

April 8, 2009

# If You Don't Have IPS, You Deserve To Be Hacked

by John Kindervag  
for Security & Risk Professionals



April 8, 2009

## If You Don't Have IPS, You Deserve To Be Hacked

by **John Kindervag**

with Robert Whiteley and Margaret Ryan

### EXECUTIVE SUMMARY

In the beginning was the alert, but the alert drove everyone crazy so the IT staff quit looking at the logs. That long-gone era represents the glory days of intrusion detection systems (IDS). Clearly, the security industry has evolved beyond the time when IDS provided any real security benefit to an organization. But intrusion detection refuses to die. Chances are that you are still using it, even though it is common knowledge among security and risk management professionals that IDS is not adequate or proactive enough for modern networks. On the other hand, intrusion prevention systems (IPS) are a mature and robust technology that you should deploy as the keystone of your threat management strategy. Refusing to deploy IPS will increase your likelihood of being hacked — which you will deserve — and leave you without a necessary modern control within your security architecture.

### TABLE OF CONTENTS

#### 2 **IDS: The Boy Who Cried Wolf**

IDS Brings Its Baggage To IPS

IPS Is More Than Just The Evolution Of IDS

#### 4 **Why IPS Should Be Deployed In Every Network**

IPS Is Defined By Proactive Security Features

IPS Has Created A Paradigm Shift That Hardens The Network And Reduces The Staff Burden

#### 7 **Properly Deploying IPS Means Placing It In Five Key Points In Your Network**

Placement Of IPS Sensors Should Be Based On All Ingress Traffic Points

#### 10 **IPS Is Converging With Other Network Security Technologies**

#### RECOMMENDATIONS

#### 11 **Emphasize Performance And Scalability, Reporting, And Management**

#### 12 **Supplemental Material**

### NOTES & RESOURCES

Forrester interviewed eight vendor companies, including Check Point Software Technologies, IBM Internet Security Systems, Juniper Networks, Palo Alto Networks, SonicWALL, Sourcefire, TippingPoint Technologies, and Top Layer Networks.

#### **Related Research Documents**

["Threat Alert: Wireless Is The New Internet"](#)  
August 12, 2008

["Network Intrusion Prevention Comes Of Age"](#)  
June 23, 2005

["Why Three Out Of Four Network Intrusion Detection Deployments Fail"](#)  
September 4, 2002

## IDS: THE BOY WHO CRIED WOLF

In the well-known fable *The Boy Who Cried Wolf* (also known as *The Shepherd Boy and the Wolf*), Aesop describes a young shepherd boy who takes pleasure in punking the people of his little town by yelling “wolf” and then enjoying a laugh as they rush out to help him fend off a nonexistent attack. After just a few false alarms, the townspeople refuse to respond anymore, and when a wolf actually appears and attacks the sheep, the boy’s cries go unheeded. Aesop ends his fable with a moral: “There is no believing a liar, even when he speaks the truth.”<sup>1</sup>

The foolish shepherd boy serves as an apt metaphor for intrusion detection. During the heyday of IDS, so many false alerts were sent by these systems to security analysts that new alerts were routinely ignored. IDS became a checkbox and not a tool, and the systems were deployed simply because their deployment was considered a best practice.<sup>2</sup> As the technology matured, security staff was gun-shy and refused to embrace new technologies such as IPS, fearing the same false-positive/false-negative problems that plagued IDS. Today, however, the technology has matured to the point where IPS devices function nearly flawlessly and provide a significant uplift to any organization’s security posture. IPS is the most advanced security tool in the arsenal right now, and it provides a proactive security control for any network. A network that is properly protected by IPS devices is unattractive to hackers. Because cyber-crimes are often opportunistic, most attackers will not expend the energy to penetrate an IPS-protected network and will move on to softer targets. Not implementing IPS is an open invitation to be hacked.

## IDS Brings Its Baggage To IPS

The bad reputation that IDS had in the security community brings undeserved baggage to the world of IPS. IPS is unfairly compared to IDS and is meanwhile a superior and valuable technology. IPS will succeed because IDS:

- **Didn’t stop anything.** The passivity of IDS is its fatal flaw. In his seminal book *Secrets & Lies*, security guru Bruce Schneier compares IDS to an incompetent medic “who looks over your bleeding body, saying: ‘That looks like a sucking chest wound. I’d get that checked if I were you.’ IDS is not a substitute for good proactive security.”<sup>3</sup> In real life, IDS devices didn’t stop anything. Shuns and Transmission Control Protocol (TCP) resets don’t count. Early on, attackers learned that they could force IDS to create an internal denial-of-service condition on routers and firewalls by using shuns — the creation of temporary dynamic access control lists (ACLs) or firewall rules. More than one company brought its own network down through the reliance on shuns.

