White Paper

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?

A next-generation firewall should provide an “all in one” solution featuring a range of next-generation firewall services that are affordable and easy to deploy and manage. This paper will help you evaluate next-generation firewalls to make the best selection for your midsize organization.

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 to deploy a next-generation firewall solution that can provide continuous security and end-to-end visibility across the security 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.

Making the move to a new security model

A next-generation firewall is an important component of a threat-centric security model. It’s important to move to a threat-centric model to gain visibility across your network and respond appropriately to threats before, during, and after an attack. As you evaluate next-generation firewalls for your organization, 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 protection 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 based on user, group, and device type (specific version of Apple iPhone, iPod, Android mobile devices, etc.).

Additionally, when multiple services are enabled, a next-generation firewall solution should not significantly degrade performance while it is ensuring protection, policy, consistency, and context all at once, and at wire speed.

Consider these key 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 and network traffic. A solution built on a comprehensive stateful firewall foundation can provide visibility into potential security gaps, such as open ports. The firewall should feature an extensive stateful inspection engine that helps protect critical assets while also delivering high-performance security and reliability. The next-generation firewall should maximize 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 to deliver secure, reliable access and robust perimeter security.

The next-generation firewall must also 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. Make sure that your firewall also provides visibility to users, devices, and applications.

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, who the users are, and what types of devices they are using to gain access to the network.

A next-generation firewall that can enable user identity, application, and device awareness helps you enforce access control and mitigate threats based on the context of the request. Network-wide identity and fine-grained behavior controls combined with VPN technology can help you secure your network and your mobile users.

3. Does the firewall provide proactive threat protection?

A proactive next-generation firewall will block the majority (> 80 percent) of malware at the gateway, with minimal intervention required from administrators.

Look for a strong integrated web filtering database. Web filtering solutions that allow you to create more than one URL filtering policy let you deliver differentiated access to the Internet. You can create web or URL filtering rules for different users and groups, according to their requirements.

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. In the past, this was the only way organizations could scale as their needs changed. Now, with next-generation firewalls, you can reduce the number of boxes to manage and deploy with a single-box solution that combines firewall, VPN, web security, anti-malware, and intrusion prevention system (IPS) solutions.

Purpose-built security acceleration hardware (for example, crypto and regular expression to speed up VPN and IPS processing) needs to be part of the base platform to deliver multiple layers of advanced security on top of the firewall without performance impact.

To simplify administration, look for advanced security services that can be turned on simply by activating the appropriate software license. Expanded security services should be delivered with minimal impact to network performance.

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.

Next-generation firewall services that offer very granular controls allow administrators to create firewall policies that match the nuanced business needs of today. Granular application 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. Administrators must be able to easily identify tens of thousands of applications and micro-applications, such as games for Facebook (for example, FarmVille, Candy Crush Saga, and Bingo Blingo), Facebook Messages, and Facebook Chat, when making access control decisions.

A next-generation firewall should be able to identify application behavior: what action a user is taking within an application. Administrators also should be able to set granular controls for specific categories like Facebook Video—for example, allowing users to view and tag videos, but not upload videos.

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. Look for a firewall that helps you support your organization's bring-your-own-device (BYOD) practices more securely.

Insight into device profiles, device postures, and 802.1x authentication details 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.

Look for a firewall that provides zero-day protection to all users, regardless of location. A best practice is to deliver web security, application control, management, and reporting 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.

A next-generation firewall should be an easily manageable single-box solution that supports your midsize organization as it grows. Does your next-generation firewall 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? Does it simplify next-generation firewall deployment and reduce administration complexity with a single, unified management console?

Additionally, can your vendor help you scale as your organization grows and your requirements change? Turn to a single source vendor that can help you deploy a comprehensive security solution that includes next-generation firewall, next-generation IPS, and advanced anti-malware protection for advanced threat protection, integrating real-time contextual awareness, intelligent security automation, and industry-leading threat prevention effectiveness.

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.

In addition to offering innovative firewall solutions, the vendor must be able to provide professional services to help improve your migration experience, minimize disruption, and support business continuity during migration.

When choosing a firewall vendor, make sure the vendor and its specialized partners can help your organization achieve both an accurate and complete migration. Whether you're upgrading to a new platform, or migrating from a third-party platform, confirm that the services provider has the deep experience, knowledge, leading practices, and tools required to mitigate risk as your organization migrates to a next-generation solution. Ask about service flexibility: Does the vendor only perform these services through on-site delivery? Can they be done remotely, or through a combination of on-site and remote delivery to support your organization's needs, preferences, and cost-sensitivity?

Technical assistance after installation is also an important consideration. Does your vendor provide your IT personnel with anytime access (24 hours, 365 days a year) to specialized engineers? Do they provide flexible hardware coverage, and proactive device diagnostics, self-support resources, tools, or online training? Great technical support helps reduce network downtime and keeps your organization up and running.

