CDW PEOPLE WHO GET IT

NEXT-GENERATION FIREWALLS: THE NEW NORM IN DEFENSE

Evolving security threats can best be addressed by NGFWs and their enhanced feature sets.

Executive Summary

Increasingly sophisticated cyberattacks have led organizations to adopt correspondingly sophisticated levels of security control. Information security professionals now expect cyberattacks to be part of their normal operating environment and realize that these attackers wield effective tools that greatly exceed the capabilities of yesteryear's script kiddies. Such advanced weapons require equally sophisticated defensive measures.

Many enterprises currently rely upon a security infrastructure full of niche solutions that were designed to combat earlier threats. The major challenge these niche solutions pose is that they do not communicate with each other, so they can't share critical information to help establish and enforce security policies.

Next-generation firewalls (NGFWs) address this problem by providing a single point of visibility into multiple areas of security functionality. They provide security teams with the ability to control network traffic in a manner that protects enterprises against cunning attacks.

NGFWs achieve this by integrating multiple security technologies in a single platform. They combine the features of stateful inspection firewalls, intrusion prevention systems, content filtering and application control on a single piece of hardware and then allow those components to communicate with each other.

Table of Contents

For example, a firewall rule may incorporate information about the user and application into the decision about whether to allow a new connection to occur. This powerful integration provides enterprises with the security technology needed to successfully combat the modern threat in a holistic manner across the entire IT ecosystem.

Cybersecurity Quandries Today

Cyberattacks are growing both in number and sophistication. Enterprises around the world are reporting increasing levels of attack attempts and successful breaches of information security controls.

Each year, Verizon produces a *Data Breach Investigation Report* that provides insight into the nature and scope of data breaches, based on a database the telecommunications company builds from dozens of partners, including McAfee and Symantec. In the 2014 report, Verizon reported a significant milestone: It recorded more than 1,000 successful breaches of organizations, representing a steep, steady increase over the past several years.

These advanced attacks are causing significant financial damage to targeted organizations. The Ponemon Institute, in its *2013 Cost of Data Breach Study: Global Analysis* sponsored by Symantec, found that the average data breach cost American companies $277 per compromised record. This resulted in an average total cost of $5.4 million per incident.

In their June 2014 report *Net Losses: Estimating the Global Cost of Cybercrime,* researchers from McAfee and the Center for Strategic and International Studies (CSIS) estimated the total worldwide costs of cybercrime at more than $400 billion.

The most significant change in the cybersecurity landscape over the past decade is the emergence of the advanced persistent threat. APTs are conducted by highly sophisticated, well-funded attackers who have a set of advanced hacking tools at their disposal. These attackers may include nation-states, organized crime, terrorists or other highly organized groups with clear objectives.

Unlike the attackers of the past, today's cybercriminals do not select a vulnerability and go out in search of a weak target susceptible to the exploitation of that vulnerability. Instead, they pick a target that meets their objectives and then carefully select or develop the tools necessary to infiltrate that enterprise.

APTs often make use of a class of vulnerabilities known as zero-day attacks. These are previously unknown attacks that were developed either by or on behalf of the attacker for proprietary use against valuable targets. The zero-day is not released into the public domain and, therefore, traditional security mechanisms are unable to defend against it because they are designed to protect only against known attacks.

NGFWs, Virtualization and Cloud Computing

Many organizations are adopting cloud computing strategies to drive efficiency and increase the effective utilization of hardware resources. Many of these strategies include the use of private or hybrid cloud models, where the enterprise builds its own protected cloud using virtualization technology from vendors such as VMware, Citrix Systems and Microsoft.

In a virtualized cloud approach, many different guest servers run on a single hardware platform, with shared access to networking, memory, storage and other resources. NGFWs play an important role in virtualization environments by enforcing the separation between virtual machines, allowing different security zones to coexist within the same cloud environment. Many of the major NGFW vendors, including Cisco Systems, Fortinet, Palo Alto Networks and Sourcefire offer virtualized versions of their NGFW products.

