



INSIDE NIP HYP

There's a sales blitz being launched by network intrusion-prevention suppliers, while skeptical pundits drop 'don't buy it' bombs. Take cover, and be vigilant



Battle lines have been drawn, and volleys are being lobbed between the analyst and vendor camps. In dispute: Whether intrusion prevention is out of commission or the next network security salvation. On one side, Gartner has cast intrusion detection into its "Trough of Disillusionment," saying the tech has stalled and calling for these functions to move into firewalls. Meanwhile, intrusion-prevention product vendor ForeScout Technologies vows to identify and block attackers "with 100 percent accuracy."

Call us Switzerland, but we say neither group has a lock on the truth. NIP (network intrusion-prevention) systems probably won't protect your network from the next zero-day exploit or troublesome worm, but they're not a waste of time or money, either. A NIP system is a safeguard that may protect you from known attacks and alert you to suspicious activity. Think intrusion detection with the ability to block traffic.

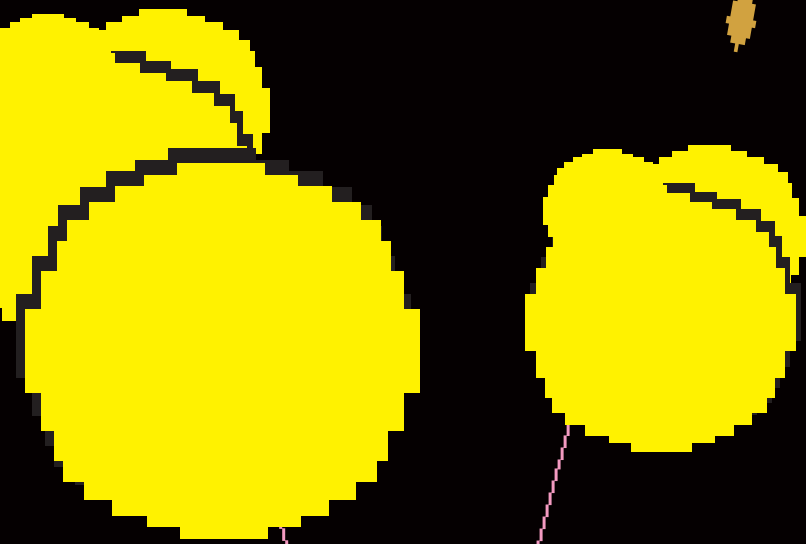
Our position puts us in the minority: Though we think NIP systems can enhance an existing security infrastructure, we don't consider integrating intrusion prevention and firewalls into a single unit a desirable goal.

Firewalls have a largely static configuration: Firewall administra-

By Mike Fratto

40	Executive Summary	40	E-Mail Poll Results	42	Focus on the
	Tested	56	Lessons Learned		

E



NIP

the Endpoint

47

NIP Attacks in the Bud

50

How We

tors define what is acceptable traffic and use the features of the firewall to instantiate this policy. Some firewalls provide better protection features than others—for example, an HTTP application-level proxy is far superior to an HTTP stateful packet-filtering firewall at blocking malicious attacks—but the basic idea is the same: Your firewall administrator can be confident that only allowable traffic will pass through. If you have doubts about your firewall, get a new one from a different vendor, send your firewall administrator to Firewall Admin 101, or get a new firewall administrator.

Not surprisingly, when we asked you why you're not blocking traffic using NID (network-based intrusion-detection) systems, 63 percent of you said you use a firewall to determine legitimate traffic (see E-Mail Poll results, starting below).

But people make mistakes, so misconfigured firewalls are a common source of network insecurity. This simple fact has been used as a selling point for both intrusion-detection and -prevention systems, with vendors claiming their products will alert you to, or block, attacks that do get through.

The answer: Instead of layering on more hardware, solve the fundamental problem of misconfiguration. Unfortunately, though, it's not that simple. If you're enforcing traffic policy on your network using a stateful packet-filter firewall—such as Cisco Systems' PIX, Check Point Software Technologies' FireWall-1 or NetScreen's eponymous product—without security servers or kernel-mode features enabled, you should know that application-layer exploits, such as server-buffer overflows or directory-traversal attacks, will zoom right through. Stateful packet filters stop at Layer 4.

