

White Paper

The Network Application Security Architecture Requirement

By Jon Oltsik

March, 2011

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



Contents

Executive Summary3

The New Network “Balancing Act”3

 Existing Security Safeguards Aren’t Enough.....4

What’s Needed? A Network Application Security Architecture.....6

The Bigger Truth8

All trademark names are property of their respective companies. Information contained in this publication has been obtained by sources The Enterprise Strategy Group (ESG) considers to be reliable but is not warranted by ESG. This publication may contain opinions of ESG, which are subject to change from time to time. This publication is copyrighted by The Enterprise Strategy Group, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of the Enterprise Strategy Group, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact ESG Client Relations at (508) 482-0188.

Executive Summary

In the past, applying network security policies at an enterprise organization meant deploying network firewalls with rules for blocking IP addresses, specific protocols, and TCP ports. This was effective for things like preventing IT employees from using cleartext Telnet traffic over port 23 for remote system administration or making sure SNMP events remained within the building. Unfortunately, existing safeguards are no longer enough. Why? Because of an onslaught of new Web-based and social networking applications. Unlike other network services, Web-based applications and social networking traffic typically travels over wide open port 80, making it more difficult to monitor application traffic, let alone block security threats. These applications can be useful, but they also introduce new risk to network performance, IT operations, and security attacks.

How can the CISO deal with burgeoning Web-based and social networking apps AND new mobile devices concurrently? This white paper concludes:

- **Mobile device use exacerbates the problem.** As if Web-based applications alone weren't enough, the risks associated with them are aggravated by the growing use of mobile devices like smart phones and tablet PCs. These new devices increase Web-based and social network application traffic and simultaneously make it more difficult to understand the person and device accessing these applications.
- **IT cannot depend upon existing security solutions for help.** Firewalls, IDS/IPS, and application firewalls offer some protection, but product gaps leave organizations vulnerable. For example, application firewalls may block some Web applications but still allow enough YouTube or Skype traffic to impact network performance overall. Regrettably, historical defenses based upon "islands of security" are no match for the traffic volume, malicious code threats, and ever-changing patterns of today's Web-based applications and social networks.
- **Large organizations need a new architectural solution.** To address the threats posed by Web-based applications and social networking, enterprises need a new network application security architecture. Why an architecture? Because of the need for an integrated scalable security solution that extends existing security safeguards for policy enforcement, provides central command-and-control, and interoperates with the network itself. The network application security architecture will provide application visibility, user/device context, and centralized policy management.

The New Network "Balancing Act"

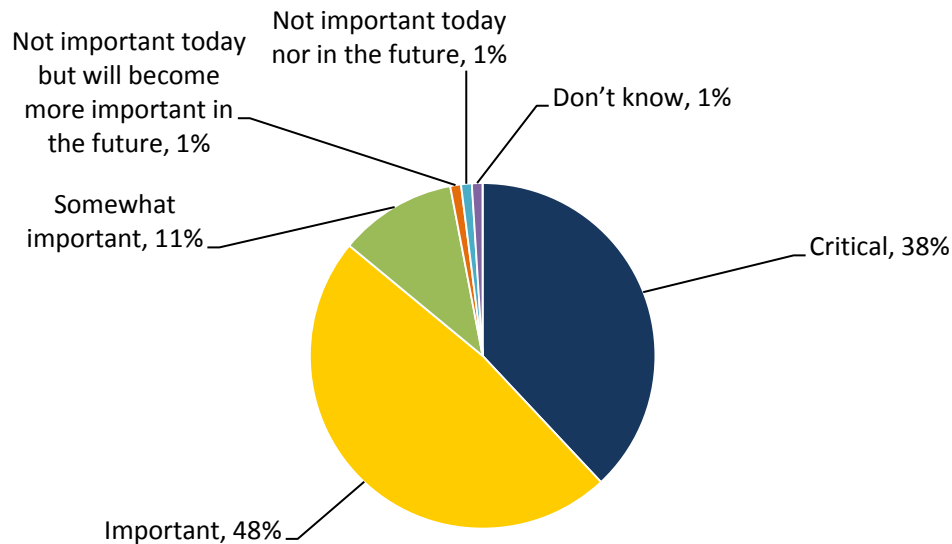
Over the past few years, IT managers have had to deal with an avalanche of changes. Some of these changes, like server virtualization and SOA, are profound but still managed within the confines of the IT department. Yes, these changes impacted network security, but IT managers were usually able to anticipate—and address—these changes as part of IT project management and deployment plans. Unfortunately, CIOs face additional changes that are much harder to control. The last few years initiated a new trend, the consumerization of IT technologies, leading to an onslaught of:

