SOLUTION SHOWCASE

Cisco Introduces an Enhanced Next-generation Firewall Platform

Date: February 2016 **Author:** Jon Oltsik, Senior Principal Analyst

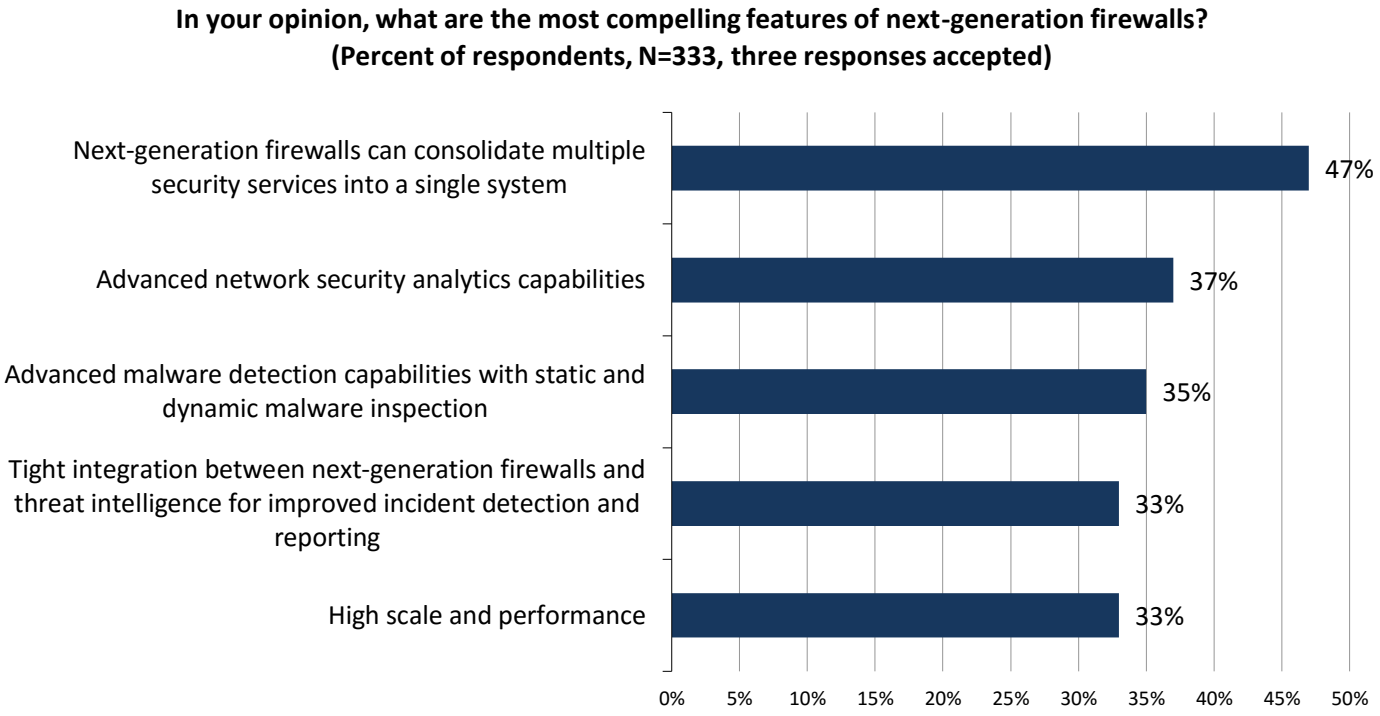
Abstract: When first introduced, next-generation firewalls were marketed as a panacea, consolidating application and network protection on dedicated network appliances. Yes, NGFWs represented a step forward, but many offerings were still light on software integration, threat management capabilities, high performance, and overall systems management. ESG believes that these shortcomings will be addressed with the introduction of next-generation firewall platforms, built for extensibility, high throughput, comprehensive threat management, and central command and control. Cisco's Firepower NGFW announcement represents this type of platform, which should get the attention of enterprise CISOs seeking to decrease risk, improve threat management, and streamline security operations.

