White Paper

Network Security Demands a Full-service Hybrid Proxy Architecture

By Jon Oltsik, ESG Senior Principal Analyst

June 2017

This ESG White Paper was commissioned by Symantec and is distributed under license from ESG.

Contents

Executive Summary

According to ESG research, organizations of all sizes will make the most significant investments in network security more than any other cybersecurity area in 2017.[1] This seems odd since CISOs have invested in firewalls, IDP, and lots of other gateway devices since they started connecting corporate networks to the public Internet. Why do organizations continue to spend on network security? What's changing? What's really needed in this area? This white paper concludes:

- **Business and IT initiatives are driving rapid networking changes.** Over the past 7 years, organizations have embraced cloud computing, digital transformation, IoT, mobility, and a host of other business and IT initiatives. This led to a situation where network security technologies were always trying to catch up to rapid changes to the network itself.

- **Legacy technologies and strategies are no longer appropriate.** Faced with rapid change, CISOs defaulted to a historical pattern by simply buying new network security appliances and adding them to the network. Unfortunately, this put too many "bumps in the wire," adding complexity and performance bottlenecks to network connectivity. On the security side, an abundance of network security devices added overhead to security management and operations, making the cybersecurity staff less productive or effective.

- **Next-generation firewalls (NGFWs) proved to be a stop-gap at best.** Next-generation firewalls were supposed to address network complexity and operations overhead by aggregating network security appliances and management into a single device. As business and IT initiatives evolved, however, NGFW performance and functionality limitations became more disruptive, rendering these boxes inadequate.

- **Organizations need a full-service hybrid proxy security architecture**. It's time for CISOs to stop thinking about network perimeters and security appliances, and envision network security built upon a proxy-based architecture composed of distributed network services. This type of full-service architecture is designed for central management and distributed enforcement to mitigate risk while preventing/detecting threats regardless of user location, application location, or device type.

Network Security History Circa 2012

A few short years ago, the network security model seemed to be trending toward a new pattern. Large organizations needed to modify their network security controls because:

- **BYOD initiatives were gaining traction.** With the popularity of smartphones and tablets, many organizations introduced BYOD policies by 2010, adding hundreds or thousands of new devices to the network. This changed network security requirements as these devices are mobile by design and offer limited onboard security protection. CISOs needed a way to provide secure network access while monitoring devices and network traffic for anomalous/suspicious activities.

- **Organizations were experimenting with cloud computing.** By 2012, many organizations were actively moving workloads or files to the public cloud, building private clouds, and leveraging SaaS applications like Salesforce and ServiceNow. These business and IT initiatives presented new network security challenges by introducing virtual networks and moving applications and data outside of the purview of security controls and monitoring tools.

- **More network traffic was encrypted.** By 2012, an increasing amount of network traffic was encrypted using SSL/TLS. While this helped protect the confidentiality and integrity of network communications, it also meant that network

[1] Source: ESG Brief, *2017 Cybersecurity Spending Trends*, March 2017.

security devices were no longer capable of inspecting and filtering encrypted network packets. This was especially problematic as cyber-adversaries used SSL/TLS encryption to cloak cyber-attacks to circumvent security controls used for detection.

- **APTs were top of mind.** The term advanced persistent threats (APTs) became mainstream within the cybersecurity community after the Google Aurora attack in 2009. These "low and slow" cyber-attacks often circumvented traditional network security controls to gain a foothold on corporate networks, then gradually spread until cyber-adversaries discovered and exfiltrated sensitive data. Given the stealthy nature and damaging results of APTs, many CISOs scrambled to find appropriate security controls capable of preventing and detecting them.

At the time, network perimeters were anchored by a few staple security devices such as firewalls, IDPs, and gateway AV appliances. As organizations faced the changes described above, they quickly realized that existing perimeter security devices were no longer adequate. Why? Mobile devices and cloud-based services communicated outside the perimeter, rendering security devices blind and dumb. Encrypted traffic bypassed the security perimeter, free to roam and compromise internal networks and hosts. Finally, most traditional security devices couldn't dig deep into network content to detect and block sophisticated cyber-threats.

Faced with new security requirements, cybersecurity professionals did what they always did—they purchased additional perimeter network security gateways to intercept, inspect, and filter network packets. Some organizations added several new "boxes" including anti-malware sandboxes, SSL decryption appliances, and cloud access security brokers (CASBs).