- **New types of Web-based applications.** IT managers have long been challenged by things like Web mail and instant messaging (IM), but this is just the tip of the iceberg. Today's employees can make Internet phone calls using Skype, watch full length videos on YouTube, or connect with friends via Facebook, LinkedIn, or industry-specific social networking sites like GovLoop. In some cases, these applications can enhance productivity, but they can also become a resource drain if they aren't adequately managed.
- **An army of new devices.** While PC management remains difficult, IT administrators are now being asked to support new devices including Macintosh PCs, smart phones, and tablets. A few years ago, these devices were viewed as a novelty, primarily used by executive management to access e-mail from the road, but now many organizations have gone well beyond this fringe use-case. In a recent survey of enterprise organizations (i.e. 1,000 employees or more), more than three-quarters of firms believe that mobile devices

are either a “critical” or “important” part of employee productivity or business processes (see Figure 1).¹ Of course, Web-based applications and social networking is a primary mobile device application.

Figure 1. Mobile Devices Have Become Important Business Tools for Enterprise Organizations

How important would you say the use of mobile devices by employees is to your organization’s business processes and productivity? (Percent of respondents, N=174)



Source: Enterprise Strategy Group, 2011.

Consumer-oriented Web-based applications and multiple devices per user present a new opportunity for progressive CIOs. How? Web-based applications can help employees collaborate with others inside and outside the organization to broaden their skill sets or to address a particularly vexing problem. Mobile devices can be used for location-aware and graphically-oriented applications or simply to provide real-time e-mail access at all times. In spite of these benefits, however, new applications and devices carry a burden as well: new security challenges. Consumer-oriented applications can require inordinate network resources for one thing and social networking sites like Facebook and Twitter are often used by cyber criminals for malware distribution and social engineering scams. Similarly, Android and Apple iOS platforms are quickly becoming a new and attractive hacker target.

CISOs face a daunting challenge: given the potential productivity losses, few organizations will opt for draconian measures like blocking Web-based applications or denying network access to mobile devices. Rather, most want to control access and monitor user and network behavior to enable business processes while protecting their precious IT assets. This is certainly a worthwhile goal, but the question remains: How can this be done?

Existing Security Safeguards Aren't Enough

New applications and devices are nothing new. CISOs have had to deal with Web mail, IM, and a myriad of other Web-based applications and services for years. The same is true for Blackberry and Windows Mobile phones which have long had access to corporate application and data. This being the case, skeptical security professionals may believe that existing network security safeguards like firewalls, IDS/IPS appliances, and various network gateways can offer ample protection from the Web-based application and mobile device threats du jour. Sadly, this is not the case. While they do provide some protection, existing security defenses are no longer adequate because they lack:

- **Application visibility.** Blocking IP addresses, ports, and protocols provides basic network security, but these defenses provide carte blanche to applications—and attacks—riding along with HTTP traffic over open port 80. Proper visibility tools also require the scale to handle the growing bandwidth demands of these Web 2.0

¹ Source: ESG Research, 2010.

applications. Some “port-agile” applications actually hop from port to port and thus cannot be blocked by simple firewall rules. When network security tools lack application visibility, CISOs may have a single binary option: allow or deny application traffic.

