White Paper

Requirements When Considering a Next-Generation Firewall

What You Will Learn

The checklist provided in this document details six must-have capabilities to look for when evaluating a next-generation firewall (NGFW) to determine whether the solution can provide comprehensive protection for your entire enterprise.

An NGFW must be able to:

- Integrate security functions tightly to provide highly effective threat and advanced malware protection
- Provide actionable indications of compromise to identify malware activity
- Offer comprehensive network visibility
- Help reduce complexity and costs
- Integrate and interface smoothly and transparently with third-party security solutions
- Provide investment protection

Background

Cybersecurity systems that rely exclusively on point-in-time defenses and techniques simply cannot keep pace with today's sophisticated and ever-evolving multi-vector attack methods. In fact, according to the Cisco 2014 Annual Security Report, every organization should assume it has been hacked.[1] Cisco threat researchers found that malicious traffic was visible on 100 percent of the corporate networks that they observed, meaning there was evidence that adversaries had penetrated those networks and were probably operating undetected over a long period.[2]

Today's multi-vector and persistent threats, fluid IT environments, and increasing network speeds are prompting more organizations to seek an NGFW solution that can also provide layered threat protection and integrated threat defense with best-in-class security technologies that work together transparently. However, while a range of solutions have emerged to try to meet this need, the NGFW just described is rare.

This checklist, and other purchase considerations outlined in this document, can help you confirm that you are investing in a truly effective NGFW solution. The firewall should provide a holistic view of the network, analyze real-time threats and network traffic effectively with scale, and help your organization defend against targeted and persistent malware attacks, including emerging threats.

The Foundation

As a first step in evaluating solutions, consider the foundation of the NGFW. This will be the starting point for your purchasing decision. To provide an integrated threat defense and multi-layered threat protection, the NGFW must

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

be built on a comprehensive stateful firewall foundation. Look also for a solution with a pedigree of proven performance.

The NGFW foundation should feature an extensive stateful inspection engine that helps protect critical assets by providing comprehensive visibility into underlying threats. The NGFW also should be robust enough to deliver highly effective threat protection at scale, even when multiple services are enabled. In addition, it should be able to identify not only threats but also users and devices that are connected to the network, and monitor their activities to determine anomalies.

The NGFW Checklist

Consult this checklist to confirm that the NGFW solution you are considering can provide protection, enforce policy, achieve consistency, and capture and share context all at once, and at wire speed:

- **The solution integrates security functions tightly to provide highly effective threat and advanced malware protection.**

  An NGFW should have tightly integrated security layers that communicate with each other. New ways of working, such as cloud computing and mobility, are expanding the attack surface area; correlation of threat intelligence among all security layers can identify attacks that slip through typical gaps in protection and evade detection. This level of protection requires ongoing coordination between defenses on the network, endpoints, and the central management console to help security teams track threats and initiate remediation activities rapidly.

  Look for a threat-focused NGFW that offers comprehensive threat and advanced malware protection to identify and protect against threats. Threat detection capabilities in the NGFW solution should help security teams not only to discover and stop malware, but also to understand it.

- **The NGFW provides actionable indications of compromise to identify malware activity.**

  Indications of compromise, or IoCs, are “tags” on a host that indicate that an infection has probably occurred. IoCs correlate network and endpoint security intelligence. They can identify malware activity on hosts and endpoints and provide highly accurate visibility into suspect and malicious behavior.

  An NGFW solution with these capabilities leads to faster identification, containment, and remediation.

- **The NGFW offers comprehensive network visibility.**

  An NGFW should provide full contextual awareness with a clear, holistic view of what is happening on the network at all times: users and devices, communications between virtual machines, threats and vulnerabilities, applications and website accesses, file transfers, and more.

  Comprehensive network visibility should entail a continuous and passive monitoring of all the assets in your network. This information can be used, through automation, to optimize security effectiveness with dynamic controls that respond in real time to changes in the IT environment or threat landscape. The solution should provide real-time insight that helps security teams to identify and address security gaps, fine-tune security policy, and ultimately, reduce the number of significant events.

