Cisco ASA Next-Generation Firewall Services

Q. What are Cisco® ASA Next-Generation Firewall Services?

A. Cisco ASA Next-Generation Firewall Services are a modular security service that extends the Cisco ASA 5500-X Series Next-Generation Firewall platform. The solution blends a proven, stateful inspection firewall with next-generation capabilities and a host of additional network-based security controls for end-to-end network intelligence and streamlined security operations. Cisco ASA Next-Generation Firewall Services enable organizations to rapidly adapt to dynamic business needs while maintaining the highest levels of security. Cisco ASA Next-Generation Firewall Services deliver application and user ID awareness capabilities for enhanced visibility and control of network traffic. In addition, Cisco ASA Next-Generation Firewall Services enable administrators to control specific behaviors within allowed microapplications, restrict web and web application use based on the reputation of the site, proactively protect against Internet threats, and enforce differentiated policies based on the user, device, role, application type, and threat profile.

Q. What are the benefits of Cisco ASA Next-Generation Firewall Services?

A. Cisco ASA Next-Generation Firewall Services empower enterprises to finally say yes to applications, devices, and the evolving global workforce. Most next-generation firewalls differ from classic firewalls in that they can identify which applications are being requested and which user has requested them. Application and user awareness can be effective, but with so much more happening in the network, these firewalls simply cannot provide the level of visibility and control that administrators need to help them effectively manage their complex network security challenges. Cisco ASA Next-Generation Firewall Services are different. Cisco ASA Next-Generation Firewall Services provide the application and user ID awareness that is essential for any next-generation firewall. In addition, they deliver:

- Precise application visibility and control, including behavior controls within allowed microapplications
- Reputation-based web security
- Passive and active authentication
- User device information
- Near-real-time threat protection

Q. Do Cisco ASA Next-Generation Firewall Services protect against zero-day threats and other malware?

A. Yes. Cisco ASA Next-Generation Firewall Services use threat intelligence feeds from Cisco Security Intelligence Operations (SIO), which employ the global footprint of Cisco security deployments (more than 2 million devices) to analyze 70 percent of the world's Internet traffic from email, intrusion prevention system (IPS) activity, and web threat vectors. The feeds are updated every three to five minutes for near-real-time protection from zero-day threats.

Q. Will I have to overwrite my existing classic firewall policies?

A. No. Cisco ASA Next-Generation Firewall Services enable organizations to continue to use their existing firewall rules and objects while adding richer, context-aware rules that can act intelligently on contextual information. Cisco ASA Next-Generation Firewall Services support Layer 3 and Layer 4 stateful firewall features, including access control, network address translation, and stateful inspection. Organizations can keep their existing stateful inspection firewall policies while adding rich Layer 7 context-aware rules.

Q. Which Cisco ASA platforms support Cisco ASA Next-Generation Firewall Services?

A. Cisco ASA Next-Generation Firewall Services include Cisco Application Visibility and Control (AVC), Cisco Web Security Essentials (WSE), and Cisco Intrusion Prevention System (IPS). All of them are supported on ASA 5500-X Series Next-Generation Firewall models: 5512-X, 5515-X, 5525-X, 5545-X, 5555-X, 5585-X SSP-10, 5585-X SSP-20, 5585-X SSP-40, and 5585-X SSP-60.

Q. Can Cisco ASA Next-Generation Firewall Services be deployed as a virtual machine on a VMware ESX host?

A. No. Cisco ASA Next-Generation Firewall Services are not available in a virtual form factor.

Q. What is the best deployment scenario for Cisco ASA Next-Generation Firewall Services?

A. The majority of the application signatures that are currently supported by Cisco ASA Next-Generation Firewall Services are focused on protecting Internet activity. In addition, Cisco ASA Next-Generation Firewall Services bundle powerful URL filtering, intrusion prevention, and reputation-based filtering that are most useful at the network edge. Future releases will include signatures and capabilities that will be more useful in data center deployments.

Q. How are Cisco ASA Next-Generation Firewall Services managed?

A. Cisco ASA Next-Generation Firewall Services are managed by Cisco Prime™ Security Manager, which supports both single- and multidevice manager form factors.

Application Awareness

Q. How are applications recognized?

A. Cisco ASA Next-Generation Firewall Services provide visibility and control into more than 1200 applications and 150,000 microapplications. Organizations can provide individual or group-based access to specific components of an application while disabling other components (such as allowing Facebook for general use while blocking Facebook games). Specific behaviors can also be blocked within allowed microapplications for an additional layer of control. Application recognition is based on signatures, heuristics, and content scanning, removing the need to tie applications to ports. As a result, administrators can easily block port- and protocol-hopping applications such as Skype and other peer-to-peer (P2P) applications for more effective security while writing fewer policies.