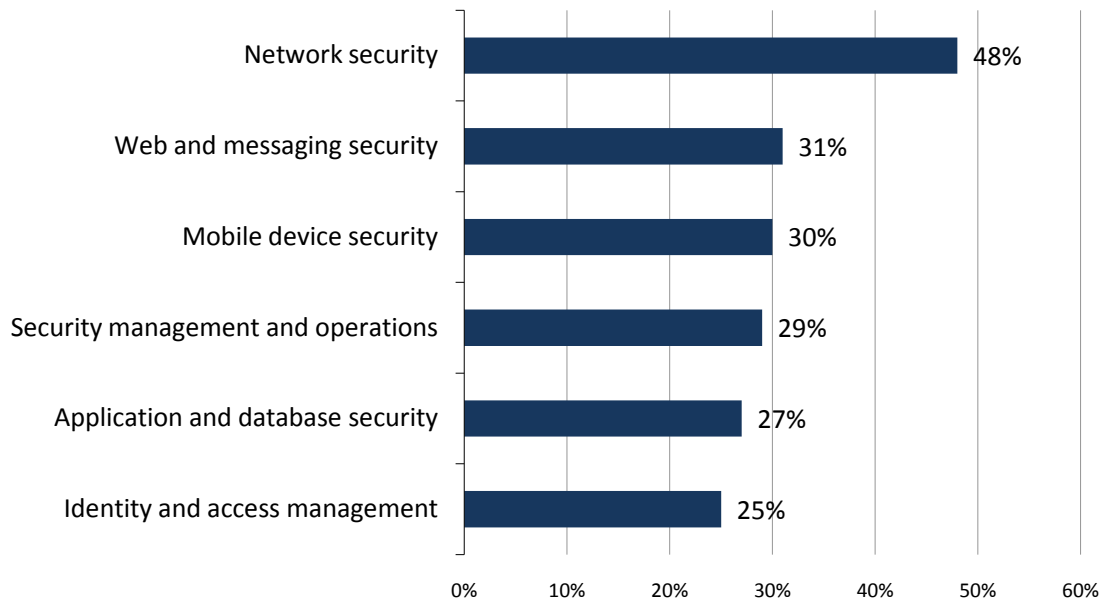
- **A scalable architectural approach.** Most organizations acquire tactical security tools over time in a piecemeal fashion, which can lead to gaps in visibility, functionality, and security defenses. For example, an IDS/IPS rule may recognize a malicious code threat propagated by LinkedIn, but a single signature can’t identify applications, restrict application access, or throttle network traffic. What about UTM devices? Most of these systems lack the right application layer functionality and can’t scale performance when multiple packet filtering operations are required concurrently. While many of these security functionality gaps are not new, Web-based applications accentuate stovepipe security tool weaknesses.
- **Integration with the network.** Even with strong security controls, Web-based applications can act as a denial-of-service attack by hogging network resources. If the entire inside sales department is watching YouTube videos during their lunch break, it could slow networks to a crawl and disrupt latency-sensitive applications like IP telephony.

These functionality and integration holes lead to inevitable security problems. Organizations have no visibility into who is using which Web-based application. Network traffic spikes impact mission-critical applications. Help desk call volume escalates. In the meantime, CIOs are forced to handle increasingly complex network security with point tools, reactive policies, one-off security enforcement, and guesswork. Little wonder, then, why many organizations are willing to throw money at the problem. According to ESG research, global companies plan to address these shortcomings by purchasing an assortment of security tools in areas like network security, Web/messaging security, mobile device security, and others to fill these gaps (see Figure 2).²

Yes, these next-generation tools may improve functionality, but there must be a better solution than simply bringing in new tactical stovepipe tools.

Figure 2. Security Spending Intentions for 2011

With regards to specific spending plans for security, in which of the following areas will your organization make the most significant investments over the next 12-18 months? (Percent of respondents, N=286, five responses accepted)



Source: Enterprise Strategy Group, 2011.

