#210153
October 2010
Commissioned by
NETGEAR®

ProSecure™ UTM25 and UTM50 UTM Firewall Appliances for Defense against Web 2.0/ Social Media Threats:

Malware Detection Evaluation against Competing Products

Executive Summary

Unified Threat Management (UTM) firewall appliances aimed at small and medium businesses should deliver protection right out of the box against malware threats propagating on the Internet. Web 2.0 platforms – like Facebook, Twitter, and YouTube – have reached a social tipping point, transforming the way we socialize, conduct business, and interact with others on a global scale. That said, Web 2.0 and social media tools are fraught with danger. The explosion of Web use poses alarming operational risks to businesses that transforms the threat landscape into an N x N "pull" mechanism.

No longer are malware and virus infections single-point events, pushed into an organization by a single threat. N number of users in an organization are going to N different websites on the internet and are literally pulling threats into the organization.

Continued on next page ...

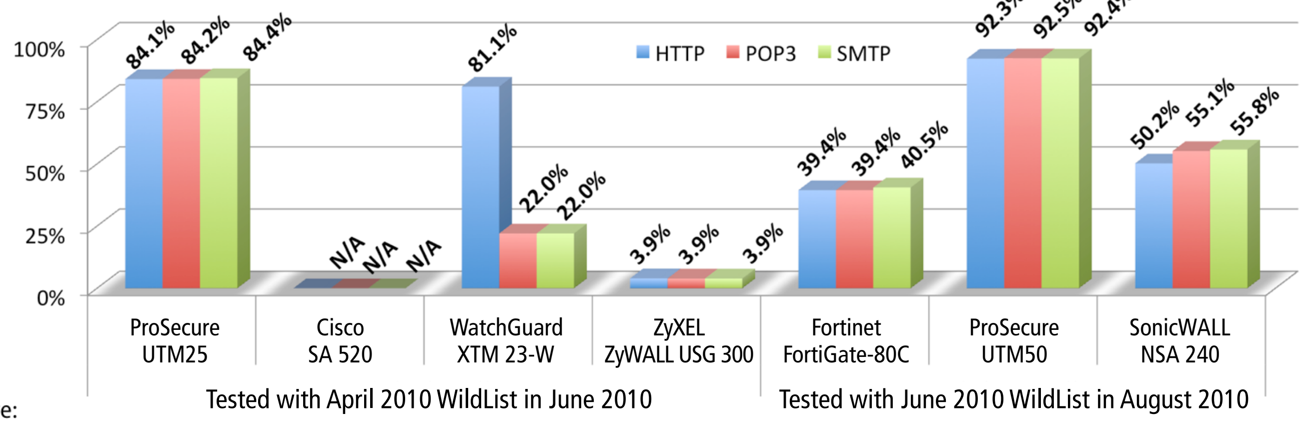
The Bottom Line

1 Zoo malware detection among vendors varied greatly – NETGEAR ProSecure UTM appliances detected the most threats

2 Extended WildList malware detection among vendors also varied - NETGEAR ProSecure UTM appliances detected the most threats

3 Some products did not detect malware equally across all protocols tested

Zoo Malware Detection Rate Comparison Over HTTP, POP3, and SMTP Protocols
(As Reported by AV-Test)



Note:

- "Zoo" malware refers, collectively, to adware/spyware, backdoors, trojans, bots/zombies, viruses, worms, etc.
- Tests were performed separately for each protocol.
- Tests were performed by AV-Test GmbH, using 60,000 sample comprised of a wide range of threats propagating on the Internet.
- Cisco results are not available as Cisco relies solely on URL reputation filtering but no Anti-Virus/Anti-Malware scanning for HTTP traffic. For POP3- and SMTP-based Email traffic, Cisco relies on server-side malware scanning which proved incompatible with current test methodology.