Overview

According to ESG research, in 2014, 30% of enterprise organizations reported having deployed next-generation firewalls, while another 33% were in the process of implementing an NGFW.[1] Why are these devices so popular? ESG research revealed that security professionals found NGFW features like security service consolidation, advanced network security analytics capabilities, and advanced malware detection capabilities especially compelling (see Figure 1).[2]

[1] Source: ESG Research Report, *Network Security Trends in the Era of Cloud and Mobile Computing*, August 2014.
[2] Source: ibid.

FIGURE 1. Top Five Most Compelling Features of Next-generation Firewalls



Source: Enterprise Strategy Group, 2016

NGFW Realities

Next-generations firewalls promised features like applications controls, network controls, and threat management capabilities on a single unified system. Unfortunately, this story is frequently too good to be true. Cybersecurity professionals often complain about NGFW shortcomings such as:

- **Performance woes.** Next-generation firewalls often come with a potpourri of services, creating the illusion that one box can replace a number of others. In reality, NGFW performance can slow to a crawl if too many services are used on a single box. Consolidation plans are sometimes thwarted when proof-of-concept testing uncovers performance and throughput issues that could throttle networks and disrupt critical business applications and services.

- **A lack of application layer integration.** In some cases, firewall services such as deep packet inspection, IDS/IPS, and anti-malware capabilities are loosely coupled at best. This really makes these NGFWs an incremental improvement of unified threat management (UTM) appliances rather than a revolutionary cybersecurity technology.

- **Basic threat management.** With early next-generation firewalls, threat management was more akin to pedestrian services such as network-based antivirus, signature-only-based intrusion detection, and stripped-down web threat protection. Some NGFWs have added malware sandboxing capabilities, but these systems are trending toward tactical integration of threat defenses rather than comprehensive threat management coverage that spans the network perimeter, internal network, and cloud-based workloads.

- **A closed architecture.** Given their heritage, some NGFWs come with an assortment of features designed into proprietary hardware appliances. These systems may open APIs or connect with a limited number of other security tools, but this is simply not enough for today's software-defined IT infrastructure featuring DevOps processes and self-service automation/orchestration tools.

- **Management challenges.** NGFWs based upon loosely coupled security services tend to be accompanied by loosely coupled management systems that treat configuration management, policy management, change management, and reporting on a service-by-service basis. This can add complexity and overhead to security operations.

A New Model for Next-generation Firewalls

Next-generation firewalls sounded promising when they were first introduced, but all of the issues described create a situation where the security team is only marginally better off than it was before deploying NGFWs. So what's needed? To meet their requirements, ESG believes that enterprise organizations should look for a next-generation firewall platform designed for (see Table 1):

- **Scale, performance, and flexibility**. Next-generation firewalls need the raw horsepower to run a number of network and security services on a single system to meet enterprise consolidation needs. This requires the right mix of high-end processors, specialized hardware components, and a modern multi-threaded operating system. Additionally, NGFWs should have flexible designs so workloads and security services can be coordinated across multiple hardware appliances, VMs, and cloud-based environments when needed.

- **Integration.** NGFWs should allow for tight integration for an assortment of security tools by providing documented APIs, interoperating with technologies from ecosystem partners, and supporting common standards. These types of integration options are the difference between legacy next-generation firewall appliances and a truly extensible platform.

- **End-to-end threat management.** Rather than bolt on basic safeguards, a next-generation endpoint platform must be tightly coupled with a broad cybersecurity spectrum including sandboxing, threat intelligence, endpoint/network indicators of compromise, and IDS/IPS alerts. This makes an NGFW platform a nexus for threat sharing, data enrichment, event correlation, and automated remediation across networks and endpoints.

- **Comprehensive management capabilities.** Firewall management must align with enterprise requirements for prevention, detection, and response. This demands intuitive end-to-end policy management across security services, central reporting, and the ability to automate, modify, or enforce policies based upon real-time changes related to threats, vulnerabilities, or internal governance needs.

