White Paper

Integrated Network Security Architecture: Threat-focused Next-generation Firewall

By Jon Oltsik, Senior Principal Analyst

September 2014

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

Contents

Executive Summary

Most large organizations address network security with an army of tactical point tools like firewalls, VPN gateways, IDSs/IPSs, network proxies, malware sandboxes, web and e-mail gateways, etc. This messy array of independent technologies was adequate ten years ago, but now presents a plethora of operational, policy enforcement, and monitoring challenges. Worse yet, network security defenses are becoming less and less effective at blocking targeted and sophisticated threats and advanced malware attacks.

How bad have things gotten and what should CISOs do to address these issues?

- **Network security is growing more difficult.** Security professionals fight through a myriad of day-to-day network security challenges around overlapping processes and controls, too many point tools, too many manual processes, and not enough security skills. Given all of these new and historical problems, today's network security is a mismatch for enterprise requirements.
- **Modern network security tools aren't enough alone.** Many organizations are embracing new network security tools like next-generation firewalls (NGFWs). Yes, NGFWs can improve security but they too often focus on limited application controls rather than providing more holistic protection against cybersecurity threats. Additionally, single tools such as malware analysis sandboxes remain tactical because they can't provide protection or enhance security visibility across the network or out into the cloud.
- **Large organizations need an interoperable network security architecture.** Enterprises need an integrated network security architecture that is more threat-centric, offers scalability, automates manual processes, and replaces point tools with interoperable network security services. A network security architecture should include central command and control, distributed enforcement, and integrated actionable intelligence.

Network Security Challenges

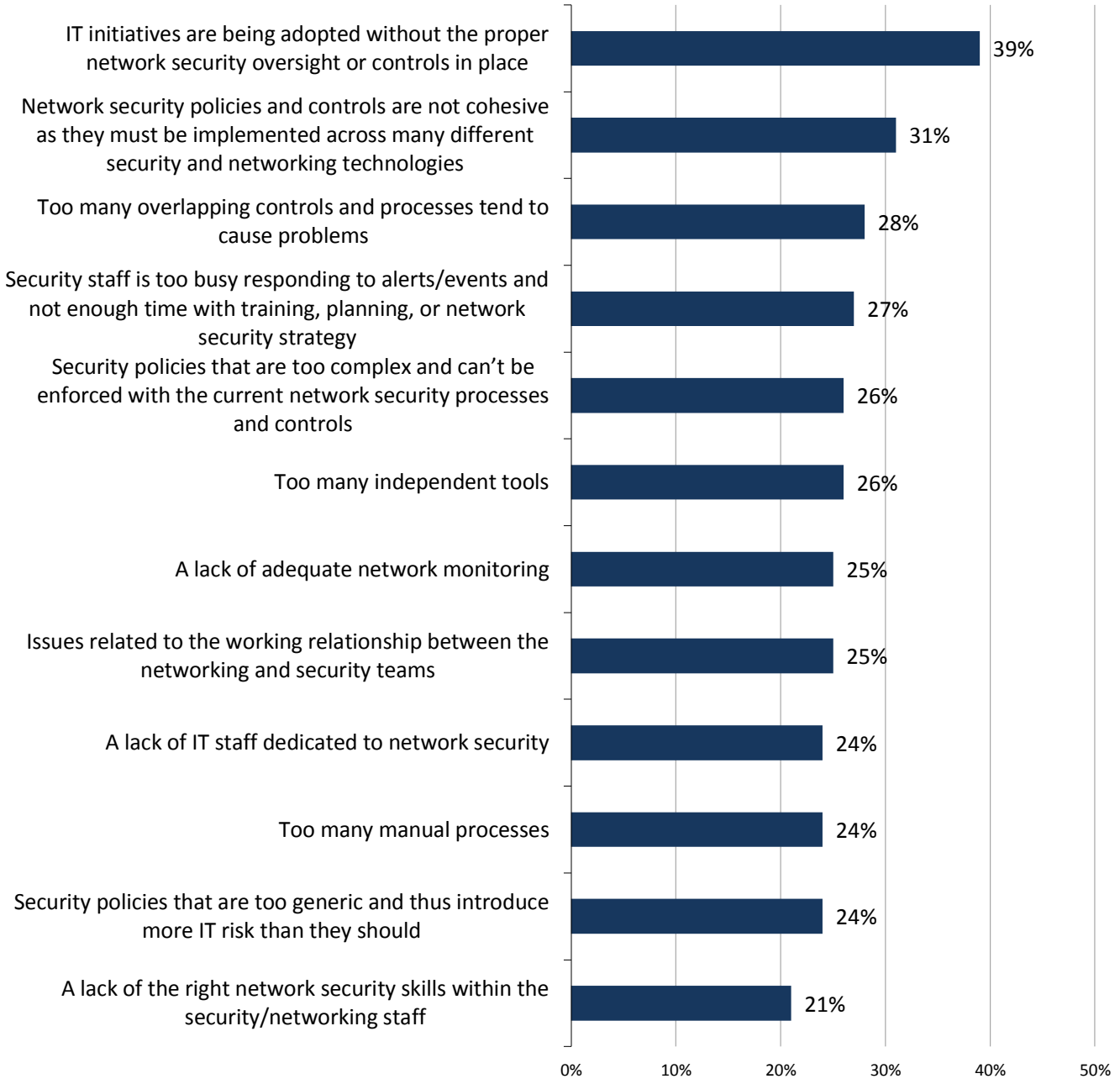
Large organizations are rapidly transforming their legacy IT infrastructures with the addition of new initiatives like cloud computing, big data analytics, mobility, and Internet of things (IoT) applications. All of these changes present a number of network security challenges for enterprise organizations (see Figure 1).[1] CISOs often struggle with network security because of:

