Selecting a Next-Generation Firewall: Top 10 Considerations

Must-Haves for Midsize Companies

What You Will Learn

Many midsize companies have reached a critical moment with their network security: They must reinforce their traditional security solution to address new trends arising from mobility and cloud, and meet a rising threat landscape. These dynamics complicate the challenge of maintaining network security, and tax the network's ability to perform optimally for the business.

Traditional firewalls are not effective at seeing what users are doing, the types of applications they're accessing, or the devices they're using. Next-generation firewalls are designed to help close some of the gaps. This document offers 10 considerations for midsize companies to weigh when evaluating a next-generation firewall solution:

1. Is the firewall built on a comprehensive stateful firewall foundation?
2. Does the solution support robust, secure remote access for mobile users?
3. Does the firewall provide proactive threat protection?
4. Can the firewall maintain performance when multiple security services are running?
5. Does the solution offer deep visibility into applications with granular application controls?
6. Is the firewall able to deliver user, network, application, and device intelligence to help drive context-aware protection?
7. Does the firewall offer cloud-based web security?
8. Can you deploy a future-proof solution that can scale as your organization grows?
9. Does the firewall vendor have extensive support and services to ease the migration path?
10. Does the firewall vendor offer attractive financing options to speed deployment time?

Cisco ASA 5500-X Next-Generation Firewall (NGFW) provides an "all in one" solution featuring a range of next-generation firewall services that are affordable and easy to deploy and manage. Discussed in this white paper is how the Cisco ASA 5500-X NGFW—as compared to other next-generation firewall solutions currently available in the market—helps organizations of all sizes to:

- Stay ahead of today's emerging threats with collective security intelligence
- See and control user activity, device access, and malicious behavior
- Reduce complexity, capital, and operating costs with fewer devices to manage and deploy

Chance of a Network Compromise: 100 Percent

According to the Cisco 2014 Annual Security Report, "all organizations should assume they've been hacked."[1] Cisco Security Intelligence Operations (SIO) researchers found that malicious traffic is visible on 100 percent of corporate networks; this means there is evidence that adversaries have penetrated these networks and may be operating undetected over long periods.[2]

- These findings underscore why it's critical for all organizations—large or small—to deploy a next-generation firewall solution that can provide continuous security and end-to-end visibility across the network. Successful attacks are inevitable, and IT teams must be able to determine the scope of the damage, contain the event, remediate, and bring operations back to normal—fast. Organizations should therefore consider these questions when choosing a next-generation firewall solution:

1. *Cisco 2014 Annual Security Report*: http://www.cisco.com/web/offers/lp/2014-annual-security-report/index.html.
2. Ibid.

1. Is the firewall built on a comprehensive stateful firewall foundation?

A next-generation firewall needs to understand both threat traffic and network traffic. It also must be able to identify which users are connecting to the network and from where, what devices they're using, and which applications and websites they're accessing. A solution built on a comprehensive stateful firewall foundation also can provide visibility into potential security gaps, such as open ports.

The foundation for the Cisco ASA 5500-X is built on the world's most widely deployed and most proven stateful inspection firewall. It features an extensive stateful inspection engine that helps protect critical assets while also delivering high-performance security and reliability. The Cisco ASA 5500-X NGFW maximizes network security with clear, deterministic Layer 3 and Layer 4 policies. Capabilities such as site-to-site virtual private network (VPN), network address translation (NAT), and dynamic routing also help secure the perimeter and provide access control.

2. Does the solution support robust, secure remote access for mobile users?

Today's users require anywhere, anytime access to the network from a variety of company-owned and personal mobile devices. But opening up the network to accommodate this type of access leads to loss of control and visibility. To provide secure connectivity from device to application while also protecting the network, organizations need to know, at all times, what types of user devices are attempting to gain access to the network, and from what location.

Cisco provides the only next-generation firewall solution that can deliver user identity, application, and device awareness to enforce access control and mitigate threats. Cisco combines network-wide identity and fine-grained behavior controls with the class-leading VPN technology, Cisco AnyConnect®. Installed on more than 150 million endpoints, AnyConnect is the most widely used VPN, as well as the most mature and comprehensive secure mobility client in the market today. AnyConnect provides the information on user identity and location, device operating system and version, and user access privileges that the ASA 5500-X NGFW needs to enforce network access based on context.

3. Does the firewall provide proactive threat protection?

The Cisco ASA 5500-X NGFW blocks the majority (> 80 percent) of malware at the gateway, with minimal intervention required from administrators. It does this with near-real-time threat intelligence from Cisco SIO, the world's largest cloud-based security ecosystem. Cisco SIO correlates intelligence in the cloud from 100 terabits of live data feeds from more than 1.6 million deployed Cisco email, web, firewall, and intrusion prevention system (IPS) solutions.