Unfortunately, this army of new devices came with a cost. Additional network security controls increased network complexity as packets were forwarded from one security filter to the next. These inspection points also tended to interfere with network throughput, impacting latency-sensitive services like video and voice applications. Overwhelmed infosec staff also had to deal with additional operations overhead as each device required deployment, configuration, and ongoing administration.

Many Organizations Turned to NGFWs for Help

CISOs faced a difficult situation forcing them to deal with new requirements, threats, and security complexity simultaneously. Seeing this precarious situation, several security technology vendors jumped in with a new type of consolidated perimeter security offering—next-generation firewalls (NGFWs).

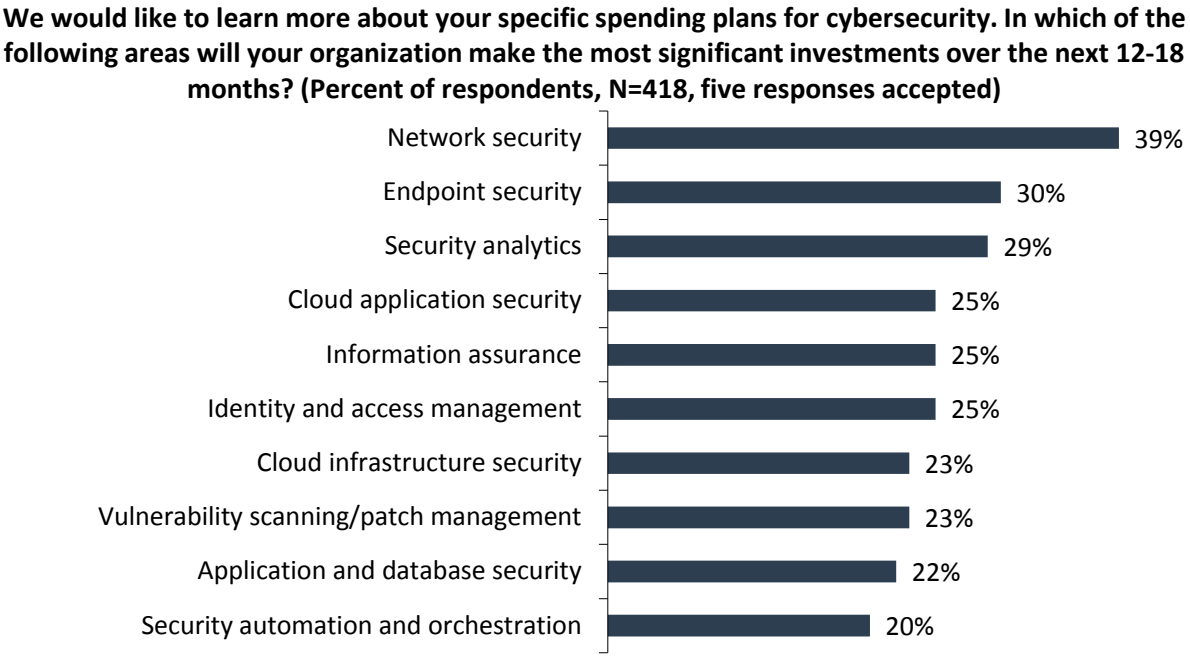
NGFWs represented the latest evolution of firewalls offering deep-packet inspection to enhance application filtering. This enabled NGFWs to implement content scanning features such as intrusion detection and prevention, user identity integration, and some aspects of web threat management. NGFWs also commonly implement virtual private networks (VPNs), enabling off-site employees to access company resources from insecure Internet connections. And since NGFWs use modern CPUs, they can provide incremental functionality like SSL decryption and malware detection sandboxing for file inspection. By consolidating multiple perimeter network security services into a single hardware appliance, NGFWs can also centralize and streamline security operations into a common management interface.

NGFWs seemed to fill network security gaps so many organizations deployed them during this timeframe.

Network Security Today

Fast forward to this year and organizations are poised to invest more in network security than any other area in 2017 (see Figure 1).[2] This is because IT infrastructure and network security has grown even more distributed and complex in the five years since 2012. For example:

Figure 1. Top Ten Most Significant Cybersecurity Investments



Source: Enterprise Strategy Group, 2017

- **Endpoints and mobile devices are universal.** Early BYOD initiatives were an early advancement toward pervasive mobility. Desktop computers have given way to laptops while applications are often written in HTML 5 to accommodate the growing population of mobile devices. Additionally, new types of IoT devices including sensors and actuators are increasingly used for specific industry applications and business processes. These trends will continue to grow in the future.