Application-proxy firewalls, like Secure Computing's Sidewinder G2 Firewall and Symantec's Enterprise Firewall, can block some attacks that violate specific protocols, but let's face facts: Protection is limited to a handful of common protocols; the rest are not supported through a proxy, or are supported through a generic proxy, which is no better than a stateful packet filter.

Still, NIP is not a replacement for firewalls and won't be in the foreseeable future. Why? The fundamental problem is false positives—the potential to block legitimate traffic. Before you can prevent attacks, you have to detect them, but NIP systems rely on intrusion detection, which is hardly an exact science. A properly configured firewall will allow in only the traffic you want, and you can bet the farm on that. We need to feel this same confidence in IDSs before we can believe in NIP systems, but IDS vendors have employed lots of talented brain cells trying to raise detection accuracy, and they're nowhere close to 100 percent.

Incoming!

Despite these caveats, we believe a properly tuned NIP device can be instrumental in warding off most malicious traffic that gets past your firewall.

There are several ways to block malicious traffic: If the NIP device is inline, offending packets can be

Executive Summary

NIP SYSTEMS

REMEMBER STAR WARS? Not the movie, the ballistic missile defense system. In 1983, President Reagan was bullish on his vision of gigantic, high-tech lasers that would vaporize any missile daring to enter U.S. airspace.

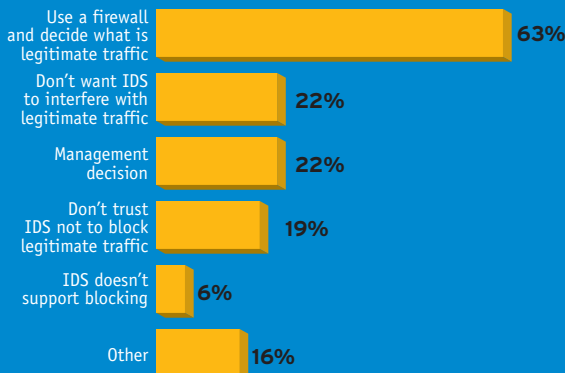
Listen to NIP system vendors, and you may have flashbacks to that scary time. Back then, it was the Democrats who questioned spending billions of dollars on the off chance of being able to shoot down an object smaller than a Volkswagen Beetle streaking through space at 10,000 miles per hour. Today, analysts and some industry pundits are taking aim at the very legitimacy of the intrusion-prevention vision and suggesting that the functionality ought to be incorporated into firewalls.

We disagree, at least for the foreseeable future. NIP systems have a place in a comprehensive security scheme. At the very least, they can buy you time to patch. We tested the NetScreen-IDP 500 and Network Associate's McAfee IntruShield 4000 in our Syracuse University Real-World Labs® and found that each did a good job blocking known attacks, though we did need to be selective about blocking so as not to shun legitimate traffic.

After firing our arsenal of malicious packets at the devices in a controlled environment, then deploying them on our live network, we gave the IntruShield 4000 our Editor's Choice award. Though it's much pricier than the IDP 500, it showed fine performance up to 1.2 Gbps, with average latency of just 1 to 2 ms.

E-MAIL POLL

If you don't block traffic using your network-based IDS, why not?



Source: NETWORK COMPUTING E-Mail Poll, 479 respondents

dropped silently, causing the connection to fail. Whether or not the connection is inline, the session can also be summarily dropped by sending TCP Resets or ICMP Unreachable messages to the client, server or both. Or, the offending IP address can be shunned—blocked—for a specific time period.

Just be sure that when blocking is enabled, you know what you're doing. When we asked what it would take to make you use blocking, 57 percent of you cited needing assurance that there would be no false positives or that traffic would be blocked effectively. These are legitimate concerns. During our tests of NIP devices (see "NIP Attacks in the Bud," page 47), only a subset of signatures were defined enough to not alert on false positives consistently. These signatures were primarily TCP-based and violated a protocol or utilized known malicious strings.