Source: Tolly/AV-Test, June, August 2010

Figure 1

Executive Summary

continued…

Tests show that the ProSecure UTM25 and UTM50 appliances demonstrated the best detection rate for viruses and worms 'propagating in the wild' (as documented in The WildList Organization International's WildList releases) as well as other important Win32 malware (known as Zoo malware) tested over HTTP, SMTP and POP3 protocols. The NETGEAR devices outperformed those of the competing, sometimes more expensive, UTM firewall appliances tested from Fortinet, SonicWALL, ZyXEL and WatchGuard.

Background

Social networks and Web 2.0 sites have become the new malware attack vectors, so much so that small and medium businesses face a daunting challenge of striking the right balance between the breadth of coverage and the associated cost of protection against an ever evolving threat landscape. Unified Threat Management (UTM) firewall appliances are very appealing to such businesses due to the combination of convenience and cost savings of having a single appliance to manage to protect multiple vectors (anti-malware, firewall, Web filtering, etc.) As the same appliance is providing multiple security services, UTM firewall vendors sometimes compromise on the resource-intensive security functions like anti-virus/anti-malware protection in the default configuration. But simply because the businesses are looking for value, does not mean that they need to settle for a lowered bar for protection out of the box.

NETGEAR, Inc.

ProSecure™ UTM25 and UTM50

Malware Detection Evaluation

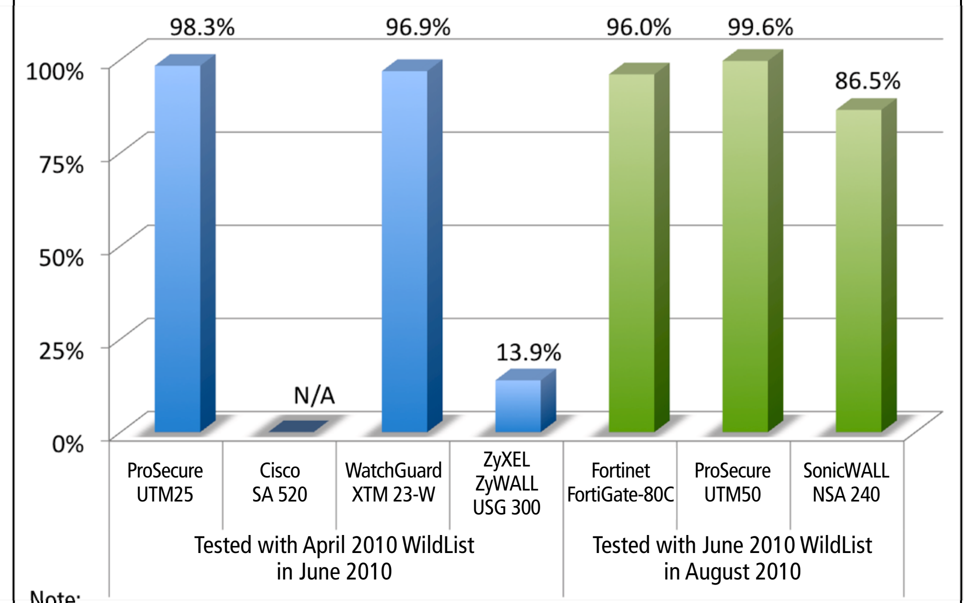
Tolly. Certified

Tested June-August 2010

Extended WildList Malware Detection Rate Over HTTP

(As Reported by AV-Test)

Higher Values are Better



Note:

- Based on the detection of 3,583 viruses and worms based on WildList Organization International's July 2009 WildList extended with important script and macro viruses chosen by AV-Test from previous WildList releases.
- Cisco results are not available as Cisco relies solely on URL reputation filtering but no Anti-Virus/Anti-Malware scanning for HTTP traffic.

Source: Tolly/AV-Test, June, August 2010

Figure 2

Tested in collaboration with AV-Test GmbH

AV-Test GmbH is a leading worldwide IT security testing and consultancy services provider.

Located in Magdeburg, Germany, the AV-Test team has more than 15 years of experience in the area of anti-virus research and data security, and is an active member of Anti-Malware Testing Standards Organization (AMTSO).

For more details on AV-Test, please visit http://av-test.org.