Attackers also realized that TCP resets, where a reset (RST) flag is sent to both ends of a TCP connection, could easily be thwarted by using Universal Data Protocol (UDP). Attacks such as SQL Slammer became famous because they could not be stopped by IDS devices.<sup>4</sup>

- **Generated too many false alerts and too much unusable data.** Since all IDS could really do was send out an alert, the cry of “wolf” was so constant that IDS analysts could not respond to each alert. In addition, the IDS generated tons of other data. While this information may have been relevant or interesting to someone in the organization, security teams did not have the bandwidth to deal with it. In reality, the true value of IDS may be in forensics, where examiners can wade through this dense data to find clues to cyber-crimes or other malicious behavior.
- **Involved manual processes.** IDS had so little intelligence that it was the job of the security engineer to tune each device manually. IDS devices primarily used some kind of pattern matching, and each signature had to be manually enabled or disabled. For example, if your network did not have any Linux devices, then attack signatures for Linux hosts would be disabled. In practice, this didn't work very well. The attacks and signatures were so complex that it was often impossible to determine the value of enabling or disabling a particular signature.

This led to the development of two schools of thought in the world of IDS management:

1. **The “let's turn almost everything on because we're afraid we'll miss something” school.**

The problem here was that turning on too many signatures ate up memory and impacted performance. Plus, this methodology meant that the IT and security staff would spend a lot of time running around with little to show for it.

2. **The “let's turn almost everything off because these dangd alerts are useless anyway” school.**

In this case, the network team might as well not have purchased IDS. Also, the security team ran the real risk of suffering an attack of which they might have otherwise been alerted in time to mitigate damage. The IDS became much easier to maintain. But at what cost to the enterprise?

### IPS Is More Than Just The Evolution Of IDS

IPS suffers from the legacy of its older, duller IDS sibling. As a habitual liar, IDS reflected poorly on the entire family. It became clear that IDS devices lacked the intelligence to effectively protect enterprise resources. Stop-gap measures such as event correlation systems were taking too long to develop, causing IDS products to get a bad reputation with IT staff. When IPS technologies began to come out, they were seen as essentially the same thing as IDS — indicated by the slash in IDS/IPS. The security world just assumed that IPS would suffer from the same flaws as its predecessor IDS, but that has proven to be untrue. Unlike IDS, IPS is:

- **More than the evolution of IDS technology.** While IPS shares some technological DNA with IDS, IPS is not just the next generation of IDS. In fact, it may be unfair for these two technologies to even share so many letters in their acronyms. The best IPS devices were built from the ground up and share little, if any, technology from the past.

- **Not just a second NIC added to an IDS.** It takes more than just adding a second network interface card (NIC) to an IDS to make an IPS. Many legacy IDS companies have tried to slap another card in their box, ramp up the marketing machine, and announce with great fanfare their new IPS. Fortunately, most of these attempts at repackaging snake oil have failed — and for good reason. There are a couple of important distinctions that limit the shoehorning of IDS software and technology in an IPS scenario.
- **Not limited to unidirectional traffic flows.** IDS devices were designed to sit off of a network tap or switch SPAN port and listen to the unidirectional traffic that came to it. The IDS then tried to assemble the entire flow and determine if the traffic was good or bad. Attackers quickly learned ways to get around IDS devices.<sup>5</sup> Tools such as fragroute were created to exploit these techniques.<sup>6</sup> In order to be an effective control, IPS devices must understand both sides of the IP conversation. IDS devices do not have this ability because they are not inline and do not see both the inbound and outbound traffic flows.
- **Able to understand traffic state.** Another problem with unidirectional traffic is that the IDS device has difficulty understanding the state of the packet. State involves numerous parameters such as the source and destination addresses of the packet, the ports that the packet is using, and the protocol information of the packet. At best, an IDS sees inbound and outbound traffic as two separate flows and must try to infer the packet state. In contrast, IPS devices see both sides of the communication and can statefully keep track of packets as they flow in real time. This is a huge advantage in understanding the packet and reduces false alerts significantly.
- **More comprehensive than emerging NBAD tools.** Network behavior anomaly detection (NBAD) is a type of control that is often considered to be part of the intrusion detection space. These products take flow data, such as NetFlow and sFlow, and do statistical analysis on it. NBAD software makes some decisions about whether that traffic is probably good or probably bad and then fires off an alert based on that. However, NBAD is not proactive enough to meet the needs of most enterprises. These products have not been especially successful in the security space and are now transitioning into a new space called network behavior analysis (NBA). NBA does not try to act like a security control and focuses instead on what flow data is good at: providing operational analysis for troubleshooting application and network performance issues.

