White Paper

NGFW Requirements for SMBs and Distributed Enterprises

The Case for NGFWs for SMBs

The need for threat-focused next-generation firewalls (NGFWs) that can effectively mitigate risks that traditional unified threat management (UTM) and point solutions cannot is highlighted by numerous studies, including one from Cisco that reported that every organization should assume it has been hacked. Cisco threat researchers found malicious traffic was visible on 100 percent of the corporate networks that they observed, with evidence that adversaries had often penetrated those networks and were frequently operating undetected over a long period.[1]

Today's multivector and persistent threats, fluid IT environments, and increasing user mobility are prompting more organizations to seek NGFW capability that provides affordable and effective layered threat protection. While a range of solutions have emerged to try to meet this need, an NGFW that includes all the necessary capabilities for effective security today is rare.

Significant security challenges are not only faced by large enterprises, **but every organization, regardless of its size**. As reported by the U.S. National Cybersecurity Alliance in 2014, 41 percent of directed cyberattacks were focused on compromising organizations with fewer than 500 employees. Further, *The New York Times* reported in 2014 that a growing number of SMBs were being asked by their larger partners to adopt stronger threat defense programs. Not surprisingly, advanced threat defense has become a boardroom conversation as organizations of all sizes seek to better protect their customer data, employee information, intellectual property, and corporate secrets.

So now it's clear that smaller organizations have a strong need for advanced threat defense, including NGFWs. According to the "2015 Cisco Security Capabilities Benchmark Study,"[2] featuring interviews with hundreds of IT professionals in nine countries, midmarket (500–999 employees) organizations mirror their larger peers in security readiness in areas that include:

- **Incidence response:** Ninety-two percent of midsize organizations have internal incidence response teams, as opposed to 93 percent of large enterprises.
- **Executive accountability:** Ninety-four percent of midsize organizations have an executive directly accountable for security, as opposed to 92 percent of larger enterprises.

NGFWs have historically been security tools best deployed by larger organizations. Until now, small and medium businesses and distributed enterprises have typically chosen between two options when deploying network security: either UTM solutions, with less-effective threat-mitigation capabilities, or multiple single-function solutions for stateful firewalling, application control, IPS, and advanced malware mitigation. SMBs have been underserved by both options—either grudgingly accepting suboptimal threat defense from UTMs or facing daunting integration and management costs with multiple point solutions. Now, however, there's a new option: **NGFWs specifically tailored for SMBs and distributed enterprises, with advanced threat protection, low TCO, and flexible management.**

[1] Cisco 2014 Annual Security Report: http://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf.
[2] Cisco 2015 Annual Security Report: http://www.cisco.com/web/offers/lp/2015-annual-security-report/index.html.

This white paper can help you confirm that your small business or distributed enterprise needs to invest in an effective NGFW solution. For small businesses, the NGFW should provide an affordable and manageable entrée to advanced threat protection. In branch offices and the distributed enterprise, NGFWs should provide a detection and enforcement point, analyzing real-time threats and network traffic at scale and benefiting from an integrated and holistic view of the network of which it is a part. In both use scenarios, the NGFW should help your organization defend against targeted and persistent malware attacks, including emerging threats.

Evaluation Criteria for Core Network Security Solutions

Whether you're assessing NGFWs or UTMs, it is important to recognize three critical success factors. Your NGFW solution must be:

- **Tailored for SMBs and distributed enterprises**
- **Threat focused for effective information security and advanced malware protection**
- **Reducing complexity and costs.**

Tailored for SMBs and Distributed Enterprises

"Fit" is critical here—not only in terms of acquisition cost and throughput, but also manageability. The majority of SMBs have limited resources, such as a common scenario where several IT personnel share the responsibility for information security among their many other job responsibilities. These SMBs need security solutions that can be efficiently managed.

While large organizations often have the resources to take advantage of security event and incident managers (SEIMs), for many smaller organizations, SEIMs may not be practical. The IT Manager responsible for security often simply wants to know what the highest priority threats are so the team can investigate and remediate quickly.

Management flexibility is also important so that as an organization grows, for instance when adding remote offices, the original investment maintains its value. Typically, on-box management is suited to single-instance deployments, and multiple instance deployments benefit from centralized management.