- **Too many disparate solutions and technology silos.** Nearly one-third (31%) of organizations are challenged by a lack of cohesiveness across network security policies and controls, 28% have issues with too many overlapping policies and controls, and 26% struggle with too many independent tools. This disjointed mess of disparate solutions and technology silos makes it difficult to prevent, detect, or remediate security incidents.
- **An abundance of manual processes.** ESG data indicates that the security staff is often putting out fires rather than attending to network security with more proactive policies or procedures. Additionally, 24% of organizations say that are challenged by too many manual processes. The combination of firefighting and manual processes can't possibly scale to meet today's risk management and emergency response requirements for network security.
- **A network security skills shortage.** ESG data also indicates that 24% of organizations are challenged by a lack of staff dedicated to network security, while 21% say that they lack the right network security skills. Given the global shortage of cybersecurity skills, this is a recipe for disaster.

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

Figure 1. Network Security Challenges

Which of the following would you consider your organization's biggest network security challenges? (Percent of respondents, N=397, five responses accepted)



Source: Enterprise Strategy Group, 2014.

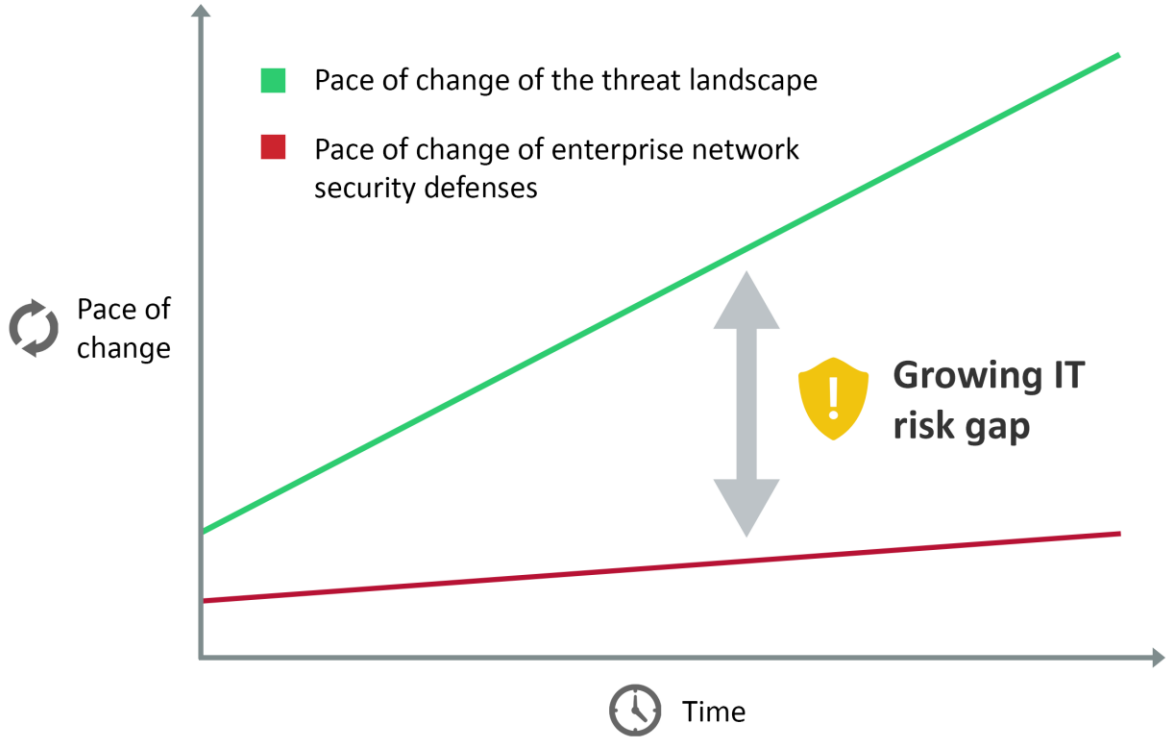
The Network Security Gap

CEOs and corporate directors must understand that network security challenges are part of a much bigger problem around cybersecurity risk management. Legacy network security based upon technology silos and manual processes, and requiring advanced security skills, can't scale to address the volume, variety, and sophistication of today's cyber-threats. Disconnected solutions contain blind spots that sophisticated attacks exploit. This is one reason why so many enterprises suffer security breaches: Hackers simply take advantage of these network security weaknesses, fly "under the radar" to circumvent network security controls, and compromise IT assets. Once