IT teams seeking to gain control in this increasingly hostile cybersecurity landscape cannot rely upon the same security controls that protected against the less sophisticated attacks of earlier eras. Traditional firewalls fall into this category. They simply are not designed to function in the application-driven modern network.

Traditional firewalls fail to provide security administrators with the visibility and control they need over network traffic to maintain a safe and secure operating environment for today's enterprises. That's where next-generation firewalls can play an important role in the security infrastructure.

What Are NGFWs?

Next-generation firewalls advance the state of the art in network security by integrating a wide variety of security technologies with an advanced network firewall. NGFWs build upon the stateful inspection approach that served enterprises well for the past decade, and supplement it with contextual information about the applications and users responsible for the traffic seeking to navigate the network. Combined with sophisticated threat intelligence information, this contextual data allows NGFWs to take actions that defend the enterprise against sophisticated threats.

One of the core features of an NGFW is its ability to allow the safe use of trusted applications without depending on control techniques that may be bypassed by advanced attackers. Some of the common evasion techniques used by these cybercriminals include:

- Altering the standard ports used by blocked applications to match the port activity of permitted applications;
- Tunneling impermissible activity through a permitted protocol, such as a virtual private network (VPN);

- Using Secure Sockets Layer/Transport Layer Security encryption to hide malicious content from inspection engines.

Each of these evasion techniques may be effective against a standard stateful inspection firewall. However, NGFWs provide protection against these approaches.

Instead of relying upon port and protocol information to create rules, they develop application profiles that allow the detection of known applications operating in nonstandard ways, as well as illicit applications attempting to masquerade as permitted applications. NGFWs also have the ability to decrypt encrypted communications and perform deep application inspection on the contents of those encrypted sessions. These capabilities allow enterprises to defend themselves against the cunning evasion techniques of modern attackers.

The application profiles available to NGFWs also provide administrators with the ability to restrict application usage in a fine-grained fashion. NGFWs integrate with an organization's identity management infrastructure to retrieve details about authorized users. This allows security administrators to create sophisticated rules, such as "Deny all use of peer-to-peer file sharing, except for staff in the marketing department" or "Block instant messaging communications for nonmanagers during business hours." This fine-grained control of users and applications is one of the hallmarks of NGFW technology.

The firewall, acting as the mediator of all inbound and outbound network communications, has a unique perspective on an enterprise network. This location offers tremendous advantage for monitoring, providing security administrators with complete visibility into all of the data traversing the network boundary. This visibility, combined with the intrusion detection and prevention capabilities of the NGFW, allows the device to block potential attacks before they enter the secure enterprise network.

All NGFWs incorporate firewall, application control and intrusion detection/prevention capabilities, but many also offer a menu of other standard and optional security features. For example, many NGFWs offer administrators a variety of content filtering technologies.

These capabilities include anti-virus filtering that scans inbound traffic for the presence of malware embedded in email, messaging, web and other applications. This anti-malware capability may be supplemented with sandboxing technology that allows for the safe "detonation" of suspicious files in a separate environment to detect malicious behavior.

The secure web gateway capabilities of NGFWs allow organizations to implement content-filtering policies that restrict the activities of users, filtering URLs based upon the categories of content they seek to access. Built-in data loss prevention (DLP) technology scans outbound traffic for signs of sensitive information leaving secure areas and allows administrators to block such attempts, logging them for further analysis.

Enterprises may also incorporate real-time threat intelligence data generated by the research arms of NGFW manufacturers and other sources. For example, this threat intelligence may include information on hostile IP addresses, recently detected malicious activity profiles and other data that the NGFW uses to provide up-to-the-minute protection for the enterprise network.

Next-generation firewalls provide enterprises with a sophisticated suite of tools in a single package, positioned at an optimal point on the organization's network. The advanced capabilities of these devices offer security administrators the threat intelligence and reaction capabilities necessary to combat advanced persistent threats and other cybersecurity issues.

Is an NGFW Just a UTM?

