Protecting Your Digital Business: The Case for Next-Generation Intrusion Prevention

What You Will Learn

Many companies that adopt a next-generation firewall (NGFW) believe that they can’t benefit from a dedicated intrusion prevention system (IPS) as well. That simply isn’t true. You should consider adding a physical or virtual NGIPS appliance to your security architecture for a number of reasons.

This white paper explains:

- How a next-generation intrusion prevention system (NGIPS) can help protect your digital business
- What capabilities to look for when you buy an NGIPS

In many cases, an NGIPS is less disruptive to your networks than the alternatives. It can be easier to implement and manage. It can also provide better visibility and protection. An NGIPS can:

- Shorten the time to detect and remediate advanced threats
- Address unpatched or unpatchable vulnerabilities
- Protect critical business areas and network segments
- Achieve high security effectiveness and exceptional throughput
- Separate network- and security-related duties

Protecting Your Digital Business

As the digital economy expands, so do the opportunities for attackers. Networks are growing. Companies are continuously acquiring other companies. They’re adding locations and branch offices. Users access your network from their own smart devices, wherever they are. Corporate apps, servers, and data are now in the cloud. A proliferation of devices in the Internet of Things (IoT), which don’t even look like computers, are connecting to your networks. For companies that sell products or services, doing so “online” is the new normal. Mission-critical activity takes place beyond the traditional perimeter, and the infrastructure is constantly changing.
We’re reminded every day that the digital economy is fragile and that malicious actors are taking advantage of this fact. The Cisco 2016 Midyear Cybersecurity Report (MCR) cites numerous attacks that have exploited vulnerabilities in the Internet infrastructure, as well as in the aging infrastructure of organizations, to make money and disrupt businesses. One high-profile example was the massive DDoS cyber attack on October 21, 2016, which affected 6 percent of Fortune 500 companies.

Advanced attackers demonstrate a level of sophistication that challenges many businesses’ ability to cope. Motivated by financial gain and sometimes hacktivism, attackers understand each of their targets, down to its likes and dislikes and how it conducts business. They exploit a growing set of attack vectors and any weakness they find, evading traditional boundaries and controls.

Once inside your network, adversaries can gain a foothold and move laterally toward their ultimate target, often high-value assets housed in your data center. Staying below your radar, they can even hijack your servers to launch new attack campaigns.

Protecting today’s complex networks requires a robust threat detection and containment approach. It needs to be based on deep visibility into users, devices, files, and applications as well as vulnerabilities. Enter next-generation IPS.

Why a Next-Generation IPS?

Many security and IT professionals believe that with the widespread availability of NGFWs, dedicated NGIPSs are no longer necessary. It is true that IPS functionality is included in NGFWs. Many small to medium-sized organizations find these new firewalls to be all that they need. But for more sophisticated companies, the decision is not so clear-cut. When they consider the level of protection, performance, and resources they need, many organizations with complex and dynamic networks opt to deploy both firewall and NGIPS solutions.

Let’s take a look at a few reasons why this may be the best approach.

Shortening the Time to Detect and RemEDIATE Advanced Threats

The IPS functionality embedded in many NGFWs and unified threat management systems (UTMs) is not comprehensive. Instead, some firewalls incorporate a subset of capabilities that are available with dedicated NGIPS solutions.

With a true NGIPS you can detect known and new threats and rapidly contain and remediate advanced attacks. Continuously updated with the latest security intelligence, an NGIPS uses the following features:

- Vulnerability-aware IPS rules to automatically detect and block attack traffic (even never seen before attacks)
- Malware file analysis
- Sandboxing technology
- Indications of compromise (IoCs)

All these help it spot targeted infections quickly before they can spread or do damage.