hackers establish a successful beachhead, they often remain invisible for months at a time as they navigate across networks, gain access to business-critical systems, and ultimately steal sensitive data.

In the past, CISOs tended to address cybersecurity threats with incremental network security technologies, processes, and staff, but this is no longer an appropriate strategy. Simply stated, cyber-threats are growing exponentially as a function of new technologies and advances in exploit techniques. Alternatively, incremental network security investments provide a marginal increase in security protection, especially in light of the operational challenges previously discussed. This situation creates a network security gap where IT risk grows on a daily basis (see Figure 2).

Figure 2. Tactical Network Security Creates a Growing IT Risk Gap



Source: Enterprise Strategy Group, 2014.

Enterprise Organizations Need an Integrated Threat-focused Network Security Architecture

Large organizations face a growing conundrum: Enterprise networks must be available, scalable, dynamic, and open to anchor today's IT and business processes, but this model has led to an alarming rise in cybersecurity risk. Legacy network security controls are no match for this fluid IT environment and changing threat landscape.

So what's needed? ESG believes that network security requirements demand a new approach for network security. Moving forward, CISOs need to think of network security in terms of a new architectural model that spans from edge to core to cloud. ESG defines an integrated network security architecture as:

An integrated system of network security hardware and software, where any security service can be applied at any point on an internal or extended network as a physical or virtual form factor. A network security architecture also provides underlying communications so that all security services and components can share and react to information in real time to fine-tune security controls, detect security events, and remediate compromised systems.