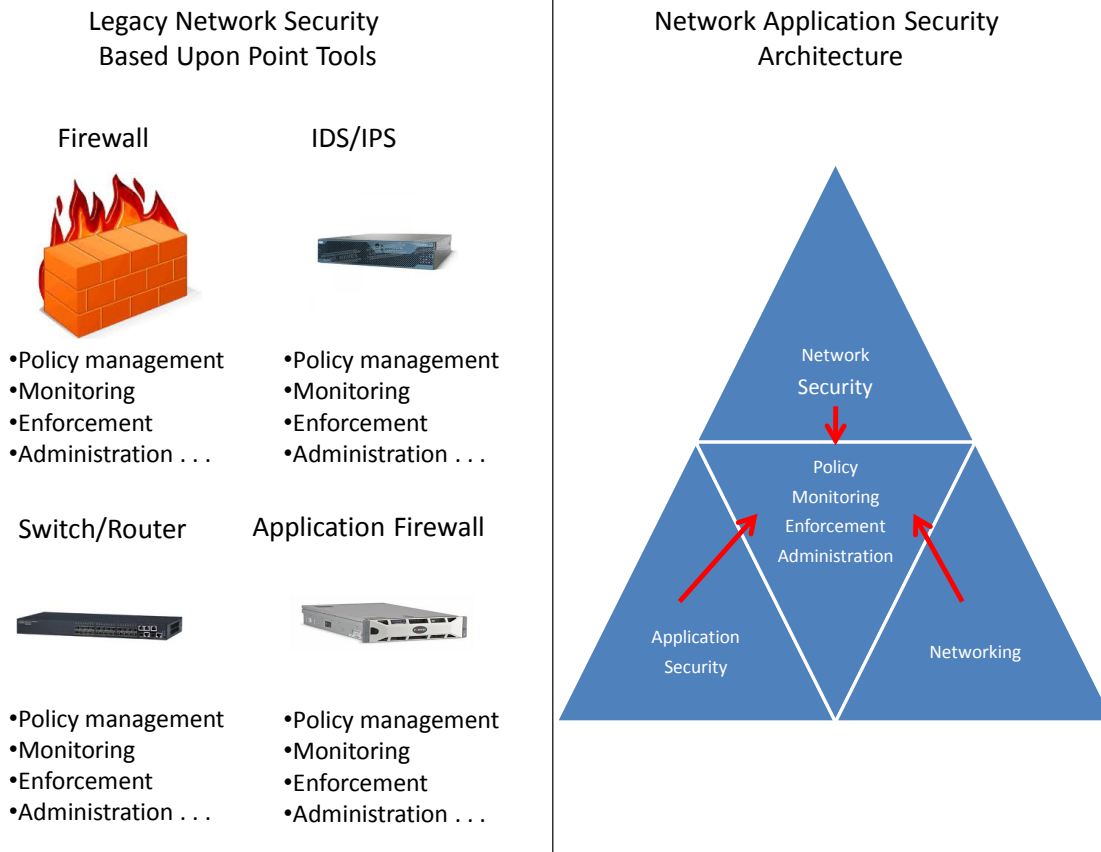
² Source: ESG Research Report, [2011 IT Spending Intentions Survey](#), January 2011.

What’s Needed? A Network Application Security Architecture

Traditional security approaches have suffered historically from two design flaws. As discussed above, many organizations purchase tactical point tools over time, leading to “islands of security.” This lack of technical integration makes existing point tools only marginally effective when dealing with security challenges presented by Web-based applications and mobile device proliferation. Aside from this, security tools have also been deployed “on top of” existing technologies like networks and applications. As such, they tend to be implemented as an afterthought, adding a layer of complexity to the existing IT and network infrastructure.

Given the scale and scope of consumer-oriented applications, CIOs need to think beyond status quo solutions and embrace a more holistic Network Application Security Architecture model (see Figure 3). Rather than separate security functionality, network application security merges application visibility, policy management, and enforcement with existing network security safeguards like firewalls, IDS/IPS, and DDOS protection. Furthermore, network application security merges security and network policy enforcement. In other words, network application security blocks unwanted application access AND prioritizes mission-critical business traffic.

Figure 3. Network Application Security Architecture Versus Legacy Security



Source: Enterprise Strategy Group, 2011.

