

Lab Testing Summary Report

October 2009

Report 091030

Product Category:
Email and Web Security

Vendors Tested:
ProSecure
Barracuda Networks,
Cisco Systems

Products Tested:
ProSecure STM600
V2.0.023

Barracuda
Spam Firewall 300
v3.5.12.025
Web Filter 210
v4.2.0.009

Cisco Spam and Virus
Blocker
v6.6.1- 014



Key findings and conclusions:

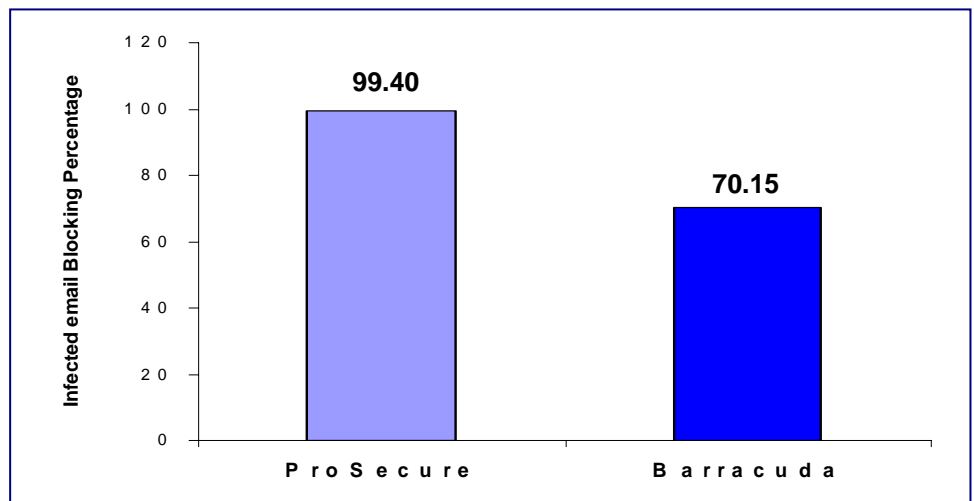
- ProSecure STM600 detected and cleaned 99.4% of infected email attachments
- 99.8% of spam email was blocked by ProSecure STM600
- During published vulnerability analysis 97.8% of HTTP exploits were blocked
- Website categorization and coverage capabilities were tested and are equal to other security appliances
- All-in-one architectural approach from ProSecure is easy to deploy and manage

ProSecure STM600, a web and email threat management appliance was evaluated as a part of Miercom's ongoing industry assessment of spam and web filtering products. We tested and compared the ProSecure, Cisco and Barracuda products which are designed for the medium business market space. The objective was to assess and determine the efficacy of spam filters based on content-analysis accuracy, email virus and malware detection, web filtering, real time web malware detection, and URL categorization and coverage capabilities. See [Figure 2](#) on page 3 for comparative results.

For this competitive analysis, Miercom reviewed ProSecure STM600, Cisco Spam and Virus Blocker and Barracuda Spam Firewall 300 and Web Filter 210. These vendors were selected because they offer Web and Spam security solutions for the mid-sized business market, and have a significant market share in security threat prevention systems.