## WHY IPS SHOULD BE DEPLOYED IN EVERY NETWORK

Luckily today, the IDS baggage has almost entirely been eliminated from modern IPS. Advances in computer hardware and software technology have greatly benefited IPS vendors. All of these advances have converged to the point where the maturity and effectiveness of IPS solutions are no longer questioned.<sup>7</sup> Given today's frightening threat environment, every security manager should deploy IPS appliances and avail themselves of the most proactive network security protection that is currently available.

## IPS Is Defined by Proactive Security Features

So what is IPS? IPS is a security technology that shares four basic features:

- **IPS is inline.** In order to understand bidirectional traffic flows and packet state, an IPS device must be inline. At Forrester, we occasionally hear about IPS vendors that function out of band. Close examination reveals that those products are really IDS solutions and that the preventative measures are merely shuns and resets. IPS hardware generally has two network interfaces per sensor and views all traffic traversing a particular network segment.

Most enterprise-class IPS appliances work in a Layer 2 transparent bridge mode so that network designs are not impacted. In this way, these devices are a bump in the wire that cannot be seen by attackers because there are no IP addresses on the bridged interfaces. Attackers will often scan particular network segments to try and determine the type of security controls that may be in place. A bridged IPS is stealthy and prevents active reconnaissance. Also, a bridged deployment means that networks won't have to be redesigned to accommodate IPS sensors.

- **IPS has the ability to block traffic in near real time.** IPS appliances must stop the bad stuff on the wire. This means that IPS cannot allow any threat traffic through the device into the network. This requires speed and intelligence. Prevention is the key word. The best IPS products are sophisticated enough to process a tremendous number of packets without buffering or dropping, while determining immediately if a packet contains a threat or not.

This is achieved through robust and highly evolved software sitting on very fast hardware with the built-in intelligence of the best security engineers in the world. There are big claims being made today, but many large organizations have deployed this technology and can testify to its true ability to stop bad traffic before it can damage important resources.

- **IPS has few, if any, false positives or negatives.** A convergence of improved software, faster hardware, and the ability to move beyond simple signature means that top IPS vendors rarely, if ever, have a problem with false alerts.

Because the system looks at the entire packet through Layer 7, it can internally correlate all of the information about the packet state, flows, payload, and other elements in near real time to know with great certainty whether or not a packet should be allowed to pass. Based on discussions with clients, Forrester feels that the fear of false positives and negatives is much more common than an actual false alert. In fact, Forrester has not had any clients using true IPS devices report problems with false alerts.

- **IPS is low-latency and low-impact.** Because IPS appliances are inline, it is imperative that they do not adversely affect the performance of the network. They must have the ability to allow traffic to pass if a sensor fails. They must be fast enough so that applications perform optimally.

This is especially important in networks using real-time traffic, such as voice over IP (VoIP). IP telephony is prone to jitter and other forms of call degradation whenever latency is induced. Modern IPS technology is fast enough that latency is typically not an issue in VoIP-enabled networks.