To make this happen, network application security must include:

- **Application visibility.** Before taking any security action, it is important to first understand the scope of the problem: which applications are being accessed. This is more difficult than it seems. Many application formats are unique, port-agile, and unusual, while others look like common HTTP traffic flowing over port 80. To address these blind spots, network application security must assess all traffic and identify all internal and Web-based applications accurately. This application visibility requirement adheres to the old business adage, “you can’t manage what you can’t measure.”

- **User context.** Aside from what applications are being used, it is also important to know which employees are accessing them. Why? Because it is critical to know who is doing what in order to assess risk. An HR recruiter may have a valid business reason for accessing LinkedIn, but a manufacturing manager spending three hours a day “Skyping” with people in South America may indicate a problem employee and a potential security risk. Ultimately, CISOs want to create a matrix of Web application access patterns by users and groups and then present this to HR, business managers, and the CIO as background for future policy decisions.
- **Application policy management.** Armed with user-based application usage knowledge, CISOs can then take the next logical step and analyze whether existing application access patterns improve productivity or simply increase risk. Should all employees be able to talk to contacts abroad via Skype during business hours? Should some or all employees have access to Facebook? Should some Facebook applications be prohibited and some allowed? Based on the answers to these questions, CIOs can work with business managers to create acceptable use policies for consumer-oriented application usage. In addition, organizations can look at traffic patterns for critical applications and then implement policies to prioritize this traffic at all times.
- **Common application policy enforcement.** Few organizations want to block all Web applications. Rather, CIOs would prefer to grant access to a handful of applications to specific groups of users. Furthermore, application access may permit some functionality and deny others. For example, employees may be allowed to update their Facebook accounts from work, but be prohibited from using its communications features, playing games, or uploading videos to their accounts. This can only be done when network application security combines deep Web-based application knowledge with user context, lives at the network perimeter, and has the processing horsepower to enforce security policies at line speed.
- **Threat management functionality.** Since social networking sites have become a nexus for malicious code and social engineering exploits, network application security must also include security countermeasures that detect or prevent known attacks. Network application security does this through tight integration between Web application firewalls and existing security tools like firewalls and IDS/IPSs, reducing risk in several ways. Only a small subset of users can be provided with access to Facebook, limiting overall exposure. These users may be restricted to particular Facebook functions, further reducing the potential attack surface. Dedicated security systems like IPS/IDS can also weed out malicious code with attack signatures or behavioral heuristics. This kind of defense-in-depth is also useful for preventing DDoS attacks against critical internal applications emanating from the Web.
- **Network integration.** Finally, network application security works with the underlying network itself to prioritize traffic based on its identity and profile. This enables business-centric policy enforcement like ensuring that latency-sensitive applications like IP telephony always get network priority over Web-based application traffic. The network can then measure traffic thresholds and throttle Web application traffic when necessary.

In essence, network application security combines all of these requirements into a simple and scalable set of solutions. Application monitoring and policy management are centralized so IT can respond to business needs more efficiently. Finally, policy enforcement is coordinated over existing security systems, application-specific security safeguards, and within the network itself. This demands tight integration in security and networking operating systems and hardware.

The Bigger Truth

On balance, the role of a CISO is to help the organization minimize risk as it gains productivity benefits from IT applications and services. The most difficult aspect of this job is keeping up with perpetual changes on both sides—security and operational risks as well as new IT systems and devices.

Web-based applications, social networking sites, and mobile devices are a clear example of this type of quandary. New applications and devices can help IT improve productivity, enable business processes, and empower employees, but they also introduce new risks. Unfortunately, CISOs cannot address these new risks with their existing portfolios of status quo security tools that weren't designed for this purpose.

What's needed? A holistic solution that can be used to support business needs, HR policies, network capacity requirements, and risk management objectives. ESG calls this a Network Application Security Architecture that offers:

1. Network, application, and security intelligence to provide a map of who is using which applications.
2. Central policy management and command-and-control.
3. Integrated enforcement of application access control, network priority, and application security.

Without this type of architecture, large organizations will face a Faustian compromise between business benefits on one hand and increased chaos on the other. By implementing a Network Application Security Architecture, CIOs can gain business benefits from new applications and devices while minimizing risk.



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