



Lab Testing Summary Report

June 2005
Report 050610

Product Category:
Intrusion
Prevention Systems

Vendors Tested:
Cisco Systems
and
**TippingPoint, a
division of 3Com**

Products Tested:
**Cisco Systems
IPS 4255**
and
**TippingPoint
UnityOne-1200 IPS**



Key Findings and Conclusions:

- The Cisco IPS 4255 detects and blocks more network threats than the TippingPoint UnityOne-1200
- The Cisco IPS 4255 allows much more granular customization of actions in response to triggered signatures – existing or user-defined signatures – than the UnityOne-1200 system
- The Cisco IPS 4255 can block potential attacks based on target IP address, asset value, and OS relevance, allowing strict policies to be designed to protect critical servers
- The Cisco IPS 4255 and UnityOne-1200 provide similar single-system management. Cisco significantly expands beyond single-device management with a more extensive capability to correlate reports from multiple and diverse security devices

Cisco Systems engaged Miercom to independently test the Cisco IPS 4255 Intrusion Prevention System (IPS) against the TippingPoint UnityOne-1200® IPS. The evaluation focused on three main areas of IPS functionality: effectiveness in blocking a common set of attack tests, architectural facilities for customizing signature handling, and breadth of IPS management.

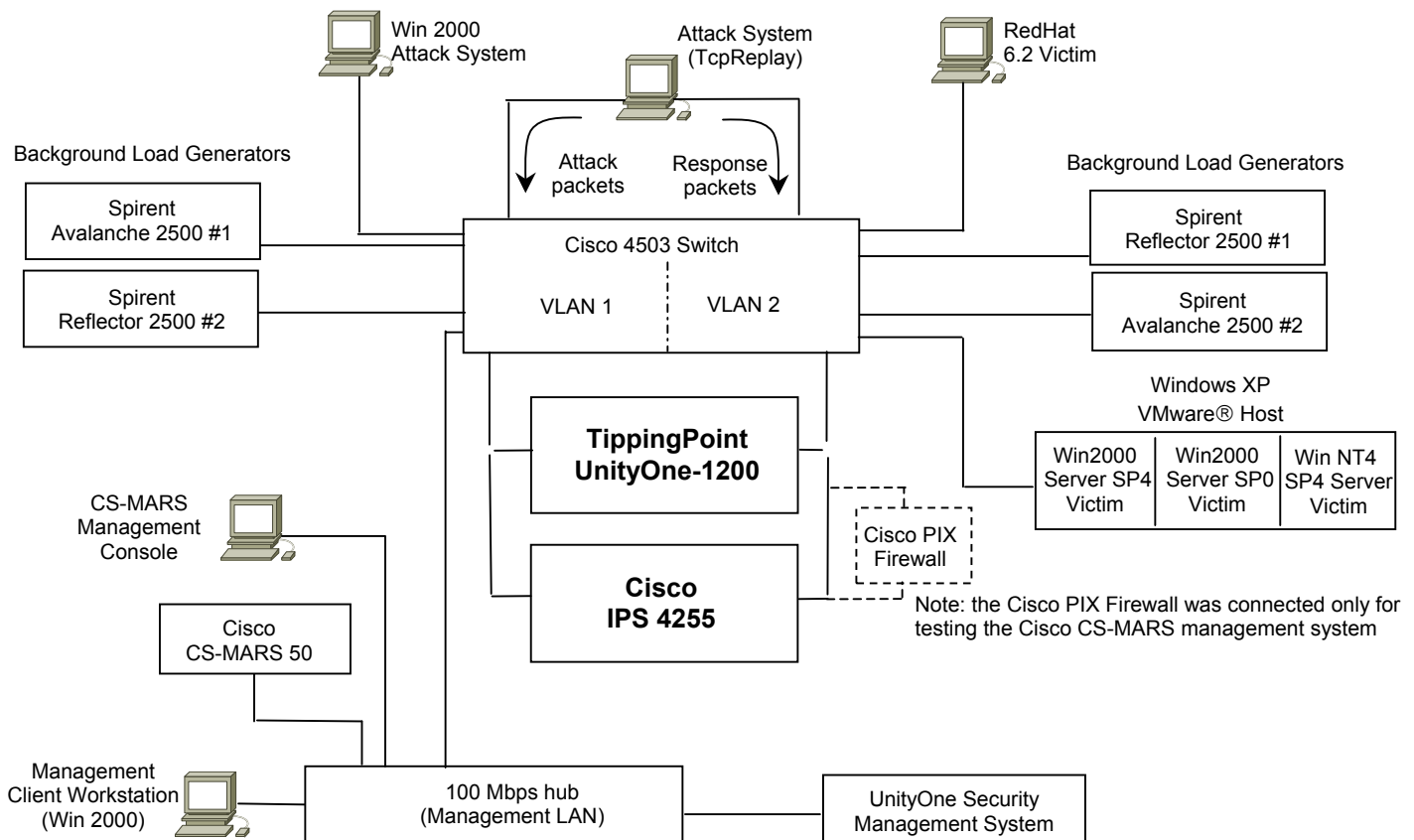
As part of our evaluation, we executed a set of attack tests including backdoors, viruses, and evasions. We configured each appliance between two LAN segments and executed the tests under load. Some of the attack tests were packet-stream replays of known attacks, while others were real attacks launched from an attack computer to a target system. The Cisco IPS 4255 detected all the attacks we delivered, however the UnityOne-1200 failed to recognize a number of the attacks. A summary of the results are shown in the table below.