  The NGFW also should be capable of automating the defense response after an attack, including infection scoping and containment, further reducing the burden on security teams.

- **The NGFW helps reduce complexity and costs.**

An NGFW that is effective against advanced threats unifies security across defense layers. An integrated, multi-layered approach can provide greater visibility into threats and consequently, better protection. Consolidating multiple boxes onto a single platform also eliminates the complexity and cost of purchasing and managing multiple solutions.

Look for an NGFW that also provides:

- **High scalability:** An NGFW with multi-layered threat protection will allow security administrators to deliver consistent and robust security at scale to small branch offices, Internet edge sites, and even large data centers in both physical and virtual environments.
- **Automation of routine security tasks:** The NGFW solution should automate these activities:
  - **Impact assessment:** The automatic correlation of threats against host vulnerability intelligence, network topology, and attack context helps security analysts focus their attention on only those intrusion events that warrant monitoring and a swift response.
  - **Policy tuning:** The automation of provisioning, tuning, and consistent enforcement of security policies throughout the enterprise helps security teams optimize security effectiveness and respond in real time to changing conditions and new attacks. The automation of security policy management is especially critical for resource-strapped IT departments.
  - **User identification:** The NGFW should be able to easily attribute user identities to security events. This saves security analysts time, helping them to contain and remediate threats more quickly.
- **The NGFW integrates and interfaces smoothly and transparently with third-party security solutions.**

An NGFW solution can help improve your total cost of ownership (TCO) and reduce the complexity of maintaining effective security for your environment in another way: by easily integrating and interfacing with third-party technologies. These include vulnerability scanners, software management solutions, trouble-ticketing systems, and security information and event management (SIEM) platforms that you have already deployed or need to implement.

Integration with third-party solutions deepens the multi-layered protection an NGFW solution provides by combining essential security layers into one platform. This approach simplifies security deployment and ongoing operational activities by supporting existing security technologies and sharing intelligence to coordinate and streamline responses.

Look for an NGFW that supports a rich solution “ecosystem” through open APIs for third-party technologies including:

- Vulnerability management systems
- Network visualization and SIEM systems
- Network access control (NAC)
- Network forensics
- Event response workflow

OTHER PURCHASE CONSIDERATIONS: MIGRATION SERVICES AND TECHNICAL SUPPORT

Migrating to an NGFW is a major undertaking. When moving to an NGFW, and away from third-party or traditional firewalls, look for a vendor that provides services to assist the migration. Onsite and remotely delivered professional migration services can help to simplify and speed the process. Any NGFW vendor, or its certified partners, should be able to provide deep experience, knowledge, leading practices, and tools to reduce disruption and support business continuity during the migration—and do so cost-effectively.

The level and quality of technical support an NGFW vendor will provide to your organization during and after migration should also be included in your technology evaluation. Remote management services, for example, can help to reduce TCO by continuously monitoring and managing network security and freeing your IT talent to concentrate on key business priorities. In addition, services that provide an ongoing examination of security posture, policies, and the effectiveness of your security infrastructure help you to evolve and improve your security program.

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

- The NGFW solution provides investment protection.

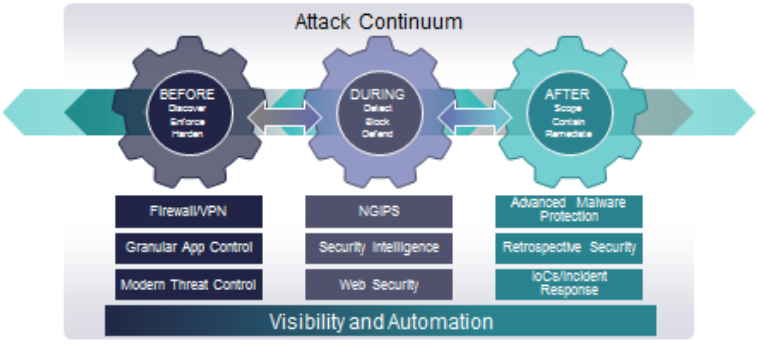
When preparing to invest in a next-generation security solution that can provide comprehensive protection for your whole enterprise, you may want to consider alternatives beyond a direct purchase. Look for an NGFW vendor that provides different purchasing options and gives your organization the opportunity to:

- Lower costs and improve productivity through shorter IT lifecycles and proactive management
- Renew technology assets in line with both your current business strategy and your future vision, and maintain predictable budgets
- Access end-to-end and affordable financing solutions that include hardware, software, and complementary third-party equipment

An NGFW That Meets the Checklist: Cisco ASA with FirePOWER Services

Cisco ASA with FirePOWER Services meets the criteria outlined in the checklist above. In fact, it is the only enterprise-class NGFW solution that delivers integrated threat defense across the entire attack continuum: before, during, and after an attack (see Figure 1).

Figure 1. Integrated Threat Defense Across the Attack Continuum



Cisco ASA with FirePOWER Services is the first adaptive, threat-focused NGFW designed for a new era of threat and advanced malware protection. Its dynamic controls provide unprecedented visibility and protection against threats in real time. The NGFW solution combines the proven security capabilities of:

- **Cisco Adaptive Security Appliance (ASA)**, the world's most widely deployed, enterprise-class stateful firewall with remote access VPN and advanced clustering for highly secure, high-performance access and high availability to help ensure business continuity.

- **FirePOWER Services**, the industry-leading threat and advanced malware protection from Sourcefire® that delivers top-ranked threat effectiveness as measured in independent testing by NSS Labs.[3]

Cisco ASA with FirePOWER Services: Multi-layered Threat Protection and Integrated Threat Defense in a Single Platform

As shown in Figure 2, Cisco ASA with FirePOWER Services delivers the following features in one platform:

- **Superior multi-layered threat protection** from both known and unknown threats, including targeted and persistent malware attacks.
- **Advanced Malware Protection** (AMP) that provides industry-leading breach detection effectiveness, a low TCO, and superior protection value. It uses big data to detect, understand, and block advanced malware outbreaks. AMP provides the visibility and control needed to stop threats missed by other security layers.
- **Actionable IOCs**: Cisco ASA with FirePOWER Services provides holistic, actionable IoCs that correlate detailed network and endpoint event information, providing security teams with even deeper visibility into malware infections. The NGFW solution can also correlate all intrusion events and automatically conduct an impact assessment of an attack against the target.
- **Comprehensive network visibility and control:** Cisco ASA with FirePOWER Services is centrally managed by the Cisco FireSIGHT™ Management Center. It provides unprecedented network visibility and automation required to respond to changing conditions and new attacks. With the FireSIGHT Management Center, security teams can see what is happening on the network at all times: users, devices, communications between virtual machines, vulnerabilities, threats, client-side applications, files, and websites.

The industry-leading Cisco ASA with FirePOWER Services next-generation intrusion prevention system (NGIPS) provides highly effective threat prevention and full contextual awareness of users, infrastructure, applications, and content to detect multi-vector threats and automate defense response. Content awareness with malware file trajectory aids infection scoping and root cause determination to speed time to remediation.

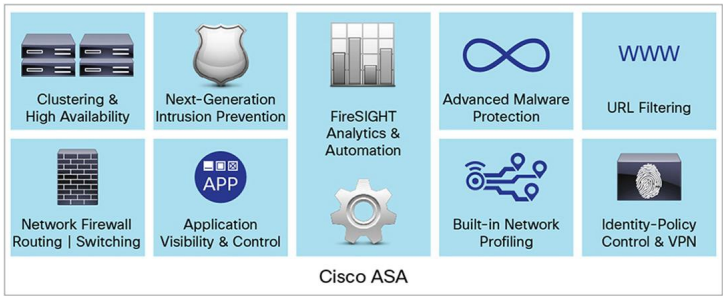
Administrators can manage hundreds of appliances centrally using the FireSIGHT Management Center. And with the granular Application Visibility and Control (AVC) that Cisco ASA with FirePOWER Services provides, they can optimize security effectiveness with 3000 application-layer and risk-based controls that can invoke tailored IPS threat detection policies.