Source: AV-Test GmbH

Detailed Summary of Malware Detection over HTTP Protocol

(As Reported by AV-Test)

HTTP	Tested in June 2010 Using the April 2010 WildList							Tested in August 2010 Using the June 2010 WildList						
	Malware Samples Tested	ProSecure UTM25 Malware Detected		WatchGuard XTM 23-W Malware Detected		ZyXEL ZyWALL USG 300 Malware Detected		Malware Samples Tested	Fortinet FortiGate-80C Malware Detected		ProSecure UTM50 Malware Detected		SonicWALL NSA 240 Malware Detected	
		Numbers	%	Numbers	%	Numbers	%		Numbers	%	Numbers	%	Numbers	%
Extended WildList Malware	4,578	4,502	98.3%	4,436	96.9%	636	13.9%	4,812	4,620	96.0%	4,794	99.6%	4,162	86.5%
File viruses and worms (Win32)	4,467	4,391	98.3%	4,329	96.9%	636	14.2%	4,701	4,509	95.9%	4,683	99.6%	4,140	88.1%
Macro viruses (MS Office)	89	89	100.0%	89	100.0%	0	0.0%	89	89	100.0%	89	100.0%	5	5.6%
Script viruses (JS, VBS)	22	22	100.0%	18	81.8%	0	0.0%	22	22	100.0%	22	100.0%	17	77.3%
Other important Win32 malware (aka 'zoo malware')	60,000	50,448	84.1%	48,647	81.1%	2,368	4.0%	60,000	23,658	39.4%	55,374	92.3%	30,112	50.2%
Ad-/Spyware	10,000	8,110	81.1%	6,732	67.3%	19	0.2%	10,000	1,527	15.3%	8,261	82.6%	3,232	32.3%
Backdoors	10,000	8,861	88.6%	7,604	76.0%	1,212	12.1%	10,000	3,732	37.3%	9,273	92.7%	5,130	51.3%
Bots (Zombies)	8,848	6,267	70.8%	7,533	85.1%	380	4.3%	8,848	3,697	41.8%	8,262	93.4%	4,442	50.2%
Trojan Horses	11,152	8,878	79.6%	7,839	70.3%	117	1.1%	11,152	2,440	21.9%	10,218	91.6%	3,689	33.1%
Viruses	10,000	8,791	87.9%	9,486	94.9%	577	5.8%	10,000	6,135	61.4%	9,732	97.3%	6,088	60.9%
Worms	10,000	9,541	95.4%	9,453	94.5%	63	0.6%	10,000	6,127	61.3%	9,628	96.3%	7,531	75.3%

Note:

- Extended WildList malware consisted of the viruses and worms listed in The WildList Organization International's April and June 2010 issues of WildList, plus important macro and script viruses chosen by AV-Test from previous WildList releases.
- The zoo malware were collected by AV-Test GmbH from all around the world, representing the most prevalent threats propagating around the Internet.
- Cisco SA 520 could not be tested in the lab using the current methodology, as it does not perform malware scanning on Web/HTTP traffic but rather uses reputation-based URL filtering to scan for malware. Hence no results appear for Cisco SA 520.

Source: Tolly/AV-Test, June, August 2010

Figure 3

Tolly engineers, in collaboration with AV-Test GmbH - a leading authority on anti-malware research and testing, evaluated the malware detection accuracy of NETGEAR ProSecure UTM25, ProSecure UTM50, Fortinet FortiGate-80C SonicWALL NSA 240, WatchGuard XTM 23-W, Cisco SA 520, and ZyXEL ZyWALL USG 300 appliances. Tests focused on the malware detection capabilities of the UTM firewall appliances using their default security policies, over the Web traffic and email vectors using HTTP, POP3, and SMTP protocols.

Cisco SA 520 Testing Challenges

The Cisco SA 520 in particular presented challenges to test its performance in a lab environment. The Cisco appliance uses a reputation-based filtering to defending against Web-based malware. While this is an increasingly popular approach to perimeter security, unknown malicious URLs can still penetrate the defenses, as the URL is not yet blacklisted, and the Cisco appliance does not inspect the incoming traffic for malicious payloads. All the other products under test use Anti-Virus/Anti-Malware scanning and in some cases supplemented by reputation-based filtering.

