Miercom

Lab Testing Summary Report

October 2005
Report 050914

Product Category:
Unified Threat Management (UTM) Security Appliances

Systems Tested:

Cisco Systems® ASA 5520

Check Point® VPN-1® Pro

Fortinet® FortiGate™ 1000

Juniper Networks® NetScreen-208™

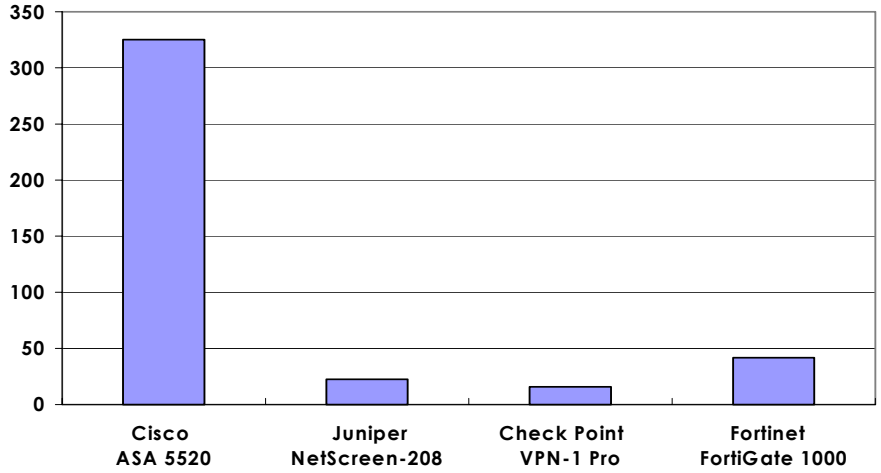
Miercom PERFORMANCE VERIFIED™

Key Findings and Conclusions:

- **The Cisco ASA 5520 performed more than six times better in throughput than the competitive solutions in real-world multi-function threat mitigation**
- **The Cisco ASA 5520 delivered over three times more 3DES-encrypted VPN throughput than competitors when tested using real-world traffic**
- **The Cisco ASA 5520 scored 100 percent overall threat-detection success; competitors averaged only 30 to 40 percent**
- **The Cisco ASA 5520 demonstrated the highest connection-establishment rate, surpassing the closest competitor by more than four times, in real-world, multi-function, threat-mitigation performance comparisons**

Cisco Systems® engaged Miercom to independently test the Cisco ASA 5520 Adaptive Security Appliance against several other comparable, competitive Unified Threat Management (UTM) security appliances – the Check Point® VPN-1® Pro, the Fortinet® FortiGate™ 1000, and Juniper Networks® NetScreen-208™. Performance areas examined included: unified firewall and IPS throughput performance, VPN throughput performance, IPS threat-prevention capability; and connections-per-second performance.