A threat-focused integrated network security architecture is based upon the same types of firewalls (next-generation firewalls and standard firewalls), IDSs/IPSs, and other security technologies in use today. The major difference, however, is that individual devices interoperate and cooperate more fluidly across the network, sharing their telemetry intelligence and, by doing so, continually informing one another and better acting in unison. Additionally, network security functions like firewalling or IDS/IPS can be thought of as services and applied consistently across the LAN, corporate data center, or external cloud provider where and when they are needed.

To truly provide for integration, comprehensive coverage, and interoperability, a threat-focused integrated network security architecture must be based upon three things:

1. **Central command and control.**
2. **Distributed enforcement.**
3. **Integrated actionable intelligence.**

Central Command and Control

One of the primary challenges associated with legacy network security technology is related to management and operations. Each network security device has its own policy engine, provisioning, configuration, and reporting, causing a few major problems associated with operational overhead and redundant tasks. What's more, it is difficult if not impossible to piece together the status of enterprise security by looking at an assortment of tactical reports.

To alleviate these problems, an integrated network security architecture must start with central command and control for:

- **Service management.** Provisioning, configuring, and changing network security services must be managed centrally, supported by an intuitive GUI and workflow engine, and interoperate with other IT operations tools. For example, network security professionals should have the ability to provision and configure firewall rules, VLANs, and router/switch ACLs from a single GUI. This alone should simplify network security controls, enhance protection, and streamline network security operations.
- **Interoperability with server virtualization and cloud orchestration.** Higher-level tools for configuring virtual workloads for VMware, Hyper-V, OpenStack, or AWS need to be supported with appropriate network security controls. With central command and control, a network security architecture should offer the appropriate APIs to align cloud benefits like rapid provisioning and self-service with the appropriate layers of network security protection**.**
- **Monitoring and reporting.** Aside from management and operations functions, an integrated network security architecture should also offer central monitoring and reporting aligned with activities like event management. Security analysts should have the ability to pivot from one report to another or correlate multiple reports quickly for a more accurate and timely view of network security status. To alleviate blind spots, central monitoring and reporting should also monitor virtual and cloud-based controls along with physical network security devices.
- **Advanced visibility.** Beyond monitoring, security analysts need a depth of visibility into their environments in order to spot multi-vector threats and to see what users, applications, content, and devices are on the network and what each are doing to implement effective security policy to accelerate threat detection and response.

Distributed Enforcement

With central command and control, CISOs can create global security policies, but these policies will still need to be enforced by various security services residing throughout the network. An integrated network security architecture also provides for this requirement with:

- **Support for any form factor in any location.** Network security services must be available in any location, in any form factor, and in any combination. This allows the security team to apply granular network security policies to network segments, flows, applications, or specific groups of users. For example, retail companies can use a combination of physical and virtual network security controls to ensure that POS systems can only connect with specific IP addresses through a combination of firewalls, IDSs/IPSs, and advanced malware detection tools. Alternatively, users on the corporate LAN can receive different access policies than those working at home across public networks.
- **A portfolio of network security services.** A network security architecture must perform L2-7 tasks, and support all types of packet filtering at any point in LAN, WAN, or cloud. Packet filtering is a broad category here and includes inspecting for threats such as viruses, worms, DDoS attacks, SPAM, phishing, web threats, content leakages, and application-layer attacks. The combination of multiple form factors and multiple services lets enterprises create superior layered security stacks that can be tailored to different network flows, user groups, and mobility requirements or rapidly adjusted to address new types of threats.
- **Network and endpoint security integration.** In the past, network and endpoint security were often managed by different security groups using disparate processes and tools, but given the current insidious threat landscape, this no longer makes sense. To bridge this gap, a network security architecture should provide tight integration between network and endpoint prevention controls and detection analytics. For example, application controls should be consistent across NGFWs and endpoints to protect sensitive assets when users connect to the network via the corporate LAN or from remote public networks across the globe. To improve incident detection, analysis sandboxes should interoperate with endpoint agents to correlate anomalous suspicious network traffic with anomalous system activities.