Q. What about nonstandard ports?

A. Cisco ASA Next-Generation Firewall Services can identify traffic even when it is using nonstandard ports. For example, if HTTP is running on port 8080 or Secure Shell (SSH) Protocol is running on port 16022, Cisco ASA Next-Generation Firewall Services will still identify the traffic correctly as HTTP or SSH.

Q. What if there are multiple applications in a single flow?

A. Cisco ASA Next-Generation Firewall Services employ deep packet inspection for application recognition and therefore do not require a separate connection per application. For example, modern browsers send multiple HTTP Group Encrypted Transport requests over the same persistent TCP connection. Cisco ASA Next-Generation Firewall Services will subject each of these requests to classification and threat analysis using application signatures, IPS signatures, URL filtering, and web reputation. If two transactions share the same connection, they will still be identified as separate transactions, each having its own deep packet inspection results.

Q. How is unidentified (unknown) traffic handled?

A. After administrators create rules for the applications they care about, the rest of the traffic will fall to the bottom policy, and administrators will be able to choose an action for that policy. Also, with Cisco ASA Next-Generation Firewall Services, the Layer 3 and Layer 4 rules on the Cisco ASA security appliance will continue to run, reducing the surface area of traffic. (For example, inbound access can still be controlled very tightly with Layer 3 and Layer 4 rules.) In a future version, Cisco ASA Next-Generation Firewall Services will enable administrators to create rules for unknown traffic on a per-policy basis.

Q. Does Cisco deliver newer application recognition signatures?

A. Yes. New application signatures are usually released on a monthly basis. When the new application signatures are updated in the Cisco cloud infrastructure, Cisco ASA Next-Generation Firewall Services devices are updated within a few minutes.

Q. How can I determine what applications are supported?

A. Cisco Prime Security Manager provides an application browser, which enables administrators to identify all applications and microapplications that are supported by Cisco ASA Next-Generation Firewall Services. Cisco Prime Security Manager also includes quick filtering capabilities, so administrators can search for specific applications.

Q. Can I create my own custom application signatures?

A. Not with the current release. Currently, Cisco ASA Next-Generation Firewall Services include a robust set of more than 1200 applications and 150000 micro-applications. The ability for administrators to create their own application signatures is a feature that will be included in a future release.

Q. Can I create my own custom application categories?

A. Yes. Cisco ASA Next-Generation Firewall Services supports custom objects that are based on existing applications.

Q. Some applications like Skype use port hopping and other evasive techniques. Can Cisco ASA Next-Generation Firewall Services recognize these applications?

A. Yes. Cisco ASA Next-Generation Firewall Services recognize applications based on signatures, heuristics, and content scanning, removing the need to tie applications to ports. As a result, administrators will be able to easily block port- and protocol-hopping applications such as Skype.

Q. How are users identified?

A. Users can be identified via both passive and active methods. Passively identified users are determined using the Cisco Active Directory agent to create an IP-to-user mapping from the Active Directory logs. This is the same process used by the Cisco ASA Identity Firewall feature available in Cisco ASA Software Release 8.4.2 and later. Cisco ASA Next-Generation Firewall Services can also actively identify users through true authentication with schemes such as Microsoft Windows NT LAN Manager (NTLM), Kerberos, and Lightweight Directory Access Protocol (LDAP). This type of authentication can prompt the user for credentials or be handled transparently by the browser. Future releases of Cisco ASA Next-Generation Firewall Services will also use the 802.1X authentication performed in the network by the Cisco TrustSec® infrastructure to identify users and devices.

Q. Do Cisco ASA Next-Generation Firewall Services work with the Cisco Identity Services Engine (ISE) for identity enforcement?

A. Not with the current release. Currently, Cisco ASA Next-Generation Firewall Services use the Cisco Active Directory agent, which is a component of the Cisco ISE, for identification. The Active Directory agent tracks all users who are logged into the network and maps the source IP addresses. In a future release, Cisco ASA Next-Generation Firewall Services will also support access control based on Cisco TrustSec tags.

Device-Type Enforcement

Q. How are devices identified?

A. Cisco ASA Next-Generation Firewall Services use the Cisco AnyConnect® Secure Mobility Client to determine the specific types of devices attempting to gain access to the network as well as their locations (on-premises or off-premises), to enable administrators to confidently allow devices while maintaining high levels of network protection and control. If AnyConnect is not used, Cisco ASA Next-Generation Firewall Services will use the UserAgent field of the HTTP header for this identification.

Q. Can Cisco ASA Next-Generation Firewall Services use device-type enforcement for nonweb traffic?

A. Yes. Cisco ASA Next-Generation Firewall Services can get device-type information from devices running the Cisco AnyConnect Secure Mobility Client. Cisco ASA Next-Generation Firewall Services can use this information for access control enforcement, even if the traffic from these clients is not web-based.