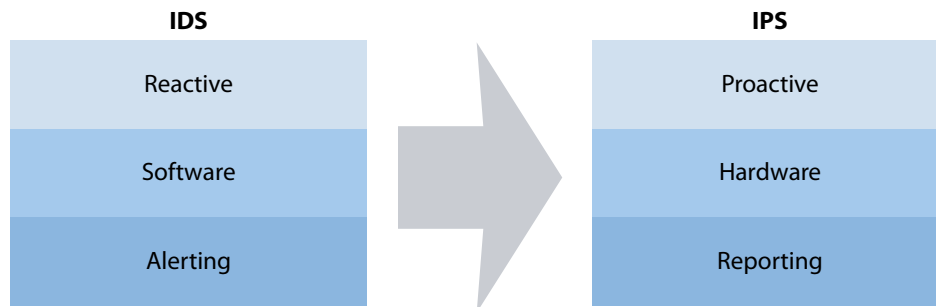
Low impact also means ease of management and updates. An IPS must make the security team's job easier, not harder. To this end, most of today's IPS technology provides centralized, graphical user interface (GUI)-based administration of multiple devices in a single interface. Most will also provide automatic software and signature updates with new filters and rules having a default enable or disable setting that is already built in. This default mode is valuable because the vendor will often have considerably better insight into whether or not a signature should be enabled.

### IPS Has Created A Paradigm Shift That Hardens The Network And Reduces The Staff Burden

As IPS technology has become increasingly trusted among large corporate networks, it has signaled a noteworthy paradigm shift in information security from (see Figure 1):

- **Reactive to proactive.** Because IPS devices are inline and able to stop bad stuff on the wire, they have created an expectation that security should be proactive. In modern information security, alerts should be reserved for saying: "Hey, look at the cool attack we just stopped from getting into our network."
- **Software to hardware.** IDS products were software only and therefore performance-challenged. The IPS world began when vendors realized that general x86 hardware was not fast enough. Those early IPS pioneers invested vast sums of money in creating custom silicon such as purpose-built application-specific integrated circuit (ASIC) and field-programmable gate array (FPGA) chips.<sup>8</sup> This will change as new silicon manufacturers recognize the need for this type of high-speed chip. Also, IPS vendors may be able to eventually leverage off-the-shelf chips as general-purpose chip manufacturers move toward 10, 20, or even 80 cores.
- **Alerting to reporting.** As alerts become decreasingly necessary in the IPS world, reporting becomes more important. Many companies have an automatic daily report generated to document attacks that were blocked. IPS devices eliminate some of the need for security information management (SIM) as event correlation becomes less desirable because attacks do not typically get to the internal network where they can be correlated. Another driver of this trend is regulatory compliance. The data contained in IPS is often useful for validating compliance objectives and is highly valued by auditors for this purpose.

**Figure 1** IPS Created A Paradigm Shift That Hardens The Network And Reduces The Staff Burden



46812

Source: Forrester Research, Inc.

### PROPERLY DEPLOYING IPS MEANS PLACING IT IN FIVE KEY POINTS IN YOUR NETWORK

It is important to design IPS placement based on traffic flows and not physical segments. A more efficient and cost-effective deployment can be created by looking at how packets traverse the network. For example, all traffic from a particular demilitarized zone (DMZ) may cross an internal IPS sensor. In that case, adding IPS to that DMZ segment would be redundant. It is best to look for or create choke points where traffic is aggregated and place sensors at those natural points of aggregation.

#### Placement Of IPS Sensors Should Be Based On All Ingress Traffic Points

It is important to mandate that all ingress (inbound) traffic run through a segment of inline network intrusion protection. Trace packet flows to ensure that each packet entering your network passes through at least one IPS sensor.

It may also be beneficial to put sensors on traffic flowing between internal resources, but budget constraints often limit the ability to do this. Even though many reports say that most attacks come from the internal network, these internal trusted user attacks are not the types that use hacking tools to do the job. No IPS currently has the ability to stop trusted employees from stealing information that they have legitimate access to. Therefore, hacking-type intrusions are much more likely to come from the external network than the internal network, and IPS devices are uniquely positioned to stop this traffic in its tracks. There are several basic IPS deployment scenarios that can be adapted for any network. Consider placing the IPS (see Figure 2):

- **Behind the primary Internet firewall to protect the core network.** The first place to put an IPS sensor is directly behind the Internet firewall. The Internet is constantly scanned for potential exploitable vulnerabilities by opportunistic attackers. An automated scan may generate an automated attack or, at the very least, notify the potential attacker that your