	Cisco IPS 4255	UnityOne-1200
TESTED ATTACKS		
Backdoors	100%	100%
Viruses	100%	91%
Modified	100%	50%
Evasions	100%	55%
Known Exploits	100%	52%
Total Protection	100%	60%

Summary of 75 attack test cases, in various categories were run against both the UnityOne-1200 and the Cisco IPS 4255 appliances. The above results were obtained with all signatures in both appliances 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: The identical test-bed conditions were applied to both the Cisco IPS 4255 and the UnityOne-1200 IPS.

The TippingPoint UnityOne-1200 and Cisco IPS 4255 were each tested with all signatures enabled. Normally, a user would selectively enable signatures to minimize the occurrence of false positives events. In our testing, however, we were checking each IPS's full detection capabilities, and we enabled the complete signature set in both cases.

The Cisco IPS 4255 operating software was version 5.0 (2) with "IPS Active Update" (signature set) version s174. The UnityOne-1200 sensor software was v2.1.0.6305, and the Digital Vaccine (signature set) was v2.1.0.2897. The TippingPoint Security Management System tested was version 2.1.0.3619.

The results were obtained in all cases with background traffic loads in excess of 200 Mbps applied to both the Cisco and the TippingPoint systems. The background traffic was generated with two pairs of Spirent Avalanche/Reflector 2500 load generators, which were running v6.51. The load from the traffic generators and the outputs of the Attack System TcpReplay Tool (v2.3.3) (running on Fedora Core 3, an open-source Linux) were consolidated through two VLANs on a Cisco 4503 Catalyst switch, which was running IOS 12.1(13) EW1.

After the Cisco IPS 4255 was evaluated, the same test bed was used for the TippingPoint UnityOne-1200. The cables were removed from the Cisco IPS 4255 and the TippingPoint UnityOne-1200 was cabled in its place. The same set of attacks were run and the IPS's alerts were reviewed.

Many of the attacks delivered in these IPS tests have historically been known for some time. The attacks that were applied covered a broad spectrum, and included: Viruses, Backdoors, Well-known exploits, Password Cracker, Fragmentation, and URL Obfuscation. Other attacks were generated using exploitation and penetration testing tools such as Metasploit v2.4 and Core Impact v4.0.1.

The Cisco PIX firewall was not connected during the testing of the IPSs. It was attached only after testing to evaluate the multi-system event correlation capabilities of the CS-MARS (Cisco Security Monitoring, Analysis, and Response System) (version 3.4.2). The Cisco PIX firewall (v6.4.2) was connected inline with the Cisco IPS 4255.

Note: All publicly available documents and materials from TippingPoint, along with the considerable technical expertise and judgement of the testers, were applied to ensure the TippingPoint IPS was appropriately and optimally configured for each test scenario. TippingPoint declined requests to provide Miercom with direct technical support for this testing.

Attacks and Evasions

One key aspect of any IPS's functionality is its effectiveness in identifying network security threats. The same set of attacks and evasions were first delivered to the Cisco IPS 4255 and then to the TippingPoint UnityOne-1200. Most were a set of known exploits, previously captured and analyzed, that were obtained from various sources. The attacks covered a wide range of attack types (DoS, RPC, etc.), designed for different target operating systems, and were delivered to the IPSs using the TcpReplay application. Overall, for this set of attacks, the Cisco IPS 4255 detected and blocked 100 percent versus 52 percent for TippingPoint.

Similarly, previously identified Backdoor attacks were delivered, and both IPSs successfully detected all of these.

A set of Virus attacks was also delivered; the Cisco IPS 4255 detected slightly more than the UnityOne-1200. In discussions with Cisco, we learned that Cisco Systems has augmented their signature development teams by establishing a relationship with Trend Micro focusing on Network AV threats. As Trend Micro identifies and captures a new threat, the analysis is forwarded to Cisco. The result is an increased update frequency and broader coverage for late breaking Network AV threats.