Threat Focused

Generally, legacy NGFWs and UTMs combine multiple security functions but deliver poor security efficacy, providing neither next-generation IPS (NGIPS) functionality nor advanced malware protection. To truly be threat focused, the security solution must include stateful firewalling as well as NGIPS and advanced malware protection to provide network visibility and the ability to identify and remediate malware activity.

In addition to identifying threats, the NGFW should be able to report on indicators of compromise (IoC), based on correlation of both known and suspect behavioral factors, and monitor user activities to determine anomalies. These tools should be integrated with URL reputational filtering, and application visibility and access control to reduce threat exposure, as well as comply with regulatory and internal use policies.

The solution must also mitigate common, but important, network risks through access policies, virtual network segmentation, and secure site-to-site and remote access VPN connections. This foundational baseline is a useful starting point upon which to base your purchasing decision. For example, not all Layer 7 application control solutions include best-of-breed stateful firewalling and VPN capability.

Finally, and perhaps most importantly, the NGFW must deliver advertised performance, even when multiple security services are simultaneously enabled. The key here is to identify a vendor that works with you to appropriately size the solution to meet your environment and security requirements, and select a platform capable of meeting both your current and future needs.

Reducing Complexity and Costs

Few organizations have a dedicated security operations center (SOC) or dedicated security staff. When assessing a security solution ask the following questions:

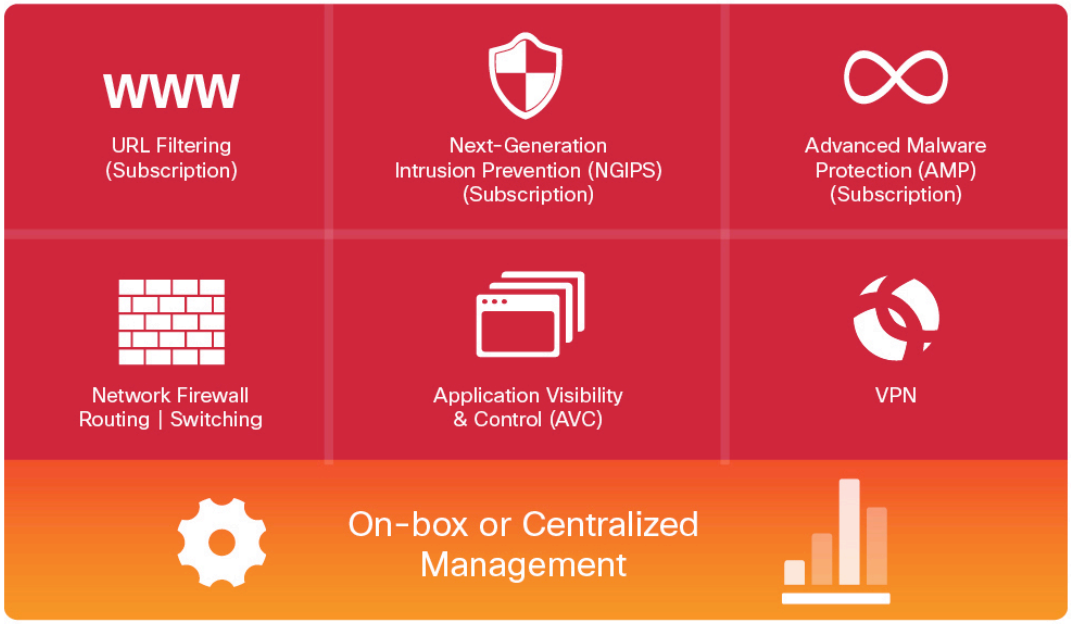
- Is the solution usable by IT generalists?
- Does it reduce staff time for time-intensive activities, such as malware remediation?
- Does it spare analysts from the tedium of identifying which events are meaningful and actionable?
- Does it provide security automation to help keep defenses tuned by automatically tailoring policies to the ever-changing environment?
- Does it provide correlated event views that streamline and speed event triage and analysis?

Meeting the Needs of SMBs: Cisco ASA with FirePOWER Services

Cisco ASA with FirePOWER™ Services models 5506-X, 5508-X and 5516-X, as well as the ruggedized 5506H-X and wireless 5506W-X variants, meet the need for superior threat protection, low TCO, and management flexibility. Stateful firewall, VPN, and all NGFW functions are combined in a single on-box manager, an enhanced version of Cisco Adaptive Security Device Manager (ASDM), which is ideal for single-instance and standalone deployments.