Cisco ASA Next-Generation Firewall Services use the same URL filtering database as Cisco Web Security solutions. Cisco SIO takes advantage of its visibility into more than a third of global Internet traffic to update this database—which includes more than 50 million blocked sites—every five minutes. Unlike next-generation firewalls that use third-party URL filtering solutions, Cisco owns its technology. And while some vendors only allow one URL filtering policy for the enterprise, organizations can use Cisco ASA Next-Generation Firewall Services to create URL-based rules for users and groups, creating differentiated access to the Internet.

4. Can the firewall maintain performance when multiple security services are running?

Purchasing, deploying, and then managing multiple, dedicated security services modules is a complex and expensive process. But it has long been the only way for organizations to scale for security services as their needs change.

As a single-box solution that combines firewall, VPN, anti-malware, and IPS, the Cisco ASA 5500-X NGFW provides acceleration hardware as part of its base platform. Security services can be turned on simply by activating the appropriate software license. Expanded security services are also delivered with minimal impact to network performance.

A recent lab test of enterprise firewalls[3] using real-world traffic found that the ASA 5500-X NGFW with IPS enabled can process 10 percent more connections per second over IPv4 and 24 percent more over IPv6 compared to competitive products. Other findings: UDP throughput using IMIX (IPv4 and IPv6) was 57 percent better, and HTTP traffic throughput on Cisco appliances was 60 percent greater than comparable competitor products.[4]

5. Does the solution offer deep visibility into applications with granular application controls?

Organizations can't control what they can't see. To ensure acceptable use and security policies are enforced within Web 2.0 websites that contain embedded applications, a next-generation firewall solution must be able to identify and control, with precision, individual applications utilizing application signatures or other methods.

Granular control is critical, considering the volume of actions that can be performed within a commonly used application such as Facebook: posting content, "liking" a user's status, sending mail, chatting, and more. Micro-applications used within a bigger application, such as Farmville on Facebook, also must be identified and considered when making access control decisions.

Cisco ASA Next-Generation Firewall Services offer highly granular controls that allow administrators to create firewall policies that match the nuanced business needs of today. They not only identify more than 1200 applications, but also more than 150,000 micro-applications.

3. *Miercom Lab Testing Summary Report*, July 2012.
4. Ibid.

Cisco ASA Next Generation Firewall Services also identify application behavior: what action a user is taking within an application. As an example, the Facebook Videos category identifies whether a user is uploading, tagging, or posting a video. An administrator may set a granular control for this category, allowing users to view and tag videos, but not upload a video.

6. Is the firewall able to deliver user, network, application, and device intelligence to help drive context-aware protection?

Network intelligence allows organizations to set differentiated security policies for users, particularly those coming into the network from other locations and using their own devices.

Cisco ASA 5500-X NGFW receives rich information from the Cisco Identity Services Engine (ISE), which, like the Cisco AnyConnect service, helps organizations support BYOD more securely. ISE offers insight into device profiles, device postures, 802.1x authentication details, and more. This capability on the Cisco ASA 5500-X NGFW enables organizations to deliver consistent and granular access control.

7. Does the firewall offer cloud-based web security?

Threat protection delivered through the cloud can help organizations of all sizes gain a highly distributed security perimeter that can enable new applications and protect all users proactively.

Cisco Cloud Web Security, powered by Cisco SIO, is integrated into the Cisco ASA 5500-X NGFW. It provides zero-day protection to all users, regardless of location. Web security, application control, management, and reporting are fully integrated into a cloud-based service that provides industry-leading security and control, with 99.999 percent availability and uptime with zero-day threat protection through heuristics analysis.

8. Can you deploy a future-proof solution that can scale as your organization grows?

As an organization expands its operations, its security needs change. But scaling security solutions to meet changing business needs should not be cost-prohibitive—or increase administrative complexity.

Cisco provides an easily manageable single-box solution to support midsize companies as they grow. Cisco ASA 5500-X NGFW helps organizations reduce capital and operating costs by consolidating multiple security solutions including stateful firewall, VPN gateway, application control, web security, IPS, and anti-malware in one box. Cisco Prime Security Manager helps simplify Cisco ASA 5500-X NGFW deployments and reduce administration complexity with a single, unified management console.

Cisco has a complete portfolio of next-generation firewall solutions that enable organizations to scale from the smallest branch to the largest Internet-edge deployment. Additionally, Cisco's recent acquisition of Sourcefire introduces enterprise security solutions that can interoperate with the ASA 5500-X NGFW:

- **Sourcefire Next-Generation Intrusion Prevention System (NGIPS)**, which provides advanced threat protection, integrating real-time contextual awareness, intelligent security automation, and industry-leading threat prevention effectiveness.[5]
- **Advanced Malware Protection for FirePOWER™,** a comprehensive malware-defeating solution that enables malware detection and blocking, continuous analysis, and retrospective alerting that leverage Sourcefire's cloud security intelligence.

Sourcefire enterprise-class advanced malware analysis and protection solutions are among the first to use big data analytics to provide the visibility and control that organizations need to discover, understand, and stop threats missed by other security layers.

