White Paper

Testing the Efficacy of Cisco IPS

Enterprise customers considering deployment of a network device typically want to understand the performance characteristics of that device. If the device under consideration is also a security device, such as an intrusion prevention system (IPS), the security characteristics of that device are as important as its performance characteristics. An earlier white paper addressed the performance characteristics of Cisco® IPS sensors [PRF]. This paper complements the results in [PRF] with an analysis of the security characteristics of a Cisco IPS sensor.

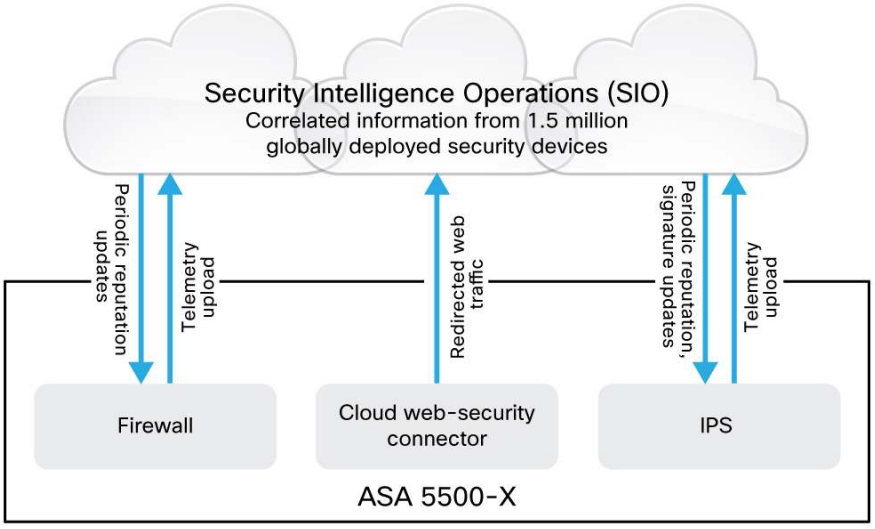
IPS in the Cisco security portfolio

Cisco's security portfolio offers three components to provide enterprises with in-depth network defense:

- A firewall that provides access control
- An IPS that provides broad protection against network threats
- A web security module that provides specialized protection against threats embedded in web traffic

These components can be deployed in multiple ways. One arrangement integrates the firewall, IPS, and web security capabilities on a single hardware appliance [CWS]. Another arrangement distributes the firewall, web security, and IPS functions onto individual hardware appliances [WSA]. These arrangements are depicted in Figures 1 and 2.

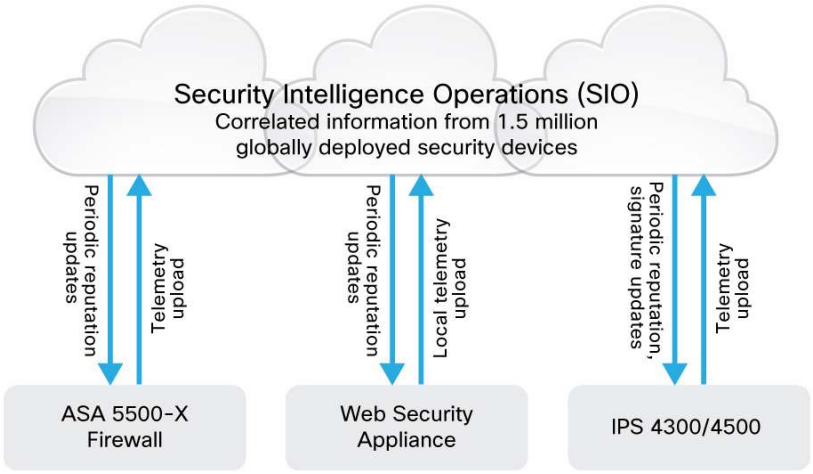
Figure 1. Integrated Cisco Security Components



All three components are connected via Cisco Security Intelligence Operations (SIO), into which the individual components feed telemetry and from which they extract network reputation[1].

[1] "Network reputation" is the calculated reputation of an individual IP address.

Figure 2. Distributed Cisco Security Components



Challenges in measuring security efficacy

With the ongoing evolution of the network threat landscape, measuring the efficacy of a security device such as an IPS sensor can be difficult. At best, the efficacy can be measured at specific points in time. However, even point-in-time measurements are complicated by the use of complementary threat prevention techniques such as network reputation.

Most tools for measuring security efficacy introduce predefined threats into the security device under test. In the case of an IPS, such tools provide a point-in-time measure of traditional IPS techniques (such as protocol-based decoding or regular-expression-based signatures) but not of Global Correlation, which relies on the measured real-world reputation of a network. Since test tools typically use synthetic network (IP) addresses as the source and destination of traffic flows, they cannot measure the efficacy of Global Correlation. Only empirical evidence can prove the efficacy of such techniques.