Furthermore, the Cisco appliance is architected to use hosted Email services (provided by Cisco partners or third-parties), which provided server-side malware scanning of the Email in the cloud. This architectural design could be a disruptive proposition for the network administrators to have to migrate on-premises Email service to a hosted service to get protection with the Cisco appliance.

Both of these architectural characteristics of the Cisco appliance made the evaluation of detection accuracy in a lab environment not feasible, and hence no results could be reported for Cisco in the context of this evaluation.

Extended WildList Malware Detection

The WildList Organization International publishes the WildList, a periodical list of viruses and worms propagating on the Internet. Engineers used the latest WildList at the time of testing (April 2010 WildList, for

Detailed Summary of Malware Detection over POP3 and SMTP Protocol

(As Reported by AV-Test)

POP3	Tested in June 2010 Using the April 2010 WildList							Tested in August 2010 Using the June 2010 WildList						
	Malware Samples Tested	ProSecure UTM25		WatchGuard XTM 23-W		ZyXEL ZyWALL USG 300		Malware Samples Tested	Fortinet FortiGate-80C		ProSecure UTM50		SonicWALL NSA 240	
		Malware Detected		Malware Detected		Malware Detected			Malware Detected		Malware Detected		Malware Detected	
		Numbers	%	Numbers	%	Numbers	%		Numbers	%	Numbers	%	Numbers	%
Extended WildList Malware	4,578	4,566	99.74%	3,632	79.34%	636	13.89%	4,812	4,620	96.01%	4,800	99.75%	4,374	90.90%
File viruses and worms (Win32)	4,467	4,455	99.73%	3,525	78.91%	636	14.24%	4,701	4,509	95.92%	4,689	99.74%	4,269	90.81%
Macro viruses (MS Office)	89	89	100.00%	89	100.00%	0	0.00%	89	89	100.00%	89	100.00%	88	98.88%
Script viruses (JS, VBS)	22	22	100.00%	18	81.82%	0	0.00%	22	22	100.00%	22	100.00%	17	77.27%
Other important Win32 malware (aka 'zoo malware')	60,000	50,504	84.17%	13,217	22.03%	2,338	3.90%	60,000	23,647	39.41%	55,489	92.48%	33,071	55.12%
Ad-/Spyware	10,000	8,193	81.93%	475	4.75%	16	0.16%	10,000	1,527	15.27%	8,284	82.84%	3,560	35.60%
Backdoors	10,000	8,802	88.02%	2,511	25.11%	1,212	12.12%	10,000	3,731	37.31%	9,290	92.90%	5,889	58.89%
Bots (Zombies)	8,848	6,277	70.94%	1,892	21.38%	375	4.24%	8,848	3,697	41.78%	8,277	93.55%	4,845	54.76%
Trojan Horses	11,152	8,894	79.75%	729	6.54%	115	1.03%	11,152	2,432	21.81%	10,234	91.77%	4,789	42.94%
Viruses	10,000	8,794	87.94%	4,033	40.33%	560	5.60%	10,000	6,133	61.33%	9,753	97.53%	6,261	62.61%
Worms	10,000	9,544	95.44%	3,577	35.77%	60	0.60%	10,000	6,127	61.27%	9,651	96.51%	7,727	77.27%