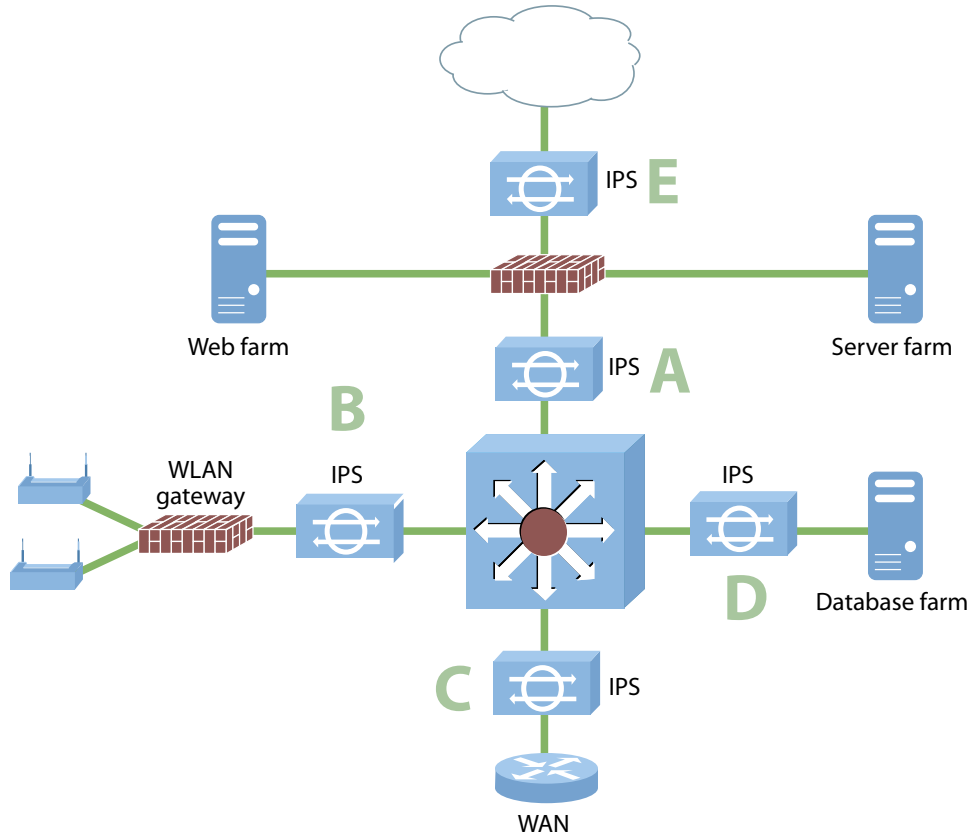
network is a prospective target. There is some thought that the first IPS sensor should go in front of the firewall to protect the firewall from attack. However, modern firewalls are very robust and are able to filter out a lot of noise that the IPS would otherwise have to process. This Internet background radiation should be prefiltered by the firewall, if possible, to increase IPS performance. This placement will also protect decrypted site-to-site or remote-access virtual private network (VPN) traffic to ensure that it is clean. VPNs should always sit in the DMZ and should never bypass the primary gateway firewall or be bridged directly onto the internal network.

Any networks prone to denial of service (DoS) types of attacks will conversely need to place an IPS sensor with DoS attack mitigation abilities outside of the firewall to protect against the threat of various DoS attacks.

- **Behind the WLAN gateway to ensure clean wireless traffic.** Wireless networks are a particularly attractive attack vector, and extra effort should be made to proactively protect them.<sup>9</sup> Wireless encryption can protect the outside of the wireless transmission. Also, wireless IPS sensors can protect against known wireless attacks, and wireless firewalls can protect against unauthorized access. But wireless is moderately easy to attack, and only a network IPS can ensure that the traffic contained in the wireless payload is actually clean.
- **Behind the WAN router to protect against remote office attacks.** One often-overlooked point of network ingress is the corporate wide area network (WAN). Because it is a private network, potential threats on the WAN may not be addressed or protected. For example, remote offices may not have as robust a network security as the main network and may be more easily breached. Once on the remote office, an attacker may be able to come into the primary network as an authorized user and attack critical resources with impunity.
- **In front of databases and other mission-critical servers.** Because IPS devices look at the entire packet up through the application layer (Layer 7), they can be effective tools for protecting internal mission-critical servers and applications such as databases, domain name system (DNS) servers, and file servers. These resources need to be protected from internal and external attacks. By deploying IPS internally in front of mission-critical assets, you can ease into comprehensive internal protection. As trust paradigms change, internal networks will be protected in the same manner as external networks.
- **In front of the firewall to protect DMZs.** If your network has multiple DMZs, many IPS vendors will tell you that you need an IPS sensor on every DMZ. This is not true. It is possible to protect the entire firewall, regardless of the number of DMZs, with just two IPS sensors. By mapping traffic flows and applying flow-based IPS enforcement, a simpler and more effective design can be developed. This is because all traffic moving across the firewall will flow through either the internal or the external sensor in real-world use. There should be no

