NOVEMBER 2005
INFORMATION SECURITY®
INFOSECURITYMAG.COM

IPS REVIEW

ON THE Line

IT'S GAME DAY FOR IPS. SEE HOW FIVE APPLIANCES MATCH UP AGAINST ATTACKS.

BY ED SKOUDIS & MIKE POOR

Are you ready to let an intrusion prevention system (IPS) determine which traffic gets through to your network? Are you calling the plays? Do you trust the guys on the line to make the right decision? E-commerce is blindingly fast. You have to anticipate the attack, recognize the tactics and respond rapidly to keep the bad guys from getting your vital business data.

As the technology matures, IPS has generated a lot of buzz in the infosecurity industry; the IDS vs. IPS debate persists two years after Gartner declared intrusion detection systems (IDS) would be dead by 2005, in favor of IPS. The trick is stopping the attacks without impeding or even limiting legitimate business traffic in the high-speed, high-volume flow of online commerce. An IDS false positive is a nuisance; automatically blocking your 24x7 production app is unacceptable.

To sort out this buzz and determine if IPS is ready to be a prime-time automated defense tool, *Information Security* conducted a detailed laboratory review of five leading network-based inline IPS appliances: Cisco Systems' Intrusion Prevention Sensor 4255 Series; Internet Security Systems' (ISS) Preventia Network Protection Appliance G400; Radware's Defense Pro; Sourcefire's 3D System Intrusion Sensor 3000; and Top Layer Networks' Attack Mitigator IPS 5500.

We evaluated and graded each appliance in several categories: response to common attacks, popular evasion strategies, and denial-of-service attempts; how well the user interface mapped into and supported the daily workflow of network management and security personnel; and overall management capabilities. Here's what happened when they took the field.

Pivotal Question

Of course, the purpose of an IPS is to detect threatening traffic, alert the security team and, if they have sufficient confidence in the detection signature, automatically block the attack. Therefore, a critical evaluation question is, "Which is better: to alert but allow an attack, or to block it silently?"

Our conversations with a number of security experts yielded a clear consensus: It's better for the tool to alert and pass the traffic than to block and not alert.

The problem of blocking without alerting is that the organization has no data to figure out what traffic is being blocked and why. If the device alerts but does not block, the signature can still be adjusted to block that traffic, albeit after the initial attack.

This question is fundamental in the ongoing debate about the role of IDS and IPS, their capabilities and approaches to defending the network.

Our testing of Sourcefire, for example, underscores this.

The recommended initial IPS configuration detected most of

our attacks and alerted us that exploits were being attempted, but only blocked a few of them. This is a likely indication of the underlying "detection first" philosophy behind the Sourcefire product. In a real-world environment, organizations would need to tune their IPS signatures, starting with alert-centric rules that are gradually ramped up to blocking rules as a given network's traffic is better understood.

Detecting and Blocking Attacks

We tested how these IPSes handled some of the most common attacks of the last few years. If a tool missed common attacks that are a year old or older, there's concern about the vendor's underlying approach to defining signatures.

We chose to attempt the following four attacks:

- The IIS Unicode exploit, which was originally published in October 2000, launched by hand from our Web browser.
- The Windows RPC-DCOM buffer-overflow attack, which was originally published in July 2003 and later included in the Blaster worm, launched from several versions of Metasploit and Core IMPACT.
- The Windows LSASS buffer-overflow attack, which was originally published in April 2004 and included in the Sasser worm, launched from Metasploit and Core IMPACT.
- The Windows SSL PCT buffer-overflow attack, which was originally published in April 2004, launched from Metasploit.

One of the biggest issues with signature-based detection is the ability to detect signs that a given vulnerability is actually being exploited, rather than merely detecting individual specimens of exploit code, which an attacker can simply modify to evade detection. The not-yet-complete transition from detecting individual exploits to detecting vulnerability exploitation is likely the primary reason we see variations of the same exploit evading these devices.

