USE CASES

NEXT-GENERATION FIREWALL IMPLEMENTATIONS: FIVE USE CASES

Don’t just sell, excel

INGRAM MICRO®

USE CASES NEXT-GENERATION FIREWALL IMPLEMENTATIONS: FIVE USE CASES

Every organization is worried about the next big security breach, the one with the potential to compromise critical systems and sensitive data, to knock the company offline at the expense of productivity and millions in revenue.

In an age where attackers are relentless and malware is increasingly sophisticated, defenders need cutting-edge tools that are up to the task of detecting stealthy threats and stopping them before damage can be done. They need advanced network security capabilities that deliver visibility, granular controls and scalability without degrading network performance.

Combining traditional firewall features with granular controls for detecting and thwarting application-specific attacks, next-generation firewalls (NGFWs) have changed the game for security practitioners and services providers. Packing the power of deep-packet inspection, antivirus and spam filtering, and application awareness in one centrally managed solution has made NGFWs an increasingly valued component in modern network environments.

The increase in network security functionality and manageability is driving opportunity for channel partners. The global NGFW market is estimated to grow from $2.39 billion in 2017 to $4.27 billion by 2022, an annual growth rate of more than 12 percent.[1] Vendors such as Check Point, Cisco, ForcePoint, Fortinet, Juniper, Palo Alto Networks, Sophos and others continue to innovate in this burgeoning market segment.

While business uses for NGFWs can differ greatly from client to client, there are some fundamental applications for the technology that transcend organizational size and vertical industry. When discussing NGFWs with customers and prospects, consider these five use cases:

Use Case 1: Fine-tune controls and protect against threats at the application level

While traditional firewalls control access and counter threats by simply blocking common ports or services, NGFWs take network defense to the next level, typically monitoring traffic in OSI Layers 2 through 7.

The added visibility, deep-packet inspection and intelligence across all ports and services in NGFWs lets administrators capture what applications are being used, what data is being sent and received, and whether the content conforms to organizational policies. This allows for the creation of granular, application-specific controls for both users and apps that are beyond the capabilities of traditional firewalls.

Use Case 2: Protect the network without degrading performance

For years it has been a vexing truism in network security: Raising the level of control reduces throughput and performance. Despite vendor claims, traditional firewalls throttle network speed as more protections and services are enabled. The problem is exacerbated when port-based firewalls are paired with other controls, creating redundant layers and policies.

1 MarketsandMarkets, “Next-Generation Firewall Market by Delivery Type, Service, Organization Size, Vertical And Region,” June 2017, https://www.marketsandmarkets.com/Market-Reports/next-generation-firewall-ngfw-market-32240698.html.

Generally speaking, NGFWs deliver constant throughput regardless of the number of protective controls and services enabled. Because NGFWs are tasked with much computational heavy lifting, most employ dedicated resources to process things like application identification, SSL termination and content inspection.

Use Case 3: Simplify security architecture

Many client organizations are drowning in complex, poorly organized and poorly managed point products with security environments in dire need of consolidation. NGFWs bring together firewall, intrusion prevention and detection, network access controls, and antivirus email filtering all in a single solution.

NGFWs also can address the complexity issue through integration with other security controls in the network such as the security information and event management (SIEM) system, threat intelligence feed, cloud sandboxing, cloud access security brokers (CASBs) and advance endpoint protection platforms.

Use Case 4: Identify and control circumventors

Even the best security policies wilt under the pervasive problem of proxies, remote-access applications and encrypted tunneling employed specifically to get around controls like firewalls, filters and secure gateways. Some of these applications have legitimate business uses; many do not. Even the legitimate ones must be tightly managed. Traditional firewalls are mostly ineffective at discerning among them and controlling their use.

The newest NGFWs pack features purpose built to deal with evasion technologies regardless of port, protocol or encryption method. And because evasion tactics evolve rapidly, it's vital to have an NGFW with intelligence features that can be easily and regularly updated and maintained.

Use Case 5: Automate security and networking operations

Distributed organizations with many far-flung locations present a significant challenge when it comes to managing, updating and enforcing policies. NGFWs, coupled with orchestration platforms available from most vendors, allow for centralized policy management across the network environment, simplifying the tedious and manual tasks of auditing and distributing firewall rules, patches and operating system updates.