For the Modified exploits we generated real attacks with the "Metasploit" and "Core Impact" security test tools. The Cisco IPS 4255 successfully detected all the exploits in this set; the UnityOne-1200 detected 50 percent.

Most of the Evasion exploits were also real attacks. Some were TCP and fragmentation evasions; some were URL Obfuscation, where a hacker might encode URL bytes different ways, to use web applications to access data or gain privileges on servers. The Cisco IPS 4255 successfully detected all the obfuscation attacks sent; the UnityOne-1200 missed 3 out of 4 of the obfuscation tests.

Signature Handling and Customization

During our evaluation of the Cisco IPS 4255 and UnityOne-1200 IPSs, we reviewed their signature-handling capabilities. Cisco calls these "Attack Classification Algorithms". We reviewed Cisco's "Risk Rating" facility and their Signature Modification and Creation facilities. For Cisco, all of the parameters used to encode the attack classification algorithms are available to the user. The TippingPoint UnityOne-1200 does not deliver customization to the same extent and to the same granularity as the Cisco IPS.

The Cisco IPS 4255 "Risk Rating" facility allows users to tailor response actions for specific target nodes, as well as adjust the threat severity of specific signatures. We assigned different Target Value Ratings for three victim

servers, making one "mission critical." We also altered the Signature Fidelity for a test signature. The Cisco IPS 4255 performed as expected – some attacks were blocked, others just alerted. Using the "Risk Rating" facility reduced false positives by performing a more detailed analysis when the alert occurred – resulting in more accurate drops without affecting legitimate traffic.

The Cisco IPS 4255 also has strong capabilities for modifying individual attack signatures or creating new signatures for specific situations. These are useful for implementing corporate policies, such as restricting employees' Internet activities. This is done via the IDM and IPS MC 2.1 (see management below), which provide wizard-based utilities to guide the user through the customization process. The Cisco IPS 4255 also lets the user create "Meta-events," which are tailored patterns of specific signatures and events. These allow for very specific sequences of packets to be detected.

IPS Management Applications

With larger networks and multiple IPS/IDS devices, the management facilities supporting these security devices become increasingly important. We reviewed three types of IPS management applications. Both Cisco and TippingPoint offer a basic application that connects to a single IPS. The Cisco application is IDM (IPS Device Manager); TippingPoint's is called LSM (Local Security Manager). Our testing found these two applications similar in usability.

Some customers would prefer multiple-device management systems. TippingPoint offers the Security Management System (SMS), which is a separate application on its own server. For the Cisco multi-system environment, we evaluated the new IPS MC v2.1 (Intrusion Prevention System, Management Center). Both of these applications allow you view IPSs throughout the network and manipulate their signature sets and software from a central site.

The CS-MARS (Cisco Security Monitoring, Analysis and Response System) is designed to provide sophisticated event management for enterprise IPS networks. It gathers information from many different security devices and performs a correlation analysis to more accurately determine which attacks are real threats. To test the system, we sent a worm attack through a network containing a Cisco IPS 4255 and a Cisco PIX firewall. The IPS events were dynamically correlated with the firewall events without user intervention. The CS-MARS 50 determined the attack never reached its final destination because it was dropped by the Cisco PIX Firewall. TippingPoint's event management is incorporated in the UnityOne SMS.

Miercom Verified Performance

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

- The Cisco IPS 4255 Intrusion Prevention System detects and blocks more network threats than the TippingPoint UnityOne-1200
- The Cisco IPS 4255 allows much more granular customization of actions in response to triggered signatures – existing or user-defined signatures – than does the UnityOne-1200 system
- Using the “Risk Rating” facilities, the Cisco IPS 4255 can block potential attacks based on target IP address, asset value, and OS relevance, allowing strict policies to be designed to protect critical servers
- The Meta-Event Generator of the Cisco IPS 4255 provides the capability to correlate complex attack sequences – creating a unique event to block the threat
- The Cisco IPS 4255 and UnityOne-1200 provide similar single-system management. Cisco significantly expands beyond single-device management with a more extensive capability to correlate reports from multiple and diverse security devices



Vendor Information:

Cisco Systems, Inc.

170 West Tasman Drive
San Jose, CA 95134 USA

www.cisco.com

Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

TippingPoint, a division of 3Com Corporation

7501 North Capital of Texas Highway
Building B
Austin, TX 78731 USA

www.tippingpoint.com

Tel: 888 648-9663

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 "NetWORKS 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 "NetWORKS 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 050610