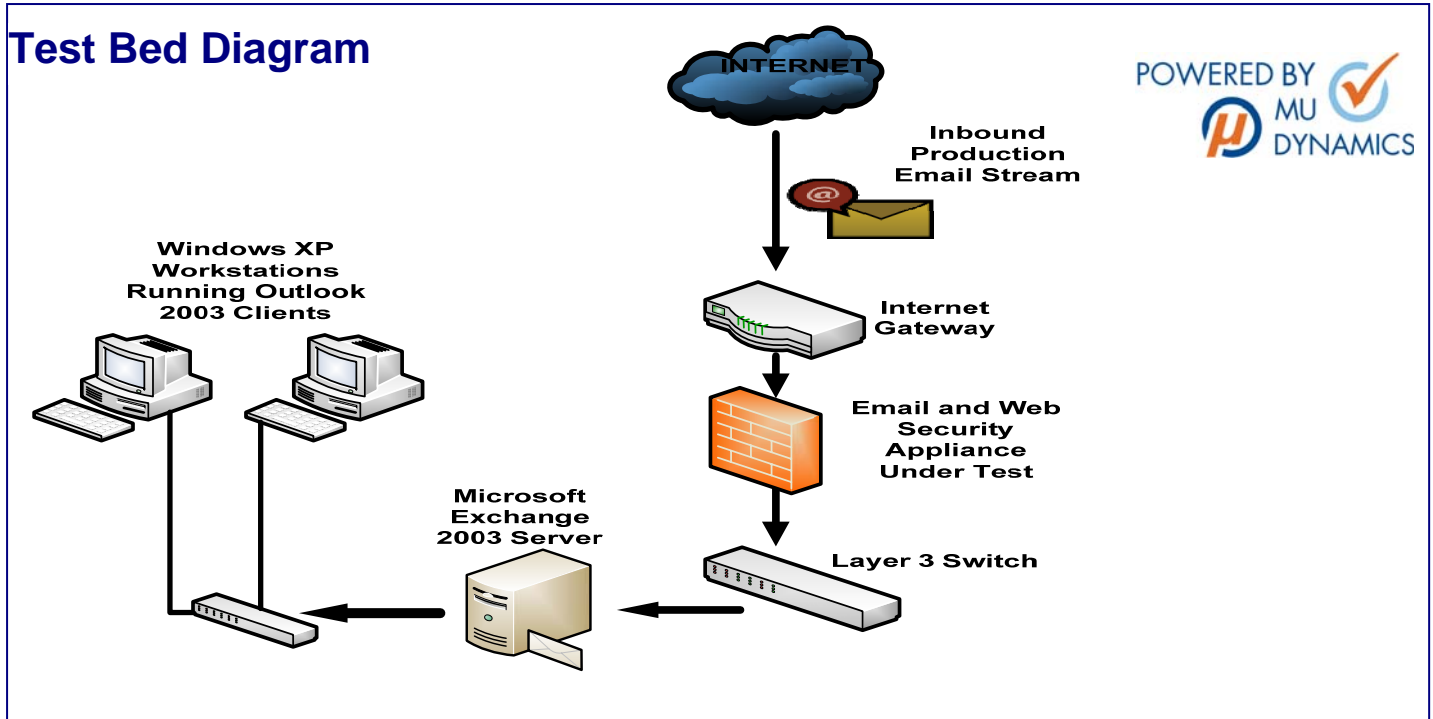
Most filtering products offer specialized filtering and are designed to filter either email or web traffic. For comprehensive Internet filtering, businesses would need to purchase multiple products. Cisco and Barracuda offer email and web security in two ([continued on page 3](#))

Figure 1: Infected email blocking results



ProSecure STM600 achieved the highest block rate of 99.40% for infected archived email attachments; Barracuda Spam Firewall 300 recorded 70.15%. Cisco Spam and Virus Blocker does not scan archived email attachments.

Test Bed Diagram



Devices Under Test

ProSecure STM600 running software v2.0.0-23, and OS v1.1.0.31; Cisco Spam & Virus Blocker with AsyncOS v 6.6.1-014, IronPort Anti-Spam v2.7.1-101, Sophos Anti-Virus and IDE rules; Barracuda Spam Firewall 300 v3.5.12.025, and Web Filter 210 v4.2.0.009. All virus definitions and signature sets were current as of the time of testing.

How We Did It

Each appliance was deployed in an out-of-the box configuration without tuning or training the spam filters. Use of third party real time blacklists was disabled and only vendor supplied reputation services were enabled. All platforms were subjected to a live production email stream. Each product received live unaltered message stream without modifications to the email headers. This deployment was essential to accurately evaluate the behavior and performance of the product when deployed in a real-world network.

Email malware detection capabilities used automated test scripts to send tens of thousands of emails with archived virus attachments less than 5 MB. Platforms were configured for a maximum of 10 MB attached files. Filtering by attached file type or extension was disabled so as to obtain accurate malware detection proficiency of each device. Each platform was subjected to 107,818 samples of malware and viruses including zero day and in the wild viruses.

Web filtering and malware detection capabilities were assessed by subjecting each platform to live Internet websites which host thousands of malware samples and include malicious content. Deep inspection and real time content analysis capabilities were tested by subjecting the products to an infected lab web server hosting 30,000 samples of malware content. The published vulnerability analysis conducted includes tens of thousands of unique exploits and was used to audit the signature set of the appliance. Website reputation checking was enabled for all platforms under test.

To assess the URL categorization and coverage capabilities of the platforms, a set of 65,535 URLs was compiled from various sources. Using automated scripts, Linux workstations accessed the sample set of URLs. All categories were enabled and set to block.

We used the Mu Dynamics (www.MuDynamics.com) Mu Test Suite to perform published vulnerability analysis. The Mu Test Suite PVA subscription distills information from the most recently discovered root-cause vulnerabilities into test cases that target the vulnerabilities that lie behind tens of thousands unique exploit vectors.

