONFIGURATION**

Tolly Group engineers deployed the FortiMail-4000A and the IronPort C350 E-mail security platforms in The Tolly Group’s corporate network each as the main E-mail security gateway for anti-spam and anti-virus filtering. Engineers configured both platforms in “gateway” mode by connecting one of the ports to the “public network” and the second port to the “private network.” (See Figure 6.)

Both platforms used out-of-the-box configurations for anti-spam filtering although engineers made a small change to the IronPort C350 by enabling the “Suspect SPAM” feature. This tags a suspect message as “Possible SPAM” and routes it to the Quarantine folder for manual assessment by an admin. Engineers enabled the Quarantine feature of both products tested to quarantine spam.

Tolly Group engineers also used the LDAP query feature available in each device under test to run recipient verification on The Tolly Group’s Active Directory server. Engineers made sure that Internet access was made available to each platform to download any newly available anti-spam and anti-virus definitions, or new firmware updates.

Testing was conducted in succession, meaning that engineers first deployed the FortiMail-4000A and then switched the platform to the IronPort C350. Each platform processed all inbound messages for a 24-hour period. Any

inbound messages that were identified as spam were tagged as “SPAM” and saved into a Quarantine directory for engineers to verify. All other E-mail messages were delivered to The Tolly Group’s corporate mail server.

**ANTI-SPAM BLOCKING PROCEDURE**

Once messages were scanned by each solution, some of the messages were tagged as “SPAM” and filtered out in a quarantine directory to allow engineers to verify manually whether the message blocked was actually spam or not.

During the manual classification, engineers determined whether messages were “unsolicited” or not by checking the following criteria: porn, sex, prescription drugs (i.e. Viagra), gibberish language, “no page found” links, no content, etc.

Engineers considered a message to be a “false positive” whenever a legitimate message was found in the quarantine directory. In the case for “false negatives,” engineers manually checked each Tolly Group employee’s mailbox for unsolicited messages found in

the directory that was not classified as spam.

In the case for “false negatives,” engineers manually checked each employee’s mailbox in Exchange Server for any possible spam/virus messages. Given that the entire organization was involved in this process directly or indirectly, there was an inevitable possibility that engineers missed some spam messages. For instance, an employee could accidentally delete the spam messages before the engineers checked out the mailbox.

Even if there was error in the “false negative” result, the error rate cannot possibly exceed 50%. This results in increasing about 15 more “false negatives” as shown in Figure 2. The Tolly Group considers that this possible error ratio would not have any noticeable impact on our main findings.