Unified threat management (UTM) products have been on the market for a decade and combine multiple security technologies on a single hardware platform. However, it is important not to confuse UTM devices with NGFWs. There are two major distinguishing factors.

First, NGFWs are enterprise-grade products. The advanced networking technology contained within an NGFW is able to handle extremely high network speeds, often exceeding 100 gigabits per second of throughput capacity. UTM products are generally not able to function in a high-performance environment and are better suited for small and midsize organizations.

Second, UTMs typically incorporate standard stateful inspection firewall functionality. They do not offer the advanced security features found in NGFWs and lack the ability to defeat common security control evasion techniques used by sophisticated attackers.

Best Practices for Selecting an NGFW

Organizations seeking to adopt an NGFW strategy should carefully select the product that best meets their security and business requirements. They should approach this in the same manner as any other technology selection process, consulting a variety of vendors and consultants. What follows is some practical advice to help enterprises select the right NGFW for their environment:

Develop requirements carefully. The NGFW fulfills numerous networking and security functions. Input from a wide variety of stakeholders — security, networking, application and virtualization teams — can provide valuable insight and assist in the development of a robust set of requirements to guide the process.

Review a variety of solutions. The NGFW market has many vendors. Organizations should consider all of the major players in the selection process and compare them with the enterprise's requirements. The selection process should

include solutions from vendors such as Cisco Systems, Fortinet, Palo Alto Networks, Sophos and Sourcefire. Each of these vendors brings different strengths, feature sets and price points to the market.

Consider differences in administrative features. IT managers must think about the administrators who will need to use these systems on a daily basis. What management features does each product offer? Are real-time analytics possible? Do the specific application monitoring and control functions of the NGFW meet the business and technical requirements?

Performance is paramount. The NGFW will, by necessity, be a chokepoint in an enterprise network, and performance issues will quickly ripple through systems and applications. Do the products under consideration offer high-performance processing? Do they run on software or purpose-built high-performance integrated circuits? Do they leverage multithreading or asynchronous parallel processing?

Does the vendor support the use of clustering to provide increased performance and resiliency?

As organizations approach the NGFW selection process, they should consider a simple principle: Design with the future in mind. While an NGFW certainly must meet existing business requirements, it also must provide an acceptable level of functionality for future use.

Enterprises should look to their strategic plan and consider whether it includes foreseeable increases in networking or security needs. With this information in mind, they can design an architectural approach that will either accommodate those needs directly or support a cost-effective expansion when required.

Infographic

View this Next Generation Security infographic, *Beyond the Surface*, for more insight into today's enterprise security issues and solutions: **www.cdw.com/nextgfw1**

Want to learn more? Contact your account manager or visit CDW.com/security and learn more about the products, technologies and industry trends that are shaping security.

Cisco Gold Partner

Staff need to access business applications while using their device of choice. But with that choice comes the need for greater visibility and control. Cisco® offers end-to-end network security solutions, helping organizations balance security with productivity. Their solutions incorporate deployed stateful inspection firewall with comprehensive, next-generation network security services.

CDW.com/cisco

Barracuda

The Barracuda® Firewall provides next-generation application control and user identity functions in an easy-to-use and affordable solution. It outperforms traditional firewalls and UTMs by integrating a powerful firewall appliance with scalable cloud content security.

CDW.com/barracuda

McAfee An Intel Company

The McAfee® Next Generation Firewall changes how network security is delivered. It complements network edge solutions with a high-performance, advanced next-generation firewall (NGFW) solution that is versatile and adaptable. It adds control, visibility and protection — including advanced anti-evasion techniques — where you need it most, including remote sites and branches, data centers and the network edge.

CDW.com/mcafee

paloalto networks

Palo Alto Networks® offers a full line of security appliances that range from the PA-200, designed for enterprise remote offices, to the PA-7050, which is a modular chassis designed for high-speed data centers. The platform architecture is based on a single-pass software engine and uses function-specific processing for networking, security, threat prevention and management to deliver predictable performance.

CDW.com

SHARE THIS WHITE PAPER

CDW PEOPLE WHO GET IT