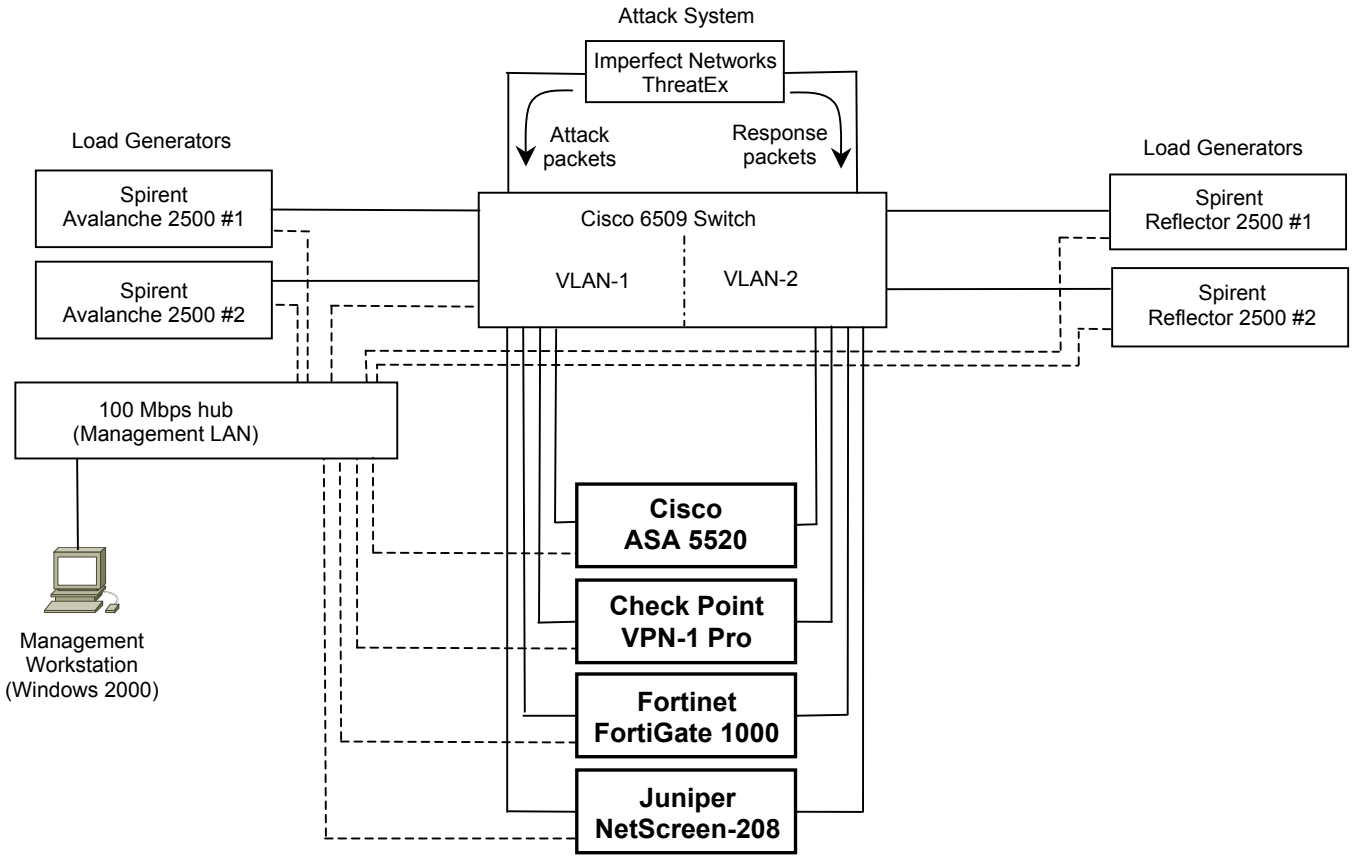
Firewall Performance (Mbps) with All Attack/Virus Signatures Enabled, 16-Kbyte HTTP Object Size



The Cisco ASA 5520 demonstrated significantly higher throughput with real-world traffic and 16-Kbyte object sizes, with all threat signatures enabled

Competitive Testing Note: The tests and test methodology that produced these results were proposed by, co-developed with and/or influenced by the vendor sponsoring this comparative review. Miercom assured their fair and accurate application. These are not the only tests or results that should guide a product selection or purchase.

Test Bed Setup



About the Testing: Identical test-bed conditions were applied to the Cisco ASA 5520 and to all the other competitive systems evaluated in this study.

The Cisco ASA 5520 (Adaptive Security Appliance) was configured with the Cisco AIP SSM-20 (Advanced Inspection and Prevention Security Services Module). The ASA software was running version 7.0.2; the AIP SSM-20 was at 5.0.4. The Signature Definition file was version S187.

The Check Point system was configured on a HP DL380 G3, employing a single 2.4 Ghz Xeon processor, with 1 GB of memory and an Intel Pro.1000 MT Dual Port Server Adaptor. The software was VPN-1 Pro Gateway NGX 6.0, Build 244. The Smart Defense Update was version 591050816. The software included WebIntellegence and SecureXL.

Fortinet's FortiGate 1000 ran version 2.80, Build 456 operating code. The FortiGuard AV (anti-virus) Definitions were version 6.037, and the FortiGuard Intrusion Definitions were version 2.226.

Juniper Networks' NetScreen-208 ran version 5.2.0 r2.0 operating code with Deep Inspection Signature Update 364. NetScreen's Deep Packet Inspection software was included in the system tested.