ISS performed best on these tests, blocking all of our common attacks except a somewhat subtle variation of the Unicode exploit.

Top Layer also did well, blocking all attacks except the RPC-DCOM exploit from both Metasploit 2.0 and Core IMPACT. Ironically, Top Layer blocked this exploit from newer versions of Metasploit, but Core IMPACT and the older tactics of Metasploit version 2.0 slipped by its detection mechanisms. This raises an important point: Many security experts try to

ABOUT THIS REVIEW

Cisco Systems' Intrusion Prevention Sensor 4255 Series

Internet Security Systems' (ISS) Preventia Network Protection Appliance G400

Radware's Defense Pro

Sourcefire's 3D System Intrusion Sensor 3000

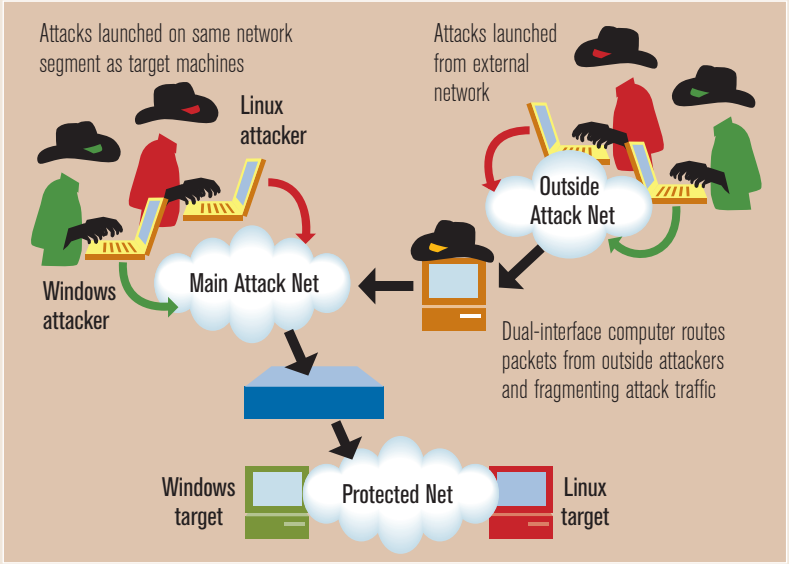
Top Layer Networks' Attack Mitigator IPS 5500

Information Security tested these five inline IPS appliances from leading vendors. Several other vendors were invited but declined to participate, citing various reasons such as impending new product releases and lack of available support resources.

We built our test lab *(see figure, below)* with the attacker network on the outside of the IPS, the protected target network on the inside, and the IPS product right in the middle, controlling the flow of traffic between the networks. We managed the IPS from an out-of-band management network interface, connected to a separate physical network.

The attacker network included a Linux and Windows machine on the same network segment as the IPS; some IPS tools are much more efficient at filtering attacks that come from the same network segment as the IPS, but buckle under the more real-world scenario of attacks that are routed from other networks. To model this situation, we introduced a dual-interface machine that focused on routing attack packets from an outside attacker network. This routing system also offered an ideal platform for fragmenting the attack packets in an attempt to evade detection.

Our attack tools included the open-source Metasploit Framework (versions 1.0, 2.0, 2.2, 2.3 and 2.4, to see how products detected exploits that have evolved over time), commercial exploitation tool Core IMPACT, Fragrouter and Toast.›



THE TRICK IS TO STOP ATTACKS WITHOUT IMPEDING LEGITIMATE TRAFFIC. AN IDS FALSE POSITIVE IS A NUISANCE; AUTOMATICALLY BLOCKING YOUR 24x7 PRODUCTION APP IS UNACCEPTABLE.

ensure that their devices block the latest and greatest attacks, and often forget to test earlier versions. IDS and IPS tools may break or delete a previous rule in favor of the newest signatures.