Point-in-time measurement of traditional IPS techniques

Thorough testing, even for a single vulnerability, is complicated and requires careful test design. We write signatures for Cisco IPS sensors to ensure that they are able to detect multiple variants of an attack, not just the most well-known versions [TST].

We use several third-party tools to track point-in-time efficacy of the traditional techniques in Cisco IPS sensors. One of these tools is BreakingPoint Storm. Figure 3 shows the standard configuration for testing Cisco IPS software and signature releases.

The BreakingPoint Storm tool contains a security test component with several presets: security levels 1 through 5 and SMTP Base64 Malware. For a point-in-time measurement, we ran the strikes (tests) in security levels 1 through 3, which contain the most pertinent network security attacks. We did not run the strikes in levels 4 and 5 and in SMTP Base64 Malware; these test for less important network threats, browser-based exploits, and exploits inside email traffic. Our research has shown that strikes outside of levels 1 through 3 are less relevant for network IPS sensors and better suited for other parts of the Cisco security portfolio, such as Cloud Web Security, Web Security Appliances, and Email Security Appliances, which are typically deployed in parallel with Cisco IPS [CWS], [WSA], [ESA]. As such, security levels 1 through 3 are the best fit for testing traditional IPS techniques.

Table 1 shows the results from a BreakingPoint (system version 2.2.7, product build 98473, strike build 108322) run against a Cisco ASA 5585-X S60/P60 appliance with Cisco ASA Software Release 7.1(6)E4, signature level 690 [SIG1], and signatures tuned to provide high efficacy against the attacks embedded in the BreakingPoint tests. While there are some operational differences between the integrated and distributed configurations described earlier, the same software codebase is used across all Cisco IPS sensors, resulting in similar efficacy across the IPS product line.

Figure 3. BreakingPoint Test Setup with Cisco IPS Sensor

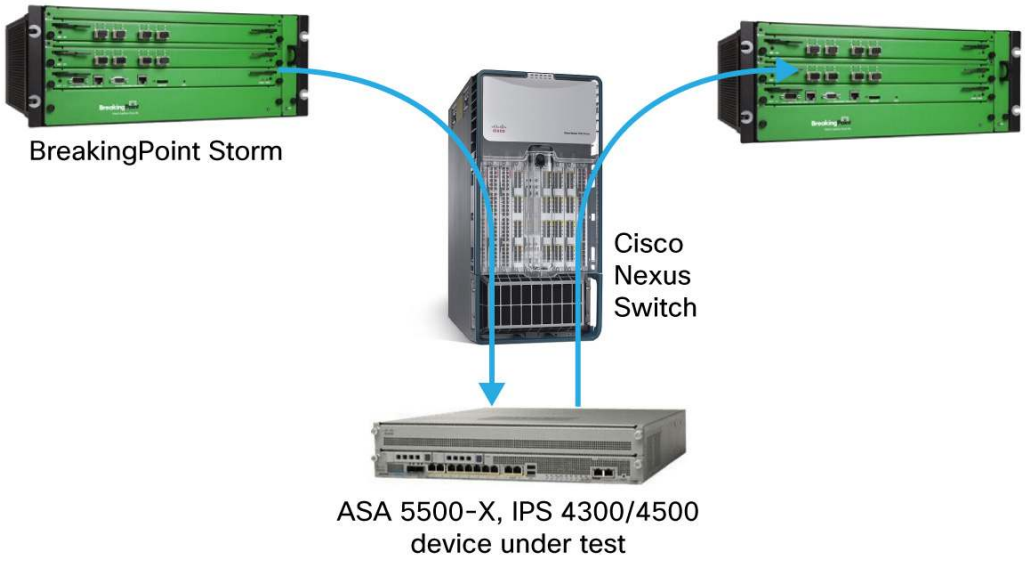


Table 1. Efficacy Test Results

Security level	Threats tested	Threats detected	Coverage
1	183	177	96.72%
2	273	260	95.24%
3	480	437	91.04%

Inspection throughput during test

The Cisco ASA 5585-X S60/P60 is rated at 10 Gbps for maximum inspection throughput using the media-rich traffic profile (described in [PRF]). We tested the inspection throughput of the IPS sensor with the same configuration and setup that was previously used for the efficacy test and found that the sensor achieved 10 Gbps of inspection throughput on the media-rich profile.

Typically, as a sensor is configured to do more or deeper inspection, performance degrades. In the efficacy test, the ASA 5585-X S60/P60 had enough inspection headroom above the stated data sheet throughput, and the performance degradation of the sensor in the face of the deployed signatures was graceful enough that the sensor achieved its advertised throughput of 10Gbps.

What threats did the sensor miss?

Cisco IPS did not catch all of the threats in the BreakingPoint security levels. In some instances, a threat was not caught, even though a signature for the threat existed on Cisco IPS, because our interpretation of the underlying CVE differs from that of the testing tool.