Patches, It's Up to You

We have to bring up the "P" word. It's easy for us to beat you with the patch stick, but the truth is, many of our production systems are woefully out of date because we share the same—legitimate—reasons for being behind on patching. Like you, the problem is mostly about not having enough time—time to schedule maintenance windows, test patched systems and keep current on new vulnerabilities.

NIP devices can help here as well. Most attacks are

against well-known applications and exploit well-known vulnerabilities, and this is where intrusion-based systems shine—detecting and blocking known attacks. They can buy you the precious time you need to patch existing servers and provide an additional detection/protection layer.

A NIP Taxonomy

Now that we've established that NIP systems can be worth the money, let's look at the technology. There are two broad types of NIP systems: signature-based IPSs, which match packets or flows to known signatures, and traffic-anomaly IPSs, which learn normal flow behavior for a network and alert to statistically significant deviant events.

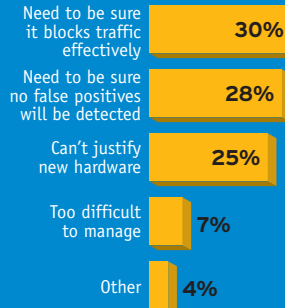
Signature-based NIP products run the gamut from purpose-built systems, like NetScreen's IDP or Network Associates' IntruShield appliances, to integration between IDSs and firewalls,

like the pairing of Internet Security Systems' Real-Secure with Check Point's FireWall-1 or Cisco's IDS with PIX. At a high level, these systems work the same: The NIP device monitors traffic flowing past the wire; attempts to match the traffic—packets or flows—to known signatures; and when there is a match, takes some action. Often, the action is just an alert, but traffic can be blocked, too. NIP vendors typically issue signatures quickly after a vulnerability is publicized, so it's wise to keep current.

Several methods are used to detect malicious activity

E-MAIL POLL

If you don't use network-based IDS blocking, what would it take for you to use it?



Source: NETWORK COMPUTING E-Mail Poll, 479 respondents

FOCUS ON THE ENDPOINT

The closer you place security tools to vulnerable systems, the safer your data. The data that is valued by attackers resides on your network-attached desktops and servers, so you need to protect the applications that hold that data—or are gateways to it—just as you protect underlying operating systems.

These are two distinct and difficult tasks, but instead of slavishly girding your network perimeter, adopt the mind-set that you'll design with a focus on protecting assets and denying malfeasants access to where those assets reside. Here are two best practices to start you on the road to enlightenment:

- » Harden the underlying OS by

removing unnecessary services and applications. The remaining services should be run on nonprivileged accounts whenever possible. Removing services takes away attackers' access methods. Removing applications hobbles attackers, temporarily at least, if they do gain access to a server because tools may not be immediately available, and potentially vulnerable programs are not accessible for local-privilege escalation attacks. Oh, and keep current on patches.

HIP (host intrusion-prevention) products may help in hardening an OS. HIP products work by passing all system-level calls for resources, like file access, to an ACL (access-

control list). Based on the ACL, the request is passed or blocked. Check out "HIP Check," at www.nwc.com/1322/1322f2.html.

- » Consider customized installations. When installing products, try to enforce secure installation practices. When administrative accounts are created within applications, for example, ensure that the passwords are complex even if the product doesn't enforce it. Try to understand what changes are made to the underlying system, and limit the features to those you need. Don't take default installation options.

For more on asset-based security, see "Secure to the Core," at www.nwc.com/1401/1401f1.html.

using signatures designed to send alerts on specific attacks and mutations of attacks. Signatures are difficult to create at the best of times, however, and without a thorough understanding of the vulnerability, signature creation is less effective. Signatures also can be based on common attack indicators. For example, they may search for binary traffic where only ASCII traffic should be; look for anomalous packets, such as telnet traffic on a high-number port; or target malformed packets. Of course, packets that match these fuzziest signatures don't always indicate an attack: For instance, the AOL Instant Messenger client for Mac OS X doesn't send a *host:* header on its HTTP/1.1 requests, which may trigger a protocol-anomaly alert.