Sourcefire detected everything except the RPC-DCOM exploit from Metasploit 1.0, but blocked only three attacks, reflecting its conservative approach for initial configuration prioritizing alerting. The IPS tool snagged all of the RPC-DCOM attempts from more modern exploits, but the original RPC-DCOM exploit flew under its radar screen.

Cisco blocked only the older variations of RPC-DCOM, while admitting some based on newer Metasploit versions and Core IMPACT. Radware scored lowest, allowing some variations of RPC-DCOM and LSASS attack through the device, without any alert.

Handling Evasion Tactics

Beyond altering the contents of the exploits themselves, other evasion tactics tweak the exploits' appearance on the network in an effort to confuse an IPS or IDS tool.

Fragrouter, a tool originally released in 1999, provides more than two-dozen methods for altering attack packets at the network layer. Many of these mechanisms slice and dice attack packets into smaller and sometimes overlapping fragments. Other mechanisms manipulate TCP connections, such as faking a connection drop with a TCP FIN/RESET packet with a bad checksum. Checking embedded protocol checksums for all packets can be problematic for IPS tools, because the processing can slow performance.

Again, ISS rose to the top. Not a single Fragrouter option penetrated the end system protected by ISS. Cisco also blocked all of the Fragrouter evasion techniques, but on several occasions didn't alert us.

That's where the good news stops. We could dodge each of the other three IPSes by sending RPC-DCOM through Fragrouter configured with the TCP FIN/RESET with a bogus checksum.

Top Layer blocked and alerted on all Fragrouter options except that bad TCP FIN/RESET ploy. Sourcefire's detection capabilities were commendable, but it allowed most of our exploit attempts, alerting us but not blocking the vast majority of attacks. However, Sourcefire didn't even alert in the bad TCP FIN/RESET checksum test. Radware failed to block or alert on two different Fragrouter configurations: the bad TCP FIN/RESET checksum, as well as an option that simply cuts packets into orderly 24-byte fragments. Radware silently blocked, but didn't alert, on several Fragrouter attacks.

Blocking Denial of Service

DoS attacks generally fall into two categories: network-based floods and malformed packet attacks. Our testing focused on the latter to determine how well each IPS solution detects and blocks packets designed to kill or impair a protected system.

We used 17 malformed packet attacks released over the past several years, wrapped inside a tool called "Toast."

None of the IPS tools blocked all of the attacks, but Top Layer alerted on and blocked 14 of them; Cisco alerted on and blocked 10, and just alerted on four others. ISS was a very close third, blocking 10 and alerting on two; Sourcefire blocked only three but alerted on 10; and Radware blocked only four while alerting on only one.

GUI and Workflow Analysis

For a security or network analyst sitting in front of an IPS console during an entire shift, interface workflow and responsiveness are critical. Differences in speed and workflow were marked enough to clearly differentiate the products, so we analyzed how well each tool supported analysis and reporting processes used by IPS administrators, as well as ease of configuration.

We were particularly impressed with Top Layer's well-designed and speedy interface. Real-time events were updated on the screen without the lag we saw with other devices, which chugged through our packets, sometimes taking several minutes to record an attack. Additionally, the Top Layer GUI's support of analysts' workflow is very logical and built for detailed monitoring, and its rules and policies are flexible and simple to configure.

Sourcefire was the only appliance that had really customizable workflows. We viewed events by event type, time threshold, source and destination addresses, and service ports. The browser-based interface was speedy and well-designed, and the open signature and traffic displays were top in the test group. We could view, edit and create rules, and then apply them easily to particular networks.

On the downside, you have to refresh the browser manually to display new events, which could cause an organization under fire to miss a vital alert.

The ISS and Cisco interfaces were less responsive and intuitive, though both let users extract packet data from an event—a useful analysis feature. Cisco's interface lets the user view the signatures being applied to traffic, which helps significantly in configuring and tuning.