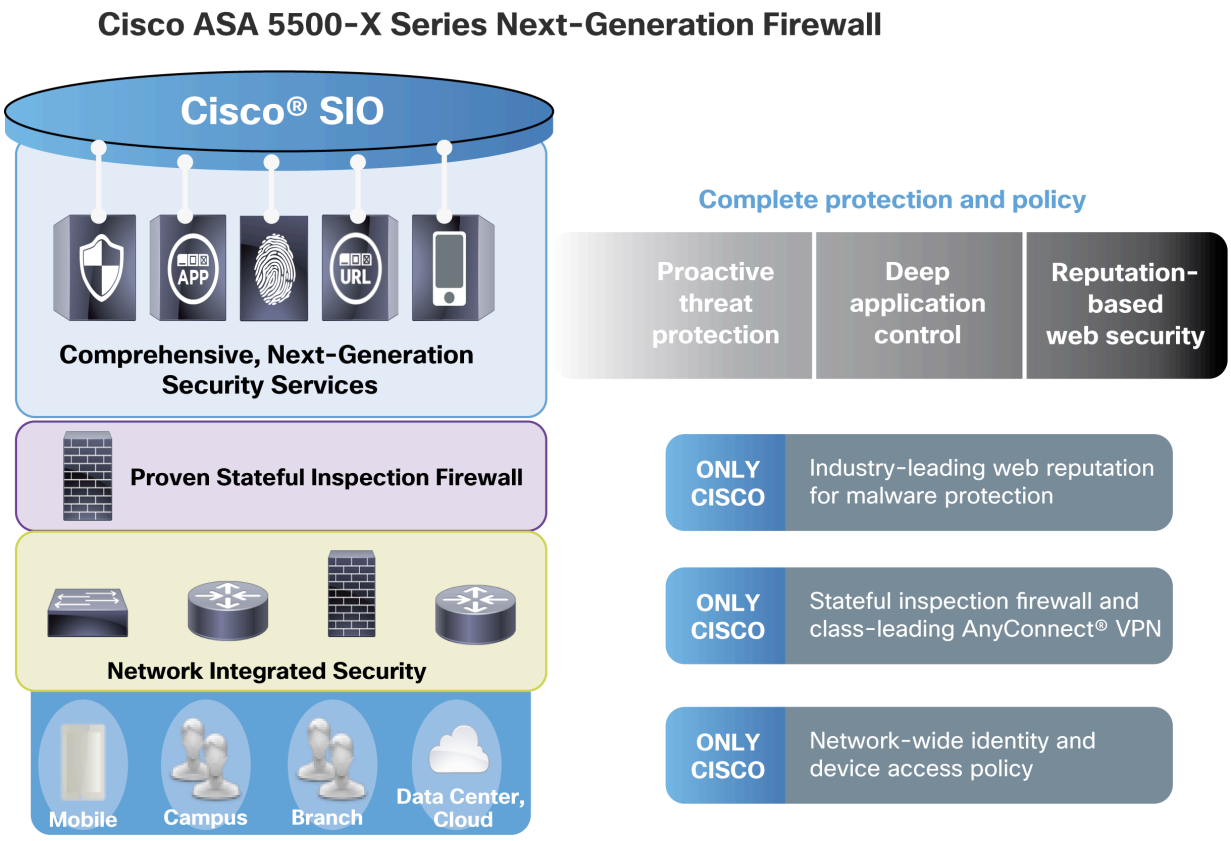
10. Does the firewall vendor offer attractive financing options to speed deployment time?

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 allows organizations to channel financial resources into other areas of the business and drive success. Look for financing options at competitive rates, with the flexibility to defer payments and fund the entire solution, from technology to services.

Stay ahead of threats while reducing cost and complexity

Cisco ASA 5500-X Series Next-Generation Firewall (NGFW) helps midsize organizations meet the key considerations outlined above, so they can stay ahead of today's emerging threats with collective security intelligence. It allows 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. Cisco, together with Sourcefire, delivers next-generation network security to address your requirements around BYOD, cloud, and emerging threats.

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



Cisco Migration Services for Firewalls, delivered by Cisco security engineers or Cisco Security Specialized Partners, helps organizations migrate smoothly to the new Cisco ASA 5500-X NGFW platform. Cisco provides expert guidance and support to help organizations maintain security during a migration, and improve the accuracy and completeness of the process. Cisco SMARTnet® Service helps reduce network downtime and other critical network issues with access to expert technical support 24 hours, 365 days a year, as well as flexible hardware coverage and proactive device diagnostics. Financing from Cisco Capital is available with terms that meet your business and financial requirements.

To learn more visit:

www.cisco.com/go/asa for more about the Cisco ASA 5500-X NGFW

www.cisco.com/go/services/security for more about Cisco Migration Services for Firewalls

www.cisco.com/go/smartnet for more about Cisco SMARTnet® Service

www.ciscocapital.com for additional information and to find a local Cisco Capital representative

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA C11-730935-00 02/14