There are many other examples of legitimate anomalous traffic that might trigger alerts, all of which reinforce our contention that before you enable intrusion prevention, you have to be confident that no legitimate traffic will be blocked. Though interesting, protocol-anomaly detection is still too immature for us to place much trust in its ability to accurately differentiate between legitimate and illegitimate traffic.

DoS (denial of service) alerts are generated by traffic that violates an adjustable but predetermined traffic rate, such as 100 unacknowledged TCP sessions in one second. Detailed knowledge of what constitutes normal traffic on your network is essential to define thresholds properly. Alternatively, DoS, or distributed DoS, detection is based on statistical analysis of common types of traffic. After a learning period, the NIP has a picture of "normal" traffic. Bursts that are statistically significant may indicate a DoS or DDoS attack. Or, they may just indicate an abnormal spike in traffic, as when a Web site is "Slashdotted."

Traffic-analysis intrusion-prevention products, like those from Arbor Networks, Lancope and Mazu Networks, monitor traffic patterns and capture snapshots of what constitutes normal traffic—traffic rates, which computers make connections to other computers, and so on—creating a picture of network behavior.

Normal traffic also can be defined as part of policy enforcement. If your organization's policy is to disallow telnet anywhere on the network, instances of telnet being used constitute, at minimum, a breach of policy.

The Bottom Line

You do need NIP systems, but not because they're going to solve your security problems. They won't. You need them because you most likely have inadequate desktop and server controls. You probably don't have the resources to maintain application patches. And way too many network applications are poorly designed and/or improperly installed, leaving security holes.

During briefings with TippingPoint Technologies, the company told us its UnityOne product "patches the

network." This is an absurd statement because while the UnityOne appliance may block attacks, that is not a patch—the end system is still vulnerable.

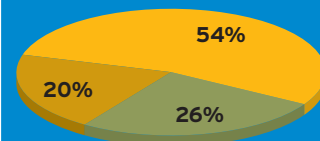
Remember, attacks don't always come through the perimeter. Recently, SQL Slammer ravaged networks when remote users connected to the network with infected laptops. To effectively stop attacks, you need to focus on the ultimate targets: your servers and desktops. And that means desktop and server management.

But organizations don't embark on desktop- and server-management projects for security reasons. Even though a well-planned strategy can spawn tons of benefits, including centralized control, updates and software distribution, these projects are complex and costly, and often don't provide the specific security features necessary to minimize risk. This has given rise to a host of cottage industries—for example, patch management (see "PatchLink Helps Keep Windows Closed," at www.nwc.com/1318/1318f3.html) and security-policy monitoring (see "Policy Enforcers," at www.nwc.com/1410/1410f2.html), two key areas underserved by desktop management. Those two product areas focus on where the problem is—at the endpoint. Keep your Internet Information Systems Web servers patched, and who cares if someone attempts a Unicode directory traversal? The attack will fail, and that's the point, right?

A wise woman (my wife) said recently that we don't need electric fences if we lock our doors. Intrusion prevention is the necessary fence because we don't, can't or won't lock our desktop and server doors.

E-MAIL POLL

Do you think intrusion prevention will solve your security problems?



● Yes
● No
● Don't know

Source: NETWORK COMPUTING E-Mail Poll, 479 respondents

WebLinks

Find "Inside the NIP Hype War" online at www.nwc.com/1417/1417f1.html

Find "NIP Attacks in the Bud" online at www.nwc.com/1417/1417f2.html

Security white papers & research reports, www.nwc.com/go/sec-papers.html

Security books at www.nwc.com/go/sec-books.html

Our weekly vulnerability and patch newsletter, www.nwc.com/go/sac.html

The current Internet threat report, www.nwc.com/go/alert.html

"Intrusion Detection: Bright Future or Dead End?," www.techweb.com/tech/security/20030618_security

"Don't Get Bitten by NIP Hype," www.nwc.com/1411/1411colshipley.html

"Intrusion Detection, Or Intrusion Prevention?," www.techweb.com/tech/security/20030212_security

"Security Gets HIP," www.techweb.com/tech/security/20020410_security