SMTP	Tested in June 2010 Using the April 2010 WildList							Tested in August 2010 Using the June 2010 WildList						
	Malware Samples Tested	ProSecure UTM25		WatchGuard XTM 23-W		ZyXEL ZyWALL USG 300		Malware Samples Tested	Fortinet FortiGate-80C		ProSecure UTM50		SonicWALL NSA 240	
		Malware Detected		Malware Detected		Malware Detected			Malware Detected		Malware Detected		Malware Detected	
		Numbers	%	Numbers	%	Numbers	%		Numbers	%	Numbers	%	Numbers	%
Extended WildList Malware	4578	4566	99.74%	3632	79.34%	636	13.89%	4,812	4,620	96.01%	4,800	99.75%	4,486	93.23%
File viruses and worms (Win32)	4,467	4,455	99.73%	3,525	78.91%	636	14.24%	4,701	4,509	95.92%	4,689	99.74%	4,381	93.19%
Macro viruses (MS Office)	89	89	100.00%	89	100.00%	0	0.00%	89	89	100.00%	89	100.00%	88	98.88%
Script viruses (JS, VBS)	22	22	100.00%	18	81.82%	0	0.00%	22	22	100.00%	22	100.00%	17	77.27%
Other important Win32 malware (aka 'zoo malware')	60,000	50,663	84.44%	13,217	22.03%	2,338	3.90%	60,000	24,279	40.47%	55,446	92.41%	33,465	55.78%
Ad-/Spyware	10,000	8,224	82.24%	475	4.75%	16	0.16%	10,000	1,621	16.21%	8,229	82.29%	3,568	35.68%
Backdoors	10,000	8,819	88.19%	2,511	25.11%	1,212	12.12%	10,000	3,912	39.12%	9,295	92.95%	5,949	59.49%
Bots (Zombies)	8,848	6,304	71.25%	1,892	21.38%	375	4.24%	8,848	3,839	43.39%	8,280	93.58%	4,908	55.47%
Trojan Horses	11,152	8,945	80.21%	729	6.54%	115	1.03%	11,152	2,512	22.53%	10,236	91.79%	4,794	42.99%
Viruses	10,000	8,824	88.24%	4,033	40.33%	560	5.60%	10,000	6,247	62.47%	9,755	97.55%	6,346	63.46%
Worms	10,000	9,547	95.47%	3,577	35.77%	60	0.60%	10,000	6,148	61.48%	9,651	96.51%	7,900	79.00%

Note:

- Tests were first done over POP3 protocol, and then using SMTP protocol. Test results were identical.
- Extended WildList malware consisted of the viruses and worms listed in The WildList Organization International's April and June 2010 issues of the WildList, plus important macro and script viruses chosen by AV-Test from previous WildList releases.
- The zoo malware were collected by AV-Test GmbH from all around the world, representing the most prevalent threats propagating around the Internet.
- Cisco SA 520 could not be tested in the lab using the current methodology, as it performs malware scanning of Email traffic on the hosted servers in the cloud. Hence no results appear for Cisco SA 520.

Source: Tolly/AV-Test, June, August 2010

Figure 4

Why Test Zoo Malware?

Zoo malware represents a growing threat to consumer and business network security. With the advent of new attack vectors through adware, spyware, social networking, URL shortening services that hide the actual URLs that could sometimes be malicious, etc., it is becoming increasingly challenging to rely on traditional methods of signature-based defenses. Many products are being optimized to perform well in detecting the latest WildList viruses, while faring poorly in defending against zero-day attacks and other zoo malware. So, it is important to also evaluate a product's ability to defend against zoo malware.

Source: Tolly

the test phase in June 2010; and the June 2010 WildList for the test phase in August 2010) available at the time of testing, and extended it with a set of important macro and script viruses chosen by AV-Test from the previous WildList releases.

This is the standard test methodology that has been employed by AV-Test to test products from vendors across the industry for the past 10 years. While new viruses and worms get released all the time, detection for the latest WildList gives a good idea about the currency and breadth of protection offered by the UTM firewall appliances in their default security policy with the latest security updates. Detection for macro and script viruses that have been listed on previous WildList releases provides an additional measure of protection. Figures 1 through 4 show that ProSecure demonstrated the best detection for the Extended WildList malware test samples over HTTP, POP3 and SMTP protocols.

In contrast, the closest performing competitors in detecting the Extended WildList malware over HTTP traffic were the WatchGuard XTM 23-W with 96.9% and the Fortinet FortiGate-80C with 96.6% detection. In the same test, SonicWALL's NSA

Polymorphic Viruses

Polymorphic viruses try to avoid detection by anti-virus tools by constantly changing [or mutating] their code and/or using encryption upon successful infection. It is a constant battle between the detection technology from anti-virus researchers and the evasion techniques used by virus writers to constantly stay one step ahead of each other.