- **Automation—to reduce cost and complexity:** The Cisco FireSIGHT Management Center also helps administrators streamline operations to correlate threats, assess their impact, automatically tune security policy, and easily attribute user identities to security events. It continually monitors how the network changes over time, automatically assessing threats to determine which require immediate attention. With this insight, security teams can focus response efforts on remediation and adapt network defenses.

[3] "NSS Labs Security Value Map for Breach Detection Systems: Sourcefire Advanced Malware Protection Is a Leader in Security Effectiveness and TCO," Sourcefire.com: https://info.sourcefire.com/NSSBreachDetectionReportSEM.html?gclid=Cj0KEQjw7b-gBRC45uLY_avSrdgBEiQAD3OIx8BtffrsQkNYs3AtCojRqyy42V1yLfGyh78OMov3iUAaAlNc8P8HAQ.

- **Third-party integration:** Cisco ASA with FirePOWER Services can interface smoothly and transparently with third-party security solutions, including vulnerability management scanners, software management, and trouble-ticketing systems, to improve TCO. You get the benefits of an open system that interfaces with Cisco OpenSource capabilities. OpenAppID, an open, application-focused detection language and processing module for Snort®, the IPS and intrusion detection system (IPS/IDS) developed by Sourcefire, lets IT teams create, share, and implement application detection.

Figure 2. Cisco ASA with FirePOWER Services



Cisco ASA with FirePOWER Services: Additional Purchase Considerations

When you select Cisco ASA with FirePOWER Services as your NGFW solution, you will have access to:

- **Investment protection:** Cisco Capital® financing is available with terms that meet your business and budgetary requirements. With a fair-market-value lease from Cisco Capital, you can pay for the use of the equipment, not its ownership. You have the flexibility to upgrade or refresh your equipment as needed while eliminating technology obsolescence.
- **Services and technical support:** Cisco has achieved certification under the J.D. Power Certified Technology Service and Support Program for five consecutive years and eight years overall.[4] Cisco services and support offerings for Cisco ASA with FirePOWER Services include:
  - **Cisco Migration Services for Firewalls**, delivered by Cisco security engineers or Cisco Security Specialized Partners, help organizations migrate smoothly to Cisco ASA with FirePOWER Services. Cisco provides expert guidance and support to help maintain security during a migration and to improve the accuracy and completeness of the process.
  - **Cisco Remote Management Services** help reduce TCO further by continuously managing security networks and freeing your IT resources to concentrate on other value-adding business priorities.
  - **Cisco Network Optimization Services** feature smart analytic tools with an intuitive graphics interface to deliver unmatched insight into network performance, so customers can reduce network complexity, improve operational excellence, monitor policy compliance, mitigate risks, and proactively detect and preempt potential network disruptions. The service dramatically improves return on investment, exceeding 120 percent in a study by Forrester Research.[5]

[4] "Cisco Recognized for Excellence in Certified Technology Service and Support Program for a Fifth Consecutive Year and Eighth Year Overall," J.D. Power media release, July 21, 2014: http://www.jdpower.com/press-releases/certified-technology-service-and-support-program#sthash.7oyGxBUo.dpuf.

[5] *The Total Economic Impact™ of Cisco SP Network Optimization Service and Focused Technical Support*, report prepared for Cisco by Forrester Research, November 2009: http://www.cisco.com/en/US/services/ps6889/TEI_of_SP_NOS_FTS_Forrester.pdf.

- **Cisco SMARTnet® Service** helps to 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.

To Download the Software

Visit the Cisco Software Center to download Cisco ASA with FirePOWER Services software.

For More Information

To learn more, visit:

- www.cisco.com/go/asafps for more about Cisco ASA with FirePOWER Services
- www.cisco.com/go/asa for more about Cisco ASA 5500-X Series Next-Generation Firewalls
- 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 links to local Cisco Capital representatives

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 C11-733098-00 10/14