Four sets of tests were run. The first two – Firewall performance tests – measured connections per second and firewall throughput with all threat signatures enabled. Normally, a user selectively enables signatures to minimize the occurrence of false positives events. In our testing, however, we were checking each IPS' full detection capabilities, and also exercising the systems under load. So the complete signature sets were enabled in these cases. The third test was the VPN site-to-site termination test; in this case the vendors' "default" firewall settings were enabled. The fourth test was the IPS threat prevention tests, where all signatures, for all devices, were enabled.

The traffic for all the performance tests was generated with two pairs of Spirent Avalanche/Reflector 2500 load generators, which ran v7.0 (build 36784). The load from the traffic generators and the outputs of the Attack System – the Imperfect Networks ThreatEx Appliance (v1.60b) – were connected through the same VLANs on a Cisco 6509 Catalyst switch, which was running IOS 12.2.

Note: All publicly available documents and materials from the competitive vendors, along with the considerable technical expertise and judgment of the testers, were applied to ensure these vendors' units were appropriately and optimally configured for each test scenario. Check Point, Fortinet and Juniper all declined requests to provide Miercom with direct technical support for this testing.

Unified Threat Management

Unified Threat Management (UTM) devices have recently become very popular because they address multiple security-related threats, all in one unit. Many current UTM products are offered as security appliances (pre-packaged hardware and software). Some, however, are offered as software products running on standard Intel PC/server platforms.

For this comparative study, all the devices tested provide firewall capabilities, IPS (intrusion prevention system) capabilities, and VPN gateway capabilities.

All the vendors offer a range of devices that address these functions. The products we selected for this evaluation were chosen because they are in approximately the same price range. The basic Check Point VPN-1 Pro (with WebIntelligence and SecureXL) – a software-only product – costs more than the other systems, but the price is still fairly close to the other systems tested.

The price of these products is very much tied to performance. All the vendors offer higher-end units with much more performance and capability, but at a significantly higher price. The goal of this evaluation was to compare similarly priced systems.

Workloads and Performance

The traffic load for our performance tests was generated using Spirent's Avalanche/Reflector load generators (see details on page 2). The Avalanche/Reflector systems were set to automatically generate high rates of TCP/IP traffic, which were directed to the particular UTM device being tested (one at a time, in turn). The generated TCP/IP traffic simulates real-world HTTP 1.1 Web traffic between typical users and Web servers.

For the HTTP traffic, thousands of TCP/IP connections were setup and terminated during each test run. Each test, lasting two to three minutes, consisted of "ramp up", "steady state" and "ramp down" phases. The load on each system under test was increased until connections started dropping (as reported by the Avalanche/Reflector system). At this point the "maximum" throughput was recorded. To confirm this, the traffic load was increased beyond this point. In some cases, the overall throughput increased minimally; while in other cases throughput dropped. As more traffic was applied, more and more connections were dropped.

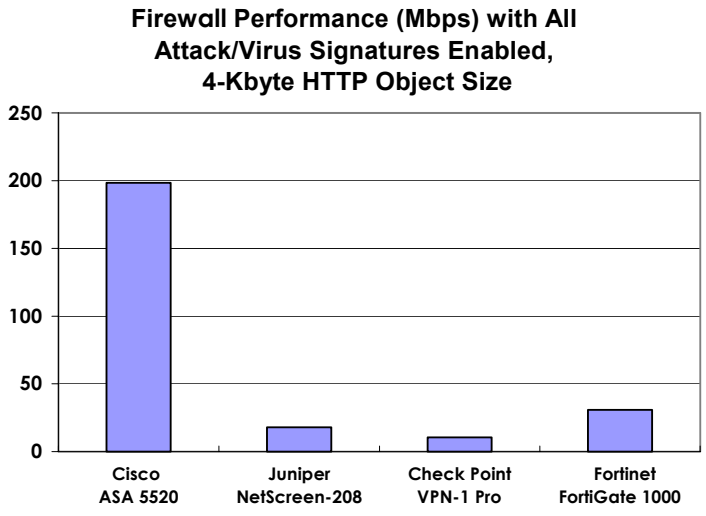
Higher throughput could have been achieved with UDP traffic, but UDP does not exercise connection setup and teardown, and other TCP-related logic, which is central to Firewall operation and performance. Also, the overwhelming percentage of network traffic these days is TCP/IP.