- **Cloud workloads and technologies are becoming the rule.** Since 2012, cloud computing has expanded beyond test and development to host full production applications. Many industries (like the U.S. Federal Government) now think in terms of "cloud-first" when developing and deploying business applications. Similarly, enterprise organizations now consume a wide range of SaaS applications rather than develop and/or deploy them in their own data centers. The move to cloud can also result in unsanctioned "shadow IT" applications and the flow of sensitive data to and from cloud-based applications.

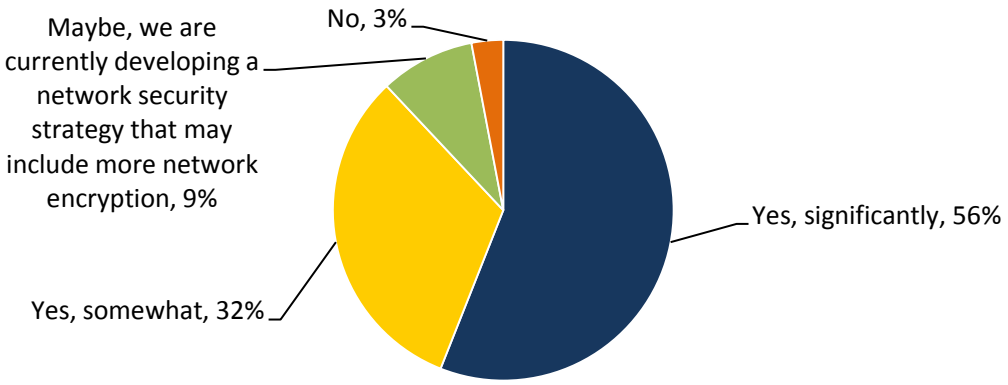
- **Network encryption is ubiquitous.** Internal and external networks now default to SSL/TLS encryption. In fact, ESG research from 2014 indicated that 54% of enterprise organizations encrypt more than 50% of their network traffic. Not surprisingly, most cybersecurity professionals at the time believed that encrypted network traffic would only increase, so it is likely that in 2017 more traffic is encrypted at more organizations (see Figure 2).[3] Furthermore, this complicates network security as traffic must be decrypted for security inspection.

[2] Source: ESG Brief, *2017 Cybersecurity Spending Trends*, March 2017.
[3] Source: ESG Research Survey, *Trends in SSL/TLS*, November 2014.

- **Sophisticated targeted attacks still cause mayhem.** New types of damaging cyber-attacks still haunt large organizations, including ransomware, IoT-based DDoS attacks, and continued targeted attacks. According to the most recent *Symantec Internet Security Threat Report*, a total of 1,209 security breaches in 2016 exposed the identities of 1.1 billion people and 15 of these breaches exposed more than 10 million identities. Incidents like the recent WannaCry global ransomware attack and the 2016 Mirai DDoS attack on Dyn/DNS demonstrate that damages from cyber-attacks may have gotten worse since 2012.

Figure 2. Percentage of Encrypted Network Traffic

Do you believe that the percentage of your organization's network traffic that is encrypted will increase over the next 24 months? (Percent of respondents, N=150)



Source: Enterprise Strategy Group, 2017

Increasing IT and network security complexity has also exposed NGFW weaknesses. Each NGFW feature consumes a large amount of processing power and memory so overall performance can degrade when simultaneously decrypting SSL traffic and executing deep-packet inspection. The system may not be able to keep up with line rates, or may have to limit the number of SSL connections. End users would perceive this as a slowdown in the network, or worse, a broken network connection.

Malware detection engines in an NGFW are also limited. To search for malware, NGFWs inspect each packet as it streams through the firewall, searching for signatures or malicious content. When malware is detected, the NGFW halts the connection, terminating communication. By the time an NGFW stream-based detection operation finds an issue, it may be too late to prevent infection or damage. Stream-based malware detection can also be challenged by packet ordering and/or fragmentation issues. Packets can arrive out of order or divided into smaller packet sizes to evade signature detection, either through natural network behavior or through malicious intent at obfuscation, and this can prevent the detection of malware. NGFWs are also challenged by attack patterns using HTTP version handling, deflate attacks, chunked encoding, etc.