The tests in this report are intended to be reproducible for customers who wish to recreate them with the appropriate test and measurement equipment. Contact reviews@miercom.com for additional details on the configurations applied to the system under test and test tools used. Miercom recommends customers conduct their own needs analysis study and test specifically for the expected environment for product deployment before making a selection.

(continued from page 1) different product lines. ProSecure implements an all-in-one approach, offering both email and web security functionality in the STM600 appliance.

Spam Detection Efficacy

Previous methods of blocking spam, implementing rules based on keywords or blacklisting Domain names and IP addresses do not afford adequate protection now. Increased sophisticated tools used by spammers and the sheer volume of spam prevalent across the Internet requires the use of anti – spam engines that block or quarantine spam. We evaluated the effectiveness of spam detection with two criteria in mind – minimal administration and content analysis accuracy. The appliances were deployed in out-of-the box settings in order to assess the anti-spam efficacy without tuning or training any of the spam filters.

Each appliance was subjected to Miercom production email stream, receiving approximately 3,000 emails per day. This presented a demanding test bed with email traffic consisting of articles, industry newsletters, customer inquires and other email resembling spam, which were actually legitimate messages.

ProSecure STM600 delivered a high spam block rate of 99.83%, which is on par with the Cisco Spam & Virus Blocker with a 99.97% block rate and Barracuda which delivered 99.14% block rate. See Figure 3 for details.

Spam detection efficacy was also evaluated for POP3 protocol. Utilizing an in-house POP3 server, the ProSecure and Barracuda platforms were tested with 9,209 unfiltered real-world emails. ProSecure achieved a spam block rate of 87.51%, outperforming the Barracuda appliance by 5%. Note: Cisco Spam & Virus Blocker does not

support spam and virus protection for POP3 and could not be evaluated for this test case.

Figure 3: Spam email blocked in a live production environment with 15,000 emails

Product	Actual Spam	Detected Spam	% Detected	False Positives
ProSecure	13,717	13,694	99.83	1
Cisco	14,913	14,913	99.97	0
Barracuda	12,537	12,537	99.14	3

Email Malware Detection Effectiveness

Virus and malware detection capabilities were evaluated using a mix of Win32 malware samples along with zero day and in the wild viruses. We subjected each device to over 100,000 Win32 malware as email attachments.

With constant emergence of new threats and attack vectors, virus engines need to maintain a comprehensive database and to keep up with sophisticated techniques used to conceal malware. One such complex method of spreading infection is by wrapping the virus into an archive file, for example a zip archive.

To test for these threats we archived the viruses and emailed them as 5 MB attachments. All appliances were configured to scan for an attachment of up to 10 MB. Dropping attachments by archived extensions filtering was disabled.

STM600 proved to be the most effective, detecting and blocking 99.4% of the malware infected emails; see Figure 1 on page 1. The Barracuda Spam Firewall achieved a 70.15% block rate. However, scanning for archived attachments led to high consumption of system resources, and unacceptable levels of latency. Also the Barracuda management GUI became unresponsive. This was not observed on the ProSecure.

Figure 2: Product and Result Comparison:

	Email Malware Detection	Spam Detection	POP3 Spam Detection	Web Malware Detection	HTTP Published Vulnerability Assessment	URL Categorization Accuracy
ProSecure STM600	99.40%	99.83%	87.51%	89.90%	97.78%	73.81%
Barracuda Spam & Virus Firewall 300	70.15%	99.14%	82.59%	N/A	N/A	N/A
Barracuda Web Filter 210	N/A	N/A	N/A	89.82%	0% See Note 2	76.80%
Cisco Spam & Virus Blocker	0% See Note 1	99.97%	N/A	N/A	N/A	N/A

Note 1: The Cisco Spam and Virus Blocker does not scan compressed archive files (e.g. zip, rar). In a re-test with uncompressed virus attachments, the Cisco had a 97.1% detection rate.

Note 2: The Barracuda Web Filter performs real-time virus scanning for only certain MIME types.

The Cisco product did not detect any viruses in the infected archived attachments. Cisco TAC engineers confirmed the Spam & Virus Blocker is unable to detect malware in archived files (e.g. zip, rar). Since this platform did not offer protection against archived malware, we wished to verify the detection and scanning capability of the virus engine. We repeated the test, using non-archived malware attachments only. This time the Cisco Spam & Virus Blocker delivered a block rate of 97.1%

Web Malware Detection Proficiency

While spam email is highly annoying, malicious websites are dangerous. Millions of URLs are engaged in malicious activities. With rising popularity of Web 2.0, allowing attackers to upload malicious content, it becomes essential for a web security appliance to detect malicious content based on real-time analysis of content and not just by reputation or lists.