Where centralized management is the preferred option, ASA with FirePOWER Services is managed by Cisco Security Manager (CSM) and the Cisco FireSIGHT™ Management Center. When used with centralized management, it is the only NGFW solution that delivers integrated threat defense across the entire attack continuum—before, during, and after an attack (see Figure 1).

Figure 1. Cisco ASA with FirePOWER Services



Cisco ASA with FirePOWER Services is the first 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) and FirePOWER Services**.

Cisco ASA

Cisco ASA is 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. Also, the solution is tightly integrated with Cisco AnyConnect® Mobility Client Version 4, which, among other things, supports split VPN tunneling on an application-by-application basis. Cisco AnyConnect VPN Client is the world's most widely deployed VPN client, with more than 130 million clients in use. For organizations that prefer to use native VPN clients, many are supported by Cisco ASA as well, including native Apple iOS and Samsung Android clients.

Cisco FirePOWER Services

Best-of-Breed Multi-layered Threat Protection on a Single Platform

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

[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=Cj0KEQjw7bgBRC45uLY_avSrdgBEiQAD3Olx8BtffrsQkNYs3AtCojRqyy42V1yLfGyh78OMov3iUAaAlNc8P8HAQ.

As shown in Figure 1, Cisco ASA with FirePOWER Services can enable:

- **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.
- **A next-generation intrusion prevention system (NGIPS)** that 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. Competing UTM and NGFW solutions provide basic IPS capability, but not the full NGIPS capability as defined by Gartner Group.
- **Granular Application Visibility and Control (AVC)** that optimizes security effectiveness with 3000 application-layer and risk-based controls that can invoke tailored IPS threat detection policies.
- **VPN capability** robust enough to deliver not only traditional site-to-site and remote access VPN capabilities, but also strong VPN capabilities for mobile devices, including the option for split-tunneling of critical enterprise apps but not user apps for personal needs.

Flexible Management Options

Cisco ASA with FirePOWER Services provides a choice of management solutions, both centralized and on-box managers. Cisco Adaptive Security Device Manager (ASDM), 7.3, and later, is the recommended on-box manager for single-instance deployments. ASDM features consolidated management of all NGFW functions and reduces staff time dedicated to NGFW management. For multiple instance deployments, Cisco ASA with FirePOWER Services can be centrally managed by the Cisco FireSIGHT Management Center. It provides unprecedented network visibility and automation 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 following Table 1 summarizes the differences between the Cisco FireSIGHT Management Center and ASDM managers.

Table 1. Comparison: Cisco FireSIGHT Management Center and Adaptive Security Device Manager (ASDM)

Features	FireSIGHT Management Center (Centralized, Off-Box Management)	ASDM Integrated Local Management (On-Box Manager)
Overview	Manage up to 300 ASA with FirePOWER Services sensors per FireSIGHT instance. FireSIGHT is used in conjunction with Cisco Security Manager (CSM).	Local, on-box manager, delivered by default with all configurations: Optimized for smaller organizations and single-instance deployments. Features integrated management of all product functionality with ease-of-use emphasis.
Contextual Awareness and Visibility	Extended functionality: Include base functionality plus ability to passively detect network hosts, Context Explorer capability, and file trajectory.	Base functionality: Geolocation and client tags supported by default. IPS events may be exported to SEIM for SEIM-based contextual awareness.
Network AMP	Extended functionality: Includes base functionality plus file capture, sandboxing, and dynamic analysis. FireSIGHT required with the Cisco Advanced Malware Protection for Endpoint solution (maximizes visibility, enables client remediation).	Base functionality: Detects and block malware and prohibited file types through file analysis. Includes access to Cisco malware analysis cloud (file hashes, not files, are sent to the cloud for analysis.)