TABLE 1. Aspects of a Next-generation Firewall Platform

Requirement	Description	Rationale
Scale, performance, and flexibility	High-performance hardware and software. Ability to run security services across appliances or deploy them as VMs.	Enterprises need high system performance and throughput to consolidate security functions without disrupting applications and services. There is also the need to be able to distribute security services to accommodate changes to IT infrastructure, software-defined networks, and cloud computing.
Integration	Open documented APIs, partner ecosystems, and standards adoption.	Enterprises need the ability to get more value out of existing tools and easily integrate new ones. There is a further need to interoperate security functions as service chains in risk management and incident response workflows.
End-to-end threat management	Tightly coupled threat management services including malware sandboxing, IDS/IPS, threat intelligence, and endpoint/network forensics.	Enterprises need tight coordination between threat management tools to decrease the attack surface, detect cyber-attacks in progress, and accelerate incident response tasks.

Source: Enterprise Strategy Group, 2016

Cisco's NGFW Platform

Cisco Systems has a long history in network security that spans multiple changes to firewall technology, including packet filtering, stateful inspection, deep packet inspection (DPI), and next-generation firewalls. Cisco is now moving further forward with its new Firepower NGFW. Firepower NGFW combines a number of Cisco and Sourcefire security services into a common platform that spans incident prevention, detection, and response. Specifically, Cisco's product announcement includes:

- The introduction of Firepower NGFW. This announcement marks true software-level integration between the Cisco ASA firewall, Sourcefire next-generation IPS, Advanced Malware Protection (AMP), and other Cisco security assets. Cisco touts this platform as "the industry's first fully-integrated, threat-focused, next-generation firewall," and believes it can provide better protection and management while streamlining security operations.

- A series of new appliances. Cisco is introducing the FirePower 4100 Series appliances, a family of low-latency/high-throughput appliances offering an integrated inspection engine for firewalling, next-generation IPS, URL filtering, and advanced malware prevention/detection in a 1 RU density-optimized design.

- Firepower Management Center 6.0. To complement its new NGFW platform, Cisco also announced a new security management system designed to provide IT personnel and SOC teams with options for granular policy management, service chaining, and security analytics. With Firepower Management Center 6.0, Cisco wants to simplify security operations while providing cybersecurity teams with a more powerful and efficient toolset.

The Firepower NGFW platform targets specific use cases such as Internet edge environments, but isn't for everyone. For example, Firepower NGFW software won't offer elements like VPN, clustering, or multi-tenancy support in its initial release. However, Cisco can still service these customers with other software and products such as its ASA firewall

(available to run as software on the new appliances as well) with FirePOWER Services. Cisco plans to continue to support these existing systems while adding enhancements to the Firepower NGFWs over time.

With the introduction of Firepower NGFW, Cisco is making the transition from firewall appliances to a more modern NGFW platform. This shift should be noteworthy for enterprise CISOs looking to decrease risk, improve protection, accelerate incident response tasks, and streamline security operations.

The Bigger Truth

Cybersecurity professionals have been searching for some type of "silver bullet" solution that can be deployed on the network quickly and deliver vast improvements in prevention, detection, and response. Unfortunately, no such "silver bullet" solution exists. Savvy CISOs know that strong cybersecurity depends upon formal processes, the right policies, central command and control, distributed policy enforcement, and real-time comprehensive visibility. Firewall technology has evolved to be an essential cog in the overall cybersecurity machine, but it remains one of a multitude of puzzle pieces needed.

A next-generation firewall platform is designed with this situation in mind as it extends and integrates firewall capabilities to improve threat prevention, detection, and remediation. NGFW platforms interoperate with other security tools to align with the old adage, "The whole is greater than the sum of its parts." Finally, a next-generation firewall platform is designed with management in mind to improve the productivity of overwhelmed and understaffed cybersecurity teams.

Cisco has been an active participant in the evolution of network security and its recent announcement is further proof that it will continue to do so. Its introduction of a new platform, new NGFW appliances, and a more comprehensive solution for security management is simply the latest chapter in its network security pedigree.