DMZ-to-DMZ traffic by default. If there is inter-DMZ traffic across the firewall, then those interfaces are effectively the same DMZ, and therefore a DMZ redesign is in order. By properly thinking through DMZ architectures, you can create a cost-effective and more operational IPS deployment.

**Figure 2** The IPS Should Be Placed In Five Key Choke Points In The Network



- 1: IPS behind firewall to protect core
- 2: IPS behind WLAN gateway to ensure clean WL traffic
- 3: IPS behind WAN router to protect against remote office attacks
- 4: IPS in front of databases and other mission-critical servers
- 5: IPS in front of firewall to protect DMZs

## IPS IS CONVERGING WITH OTHER NETWORK SECURITY TECHNOLOGIES

The days of detection-only devices are coming to an end. The fear, uncertainty, and doubt (FUD) of the IPS shutting down the network are over. Adoption at major companies is so widespread that the technological laggards are sure to follow soon. In the near future, it may be impossible to get a pure-play IDS that isn't just open source software. The path forged by IPS solutions has had a large impact on the way security products are created. Increasing numbers of vendors now realize the value of high-speed hardware. IPS appliances were the first generation of intelligent devices that seemed to just work without constant human intervention. The pioneering features that came out of this industry such as automatic updates and vendor-recommended policy settings transformed the top players in this space into "set it and forget it" products in many enterprise networks. These types of customer expectations will continue to grow, forcing IPS vendors to evolve and improve as technologies change and to adapt to the new and agile threat landscape. Forrester sees more IPS being deployed in the internal network as IPS functionality begins to merge with network access control.

Additionally, other threat prevention technologies such as Web application firewalls seem to be converging with traditional IPS. We expect that the future will provide full Layer 7 prevention capabilities in a single box, without protocol breakouts, so that one appliance protects network and Web resources. Other factors to include are the improved speeds in network processors and merchant silicon that will certainly make IPS more affordable in the future. As IPS becomes more cost-effective, we anticipate that it will be deployed in many more places throughout enterprise networks. Recent attacks have shown that the lack of visibility regarding the happenings on the internal network can be highly dangerous and embarrassing.<sup>10</sup> By deploying internal IPS solutions, security teams greatly uplift their ability to stop internal attacks before they can do damage to the network or the company's reputation.

There are other innovations that will impact the future of IPS and its descendants:

- **Higher-speed networks.** It wasn't long ago that a 100 MB local area network (LAN) felt fast. Now, it is not uncommon to see gigabit links to the desktop and 10 Gb uplinks in the core. Researchers continue to push the limits of Ethernet, and there are dreams of terabit networks.

With additional speed comes additional traffic. The users' need for bandwidth is insatiable. If the past is any guide, these types of advancements will need improved security because they will enable new threats and attacks. IPS technology will be the foundation of future high-speed security devices that are designed to meet the needs of the next generation of networks.

- **Unified communications.** Convergence is the C-level executive's favorite word. The idea that everything will be on the same network and that everyone will be able to talk to each other is IT's siren song. Companies rush headlong into convergence projects and pull voice, video, and data into a single network, often giving little thought to the security implication of their actions.

This mash-up of protocols typically involves a fair bit of jury-rigging and can often open unseen or unexpected holes for potential attackers.

Technologies that were never meant to be packetized, such as voice, are chopped up into little bits and bytes and then pushed kicking and screaming onto the network. The resulting protocols can be complex, fragile, ugly, and difficult to properly secure. The intelligence and flexibility of IPS technology is best positioned among all of today's security tools to protect these types of converged networks.