ISS won't let customers see the details of its proprietary signatures, keeping its "secret sauce" quite secret. However, in defense of its closed signatures, ISS was the best at detecting our attacks and evasion tactics.

Radware's interface is responsive, but difficult to work with. You view real-time events through the product's dashboard—a window with a sonar-like screen. However, as we attacked with different exploits, the sonar screen became cluttered with messages to the point where it was unreadable. The Radware GUI allowed us to assign rules and policies to particular devices, but wasn't very intuitive.

SCOREBOARD

	Cisco Systems Intrusion Prevention Sensor 4255 Series www.cisco.com	Internet Security Systems Preventia Network Protection Appliance G400 www.iss.net	Radware Defense Pro www.radware.com	Sourcefire* 3D System Intrusion Sensor 3000 www.sourcefire.com	Top Layer Networks Attack Mitigator IPS 5500 www.toplayer.com
Attack detection/blocking	B	A	C	B+	A-
Evasion detection/blocking	A-	A	C	B	B
Anti-DoS capability for malformed packets	A-	B+	D	B-	A
Interface utility/speed	B-	B	C	A	A
Signature customization	A-	C-	A	A	A
Setup/deployment	C	B	C-	B-	A
Final Score	**B** Solid detection tool; falls somewhat short on usability.	**B+** Closed signature base offset by stellar detection.	**C+** Signature customization is excellent; otherwise trails the pack.	**B+** An excellent choice for customizing signatures and tuning blocking to policy, but requires significant tuning.	**A-** Outstanding in almost every category; could improve evasion tactics detection.

*Sourcefire is being acquired by Check Point Software Technologies.

Setup and Deployment

We worked with technical support to help us through each of the installations. The Top Layer product was the easiest to set up and deploy; the appliance came with a complete setup guide, administration manual and a virtual front panel in the GUI application. Using the front panel configuration feature, we were able to set up the management port, configure the IPS port bridge and apply signatures with little of the guesswork required for other products.

ISS was pretty easy to plug into our network and tweak with no real problem, but lacked Top Layer's intuitive deployment GUI.

By default, the Sourcefire product operates as an inline IDS, detecting attacks but not blocking anything. We needed about a half-hour on the phone with Sourcefire technical support to create a reasonable configuration.

Cisco's technical support guided us through a set of command-line scripts to make the product work in our environment. While not too complicated, this hour-long walk through an arcane command-line session made deployment less smooth than with other products.

Radware was problematic. When applying the default rule set for a corporate gateway device, the appliance would not block any of our attacks. We spent more than two hours on the phone with Radware troubleshooting this dilemma. We finally had to apply signatures to the interface by enabling all the corporate policies (Gateway, LAN, DMZ, etc.) to get the Radware device to block anything.

Final Score

Top Layer gets our overall nod, with its solid detection capabilities and crisp management interface. Close behind were Sourcefire and ISS, reflecting two very different philosophies. Sourcefire features great customizability of both workflow and signature sets, but you'll need adequate staff resources to create custom configurations that block adequately in your environment. If you lack the resources for fine-tuning signatures, the ISS product's out-of-the-box blocking and anti-evasion capabilities are top-notch.

Cisco's product did very well in our evasion and DoS tests, and performed reasonably well elsewhere. Radware lagged in each of our tests.

The one thing that really surprised us, however, was how two security engineers could bypass most of these IPS devices within a few hours of testing. We strongly recommend setting up a similar test bed for these tools while you pilot them for your enterprise. Your feedback to the vendor plays a critical role in the improvement of the product space.

Contributing editor Ed Skoudis, CISSP, is cofounder of security consultancy Intelguardians and author of Malware: Fighting Malicious Code *and* Counter Hack Reloaded, *the soon-to-be-released update to his best-selling book,* Counter Hack.

Mike Poor is a senior security consultant at Intelguardians, where he specializes in penetration tests, security audits and architecture reviews. Send your thoughts on this article to feedback@infosecuritymag.com.