The WildList viruses and worms include polymorphic variants, and a high detection rate for the latest WildList malware indicates that an anti-malware product is providing effective protection against the latest threats on the Internet.

Source: Tolly

Devices Under Test and Version Info

Developer, Distributor	NETGEAR, Inc.		Fortinet, Inc.	SonicWALL, Inc.	ZyXEL Corporation	WatchGuard Technologies, Inc.	Cisco Systems, Inc.
Product name	**ProSecure UTM25**	**ProSecure UTM50**	**FortiGate-80C**	**NSA 240**	**ZyWALL USG 300**	**XTM 23-W**	**Security Appliance SA 520**
Language of the tested version	English	English	English	English	English	English	English
Appliance OS version	1.0.16.3	1.1.16-0	4.0,build0279,100519 (MR2 Patch 1)	5.6.0.3-40o	2.20 (AQE.0) / 1.05	11.2.3 B267305	1.1.42
Appliance OS date	n/a	n/a	n/a	n/a	2010-03-10	n/a	n/a
Signature version	20100528.1138.0.0 / 201006101131	201008111101	12.00235	n/a	3200 / 1636 Kaspersky Engine	3485 / 11.6.10	n/a
Signature date*	2010-06-09	2010-08-11	2010-08-10	2010-08-10	2010-06-02	2010-06-08	n/a

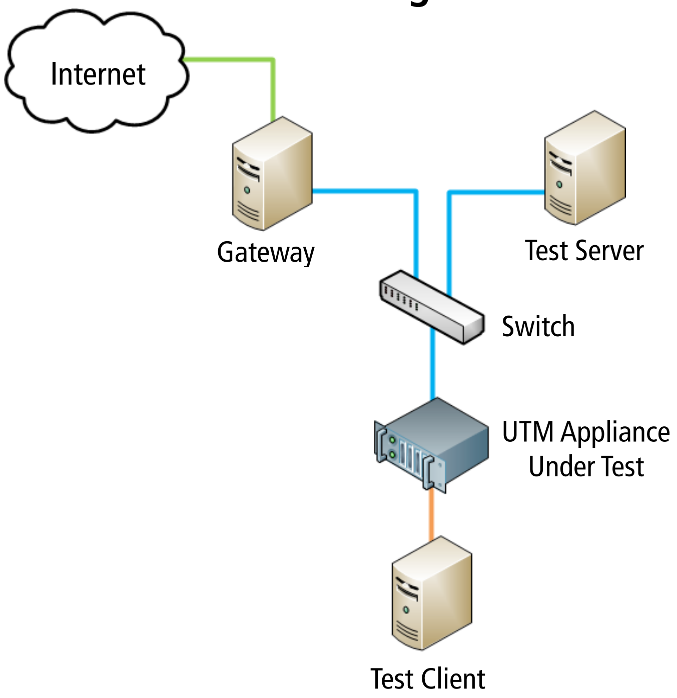
Note:

- Tests took place in two windows: in June 2010 and then in August 2010. The appliances were updated to their latest software/ signature levels before the start of the test, and then isolated from the Internet to set the appliance configuration in stone. The signature date shown indicates the latest available signature set at the time of the update.

Source: Tolly/AV-Test, June, August 2010

Figure 5

Test Bed Diagram



Source: Tolly/AV-Test, June, August 2010

Figure 6

240 appliance detected about 86.5% of the Extended WildList malware; while the ZyXEL ZyWALL USG 300 appliance performed the worst of the field, by detecting just about 14.9% of the malware samples.

When testing the Extended WildList malware detection over POP3 and SMTP protocols, ProSecure's competitors once again demonstrated significantly lower detection. In contrast to ProSecure's 99.7%-99.8% detection for the UTM25 and UTM50 respectively, the next best performer was the Fortinet FortiGate-80C with around 96% detection, followed by SonicWALL's NSA 240 detecting around 90.9%-93.2%. Next up was the WatchGuard XTM 23-W detecting 79.3% of the malware. The ZyXEL appliance once again performed the worst among the appliances under test - detecting just around 13.9%.

