Next-Generation Firewalls: An Investment Checklist

What You Will Learn

When you buy a next-generation firewall (NGFW), you want to determine whether the solution can give you comprehensive protection for your entire enterprise. You need to look for eight must-have capabilities. The NGFW should:

1. Integrate security functions tightly to provide effective threat and advanced malware protection
2. Provide complete and unified management
3. Provide actionable indications of compromise to identify malicious activity across networks and endpoints
4. Offer comprehensive network visibility
5. Protect users anywhere they go, even when the VPN is off
6. Help reduce complexity and costs
7. Integrate and interface with third-party security solutions
8. Provide investment protection

This white paper explains this checklist in depth. It also provides examples of the benefits that a truly effective NGFW solution can deliver.

Background

Cybersecurity systems that rely exclusively on point-in-time defenses and techniques cannot keep pace with today's sophisticated and ever-evolving multivector attack methods. In fact, according to the Cisco 2016 Annual Security Report, nimble attackers are tapping into legitimate online resources to launch campaigns and boost profits. Their methods include leaching server capacity to steal data and demand ransoms, and using malicious browser extensions to exfiltrate data.[1] Organizations must continue to strive for the best threat protection possible. But they must also focus on time to detection (TTD), an increasingly important metric since the rise in evasive activity by adversaries. Current industry measures for TTD are 100 to 200 days, which is far too long.[2]

The introduction of next-generation firewalls (NGFWs) was an important step forward, but typical NGFWs have put their focus on application access control with scant attention paid to threat defense capabilities. A typical NGFW also loses visibility and can't protect users if they're outside the traditional network perimeter or when they bypass the VPN to access the Internet. Some NGFWs have added first-generation intrusion prevention and an assortment of unintegrated products. But these solutions do little to protect against the risks posed by sophisticated attackers and advanced malware. Nor can they protect roaming users simply and cost-effectively. Furthermore, these NGFWs offer little assistance after an infection occurs. They can't help scope the infection, contain it, or remediate quickly.

Today's multivector and persistent threats, fluid IT environments, and increasing network demands are prompting more organizations to seek a better NGFW solution. They want one that can provide layered threat protection and integrated defenses. They want best-in-class security technologies that work together transparently, follow the user, and mitigate risk when an attack penetrates the network.

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 and analyze real-time threats and network traffic effectively with scale. It should help your organization defend against targeted and persistent malware attacks, including emerging threats. And it should reduce complexity.

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 integrated defenses and multilayered threat protection, the NGFW must 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. It should give you comprehensive visibility into underlying threats so you can protect your critical assets. The NGFW should also 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. It should monitor their activities to determine anomalies. It should extend protection to roaming users, even when they aren't connected to the corporate network. Finally, it should provide comprehensive visibility and correlated information in a single console for insightful management.

1. Cisco 2016 Annual Security Report: http://www.cisco.com/c/en/us/products/security/annual_security_report.html
2. Ibid.

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, in real time.

1. The solution integrates security functions tightly to provide effective protection against threats and advanced malware.

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. The correlation of threat intelligence across 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 and endpoints so security teams can track threats and initiate remediation activities rapidly.

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

2. The NGFW includes unified management.

It is not sufficient to integrate security functions tightly. An NGFW must do so within a platform that offers a single management interface and streamlines operations. Managing all security functions through a central console simplifies the administration of an integrated security architecture. And it accelerates detection and response. For security departments that are understaffed or lacking expertise, the ability to address today's dynamic and sophisticated threats while reducing complexity is paramount.

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

Indications of compromise, or IoCs, use "tags" on a host that indicate that an infection has probably occurred. IoCs correlate network and endpoint security intelligence. They can identify malware activity involving 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.

4. 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. Visibility should include 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. Dynamic controls should 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 should also be able to automate the defense response after an attack, including infection scoping and containment. Automation will further reduce the burden on security teams.

5. The NGFW protects users anywhere they go, even when the VPN is off.

The NGFW must provide visibility and protection outside the corporate perimeter, even when users connect directly to the Internet. The solution must be able to extend protection to mobile users that often rely on cloud apps to do their job. They may inadvertently bypass the VPN or no longer need access to the corporate network to do their work. An integrated approach eliminates the need to deploy additional agents to protect users as they roam.