Tests were conducted using over 500 live websites, each hosting thousands of malware instances and malicious content. Additionally we built a web server and hosted 30,000 samples Win32 malware in archived and non-archived format. We also conducted published vulnerability analysis which targets the vulnerabilities behind tens of thousands of unique exploits. This was performed to audit the signature set of the appliance for port 80 HTTP exploits. Website reputation checking features were enabled for this test. When tested with the live malicious websites, both ProSecure and Barracuda appliance fared equally well, blocking nearly 90% of the websites based on reputation and real time analysis of content. See [Figure 3](#) on page 3.

When conducting published vulnerability analysis and tests with the infected web server, the Barracuda Web Filter 210 offered no protection and blocked none of the threats. Barracuda engineers explained that the appliance blocks access to web sites based on domain, URL pattern, or content category and reputation. It offers real time virus scanning of content only for certain MIME types.

ProSecure achieved a block rate of 99.1% when tested with the infected lab web server and 97.78% for HTTP published vulnerability analysis.

By utilizing real time scanning, ProSecure overcomes the limitations of just employing reputation and URL databases for web filtering.

This deep content inspection adds an additional level of security and protects against malware from friendly URLs, such as many Web 2.0 sites

URL Categorization and Coverage

We conducted testing to compare the URL databases of the ProSecure STM600 and Barracuda Web Filter 210. The goal was to evaluate the coverage and accuracy of the appliances to categorize URLs.

By applying the Long Tail Curve to website browsing behavior, a sample set of 65,535 URLs was created.

The Long Tail Curve phenomenon when applied to website browsing behavior, explains that 50% of user browsing occurs among the most popular websites. But the rest is randomly distributed.

For this assessment all categories of classifications were enabled with settings to block and give an alert when a website matched one of the defined filtering categories. As long as a URL was correctly classified, the vendor got credit for having the URL in its database. If the website was not classified under a category or incorrectly categorized, it was considered a miss.

STM 600 scored on par with Barracuda Web Filter 210, accurately categorizing 73.8% of the websites in the sample set. See [Figure 4](#) for results.

Figure 4: Web and URL Filtering

Web Filter	Total URLs	Blocked URLs	Missed URLs	Accuracy
ProSecure	65,535	48,373	17,162	73.8%
Barracuda	65,535	50,332	15,203	76.8%

Bottom line

ProSecure STM600 provides enterprise class web and email security services, all in one appliance. Employing over 3 million signatures and real time content analysis, the ProSecure platform overcomes the limitations of using only reputation and URL database for filtering.

The results from the lab demonstrated that ProSecure outperforms Cisco and Barracuda appliances in malware detection proficiency over HTTP, SMTP and POP3. In addition ProSecure STM600 is on par with Cisco and Barracuda platforms in spam filtering effectiveness and URL coverage and categorization.

Miercom Performance Verified

Based on hands on testing, ProSecure STM600 proved:

- ProSecure STM600 detected and cleaned 99.4% of infected email attachments
- ProSecure blocked 99.8% of spam email
- During published vulnerability analysis 97.8% of HTTP exploits were blocked
- All-in-one architectural approach from ProSecure is easy to deploy and manage



ProSecure STM600



NETGEAR, Inc.
350 East Plumeria Drive
San Jose, CA 95134-1911
(408) 907-8000
www.prosecure.netgear.com

About Miercom's Product Testing Services

Hundreds of product-comparison analyses have been published over the years in such leading network trade periodicals as Network World, Business Communications Review - NoJitter, Communications News, xchange, Internet Telephony and other leading publications. Miercom's reputation as the leading, independent product test center is unquestioned.

Miercom's private test services include competitive product analyses, as well as individual product evaluations. Miercom features comprehensive certification and test programs including: [Certified Interoperable](#), [Certified Reliable](#), [Certified Secure](#) and [Certified Green](#). Products may also be evaluated under the [NetWORKS As Advertised](#) program, the industry's most thorough and trusted assessment for product usability and performance.



Report 091030

reviews@miercom.com

www.miercom.com

 Before printing, please consider electronic distribution

Product names or services mentioned in this report are registered trademarks of their respective owners. Miercom (Mier Communications, Inc.) makes every effort to ensure that information contained within our reports is accurate and complete, but is not liable for any errors, inaccuracies or omissions. Miercom is not liable for damages arising out of or related to the information contained within this report.