Just as they did in 2012, CISOs face yet another conundrum. NGFWs can't keep up with IT performance needs or prevent/detect sophisticated security attacks. Rather than try to rely on an ineffective network security-in-a-box approach, large organizations need a better network security solution as soon as possible.

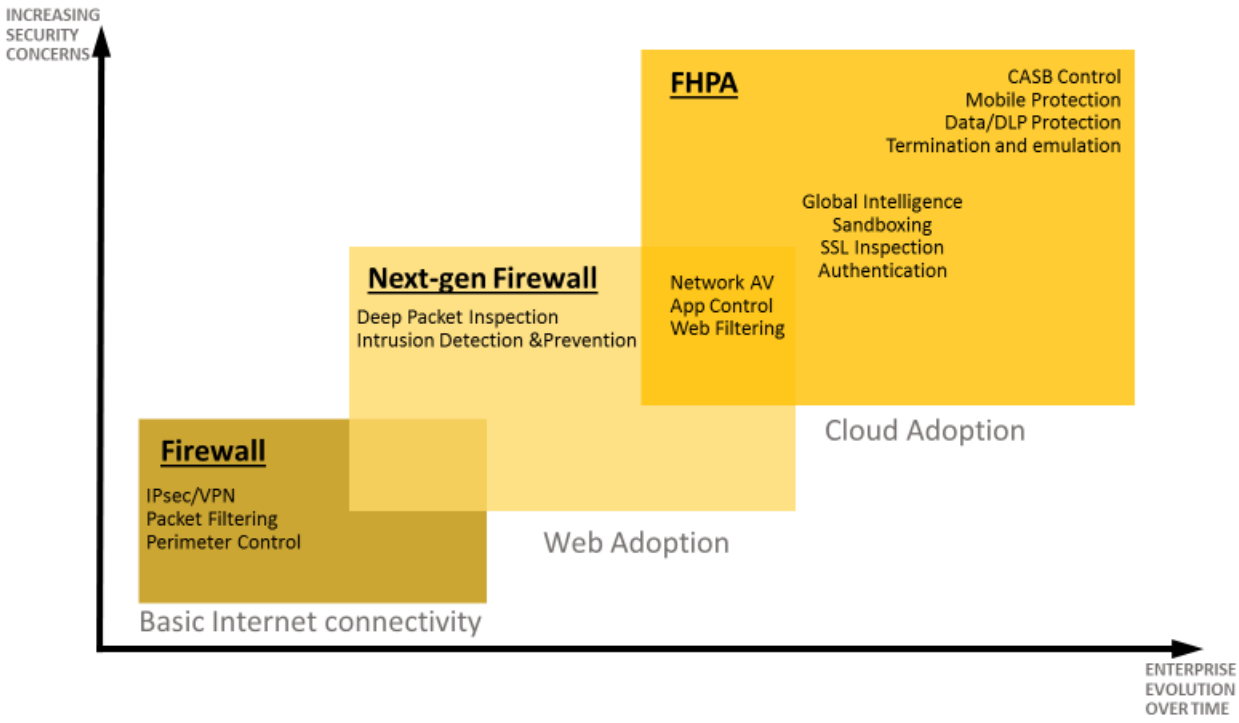
Enterprise Organizations Need a Full-service Hybrid Proxy Security Architecture

Firewalls will always maintain a role of filtering network ports and protocols as packets ingress/egress corporate networks. Nevertheless, NGFW performance and security limitations make it a mismatch for emerging enterprise security requirements.

So, what's needed? A full-service hybrid proxy security architecture (FHPA). FHPA builds upon network security technologies of the past (see Figure 3) by offering the following attributes:

- **Full-service** equates to a network security architecture that provides features and functionality for mitigating risk, as well as threat prevention, detection, and response. Solutions that can help automate threat response workflows are especially useful here. For example, network security solutions that are tightly integrated with endpoint security can greatly accelerate threat detection, isolate compromised assets, and streamline remediation processes.
- **Hybrid** indicates that this type of network security architecture is composed of both on-premises and cloud-based components.
- **Proxy** technology performs two key functions: First, it hides the internal network and hosts from external prying eyes. And rather than filter traffic using streaming technology (as NGFWs do), proxies examine packets across entire network sessions to detect and block malware obfuscation techniques.
- **Architecture** specifies that multiple network security services work collectively regardless of their location (i.e., on-premises or cloud-based) or form factor (i.e., physical, software-only, virtual).