Features	FireSIGHT Management Center (Centralized, Off-Box Management)	ASDM Integrated Local Management (On-Box Manager)
Dashboard	Extended functionality: The FireSIGHT Context Explorer dashboard enables dynamically updated visualization and exploration of the network environment.	Base functionality: ASDM manager has dashboard widgets for license information, system monitoring and information, FirePOWER module details, etc. It also provides system information.
Automation, Impact Analysis, Event Correlation, etc.)	Included: Automatic threat assessment to prioritize relevance and impact, correlation and remediation features for real-time threat response, and automated policy tuning to protect against new threats.	Not available.
IPS	Extended functionality: Includes base functionality plus preprocessor tuning and full NGIPS capability as defined by Gartner Group.	Base functionality: Uses Snort IPS engine and includes IPS rule tuning.
Users/User Discovery and Geolocations	Full functionality. Integration with Active Directory and access control based on traffic geolocation.	Full functionality. Integration with Active Directory and access control based on traffic geolocation.
Application Visibility and Control (AVC)	Extended functionality: Includes base functionality plus custom application detectors based on regex match, or protocol and port detection.	Base functionality: Enables visibility and access control at Layer 7, supporting more than 3000 applications and risk-based controls.
Health Functionality	Extended functionality: Includes base functionality plus customizable health alerting on more than 30 functions.	Base functionality: Status on CPU and memory load.
System Policies	Extended Functionality. Includes base functionality plus control of over 17 access control, logging, and alerting functions. Such policies are typically similar across a deployment, in contrast to system settings, which are likely to be specific to each single appliance.	Base Functionality. Email notifications, Simple Network Management Protocol (SNMP) support, and time synchronization.
Reporting	Extended functionality: Includes base functionality plus customization templates and export capability.	Base functionality: Filtering and reporting on top traffic, file types, users, applications, and more.
Events	Extended functionality: Includes base functionality plus: greater event storage and event-per-second capability.	Base functionality: Real-time event stream for troubleshooting.
API Support	Extended functionality: Includes base functionality plus remediation, host input, and database access APIs.	Base Functionality. FirePOWER eStreamer API for simple sharing of events with SEIM platforms.

To learn more about the visibility provided by Cisco FireSIGHT Management Center, see the document "Requirements When Considering a Next-Generation Firewall."

Additional Considerations: Cisco Security Intelligence and Threat Feeds

To more effectively combat known and emerging threats, organizations need an NGFW solution that incorporates leading threat intelligence for up-to-date protection. Threat researchers from the Cisco Collective Security Intelligence (CSI) ecosystem bring together under a single umbrella the industry's leading threat intelligence by using telemetry obtained from the vast footprint of devices and sensors, public and private feeds, and the open source community at Cisco. This amounts to a daily ingest of billions of web requests and millions of emails, malware samples, and network intrusions.

Our sophisticated infrastructure and systems consume this telemetry, enabling machine-learning systems and researchers to track threats across networks, data centers, endpoints, mobile devices, virtual systems, web, email, and from the cloud to identify root causes and scope outbreaks. The resulting intelligence is translated into real-time protections for our products and services offerings that are immediately delivered globally to Cisco customers. CSI threat feeds keep Cisco security solutions continually up to date.

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

- Cisco SMARTnet Service
- Investment protection
- Services and technical support

Cisco SMARTnet Service

This service includes access to expert technical support 24 hours a day, 365 days a year, plus flexible hardware coverage. Cisco has achieved J.D. Power certification through the J.D. Power Certified Technology Service and Support Program for 5 consecutive years and 8 years overall.[4]

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 financing, 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.

Cisco Services and Technical Support

Cisco Services and support offerings for Cisco ASA with FirePOWER Services include:

- **Cisco Migration Services for Firewalls:** Delivered by Cisco or Cisco Security Specialized Partners, these services help organizations migrate easily to Cisco ASA with FirePOWER Services. Cisco provides expert guidance and support to help maintain security during a migration and to assure the accuracy and completeness of the process.
- **Cisco Remote Management Services:** With these services you can continuously manage security requirements, so your IT resources can focus on other priorities.
- **Cisco Network Optimization Services:** Delivering improved network operations, policy compliance, and network reliability, these services dramatically improve ROI, which can exceed 120 percent as shown 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-andsupport-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.

For More Information

To learn more about Cisco NGFW solutions and services, 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
- www.meraki.cisco.com for more information about Cisco Meraki Solutions
- www.cisco.com/go/mmsecurity to stay up to date on the latest trends and see what's new in security from Cisco
- www.cisco.com/go/partnermidmarket for Cisco partners to see the latest solution announcements and events

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 C11-734294-00 04/15