- **Web 2.0 and social networking.** Collaboration is another top-10 MBA buzzword. Cultural revolutions are being spearheaded by Facebook, MySpace.com, Twitter, and other Web 2.0 collaborative worlds. Companies are rushing to find ways to exploit this revolution and its incumbent technology to drive more business. The idea of user-created content is an anathema in the security world. For security people, users are the problem. Giving them increasing access to applications and data is appalling to many security professionals. There are potentially tremendous new risks that can come from Web 2.0 technology. Allowing client-side code, such as JavaScript, to be executed in the end user's browser is a scary thought for many security people, but an exciting and potentially lucrative thought for those with more nefarious intentions.

Structured query language (SQL) injection attacks, cross-site scripting (XSS), and cross-site request forgery (CSRF) are common problems that plague Web 2.0 sites.<sup>11</sup> Because IPS devices see all of the traffic in any stream and have Layer 7 visibility, they will be forced to add new protections to keep Web 2.0 applications protected.

## RECOMMENDATIONS

### EMPHASIZE PERFORMANCE AND SCALABILITY, REPORTING, AND MANAGEMENT

The development of true IPS technology allows security managers to see deep inside the packet and provides the built-in intelligence to effectively block all known attacks and many new ones. As the threat climate changes, it is important that the network security protections change as well. Today, IPS devices provide the highest level of proactive protection available. As you update your security architecture, implement IPS devices with:

- **Performance and scalability to handle increased bandwidth and attack sophistication.** Because of the interconnectedness of all networks, any network or host could theoretically be attacked at any time. There are no good neighborhoods on the Internet. As networks become faster and more distributed, solid proactive controls such as IPS make your network a less attractive target to cyber-criminals. This requires an IPS that can scale to at least 10 Gbps. Vendors such as Juniper Networks, Sourcefire, and IBM Internet Security Systems are among the best at scalability.

- **Reporting features that help with rising internal attack trends.** With a declining economy and increased corporate layoffs, internal attacks from disgruntled employees are anticipated to grow.<sup>12</sup> Most internal networks are wide open to insider abuse, attack, and fraud. By placing IPS devices on the internal LAN, enterprise security teams can anticipate, see, and stop insider attacks. Look at the reporting capability of the tool and make certain that it has the ability to provide custom reports for C-level executives, auditors, and security analysts. Also, internal IPS deployments require greater port density. Vendors such as TippingPoint Technologies and Palo Alto Networks work well in protecting internal networks and have excellent combinations of port density and reporting features.
- **A management interface with Web 2.0 features.** Look closely at the management interface when evaluating IPS products. The care and feeding of any security product is a long-term cost that is often overlooked in the evaluation process. IPS management interfaces should provide centralized management of multiple devices throughout a geographically dispersed network. The interface should be intuitive and understandable and take advantage of new GUI technologies such as personalized dashboards. Stay away from older, antiquated devices that require the use of command line interfaces because they will be less agile and more prone to misconfiguration. Check Point Software Technologies, Top Layer Networks, and SonicWALL have intuitive management interfaces.

## SUPPLEMENTAL MATERIAL

### Companies Interviewed For This Document

|                                   |                           |
|-----------------------------------|---------------------------|
| Check Point Software Technologies | SonicWALL                 |
| IBM Internet Security Systems     | Sourcefire                |
| Juniper Networks                  | TippingPoint Technologies |
| Palo Alto Networks                | Top Layer Networks        |

## ENDNOTES

- <sup>1</sup> This is from George Fyler Townsend's translation of *The Shepherd Boy and the Wolf*. Source: George Fyler Townsend, *Aesop's Fables*, Doubleday, 1968.
- <sup>2</sup> The problem of false alerts was a significant factor in stalling the growth of IDS. See the September 4, 2002, "[Why Three Out Of Four Network Intrusion Detection Deployments Fail](#)" report.
- <sup>3</sup> Source: Bruce Schneier, *Secrets & Lies: Digital Security in a Networked World*, John Wiley & Sons, 2000.
- <sup>4</sup> SQL Slammer was a legendary single packet UDP worm that exploited a buffer overflow vulnerability in Microsoft SQL Server and Microsoft SQL Server Desktop Engine (MSDE). It launched on January 25, 2003, and infected approximately 90% of vulnerable target hosts within 10 minutes of its launch. It could not be stopped by IDS devices because they had no way of proactively blocking UDP. There are numerous

detailed papers on the attack including "Inside the Slammer Worm." Source: David Moore, Vern Paxson, Stefan Savage, Colleen Shannon, Stuart Staniford, and Nicholas Weaver, "Inside the Slammer Worm," *IEEE Security & Privacy*, July/August 2003.

