IPS: OUT WITH THE OLD, IN WITH THE NEW

Two Options for Evolving Your IPS Solution

EXECUTIVE SUMMARY

Intrusion prevention systems (IPS) play a key role in securing the corporate network and data center by inspecting traffic in search for malicious content. But the IPS market is evolving, leading companies to reconsider whether to run a standalone IPS appliance or consolidate IPS and other security functions into a next-generation firewall (NGFW). Both options have pros and cons. Security directors are weighing the ability of different IPS tools and NGFWs to thwart attacks, the devices' effect on network throughput, and cost and resource considerations. The right solution depends on an organization's unique requirements.

INTRUSION PREVENTION SUPPLEMENTS FIREWALL PROTECTION

IPS is a crucial tool on the workbench of any company that is serious about security. IPS systems were developed to supplement the network firewall. At the most basic level, firewalls filter network traffic based on predefined rules, blocking entry to traffic that is not explicitly approved. IPS devices are designed to sit after the firewall and before the internal network, inspecting communications and analyzing traffic patterns in real time to detect and prevent attacks.[1] They serve as an additional layer of protection to enhance a company's security posture, and are often required for compliance with stricter government regulations. But because IPS inspections are more resource-intensive, and too many of them could affect network performance, it's important for the firewall to first screen out traffic that shouldn't be allowed onto the network.

Think of network security from the standpoint of airport security. The firewall serves as the ticketing and ID check. It compares incoming traffic against certain rules, ensuring that only communications that are explicitly allowed are able to enter. It checks where the traffic came from, who sent it, or the method of transport (application type). But it is not, strictly speaking, concerned with the payload. After tickets and IDs are checked, passengers go through a security checkpoint in which their bags are scrutinized. In this analogy, the baggage check is completed by the IPS. The IPS device checks the payload, making sure no malware or attacks get into the network in the guise of legitimate traffic. Firewalls focus on the origin of traffic, who sent the traffic, and the application type transporting the traffic. Once the firewall has answered those questions, it ignores the balance of packets in the flow. In contrast, IPS devices must inspect the payload in every packet of the flow to be sure there is no malicious content. Companies achieve the highest level of security in their network, or their data center, when they simultaneously employ both of these approaches to inspection.

AIRPORT SECURITY		NETWORK SECURITY	
Ticket and ID Check: Only authorized (those who have a ticket) can enter. Ensures passengers are who they say they are.		**Firewall:** Checks traffic against set rules to ensure only allowed traffic comes onto the network.	
Baggage Check: Even the passengers who are authorized must participate in a baggage check to make sure they are not carrying anything dangerous.		**IPS:** Reassembles traffic to properly check for unwanted files (malware) or attacks in the traffic that the firewall allows.	

EVOLUTION OF IPS AND FIREWALLS

The first generation of IPS systems focused on signature detection, comparing incoming packets against the signatures of known threats. This approach caught many attempted attacks, but as threats evolved, it left a gap in corporate security. Any attack that didn't have a recognized signature would get past the IPS.[2] Over time, it became clear that signature detection alone could not scale to adequately protect against the multipronged attack vectors of targeted threats and polymorphism.

Fortunately, IPS devices evolve as the threat landscape changes. Next-generation IPS systems have moved beyond focusing exclusively on signature detection; their packet inspection processes incorporate context, content, application, and user awareness. Next-generation, standalones IPS devices also offer advanced threat detection and tie in with reputable threat intelligence services. Including all this information in the IPS's threat analysis leads to better decisions about which packets to allow to pass. It also enables the devices to better detect zero-day attacks, advanced threats, and botnets.

At the same time, NGFWs emerged. NGFWs incorporate IPS and other types of security functionality that companies with only a first-generation firewall had to deploy and manage separately. Ultimately, however, adding these features to the NGFW is not always a perfect fit.

MARKET EVOLUTION IN PROGRESS

Different IPS vendors take different approaches to dealing with the challenges and opportunities in the market today. Some vendors have reacted by selling off IPS technologies. Others have made acquisitions to beef up their product line.

Then, there are the vendors, such as IBM, that have decided to exit the IPS market. In August 2017, the company announced it would stop selling the IBM Network Security (XGS) product line at the end of that year.[3] IBM will continue to support current customers through 2022, but these customers won't be able to add devices because IBM will no longer sell the XGS. This means customers can continue with their status quo, but they can't expand their IPS systems, and improvements or upgrades will not be forthcoming. Thus, for many IBM customers, it makes sense to start looking for a replacement very soon.

IPS devices inspect the payload in every packet of the flow to be sure there is no malicious content.

First-generation IPS systems focused on signature detection, comparing incoming packets against signatures of known threats.

Next-generation IPS moved beyond simply focusing on signature detection to packet inspection processes that include context, content, user, and application awareness.

TWO COURSES OF ACTION AVAILABLE

The turmoil in the IPS market has made the path forward a bit unclear for corporate directors of security. That's the bad news. The good news is that companies have two paths for moving forward with IPS protection: they can install both a standalone IPS and a firewall, or they can deploy an NGFW that can perform both functions. Which path makes the most sense for a particular organization depends on cost considerations and security needs.

OPTION 1: SEEK OUT A NEW STANDALONE IPS

Large campuses and data centers, for which application and data security are paramount, require the content inspection found in next-generation IPS, which is typically available only in standalone IPS devices. NSS Labs estimates that the market for implementing standalone IPS devices within data centers (the DCIPS market) is worth US$450 million annually, and projects a compound annual growth rate for this market of 15% through 2020.[4]

For enterprises with complex networks, large data centers, or particularly acute concerns about application or data security, a strong consideration should be made to install a standalone IPS in addition to a firewall. In fact, companies requiring maximum performance and security for their data center or corporate network frequently opt to deploy a NGFW firewall and standalone NGIPS.