Integrated Actionable Intelligence

While network security technologies like web threat devices, IDSs/IPSs, and antivirus gateways depend upon signature and intelligence updates from the cloud, many other network security technologies are contingent upon security personnel for configuration changes or writing new rules for blocking network connections. Alternatively, an integrated network security architecture is designed from the start to be "intelligence-driven" as it is:

- **Based upon a number of diverse data sources.** While SIEM systems typically perform security analytics based upon log events, a network security architecture will offer a rich variety of other types of data for analysis. These include network staples like NetFlow and full packet capture, but also detailed data on endpoint forensics and profiling, user/device access patterns, and cloud application auditing. When combined, correlated, and analyzed correctly, this new data can help organizations improve risk management and accelerate incident detection/response.
- **Integrated with cloud-based threat intelligence.** A network security architecture should extend to cloud-based threat intelligence, detailing things like software vulnerabilities, bad IP addresses, rogue URLs, known C&C channels, malicious files, indicators of compromise (IoCs), and rapidly changing attack patterns.
- **Built for automation.** Ultimately, a network security architecture takes advantage of internal and external security intelligence to help organizations automate their network security defenses. For example, anomalous traffic in the data center can trigger an automated firewall rule that terminates flows based upon a combination of factors like source IP, port, protocol, and DNS activities. Alternatively, when malware is detected, the network can review file downloads and retroactively discover and remediate endpoints that downloaded suspect files from particular URLs. Automated remediation activities like these can lead to continuous improvement in network security controls and help systematize security investigations for more rapid response.

In aggregate, a network security architecture can not only address existing challenges, but also provide business, IT, and security benefits (see Table 1).

Table 1. Network Security Architectures Characteristics

Network Security Architecture Property	Details	Functionality	Benefits
Central command and control	Service management, cloud/server virtualization orchestration interoperability, central monitoring and reporting	Centralizes policy management, provisioning, configuration management, change management, event management, etc.	Streamlined security operations, ease-of-use, central control and visibility across all network security elements independent of location or form factor
Distributed enforcement	Any network security service, any location, any form factor, integration between network and endpoint security	Coordination across network services, extension of security policy enforcement to the cloud	Tailored layered security for various use cases to protect users, devices, and applications, can be easily enhanced or modified for new types of threats
Integrated actionable intelligence	Diverse data sources including baked-in cloud-based threat intelligence	Provides granular details about application traffic, network traffic, endpoint activities, and new threats "in the wild"	Allows security team to make decisions based upon real-time intelligence, provides for automation for remediation processes

Source: Enterprise Strategy Group, 2014.

Cisco Network Security Architecture: Threat-focused Next-generation Firewall

While Cisco Systems has always been recognized for its network security products, the company has had to evolve its technology vision in order to keep up with burgeoning enterprise requirements and an increasingly dangerous threat landscape. In pursuit of this goal, Cisco made a bold move in 2013 with its acquisition of network security innovator Sourcefire.

While the Cisco/Sourcefire merger brought together two network security giants, there was still a lot of work ahead to integrate the technologies to form the type of enterprise-class network security architecture described previously. This effort is now starting to bear fruit with the announcement of Cisco ASA with Firepower Services. With the combination of Cisco ASA firewall and Sourcefire's next-generation IPS and advanced malware protection in a single device, Cisco now offers a comprehensive set of network security services for:

