Business white paper

Next-generation IPS and firewall

Why you need both

Next-generation firewalls include intrusion prevention system (IPS) technology that can detect and block cyber attacks. But they are not a complete substitute for a purpose-built next-generation IPS. Effective network security requires both. This paper explains how these two important security defenses work together to protect your network and your business.

Table of contents

Today's networks under attack

The headlines are staggering: 40 million credit card records stolen at Target, 56 million at Home Depot, 83 million customer records stolen at JP Morgan Chase. How do the hackers access so much data in networks that have firewalls, anti-virus software, and other defenses?

These attacks are examples of advanced persistent threats, sometimes called "low and slow" attacks. They succeed by avoiding detection and operating within the network for weeks or months—five months in the case of Home Depot—to locate and steal data. According to Frost & Sullivan,[1] today's advanced persistent threats operate according to a predictable lifecycle:

1. **Penetrate the network**—exploit a vulnerability to gain a toehold on a Web server, for example.
2. **Obfuscate evidence of the attack**—modify logs or disable anti-virus protections.
3. **Explore and spread through the network**—find valuable data.
4. **Steal or sabotage data or systems**—exfiltrate data to their site.

Securing the network requires identifying and disrupting threats at each phase of the lifecycle. And that requires both next-generation firewalls (NGFWs) and next-generation intrusion prevention systems (NGIPS)—each doing what it does best.

Next-generation enterprise firewalls

Firewalls are best at controlling access to the network from outside. They are the security guard at the gate who controls who can enter, whom you can talk to, and about what. Firewalls have advanced significantly from the early packet filters that simply rejected packets based on rules defining what protocols and ports network traffic was allowed to use. Modern third-generation enterprise firewalls are stateful access control devices that inspect deep within the packet stream for potential attacks. They identify and keep track of network conversations (connections) and can associate packets with conversations they have previously allowed based on rules. They also provide other services like network address translation and virtual private network (VPN) concentration.

Traditional firewall rules provide basic controls over connection requests using simple attributes like IP address and network port. This worked well prior to the explosion of the Web, but today's Web-enabled applications all appear on the same network port (port 80). A traditional firewall cannot differentiate among them. Attackers use this to their advantage to deliver malware from compromised websites, hijack Web-enabled applications, or control attacks and steal data through connections made to look like outbound Web browser activity.

[1] "Defending Against Increasingly Sophisticated Cyber Attacks," Chris Rodriguez, Frost & Sullivan

Next-generation enterprise firewalls help solve this problem by using deep packet inspection techniques to look deeper into the connection than traditional firewalls. This gives NGFWs two new weapons against the attacker:

- NGFWs can detect the application in use, even for Web applications. This allows you to create more sophisticated access control rules to prevent users from accessing dangerous or risky websites and to block certain actions (such as file transfer) that might be used to steal information.
- NGFWs can detect and block actual attacks with their built-in IPS technology. Like purpose-built IPS, IPS functionality in NGFWs relies on attack filters downloaded to the firewall periodically. Further, some NGFWs can compare the Internet addresses of incoming and outgoing traffic to reputation data—lists of known bad or suspect sites—to spot traffic originating from or destined to bad guys.

Because they are designed to stop attacks primarily from outside, firewalls are usually located at the edge of the network and operate on traffic coming into the network from outside and leaving the network going to outside destinations. Their performance and functionality make them an effective and cost-effective gatekeeper at Internet speeds. Effective as they are, NGFWs have limitations.

For example, firewalls must keep track of all allowed connections and other information in tables in memory. This makes them vulnerable to distributed denial of service (DDoS) attacks. In a DDoS attack, cyber criminals bombard the firewall with connection requests that can cause the tables to fill up and disable the NGFW. And that can disrupt the entire network. Many firewalls contain some DDoS protection. But those capabilities are limited, and that leads to a new need to protect the firewall with purpose-built DDoS solutions. That adds complexity and actually broadens the attack surface.

Further, because they must track connections and apply multiple security features, NGFWs trade away the performance needed to operate in the network core. This can cause unforeseen effects on performance-sensitive or legacy applications that do not tolerate firewalls well.