Figure 3. Evolution to Full-service Hybrid Proxy Security Architecture (FHPA)



Source: Enterprise Strategy Group, 2017

In aggregate, a full-service hybrid proxy security architecture provides distributed network security services that enable:

- True authentication and granular access policy enforcement. NGFW offers some authentication capabilities such as user identification, in which a user is associated with an IP address and communication from that address is assumed to come from that user. This technique is not effective against multiuser environments, and is susceptible to basic techniques like IP hijacking. A proxy-based architecture offers true authentication in which each user and new TCP connection are challenged to authenticate for access. Once an authentication decision is made, the network security architecture can enforce governance and security policies, enabling user productivity on internal and cloud-based applications and services while mitigating risk.

- Full visibility into all traffic everywhere. A full-service hybrid proxy security architecture will also include high-performance SSL decryption capabilities to allow full inspection of all network traffic. With a foundation built on network proxy functionality, an FHPA can recreate full network sessions providing monitoring oversight to all network traffic. This also provides CISOs with the ability to find and control "shadow IT" applications. By exposing all network traffic, proxies can also be aligned with technologies like DLP to enforce governance and compliance mandates.

- Tight integration across security controls and infrastructure. A full-service hybrid proxy security architecture distributes tightly integrated network security services across internal networks and the cloud at large. This enables security policy enforcement for all users regardless of whether they are in the corporate headquarters, at a remote office, or roaming and connecting over the public Internet. To maximize protection, this type of architecture also provides integration across network and endpoint security technologies. When endpoint security software detects anomalous behavior, it can query on-premises and cloud-based security services to see if this behavior is associated with known cyber-attacks. Similarly, when networks detect indicators of compromise (IoCs), they can communicate with endpoint security tools to blacklist them.

- Comprehensive threat protection. Based upon network proxy and distributed network security services, FHPA can apply many threat prevention/detection filters to all network sessions. Common threat vectors like web traffic and email can be filtered at the network gateway or in the cloud using multiple AV engines, reputation lists, global threat intelligence, and anti-malware sandboxing technologies for static and dynamic file analysis. Since these filters are distributed and available in multiple form factors, they can be deployed appropriately to offer maximum protection without disrupting network throughput.

- Central management. With tightly-coupled integration of network security services, FHPA offers the central management benefits of NGFWs without the limitations. This can enable global policy management and enforcement across on-premises, virtual, and cloud-based resources.

The Bigger Truth

Famed physicist Albert Einstein is often quoted as saying that the definition of insanity is doing the same thing and expecting different results. Regrettably, this is exactly what many enterprise organizations continue to do. New IT initiatives like cloud computing, digital transformation, IoT, and mobility are driving massive changes to networks and network security, yet CISOs continue to rely on the same controls they have in the past. The results haven't been pretty—increased risk, damaging data breaches, and complex security operations.

Given these issues, it's no surprise that many firms turned to NGFWs several years ago. After all, NGFWs promised all-inclusive network security and central management in a single hardware appliance. In reality, the NGFW story was too good to be true as these devices came with their own issues, especially around network performance, limited threat protection, and no protection or monitoring capabilities for remote users or cloud-based workloads.

ESG believes that it's time for CISOs to look beyond network security appliances and legacy strategies and think in terms of tightly connected network security services. This is exactly what's offered in a full-service hybrid proxy security architecture as described above. This type of architecture can sit behind traditional L3-L4 firewalls, offering end-to-end protection and oversight over all connected devices and workloads regardless of their location.

What's most important is that an FHPA can help CISOs meet their three most important job responsibilities:

1. **Security efficacy.** An FHPA offers capabilities to decrease the attack surface while enhancing threat prevention and detection.

2. **Operational efficiency.** A full-service hybrid proxy security architecture provides central management of all distributed network security services including traffic inspection and threat prevention, detection, and response across all on-premises, virtual, mobile, and cloud-based assets—capabilities lacking in NGFWs. This can help CISOs increase the cybersecurity team's productivity and responsiveness.

3. **Business enablement.** FHPA is built for high-performance and network security coverage of mobile users and cloud-based workloads. This provides CISOs with a foundation to support new business processes and digital transformation IT initiatives.

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides actionable insight and intelligence to the global IT community.

 www.esg-global.com

 contact@esg-global.com

 P. 508.482.0188