- <sup>5</sup> Much has been written regarding how attackers can evade IDS sensors to attack the protected resources, notably including "Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection." Source: Thomas H. Ptacek and Timothy N. Newsham, "Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection," Secure Networks, January 1998 ([http://insecure.org/stf/secnet\\_ids/secnet\\_ids.html](http://insecure.org/stf/secnet_ids/secnet_ids.html)).
- <sup>6</sup> Fragroute is an open source tool specifically designed to craft packets that will evade IDS and firewall devices. Source: Monkey.org (<http://monkey.org/~dugsong/fragroute/>).
- <sup>7</sup> As recently as 2005, Forrester still recognized struggles in the IPS market. While advancements had been made, the technology was not yet mature enough to fully endorse it. See the June 23, 2005, "[Network Intrusion Prevention Comes Of Age](#)" report.
- <sup>8</sup> Two types of silicon, known as ASIC and FPGA, have enabled the creation of the IPS space. ASIC chips are custom-designed single-purpose silicon chips. ASIC chips are extremely fast but are not reprogrammable. They are expensive, and that cost functions as a barrier to entry in the IPS market. FPGA chips provide speed approaching that of custom ASIC chips but can be reprogrammed in the field. These chips are often used by high-end IPS devices for storing filters and doing signature matches because the FPGA chips can be reprogrammed when signature updates come out.
- <sup>9</sup> Wireless networks may have been involved in some of the large recent data breaches. For more detailed information on wireless security, see the August 12, 2008, "[Threat Alert: Wireless Is The New Internet](#)" report.
- <sup>10</sup> Credit card processor Heartland Payment Systems announced that its network had been compromised and that it had suffered a potentially large data breach. According to its own statements, the attack occurred in the fall of 2008, but the company did not discover it until contacted by the credit card brands. Heartland Payment Systems' official breach Web site contains further information. Source: Heartland Payment Systems (<http://www.2008breach.com/>).
- <sup>11</sup> The OWASP Foundation tracks Web application security issues. The OWASP Top 10 list is the industry standard for categorizing Web-based attacks. Source: OWASP Foundation ([http://www.owasp.org/index.php/Top\\_10\\_2007](http://www.owasp.org/index.php/Top_10_2007)).
- <sup>12</sup> One notable example is Rajendrasinh Makwana, a former Fannie Mae IT contractor who was indicted for planting a malware bomb that would have damaged his former employer's network if it had gone off. Source: Larry Dignan, "Fannie Mae IT contractor indicted for planting malware; Mortgage giant didn't revoke server privileges," *ZDNet*, January 29th, 2009 (<http://blogs.zdnet.com/BTL/?p=11905>).

# FORRESTER<sup>®</sup>

Making Leaders Successful Every Day

## Headquarters

Forrester Research, Inc.  
400 Technology Square  
Cambridge, MA 02139 USA  
Tel: +1 617.613.6000  
Fax: +1 617.613.5000  
Email: [forrester@forrester.com](mailto:forrester@forrester.com)  
Nasdaq symbol: FORR  
[www.forrester.com](http://www.forrester.com)

## Research and Sales Offices

|           |                 |
|-----------|-----------------|
| Australia | Israel          |
| Brazil    | Japan           |
| Canada    | Korea           |
| Denmark   | The Netherlands |
| France    | Switzerland     |
| Germany   | United Kingdom  |
| Hong Kong | United States   |
| India     |                 |

*For a complete list of worldwide locations, visit [www.forrester.com/about](http://www.forrester.com/about).*

For information on hard-copy or electronic reprints, please contact Client Support at +1 866.367.7378, +1 617.613.5730, or [clientsupport@forrester.com](mailto:clientsupport@forrester.com).

We offer quantity discounts and special pricing for academic and nonprofit institutions.

Forrester Research, Inc. (Nasdaq: FORR) is an independent research company that provides pragmatic and forward-thinking advice to global leaders in business and technology. Forrester works with professionals in 19 key roles at major companies providing proprietary research, consumer insight, consulting, events, and peer-to-peer executive programs. For more than 25 years, Forrester has been making IT, marketing, and technology industry leaders successful every day. For more information, visit [www.forrester.com](http://www.forrester.com).