This shows that ProSecure UTM25 and UTM50 appliances offered the best Extended WildList malware detection over HTTP, POP3, and SMTP protocols, among the UTM firewall appliances tested, while the rest of the products offered varying performance blocking malware over different protocols.

Zoo Malware Detection

Engineers also tested the UTM firewall appliances under test with 60,000 samples of other major Win32 malware (adware/ spyware, backdoors, bots/zombies, trojan horses, viruses and worms) sometimes referred to as 'zoo malware'. These malware samples were collected by AV-Test GmbH from all over the world, and represent other major Win32 malware propagating on the Internet. These malware samples complement the Extended WildList malware samples. Tests once again examined the malware detection over HTTP, POP3, and SMTP protocols.

Test results show that the ProSecure UTM25 and UTM50 appliances once again achieved the best detected ~84% and ~92.5% respectively of the zoo malware samples over HTTP, POP3, and SMTP protocols, In contrast, its competitors detected just between just ~4% and around 81%. The WatchGuard XTM 23-W appliance detected around ~81% of the malware over HTTP traffic, while detecting just 22% of the malware over POP3 and SMTP protocols. SonicWALL's NSA 240 appliance was the next best performer with detection rates of ~50% over HTTP, ~55% over POP3 and ~56% over SMTP. The Fortinet FortiGate-80C appliance detected ~40% of the malware over HTTP, POP3, and SMTP. The ZyXEL ZyWALL appliance was once again the worst performer, detecting just ~4% of the malware over the HTTP, POP3, and SMTP protocols. See Figures 2 to 4.

The zoo malware detection tests once again show ProSecure UTM firewall appliances' superior detection of zoo malware over the competing UTM firewall appliances tested, using the default security policies.

TEST SETUP AND METHODOLOGY

Test Bed Setup

Tolly tested competing Unified Threat Management (UTM) Firewall appliances from ProSecure, Cisco, Fortinet, SonicWALL, ZyXEL and WatchGuard. See Figure 5 for detailed information on the software and hardware version of the appliances tested and Figure 6 for a diagram of the test bed. All the appliances were tested with their default security policies with the latest security updates as of the day of testing, with the appliances in a transparent proxy mode in the test network. The Fortinet FortiGate-80C were configured with 'Extended Database' signature set enabled.

Test Computers

The test systems (client, server, gateways) were all identically equipped PCs with the following specs:

- Intel Xeon X3360 processor with 2.83GHz
- 3.24 GB RAM
- 500 GB hard disc (7200 RPM)
- DVD-RW drive
- Gigabit ethernet network adapter
- Microsoft Windows XP (32-bit) with Service Pack 3

Two PCs were used per appliance for the testing: one worked as the server, one as the client.

The following software was installed on the server:

- Apache2 HTTP-Server
- MercuryMail POP3/SMTP Server

The following software was installed on the client:

- wget HTTP-Client
- Custom POP3/SMTP Client using JavaMail-API

All appliances (as well as the other systems used for the testing) had an active internet connection in place for downloading updates and query "in the cloud" services over a DSL line.

Test Methodology

Before the start of the tests, the appliances under test were updated with the latest security updates from the corresponding vendors. Once the updates were performed, the appliances were disconnected from the Internet to prevent further changes to the test configuration. The appliances were configured with their default security policies as shipped by their vendor.

There were two network segments used for the test; an internal and an external segment. The test client PC and the internal network side of the appliance under test, constitute the internal network segment. The external side of the appliance and the test server constitute the external network segment. The test server provided the Extended WildList and zoo malware test samples.

To start a certain test, the client connects to the test server and specifies to the server the test that needs to be performed. The server then creates the necessary settings and prepares the backend for the test. When the preparation is complete the client starts the test procedure.

While testing each protocol (HTTP or POP3 or SMTP) the client will fetch a list of files that should be transferred from the server. After the list is completely transferred the client will start to download the listed files one by one and create detailed log files which can be used for further analysis. The log files include MD5 checksums and HTTP response codes. All content that passes the appliance gets saved into ZIP archives for further analysis later.