- **Granular application visibility and control.** Like other NGFWs, Cisco can detect and report on application connections and apply granular control policies based upon users, groups, devices, etc. Now with FirePOWER, Cisco will likely extend its application visibility and control throughout the network and integrate these capabilities with other Cisco assets like TrustSec and its Identity Services Engine (ISE).
- **Threat-centric protection across the network and endpoints.** Cisco's network security architecture includes comprehensive threat protection and advanced malware detection/prevention functions using FirePOWER for network protection and FireAMP for endpoint security coverage. Threat detection/prevention is further enhanced with FirePOWER NGIPS, reputation- and category-based URL filtering, and its wide-ranging threat intelligence. FireAMP can also track endpoint activity for historical analysis. When a new malware file is discovered, FireAMP can apply retrospective security policies to identify and fix endpoints that encountered the file in the past. Finally, Cisco combines IPS events, threat

intelligence, and malware events to provide detailed IoCs that can help the security team improve or automate security investigations and remediation processes.

- **Multiple security services with end-to-end visibility.** Cisco now offers a full portfolio of physical and virtual security services for firewalling, application control, IDS/IPS, URL filtering, advanced malware detection/prevention, etc. This enables enterprises to customize their layered protection for users, applications, network segments, and network flows using multiple form factors and covering all network locations. Cisco also provides monitoring and visibility across all of these services/locations to eliminate blind spots.
- **Impact assessment.** The Cisco network security architecture is designed to correlate intrusion events to the possible impact an attack may have on a particular target. Cisco displays this correlation through a series of five different "impact flags." An impact flag rated as number one indicates an event that corresponds to a vulnerability mapped to a particular host that demands immediate attention, while other impact flags have lower priorities. In this way, Cisco can help already overburdened security professionals determine where to apply their scarce resources and thus improve security protection and operational efficiency.

Cisco believes that the combination of ASA and FirePOWER can improve security across the attack continuum before, during, and after a security attack. In the "before" phase, Cisco's network security architecture can be used to discover network assets, enforce security policies, and harden controls for improved protection. In the "during" timeframe, ASA and FirePOWER can be used to detect malicious/suspicious activities (on networks and endpoints), block network connections, and thus defend the network as a whole. Finally, Cisco's network security architecture can add value in the "after" period by helping security analysts scope the impact of a breach, modify controls for containment, and leverage forensic data to accelerate remediation processes.

Cisco knows that there is still work ahead and has many additional architectural features on its 12 to 18 month roadmap. Cisco also realizes that many CISOs will need help assessing their current network security defenses and creating a plan to build a network security architecture. Cisco has a number of specific services offering to help organizations in these areas.

The Bigger Truth

There are a number of widely agreed-upon cybersecurity realities:

1. IT is growing more complex, driven by virtualization, mobility, and cloud computing.
2. The threat landscape is increasingly dangerous and targeted attacks are particularly difficult to prevent, detect, and remediate.
3. Legacy network security defenses are less effective than they were in the past.
4. Many organizations are lacking network security skills in one or more area.

Overall, this paints a very frightening picture where cybersecurity risk increases on a daily basis.

As Albert Einstein once said, "The definition of insanity is doing the same thing over and over again and expecting different results." Sage advice, but this is exactly what many CISOs are doing when it comes to network security. It's time that business, IT, and security leaders realize that they are fighting a losing battle. Cybercriminals are using new types of offensive weapons and tactics, so enterprises must counter this offensive with new types of defenses that can help them improve protection, detection, and response.

ESG believes that these enhancements won't come from incremental tactical changes to legacy network security defenses. Rather, enterprises need to move forward with a more strategic change: an end-to-end integrated network security architecture. The combination of Cisco and Sourcefire offered intriguing possibilities when the two merged in 2013. Now that Cisco has integrated the best of ASA firewall, FirePOWER NGIPS, Advanced Malware Protection, and its collective threat intelligence, Cisco may establish another leadership plateau with its integrated network security architecture.

Enterprise Strategy Group | **Getting to the bigger truth.**

20 Asylum Street | Milford, MA 01757 | Tel: 508.482.0188 Fax: 508.482.0218 | www.esg-global.com