The intrusion prevention capabilities within a standalone IPS are often more robust than that functionality in most NGFWs. Even now, many NGFWs include IPS technology that is still essentially just a signature-matching engine. They inspect traffic flows for packets matching the signatures they know to be threats. But the only way they can catch morphing malware, for example, is to continue adding more and more signatures. These inadequately performing NGFWs fail to incorporate awareness of content and context into their determinations of whether a particular flow poses a threat. However, these considerations are a key criteria in choosing to deploy a sophisticated standalone NGIPS device.

Another benefit of running a standalone IPS revolves around network performance. Most NGFWs with integrated IPS, and some traditional standalone IPS systems, have difficulty scaling to meet the performance speeds of the data center. Turning on application controls and signature-matching IPS engine capabilities for example, can considerably degrade performance in most NGFWs. More sophisticated IPS technology and SSL decryption implemented in the firewall could result in even greater performance degradation.

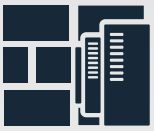
Organizations with high-performance needs may ultimately determine that achieving the company's requirements, requires the deployment of a standalone NGIPS along with a NGFW. A careful analysis of the standalone route should be reviewed, as achieving the expected level of throughput could actually be less expensive than choosing a NGFW with less than adequate next-generation IPS capabilities.

OPTION 2: TRANSITION TO IPS CAPABILITIES WITHIN A FIREWALL

Most analysts agree that the market for standalone IPS solutions either has plateaued or is declining. That's because many branch and campus locations are consolidating their security devices and implementing NGFWs that contain adequate NGIPS. Incorporating firewall, virtual private network (VPN), antivirus, and IPS functionality in a single device holds appeal, particularly for organizations that have chosen to reduce costs, seek to simplify device management, and recognize the shortage of security staff. This is leading some analysts to sound the death knell of the standalone IPS.[6]

Small, branch locations and midsize, campus locations that are separate from the corporate data center are transitioning to IPS within an NGFW. If the security decision makers are comfortable with the level of IPS functionality and performance a NGFW provides, it makes sense to spec out an IPS-in-NGFW solution. In doing so, it's important

If a company needs top-shelf performance and security for its data center or corporate network, the deployment of both **firewall** and **standalone IPS** is often non-negotiable.



The market for standalone IPS devices within data centers in particular is worth

US $450 million

annually, with a compound annual growth rate of **15%** through **2020**. Source: NSS Labs

The potential cost benefits of combining firewall and IPS functionality in a single **NGFW** are further enhanced by streamlined management.

the organization has done the appropriate risk assessment and testing to ensure throughput and performance with IPS functionality turned on meets/exceeds expectations. Another critical step for those in the decision-making tree, is to review third-party certification data from organizations such as NSS labs. These results can save the business time and money. Once the aforementioned actions have been considered, it will be evident not all NGFWs are created equal.

The cost benefits of combining firewall and IPS functionality in a single NGFW are many. All organizations are trying to balance simplification with their security requirements. By moving toward a single-pane-of-glass management scheme, considerable ease of configuration and better device visibility can be achieved. Additionally, individuals with security skills come at a cost premium, and fewer devices and skillsets to support operations must be part of the discussion. Overall, most businesses are toiling with the difficult decisions on how to balance the increasing number of security threat vectors against overall cost. While there are some organizations that are steadfast in maintaining separate next-generation IPS and NGFW devices, most organizations are seeking out the appropriate NGFW with integrated IPS functionality that meets their needs.

WHERE TO GO FROM HERE

As directors of network security look at the IPS landscape and evaluate next steps, their key considerations should include:

- The level of security sophistication their network needs
- The throughput required for the firewall and IPS—whether separate or all in one device
- Cost and staffing concerns

Some of the questions directors of network security need to ask include: Does the company still need the sophisticated inspection capabilities of a standalone IPS? Or, might it be ready to consolidate the IPS into an NGFW in order to minimize the total cost of ownership for its security environment?

Determining throughput targets and security requirements, and developing an inventory of the security skills who are on staff, will prepare the security team to enter the evolving IPS market and evaluate security options to find the best fit for the organization's needs.

[1] "Firewall vs IPS vs IDS," IP with Ease, September 14, 2017.

[2] Network World Staff, "Network IPS grows up from its IDS roots," PCWorld, accessed March 19, 2018.

[3] "Software withdrawal and support discontinuance: IBM QRadar Network and IBM Security Network Appliance selected programs," IBM United States, August 15, 2017.

[4] "How did your DCIPS product do in NSS' latest group test?," accessed March 19, 2018.

[5] "How did your DCIPS product do in NSS' latest group test?," accessed March 19, 2018.

[6] Network World Staff, "Network IPS grows up from its IDS roots," PCWorld, accessed March 19, 2018.

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
905 rue Albert Einstein
06560 Valbonne
France
Tel: +33.4.8987.0500

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730

LATIN AMERICA HEADQUARTERS
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
Tel: +1.954.368.9990

187362-0-A-EN April 6, 2018 10:07 AM

Mac:Users:susiehwang:Desktop:Egnyte:Egnyte:Shared:Creative Services:Team:Susie-Hwang:Egnyte:Shared:CREATIVE SERVICES:Team:Susie-Hwang:WP-IBM-IPS-Problem-Education:wp-ibm-ips-problem-education