For both firewall and VPN testing, test cases were run with both 4-Kbyte and 16-Kbyte HTTP Object sizes. These simulated two different types of users: 16-Kbyte objects simulate users downloading large files, while 4k-byte objects are more representative of transactional-type traffic.

For firewall throughput, IPS performance tests and connections-per-second tests, all of the vendor's threat signatures were enabled. For site-to-site VPN tests, we ran with just the vendors' "default" firewall settings – these are those settings that ship with the product "out of the box." The IPS tests specifically evaluated the devices' ability to detect each threat. No background traffic was running as the threat-detection tests were being run.

Firewall and IPS Performance

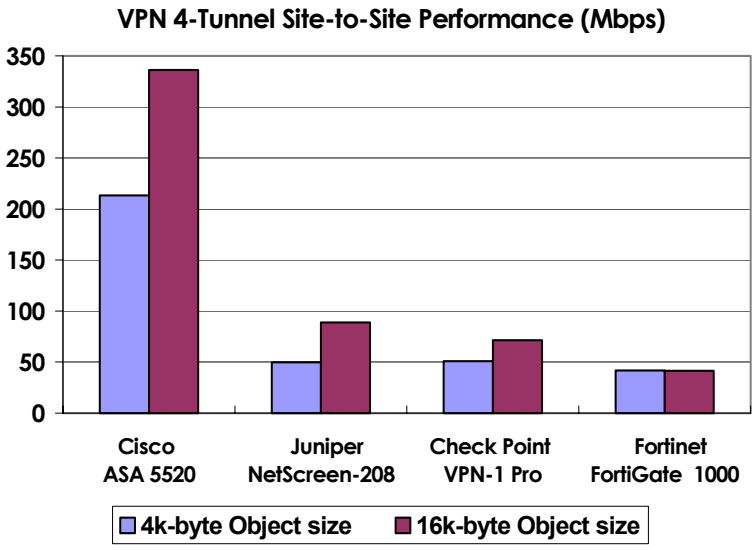
To measure firewall throughput, we ran tests with both 4-Kbyte and 16-kbyte HTTP Object sizes. The results of the 16k-byte HTTP Object-size tests are shown on page 1. The chart below shows the results of the 4-Kbyte HTTP Object sizes. The results show that the Cisco ASA 5520 continues to deliver high throughput performance, compared to competitors, even for this smaller, transactional-type traffic, with all threat signatures enabled.



The Cisco ASA 5520 demonstrated significantly higher throughput with 4-Kbyte HTTP Object Sizes and all threat signatures enabled

VPN Gateway Throughput Performance

Similar to the firewall performance, we evaluated VPN performance using 4-Kbyte and 16-Kbyte HTTP Object sizes. Again, the traffic was generated by the Spirent Avalanche/Reflector systems, simulating HTTP-TCP/IP "real-world" traffic. The VPN tests were run with four VPN tunnels, simulating four secure, site-to-site VPN connections, using 3DES encryption. The VPN tests were run with only the vendor's default firewall settings enabled (no additional settings were enabled).



The Cisco ASA 5520 demonstrated higher throughput than competitors in the 4-tunnel Site-to-Site VPN tests, with both 4-Kbyte and 16-Kbyte object sizes.