Finally, because they are positioned at the edge, NGFWs can detect phases one and four of Frost & Sullivan's four phases of advanced persistent threats (penetration of the network by the attack and exfiltration of data to the attacker's system). This is critically important, but it's not enough. Once hackers penetrate a network, they move within it to locate and steal intellectual property or customer data or to sabotage systems. And in the case of insider attacks, the attacks may originate inside the network. Missing that lateral network traffic (Frost & Sullivan's phases two and three) misses some of the key clues that an attack is underway.

NGFW plus NGIPS: working together to secure your network

NGFW

- Located at the network edge
- Controls access to the network from outside
- Detects attacks in phases 1 and 4

NGIPS

- Located in the network core
- Inspects in-network as well as inbound and outbound traffic
- Detects attacks in phases 1, 2, 3, and 4

Next-generation intrusion prevention systems

Just because you have a good security guard on duty doesn't mean you don't patrol the interior of a building. So a next-generation intrusion prevention system (NGIPS) takes up where an NGFW leaves off—in the network core. An NGIPS is purpose built to monitor network traffic and detect cyber attacks. It operates as a transparent "bump in the wire." It inspects every packet and, like the IPS in an NGFW, uses downloaded filters to identify attack signatures. NGIPS can also use reputation data to spot traffic from or to Internet sites known or suspected to be malicious.

A key difference, though, is that NGIPS are stateless. They do not attempt to relate traffic to known connections. Consequently, they operate much faster—20 Gbps for HP TippingPoint NX platform, for example—and are transparent to network traffic. They are less vulnerable to attacks that exploit state table exhaustion and result in denial of service. And while firewalls are oriented around network conversations, NGIPS see and can inspect the asymmetric traffic flows that might signal an attack.

Because the performance and transparency of an NGIPS allow you to place it within the network core, it can not only see traffic originating or destined outside the network, it can see lateral traffic within the network. While a firewall might only see traffic associated with phases one and four, an NGIPS could also see internal traffic associated with phases two and three. In fact, HP TippingPoint Next-Generation Firewall uses reputation data and malware filters specifically designed to detect this kind of traffic. This is even more critical when the attack originates from within. And according to Ponemon Institute, attacks by malicious insiders take the longest to detect and resolve—more than 65 days on average.[2]

The role of security intelligence

NGIPS and NGFW share one important attribute: they both rely on security intelligence to detect attacks. Security researchers explore widely deployed software to find vulnerabilities that hackers can exploit. And they develop the filters that identify attacks targeting the vulnerabilities. New filters are usually downloaded automatically to next-generation firewall appliances and NGIPS devices, so they can detect and block the latest threats.

HP TippingPoint—the complete solution you need

HP TippingPoint is the simple, effective, and reliable solution for network security. TippingPoint NGIPS and NGFW are managed and administered via a common security management system (SMS). The SMS gives security specialists a consolidated view of the state of their network security and provides a common set of tools for configuring, deploying, and reporting network security. Furthermore, the SMS allows you to share the IPS configuration and filter settings between your NGIPS and NGFW to ensure you have the same level of security at the perimeter and at control points within the network.

HP TippingPoint uses security intelligence and filters developed by HP Security Research and HP DVLabs—more than 3,000 HP and independent security researchers who find more vulnerabilities than anyone else in the industry. Most NGIPS and NGFWs rely on filters keyed to individual exploits. But that allows hackers to make minor modifications to the attack and elude detection. The hacker is always ahead. HP TippingPoint Next-Generation Firewall (NGFW), however, develops filters keyed to the vulnerability, rather than individual exploits. That means TippingPoint can thwart hackers by detecting new or modified exploits targeting the vulnerability.

Securing your network requires both NGFW and NGIPS—the combination of perimeter defenses and monitoring in the network core that provides the ability to detect all four phases of a cyber attack. And that creates a level of network security that neither device can achieve independently.

Learn more at
hp.com/go/TippingPoint

[2] "2014 Cost of Cyber Crime Study: United States," Ponemon Institute, October 2014

Sign up for updates
hp.com/go/getupdated

Share with colleagues

Rate this document