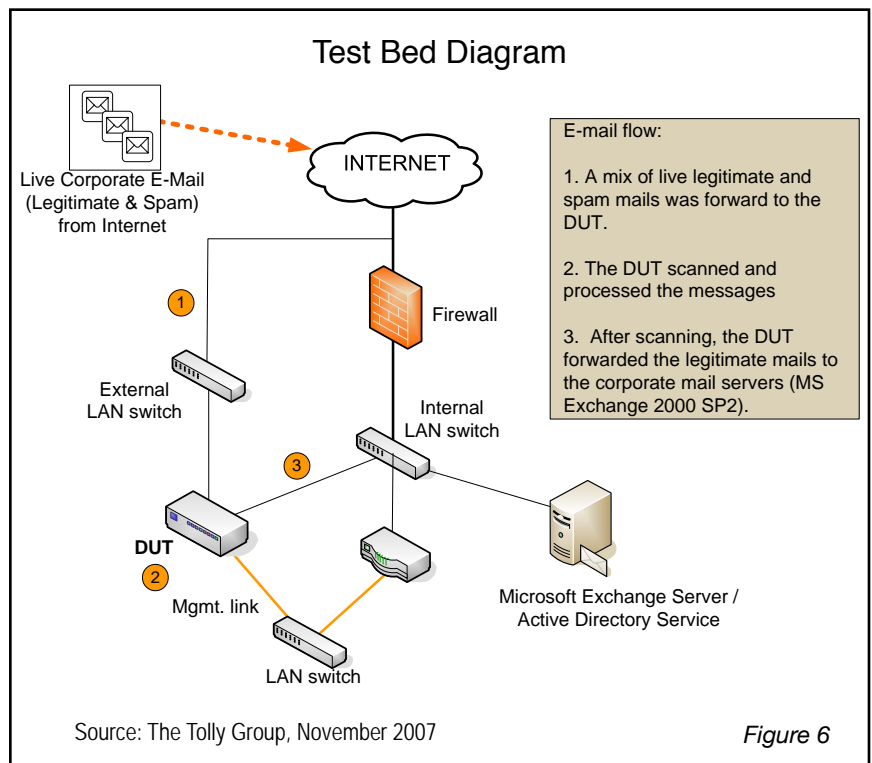


Figure 6

### Fair Testing Charter™ Interaction with Competitors

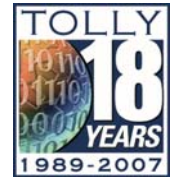


The Tolly Group contacted IronPort in October 2007 and invited the company to participate in the test. IronPort was invited to review the test plans, the product levels and configurations of the company's product and to review and comment on results specific to its C350 appliance. An IronPort representative provided insight into tuning the configuration and updating firmware of the C350 appliance.

IronPort reviewed the results of its IronPort C350. On Nov. 14th, IronPort confirmed the accuracy of the results.

For more information on this process, please see: <http://www.Tolly.com/FTC.aspx>.

The Tolly Group is a leading global provider of third-party validation services for vendors of IT products, components and services.



The company is based in Boca Raton, FL and can be reached by phone at (561) 391-5610, or via the Internet at <http://www.tolly.com>, [sales@tolly.com](mailto:sales@tolly.com)

Device Under Test Specifications				
Company	Product Name	Firmware Version	Anti-Spam Version	Anti-Virus Version
Fortinet, Inc.	FortiMail-4000A	3.00 Build 143, 071019	1.315	Fortinet Anti-Virus Engine (Ver. 2.91) / FortiGuard Anti-Virus Definition (Ver. 8.373)
IronPort Systems	IronPort C350	5.5.0-430	<ul style="list-style-type: none"> <li>- CASE Core Files Base Version 2.2.0-010</li> <li>- Structural Rules Ver. 2.2.0-010-20071105_072506</li> <li>- Content Rules (Ver. 20071106_225625)</li> <li>- Content Rules Update (Ver. 20071106_230204)</li> <li>- CASE Utilities Base Version 2.2.0-010</li> <li>- Web Reputation DB (Ver. 20071105_230000)</li> <li>- Web Reputation Rules (Ver. 20071105_230000-20071106_230000)</li> </ul>	Sophos Anti-Virus Engine 4.21 / Sophos IDE Rules (Ver. 2007110604)

## Terms of Usage

### USE THIS DOCUMENT ONLY IF YOU AGREE TO THE TERMS LISTED HEREIN.

*This document is provided, free-of-charge, to help you understand whether a given product, technology or service merits additional investigation for your particular needs. Any decision to purchase must be based on your own assessment of suitability.*

*This evaluation was focused on illustrating specific features and/or performance of the product(s) and was conducted under controlled, laboratory conditions and certain tests may have been tailored to reflect performance under ideal conditions; performance may vary under real-world conditions. Users should run tests based on their own real-world scenarios to validate performance for their own networks. Commercially reasonable efforts were made to ensure the accuracy of the data contained herein but errors and/or oversights can occur. In no event shall The Tolly Group be liable for damages of any kind including direct, indirect, special, incidental and consequential damages which may result from the use of information contained in this document*

*The test/audit documented herein may also rely on various test tools the accuracy of which is beyond our control. Furthermore, the document relies on certain representations by the sponsor that are beyond our control to verify. Among these is that the software/hardware tested is production or production track and is, or will be, available in equivalent or better form to commercial customers.*

*When foreign translations exist, the English document is considered authoritative. To assure accuracy, only use documents downloaded directly from The Tolly Group's Web site.*

*All trademarks are the property of their respective owners.*

207258-gnstufs1-cdb-29NOV07