6. The NGFW helps reduce complexity and costs.

An NGFW that is effective against advanced threats should also offer:

- Unified security across defense layers
- High scalability
- Automation of routine security tasks

An integrated, multilayered 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. Consolidation thus addresses the most commonly cited obstacle to adopting better security: resource constraints.[3]

3. Cisco 2016 Annual Security Report

An NGFW with multilayered threat protection will help security administrators deliver consistent and robust security at scale. It can support small branch offices, Internet edge sites, and even large data centers in both physical and virtual environments.

The NGFW solution should automate these activities:

- **Impact assessment:** The NGFW should automatically correlate threats against host vulnerability intelligence, network topology, and attack context. This assessment will help security analysts focus their attention on only those intrusion events that warrant monitoring and a swift response.
- **Policy tuning:** The NGFW should automate the provisioning, tuning, and consistent enforcement of security policies throughout the enterprise. Security teams will then be able to 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.

7. The NGFW integrates and interfaces smoothly and transparently with third-party security solutions.

Integration with third-party solutions deepens the multilayered protection that an NGFW solution provides. It combines essential security layers into one platform and centralizes management through a unified interface. This approach simplifies security deployment and ongoing operational activities. It supports existing security technologies and shares intelligence to coordinate and streamline responses.

An NGFW should support a rich solution "ecosystem" through open APIs for third-party technologies, including:

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

8. The solution provides investment protection.

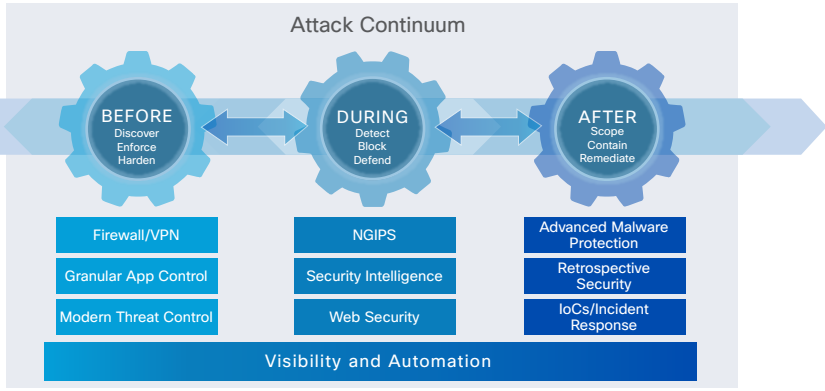
When you invest in a next-generation security solution, you are looking for comprehensive protection for your whole enterprise. You may want to consider alternatives beyond a direct purchase. An NGFW vendor should provide different purchasing options that give your organization the opportunity to:

- Lower costs and improve productivity through shorter IT lifecycles and proactive management
- Economize with "smart licensing" and "enterprise licensing" options that optimize software use and provide you with the flexibility to deploy it quickly when ready
- 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 Firepower NGFW

The Cisco Firepower™ NGFW meets the criteria outlined in the checklist above. In fact, it is the only fully integrated, threat-focused NGFW that keeps organizations safer, mitigates advanced threats faster, and streamlines operations better across the entire attack continuum: before, during, and after an attack (see Figure 1).

Figure 1. Integrated Threat Defense Across the Attack Continuum



The Cisco Firepower NGFW is designed for a new era of threat and advanced malware protection. It provides unprecedented visibility and protection against threats in real time for organizations of all sizes. Encompassing a range of appliances that are the highest performing in their class, the Cisco Firepower NGFW is:

- **Fully integrated:** It provides unified visibility and policy management of firewall, application control, threat prevention, and advanced malware protection functions from the network to the endpoint, wherever that endpoint may be.
- **Threat focused:** It provides comprehensive network visibility, outstanding threat intelligence, and threat prevention to address both known and unknown threats. Its retrospective security technology helps you quickly respond to successful attacks.[4]

Cisco Firepower NGFW: Multilayered Threat Defense in a Single Platform

As shown in Figure 2, Cisco Firepower NGFW delivers the following features in one platform:

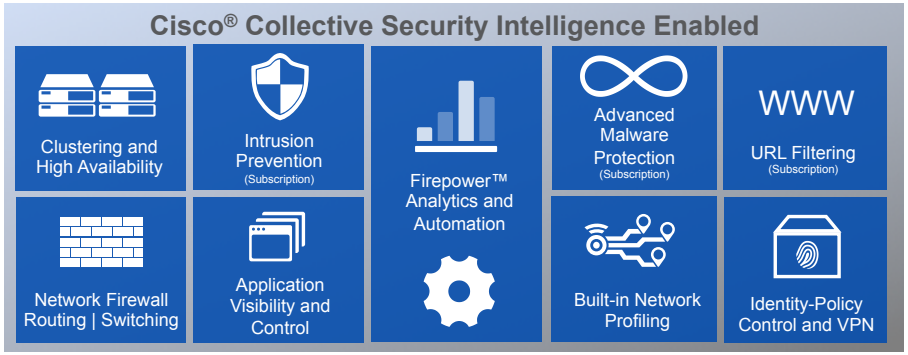
- **Superior multilayered threat protection** from both known and unknown threats, including targeted and persistent malware attacks. The Cisco Firepower NGFW includes the world's most widely deployed stateful firewalling technology. In addition, it offers a next-generation intrusion prevention system (IPS), advanced malware protection, application visibility and control, and reputation-based URL filtering along with an application-level VPN, all in a single solution in a single appliance. It also integrates with other Cisco solutions embedded in the network to automate network segmentation for rapid threat containment.
- **Cisco® Advanced Malware Protection** (AMP), which 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.
- **Unified management** through the Cisco Firepower Management Center, the nerve center of the Cisco Firepower NGFW, where administrators can manage hundreds of appliances. The Management Center provides role-based management over firewall policy and configuration, access control for more than 4000 applications, intrusion protection policies, and advanced malware analysis through a rich console.
- **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** through the Management Center, which provides unprecedented network visibility and automation so you can respond to changing conditions and new attacks. 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. Context awareness helps security teams detect multivector threats. Combined with the malware file trajectory, it aids infection scoping and root cause determination to speed time to remediation.
- **Protection for roaming users even when they're off the corporate network.** Cisco Umbrella Roaming is a cloud-delivered security service that is incorporated into the Cisco Firepower NGFW through a Cisco AnyConnect® client. By providing protection at the DNS layer, Umbrella Roaming allows you to block threats before they reach your laptops. Plus, security is enforced everywhere with no additional agents required. Umbrella Roaming provides the simplest way to protect users anywhere they go, even when the VPN is turned off.

Providing security that is greater than the sum of its parts, the integrated threat defense architecture of the Cisco Firepower NGFW also delivers:

- **Automation to reduce cost and complexity:** The Cisco Firepower Management Center 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 their network defenses.
- **Third-party integration:** To improve TCO, the Cisco Firepower NGFW interfaces smoothly and transparently with third-party security solutions, including vulnerability management scanners, software management, and trouble-ticketing systems. You can share intelligence, context, and policy controls consistently across solutions. You also gain the benefits of an open system that interfaces with Cisco OpenSource capabilities and OpenAppID, an open, application-focused detection language and processing module for Snort® that lets IT teams create, share, and implement application detection.

4. NSS Labs Security Value Map for NGFWs and Breach Detection Systems; Cisco is a leader in both. http://www.cisco.com/web/offers/NSSLabsReportNGFW.html https://info.sourcefire.com/2015NSSBreachDetectionReport-CDC.html?AMPPage

Figure 2. Cisco Firepower NGFW



Cisco Firepower NGFW: Additional Purchase Considerations

When you select the Cisco Firepower NGFW as your NGFW solution, you have access to many benefits.

Investment Protection

Cisco Capital® financing is available with terms that meet specific business and budgetary requirements. With a fair-market-value lease, organizations can pay for the use of the equipment, not its ownership. You have the flexibility to upgrade or refresh equipment as needed, 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.[5] Cisco service and support offerings for Cisco Firepower NGFW include the following:

- **Cisco Migration Services for Firewalls**, delivered by Cisco security engineers and Cisco Security Specialized Partners, help organizations migrate smoothly to the Cisco Firepower NGFW. 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. Your organization's IT team can concentrate on other value-adding business priorities.
- **Cisco Network Optimization Services** feature smart analytic tools with an intuitive graphics interface to deliver exceptional insight into network performance. Organizations can reduce network complexity, improve operational excellence, monitor policy compliance, mitigate risks, and proactively detect and preempt potential network disruptions.
- **Cisco Smart Net Total Care™ Service** helps organizations reduce network downtime and other critical network issues. You get 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 Firepower Services software.

For More Information

To learn more, visit:

- www.cisco.com/go/ngfw for more about Cisco Firepower NGFW Appliances
- www.cisco.com/go/asafps for more about Cisco ASA with FirePOWER Services
- www.cisco.com/go/services/security for more about Cisco Migration Services for Firewalls
- www.cisco.com/go/smartnet for more about the Cisco Smart Net Total Care Service
- www.ciscocapital.com for additional information and links to local Cisco Capital representatives

5. 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.