The estimated industry median time to detection of threats is currently more than 100 days. Reducing that time to a matter of hours or minutes is imperative. An NGIPS reduces the exposure window and, thus, an attacker’s time to operate. Further, an NGIPS provides perspective on the root cause and the trajectory of attack, so you can strengthen your defenses against future similar attacks. Integration with third-party solutions, like security information and event management (SIEM) systems and threat intelligence feeds, also helps to speed detection and streamline your responses.
Addressing unpatched or “unpatchable” vulnerabilities

As reported in the Cisco 2016 MCR, most successful exploits are a direct result of unpatched known vulnerabilities. Many users still do not download and install patches in a timely manner. At other times the infrastructure is not accessible, or there simply is no patch available. Attackers have time on their side. They can identify and exploit vulnerabilities in infrastructure, systems, and devices that are deployed but are not maintained or simply long forgotten.

An NGIPS doesn’t replace disciplined patching, but when patches aren’t available or practical, an NGIPS can help stop opportunistic threats. Through vulnerability-targeted IPS rules, security teams can apply a “virtual patch” until permanent fixes can be deployed. Turning on a recommended IPS rule can be simple and fast. It can require fewer resources and be less disruptive to the business than deploying thousands of updates to applications across the environment. How does the NGIPS know what rules to recommend? With context awareness it “sees” the environment it is protecting. It can determine new vulnerabilities and automatically recommend applicable protection signatures.

Achieving high security effectiveness and throughput

Security effectiveness can be measured in many ways, but having the highest possible catch rate at all traffic levels is crucial. Enabling IPS functionality when it’s not purpose-built, as is often the case with UTM and NGFW technologies, is resource intensive. It can cause intolerable performance degradation on edge-deployed firewalls. Some organizations have reported a performance degradation of up to 90 percent. The resultant time-outs or high latency may be unacceptable to the business.

In addition, threat protection must scale with throughput levels. Protection may be most important when the demand on systems is high. Passing packets uninspected just because the firewall threat inspection engine can’t keep pace is a weakness that attackers look to exploit. Deploying an NGIPS beside the firewall can increase security effectiveness while improving network performance. An NGIPS can help ensure business continuity. It can be set to fail open, allowing traffic to pass in the event of its failure.

Protecting Critical Business Areas and Network Segments

Typically, NGFWs are used only selectively in the enterprise. Firewall rule changes are generally hard to deploy and time consuming. Performance can suffer when IPS features are turned on. NGFWs can also disrupt business operations in the event of a device failure or unplanned power down. These challenges often manifest in “flat networks.” These types of networks can leave critical areas of the business unprotected, including virtualized data centers, hybrid cloud deployments, and branch offices. Further, flat networks are often insufficiently secure for organizations that face stringent compliance mandates. Security teams want the visibility and control to detect and contain threats across all portions of the extended network. Network teams want to provide this but don’t want to hamper network activity or burden their busy staff.

A true NGIPS can provide visibility and can speed threat detection and response in areas of your network that remain off limits to firewall inspection and controls. Deploying a physical NGIPS appliance allows you to detect threats that move laterally across the physical IT infrastructure. Virtual NGIPS appliances protect hybrid data centers, virtual server farm environments, and applications in the cloud, as well as branch offices and remote locations. In doing so, NGIPS appliances (physical and virtual) help you enforce consistent policy across dynamic workloads within the premises or in cloud environments. Providing a complete picture, easy management, and a consistent level of threat detection across the extended enterprise, an NGIPS protects against advanced attacks and helps to address compliance requirements.
Separating Network- and Security-Related Duties

The group that manages security policy is often not responsible for the enterprise infrastructure, and vice versa. Additionally, your organization may choose to outsource firewall management (rule changes, etc.) or security event handling and triage to third-party managed service providers for network or security operations. Outsourcing may be a way to augment your staff or reduce costs. However, it often comes with some loss of visibility into the threat environment.

A well-deployed NGIPS allows you to continue with your firewall management strategy without compromising visibility, protection, or performance. Security teams can tap into a dedicated NGIPS to gain network visibility and enforce security policy and threat detection. An NGIPS, if architected well, can keep pace with dynamic network traffic levels. In the event of a failure, it can continue to allow traffic to flow, unlike most firewalls.