Here is an example:

- CVE 2003-0245 is a vulnerability in the apr_psprintf function in the Apache Portable Runtime (APR) library for Apache 2.0.37 through 2.0.45 [CVE1]. It allows remote attackers to cause a denial of service (crash) and execute arbitrary code. BreakingPoint security level 1 includes a strike for this vulnerability. Cisco IPS has a signature for the vulnerability; it fires when the vulnerability is tested using a Cisco proprietary tool. However, the signature did not fire in the test run, as the test tool sends out a much smaller payload (1500 bytes) than is needed for an exploit (for example 20,000 bytes on Windows), in our estimation. We could modify the existing signature or write a new one to fire on a shorter payload, but that would tamper with an otherwise functioning signature set and lead to false positives in deployments. We chose to ignore the test case, even though that meant a lower coverage score.

Cisco IPS users who prefer to block test threats such as the one described above, can write their own signatures. Instructions for writing signatures for Cisco IPS sensors are available in [SIG2][2].

In general, it is possible to get a 100% score on tests such as the ones discussed in this paper by writing overly broad signatures. While such scores look good in the lab, they are misleading for real-world deployments, as the network operator would be flooded with false positives from the broad signatures. We try to minimize false positives, both by writing tight signatures and by using the “context-aware” features of Cisco IPS, such as passive OS fingerprinting. Passive OS fingerprinting detects the OS of the target system and takes this OS into account while inspecting traffic. As a result, attacks that cannot lead to a security breach do not result in a signature firing, thereby minimizing false positives. For example, if a Cisco IPS sensor detects a Windows exploit directed at a Linux system, the sensor has the ability to silently ignore the exploit (if so configured).

Measuring the effect of network reputation

Cisco introduced the use of network reputation via Global Correlation in 2009 and has substantial experience deploying Global Correlation alongside traditional IPS techniques. Since good testing tools do not currently exist for measuring the impact of network reputation, we have conducted an empirical study using data from Cisco IPS sensors deployed at customer sites across several industry segments. This study is available at http://www.cisco.com/en/US/products/ps12156/prod_white_papers_list.html. A summary of the results is presented in Table 2.

Table 2. Impact of Global Correlation

Sensor	Industry segment	Firewall access policy	Traffic blocked by Global Correlation
BNK-1	Bank	Tight	7%
IND-1	Industrial Supplies Distributor	Moderate	26%
IND-2	Industrial Supplies Distributor	Moderate	35%
PRO-1	Professional Services Firm	Moderate	44%
PRO-2	Professional Services Firm	Permissive	100%

[2] We are in the process of contacting the test tool’s developers to resolve the differing CVE interpretations noted in this paper.

Sensor	Industry segment	Firewall access policy	Traffic blocked by Global Correlation
MED-1	Medical School & Hospital	Permissive	98%

As Table 2 shows, the impact of network reputation varies depending on the access control policy on the firewall in front of a sensor and the attacks targeting an organization. When the access policy is permissive or open (as on sensors MED-1 and PRO-2), network reputation detects and stops more threats than when the access policy is tight (as on the sensor BNK-1). For the sample of sensors studied [COR], traditional IPS techniques deny about half of the bad traffic and Global Correlation denies the other half[3]. In essence, deploying Global Correlation alongside traditional IPS techniques doubled the efficacy of Cisco IPS sensors in the study.

Another result of deploying Global Correlation along with traditional IPS techniques is that the network is afforded protection, even in instances where a signature for a vulnerability is turned off or has not yet been written. If an attacker on a device with a low reputation attempts to exploit a vulnerability for which no signature protection is turned on, Cisco IPS can block the attacker based purely on network reputation.

Summary

Securing an enterprise requires a portfolio of security components. In this paper, we have examined how Cisco IPS fits within the Cisco security portfolio and explained how we test the efficacy of Cisco IPS. Our results demonstrate that Cisco IPS provides effective security with traditional IPS techniques, while preserving data sheet performance numbers. We also observed that combining traditional IPS techniques with techniques such as Global Correlation increases the efficacy of Cisco IPS even further.

About Cisco IPS

Cisco IPS is the most widely deployed IPS solution in the market. Cisco's newly refreshed IPS portfolio includes the Cisco IPS 4500 Series, the Cisco IPS 4300 Series, and IPS modules integrated into Cisco ASA 5500-X Series Adaptive Security Appliances.

For more information on Cisco IPS, visit http://www.cisco.com/go/ips.

References

[ASA] Intrusion Prevention for the Cisco ASA 5500-X Series data sheet

[COR] Global Correlation on Cisco IPS Sensors

[CVE1] CVE 2003-0245: Apache APR_PSPrintf Memory Corruption

[CWS] Cisco ASA and Cloud Web Security

[ESA] Cisco Email Security Appliance

[PRF] Performance of Cisco IPS 4500 and 4300 Series Sensors

[SIG1] Cisco IPS Signatures

[SIG2] Writing Custom Signatures for the Cisco Intrusion Prevention System

[TST] IPS Testing

[WSA] Cisco Web Security Appliance

[3] Calculated by averaging the percentage of blocked traffic across the six sensors in the study.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C11-726365-01 02/13