After the test is completed, the created log files are analyzed by comparing the MD5 checksum of the backend server content with the MD5 checksum of the fetched data. If they are equal the content is considered to have been transferred without errors. If the checksums do not match, the file is considered to have been modified.

A fully transferred test file will be counted as a failure of the appliance under test to block the malware. In the case of partially fetched data, further checks of that data can be done. These checks are not included in the standard procedure. If there is nothing left for calculating a MD5 checksum, the corresponding file is counted as blocked.

Sometimes, appliances present a block page to the user instead of transferring the file content. This block page content is also saved and would be counted towards the number of malware blocked successfully.

The fetched data is further analyzed in several ways:

- Simple check of the fetched data against a multi-scanner system, which will scan the files with approx. 30 different anti-virus command line scanners. The results of this scan show if the fetched data is still recognized as malicious content.
- Semiautomated dynamic analysis by executing the file in a sandbox environment and trace if the sample is still executable and if so which actions are done.
- Manual static analysis by using a disassembler.

About NETGEAR ProSecure™:

ProSecure™ Gateway Security Appliances employ a best-of-breed security architecture that provides up to 400x the virus and malware coverage over other solutions at speeds up to 5x faster using patent-pending Stream Scanning Technology.

ProSecure has forged security technology partnerships with industry-leading Kaspersky Lab, Commtouch®, Mailshell™, and Sophos™ to bring best-of-breed enterprise-strength Anti-virus, Anti-spam, and Web filtering security technologies to the UTM and STM platforms.

For more information please visit www.prosecure.netgear.com.

Source: NETGEAR

About Tolly

The Tolly Group companies have been delivering world-class IT services for 20 years. Tolly is a leading global provider of third-party validation services for vendors of IT products, components and services.

You can reach the company by E-mail at sales@tolly.com, or by telephone at +1 561.391.5610.

Visit Tolly on the Internet at:
http://www.tolly.com

Interaction with Competitors

Fair testing is always the goal of The Tolly Group. Depending upon the test focus, that may include reaching out to competing vendors. As the basis of this test was to benchmark the devices "out of the box" using default configurations and an industry-accepted test methodology, it was not necessary to engage the various vendors.

For more information on the Tolly Fair Testing Charter, visit:
http://www.tolly.com/FTC.aspx

Terms of Usage

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 a product must be based on your own assessment of suitability based on your needs. The document should never be used as a substitute for advice from a qualified IT or business professional. This evaluation was focused on illustrating specific features and/or performance of the product(s) and was conducted under controlled, laboratory conditions. 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.

Reasonable efforts were made to ensure the accuracy of the data contained herein but errors and/or oversights can occur. 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. Accordingly, this document is provided "as is", and Tolly Enterprises, LLC (Tolly) gives no warranty, representation or undertaking, whether express or implied, and accepts no legal responsibility, whether direct or indirect, for the accuracy, completeness, usefulness or suitability of any information contained herein. By reviewing this document, you agree that your use of any information contained herein is at your own risk, and you accept all risks and responsibility for losses, damages, costs and other consequences resulting directly or indirectly from any information or material available on it. Tolly is not responsible for, and you agree to hold Tolly and its related affiliates harmless from any loss, harm, injury or damage resulting from or arising out of your use of or reliance on any of the information provided herein.

Tolly makes no claim as to whether any product or company described herein is suitable for investment. You should obtain your own independent professional advice, whether legal, accounting or otherwise, before proceeding with any investment or project related to any information, products or companies described herein. When foreign translations exist, the English document is considered authoritative. To assure accuracy, only use documents downloaded directly from Tolly.com. No part of any document may be reproduced, in whole or in part, without the specific written permission of Tolly. All trademarks used in the document are owned by their respective owners. You agree not to use any trademark in or as the whole or part of your own trademarks in connection with any activities, products or services which are not ours, or in a manner which may be confusing, misleading or deceptive or in a manner that disparages us or our information, projects or developments.