Why Cisco Firepower NGIPS

As summarized in Figure 1, there are many reasons to consider adding a physical or virtual NGIPS appliance to your security architecture.

Figure 1. Benefits of an NGIPS, NGIPS Deployment Cases

The Cisco Firepower™ Next-Generation IPS (NGIPS) is uniquely suited to address these requirements. It protects your digital business with visibility, intelligence, automation, advanced threat protection, and performance. Multiple techniques work together to deliver industry-leading intrusion prevention capabilities. You can quickly detect and effectively protect against a wide range of network attacks.

Visibility: Cisco Firepower NGIPS continuously discovers information about your network and uses it to build network maps and host profiles. This information covers operating systems, mobile devices, files, applications, and users in your environment. It is the contextual information you need to make better decisions about intrusion events, and it is also used to enable automation.

Intelligence: Cisco’s Talos Security Intelligence and Research team detects and correlates threats in real time using the largest threat detection network in the world. Their efforts result in vulnerability-focused IPS rules and embedded IP-based, URL-based, and DNS-based security intelligence for Cisco Firepower NGIPS.
Automation: Intelligent security automation takes this intelligence and correlates intrusion events with your network's vulnerabilities. You can then focus your resources on the threats that matter most. It also analyzes your network's weaknesses and automatically recommends the appropriate security policies to put in place.

Advanced threat protection: The Cisco Firepower NGIPS threat appliance provides industry-leading threat efficacy against both known and unknown threats. Its features include:

- IPS rules that identify and block attack traffic that targets vulnerabilities in your network
- A tightly integrated defense against advanced malware, incorporating advanced analysis of network and endpoint activity
- Integrated sandboxing technology that uses hundreds of behavioral indicators to identify zero-day and evasive attacks

Performance: A range of purpose-built appliances provide the right throughput, flexibility, and scalability. Organizations of all types and sizes can achieve consistent security effectiveness while maintaining network performance. These appliances incorporate a low-latency, single-pass design and include configurable bypass (fail-to-wire) interfaces.

The Cisco Firepower NGIPS delivers an industry-leading platform validated by respected third parties. The most recent Gartner Magic Quadrant for IPS positions it as a leader. In NSS Labs' 2016 NGIPS group testing, the Cisco Firepower NGIPS demonstrated high security effectiveness, superior throughput, and low total cost of ownership (TCO). It earned a Recommended rating and placement among leaders in the NSS Security Value Map (SVM).

Additional Considerations

When you select the Cisco Firepower NGIPS, you have access to many additional benefits.

Investment Protection

Cisco Capital\textsuperscript{®} financing is available with terms that meet specific business and budgetary requirements. With a fair-market-value lease, organizations can pay for the use of the equipment, not its ownership. You have the flexibility to upgrade or refresh equipment as needed, eliminating technology obsolescence.

Services and Technical Support

Cisco has achieved certification under the J.D. Power Certified Technology Service and Support Program for five consecutive years and eight years overall.\textsuperscript{1} Cisco service and support offerings for Cisco Firepower NGIPS include the following:

- **Cisco Migration Services for Intrusion Prevention Systems**, delivered by Cisco security engineers and Cisco Security Specialized Partners, help organizations migrate smoothly to the Cisco Firepower NGIPS. Cisco provides expert guidance and support to help maintain security during a migration and to improve the accuracy and completeness of the process.

• **Cisco Remote Management Services** help reduce TCO further by continuously managing security networks. Your organization’s IT team can concentrate on other value-adding business priorities.

• **Cisco Network Optimization Services** feature smart analytic tools with an intuitive graphics interface to deliver exceptional insight into network performance. Organizations can reduce network complexity, improve operational excellence, monitor policy compliance, mitigate risks, and proactively detect and preempt potential network disruptions.

• **Cisco Smart Net Total Care™ Service** helps organizations reduce network downtime and other critical network issues. You get access to expert technical support 24 hours, 365 days a year, as well as flexible hardware coverage and proactive device diagnostics.

For More Information

To learn more, visit:

www.cisco.com/go/ngips