9. Does the firewall vendor have extensive support and services to ease the migration path?

Migrating to a next-generation firewall is a major undertaking. Every business infrastructure is unique, and maintaining security while transitioning to a new solution requires detailed planning and careful change management. Even short periods of downtime can undermine profitability and security. Any next-generation firewall vendor or their certified partners must be able to provide deep experience, knowledge, leading practices, and tools (including those of others) to minimize disruption and support business continuity during migration—and do so cost-effectively.

Cisco Migration Services for Firewalls helps organizations migrate smoothly to the new Cisco ASA 5500-X NGFW platform, whether they're transitioning from a legacy Cisco or third-party firewall. Cisco security engineers, as well as Cisco Security Specialized Partners, provide expert guidance and support to help organizations maintain security during a migration, and improve the accuracy and completeness of the process. Cisco Migration Services for Firewalls can support a migration with remote or on-site services, or a combination of the two, depending on an organization's needs and preferences.

Additionally, the Cisco SMARTnet® Service helps reduce network downtime and other critical network issues with expert technical support, flexible hardware coverage, and proactive device diagnostics. IT personnel have anytime access (24 hours, 365 days a year) to specialized engineers in the Cisco Technical Assistance Center (TAC), as well as to an extensive range of self-support resources, tools, and training through Cisco's online knowledge base.

[5] For more information on Sourcefire NGIPS, visit http://www.sourcefire.com/products/next-generation-network-security/ngips-ngfw-features.

10. Does the firewall vendor offer attractive financing options to speed deployment time?

Spreading the cost for a next-generation firewall solution over time makes budgeting easier and payments more manageable. Vendors that provide financing give organizations the freedom to acquire the technology they need to grow their business as well as the flexibility to react to changing market needs. Investing in the right technology without making a large capital expenditure also enables organizations to channel financial resources into other areas of the business and drive success.

Financing from Cisco Capital allows organizations purchasing the Cisco ASA 5500-X NGFW to take advantage of a range of financing options at competitive rates, with the flexibility to defer payments and fund the entire solution, from technology to services. Visit www.ciscocapital.com for additional information and to find a local Cisco Capital representative.

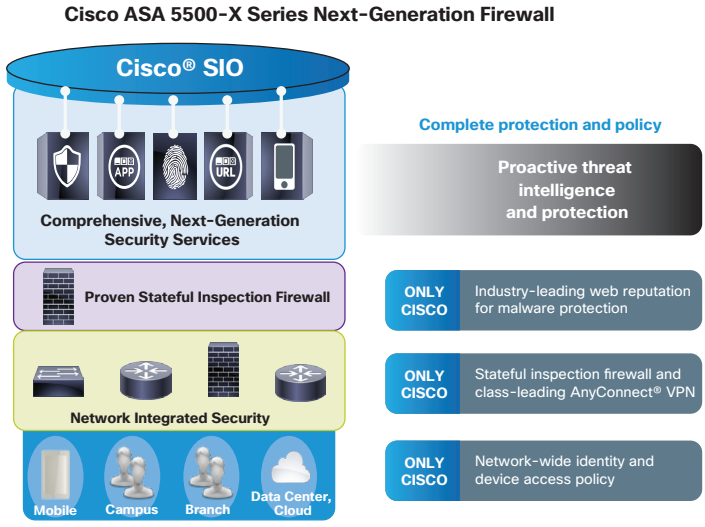
Making the Move to a New Security Model

A next-generation firewall is an important component of a threat-centric security model, which all organizations need to adopt to gain visibility across their network–and respond appropriately to threats before, during, and after an attack. As your midsize organization evaluates next-generation firewalls, keep in mind that any solution must:

- **Deliver comprehensive protection:** Defending the network in the modern threat landscape requires best-in-class anti-malware and intrusion protections based on vulnerability research, reputation scoring, and other critical factors.
- **Work with business policy:** A next-generation firewall must offer complete breadth and depth of policy enforcement for application use. It also must ensure that diverse collaboration and Web 2.0 applications used for both personal and professional reasons can be monitored and controlled, at a granular level, based on business policy.
- **Ensure policies are enforced by device and user:** A next-generation firewall must offer complete insight into what devices and users are accessing the network, and from what location. It also must ensure that security policies can be differentiated according to device type and are based on corporate policy.

A next-generation firewall solution also cannot degrade performance while ensuring protection, policy, consistency, and context all at once, and at wire speed.

Figure 1: Cisco redefines the next-generation firewall with the ASA 5500-X NGFW.



Cisco ASA 5500-X NGFW helps midsize organizations to meet these challenges, and stay ahead of today's emerging threats with collective security intelligence. It enables administrators to see and control user activity, device access, and malicious behavior. It also reduces complexity, capital, and operating costs with fewer devices to manage and deploy.

To learn more about the Cisco ASA 5500-X NGFW, visit www.cisco.com/go/asa.

C11-730935-00 02/14