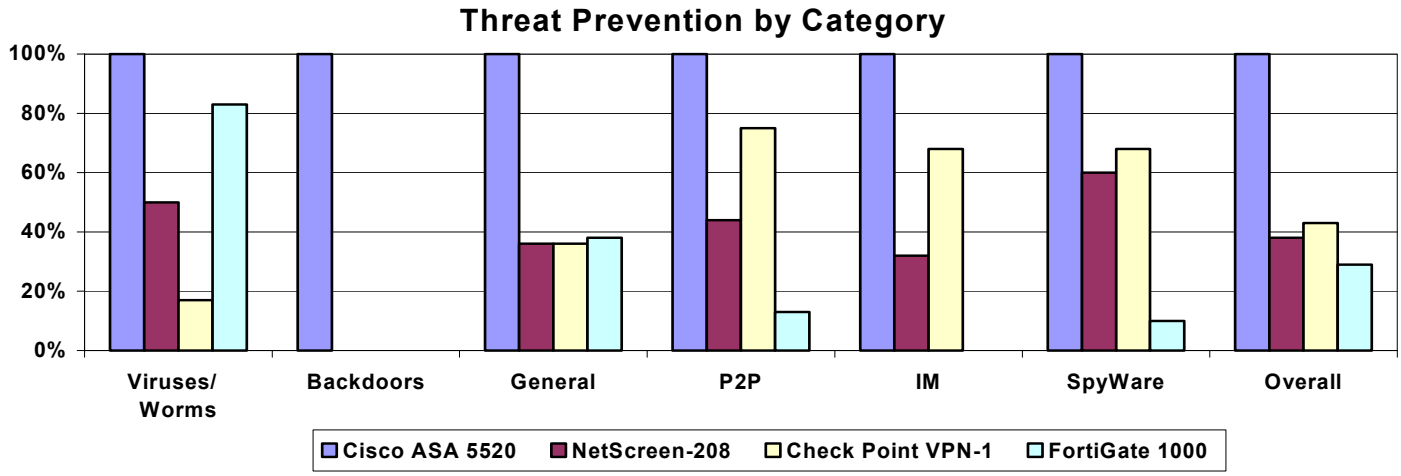
IPS Testing

The results of the IPS tests are shown below and on the next page. From a broad assortment of test cases, each involving a different category of threat, the Cisco ASA 5520 detected 100 percent of the threats in the test cases we performed.

When testing the same test cases, with the competitive security appliances, many threats were undetected to varying degrees. None of the other systems detected more than 45 percent of the collective threats in all categories. For instance, while the FortiGate 1000 detected 83 percent of the Virus/Worm test cases, overall only 29 percent of the total threats presented were detected. The Cisco ASA 5520 detected all of the Backdoor threats, while surprisingly none of the competitive systems detected any of the Backdoor test cases presented.

The IPS functionality tested included basic attacks that are typically included in most IPS tests, as well as additional test cases involving attack and threat mitigation, policy violation, and adware and spyware detection.

A total of 126 threats (test cases) were presented to all four systems tested. Each test case was executed separately for each system. All the signatures (or any other IPS-type settings) were enabled for each system. The results were examined using each system's main management screen – these were web-based applications which were configured to display the attacks as soon as they were detected.



The Cisco ASA 5520 detected 100 percent of the complete set of the threats presented, while comparable, competitive systems from Juniper, Check Point and Fortinet only detected 30 to 40 percent of the cumulative threats.

We segmented the test cases into 6 categories:

Viruses/Worms and **Backdoors** are two of the more conventional attacks, which are typically detected by IPS's. Some of the test cases we used included the "zotob", "rbot.cbq" and "netsky" viruses and worms.

The **General** category was the largest, containing old and new attacks; and attacks on a variety of client types and servers (different operating systems) as well as attacks on specific types of network devices. Representative threats in this category included the "Veritas registration overflow" and the "javaproxy.dll heap overflow" attacks.

The **P2P** (Peer-to-Peer) and **IM** (Instant Messaging) categories are part of the Policy Violations group. Recently, enterprises have started restricting P2P and IM activity at the workplace. Some of the P2P test cases included "KaZaa", "Napster", and "Gnutella" client traffic. IM signatures included "AIM", "Yahoo" and "MSN" client traffic. These signatures are normally not enabled on the firewalls, but can be enabled if required.

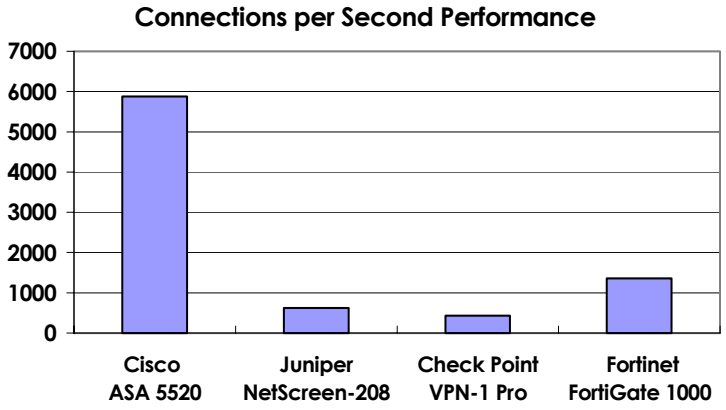
The last category is **Spyware** and **Adware**, which are also becoming more important as concern for protecting sensitive data grows. Test cases included the "Gator beacon" and "Gain adware" malware.

All the test cases for IPS testing were captured from actual live attacks in a lab environment. The captured packet traces from these live attacks (called "pcap" files) were processed by a tool, called ThreatEx (an appliance from Imperfect Networks), and then replayed by ThreatEx through the Unit Under Test.

Connections per Second

The Cisco ASA 5520 exhibited excellent performance in a multi-function environment with real-world traffic, compared to competitive security appliances. For this we ran connections-per-second, or transaction-per-second rate tests.

The connections-per-second tests were run similarly to other tests in this study. The transaction rate was increased via the Spirent Avalanche workload generators until the system-under-test started dropping transactions. The maximum connections per second were recorded. This was the maximum-load point achieved, as indicated by the Spirent Avalanche, when no transactions were dropped. All the connections-per-second tests were run with 64-byte object sizes. The below chart compares this connections-per-second performance.



The Cisco ASA 5520 achieved over four times the Connections per Second performance of comparable systems using real-world traffic in a multi-function environment with all threat signatures enabled

	Cisco ASA 5520	Juniper NetScreen-208	Check Point VPN-1	Fortinet FortiGate 1000
TESTED ATTACKS				
Viruses/Worms	100%	50%	17%	83%
Backdoors	100%	0%	0%	0%
General	100%	36%	36%	38%
P2P	100%	44%	75%	13%
IM	100%	32%	68%	0%
SpyWare	100%	60%	68%	10%
Total Protection	100%	38%	43%	29%

The Cisco ASA 5520 successfully detected 100 percent of the complete set of the threats presented in all categories in this evaluation, while comparably priced competitive systems only detected 30 to 40 percent of the threats.

Miercom Verified Performance

Based on Miercom's examination of these four systems' operation, capabilities and features, as described herein, Miercom hereby attests to these findings:

- The Cisco ASA 5520 performed more than six times better in throughput than competitive solutions in real-world multi-function threat mitigation (Firewall, IPS, Network Anti-Virus) comparisons
- The Cisco ASA 5520 delivered more than three and a half times the 3DES VPN throughput than competitive solutions when tested using real-world traffic
- The Cisco ASA 5520 delivered more than twice the threat protection of the tested Check Point, NetScreen, or FortiGate devices. The Cisco ASA 5520 scored 100% detection accuracy in each test, while competitive solutions averaged an alarming threat coverage of 30-40%
- The Cisco ASA 5520 demonstrated the highest connection establishment rate, surpassing the closest competitor by more than four times in real-world multi-function threat mitigation (Firewall, IPS, Network Anti-Virus) comparisons

Vendor Information:

Cisco Systems
170 West Tasman Drive
San Jose, CA 95134 USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Check Point Software
800 Bridge Parkway
Redwood City, CA 94065
www.checkpoint.com
Tel: 800-429-4391
650-628-2000
Fax: 650-654-4233

Fortinet
920 Stewart Drive
Sunnyvale, CA 94085 USA
www.fortinet.com
Tel: 408-235-7700
Fax: 408-235-7737

Juniper Networks
1194 North Mathilda Ave.
Sunnyvale, CA 94089 USA
www.juniper.net
Tel: 888-586-4737
408-745-2000
Fax: 408-745-2100

About Miercom's Product Testing Services…

With hundreds of its product-comparison analyses published over the years in such leading network trade periodicals as *Business Communications Review* and *Network World*, Miercom's reputation as the leading, independent product test center is unquestioned. Founded in 1988, the company has pioneered the comparative assessment of networking hardware and software, having developed methodologies for testing products from SAN switches to VoIP gateways and IP PBX's. Miercom's private test services include competitive product analyses, as well as individual product evaluations. Products submitted for review are typically evaluated under the "Net**WORKS** As Advertised™" program, in which networking-related products must endure a comprehensive, independent assessment of the products' usability and performance. Products that meet the appropriate criteria and performance levels receive the "Net**WORKS** As Advertised™" award and Miercom Labs' testimonial endorsement.

Miercom

379 Princeton-Hightstown Rd., East Windsor, NJ 08512
609-490-0200 ● fax 609-490-0610 ● www.miercom.com

Report 050914