Q. Can Cisco ASA Next-Generation Firewall Services use device-posture information to enforce access?

A. Not currently. Posture-based enforcement will be implemented in a future version.

Q. What about IP phones, video streaming servers, and other devices that do not support browsers or Cisco AnyConnect?

A. Currently, Cisco ASA Next-Generation Firewall Services cannot identify the device type for traffic that is not web-based if the source device is not running Cisco AnyConnect. In a future release, Cisco ASA Next-Generation Firewall Services will also support access control based on Cisco TrustSec tags, at which point this use case will be supported.

Encrypted Traffic

Q. Can Cisco ASA Next-Generation Firewall Services decrypt Transport Layer Security/Secure Sockets Layer or SSH traffic for inspection?

A. Currently, Cisco ASA Next-Generation Firewall Services is able to decrypt TLS/SSL. Decryption of SSH will be enabled in a future release. Cisco ASA Next-Generation Firewall Services will decrypt HTTPS traffic to identify encrypted applications. This decryption can be intelligently performed based on rich-context parameters such as source (user, subnet), destination (fully qualified domain name, web category, subnet), and reputation of the destination servers.

Q. What about remote-access (VPN) users? Do they get all the same protection?

A. Yes. Cisco ASA Next-Generation Firewall Services work with Cisco AnyConnect to provide highly secure mobility, regardless of user's location. When the user is located outside the firewall, Cisco AnyConnect will recognize that the user is in an untrusted network and will establish a connection to the most optimal network scanning element (that is, the most optimal Cisco ASA Next-Generation Firewall Services). As a result, consistent access rules can be applied to the user's traffic, even when the user is located outside the office.

Cisco IPS

Q. Do Cisco ASA Next-Generation Firewall Services support IPS functionality?

A. Yes. Cisco Next-Generation Firewall with IPS is currently supported and can simultaneously run alongside other services, including Cisco AVC and WSE.

Q. What version of Cisco ASA CX do the Cisco ASA Next-Generation Firewalls with IPS operate on?

A. Cisco ASA CX Software Release 9.2 or later is needed to run Cisco IPS on Cisco ASA 5500-X Series Next-Generation Firewalls.

Q. What is the new Cisco IPS Service on Cisco ASA 5500-X Next-Generation Firewalls?

A. Cisco IPS Service is the module that provides intrusion prevention within the Cisco ASA 5500-X Series Next-Generation Firewalls. The firewalls have multiple security services operating within them. The Cisco IPS uses the firewalls' other services such as application visibility, identity, and off-device reputation to make inspection and enforcement decisions.

Q. What is the technology overlap of the new Cisco ASA 5500-X Series Next-Generation Firewalls with Cisco IPS Service and the Cisco ASA IPS?

A. The Cisco IPS on the Cisco 5500-X Series Next-Generation Firewalls was created with some new technologies and with some technologies that were modified from the Cisco ASA IPS. Some inspection capabilities are very close to those in operation, while other structural considerations, such as updates, are new. Customer interaction is the most divergent attribute between the two offerings.

Q. What kinds of deployments were the Cisco 5500-X Series Next-Generation Firewalls with IPS designed for?

A. IPS with Next-Generation Firewall provides protection for end users and the computing environments under their direct control such as desktops, laptops, and personal communication devices. It is ideal for Internet edge deployments.

Q. Is quality of service (QoS) supported?

A. Yes. QoS is supported on Cisco ASA Next-Generation Firewall Services, but it is handled by the Cisco ASA firewall blade. Customers can create QoS rules on the ASA firewall, just as they do now. QoS based on applications, users, and other context will be supported by Cisco ASA Next-Generation Firewall Services in a future release.

Q. Are Cisco TrustSec security group tags supported?

A. Not currently. This feature will be supported by Cisco ASA Next-Generation Firewall Services in a future release.

Performance

Q. How about performance? Will the Cisco ASA Next-Generation Firewall Services blade slow down my Cisco ASA firewall?

A. As with any device performing deep packet inspection, performance will be lower than with devices that only route traffic or perform stateful inspection. However, all Cisco ASA Next-Generation Firewall Services devices will provide gigabit and multigigabit throughput levels. Unlike competitive offerings that require application control to be continuously active for all the traffic, Cisco ASA Next-Generation Firewall Services do not create any such restriction. Administrators can determine which traffic will be inspected by Cisco ASA Next-Generation Firewall Services and continue to use Layer 3 and Layer 4 rules where deep packet inspection is not required. This capability provides the flexibility for servers requiring low-latency performance to be exempted from deep packet inspection and still benefit from Cisco ASA stateful inspection. As a result, much more efficient and higher-performance firewalling is possible than with application-based rules by themselves.

Q. Do I have to re-create my existing Cisco ASA access lists on Cisco ASA Next-Generation Firewall Services?

A. No. Cisco ASA Next-Generation Firewall Services allow administrators to use existing Layer 3 and Layer 4 rules and network objects. For example, if an administrator has defined 5000 network objects on the Cisco ASA firewall, these objects can be reused in the rich rules on Cisco ASA Next-Generation Firewall Services. Administrators can migrate their current rule set to Layer 7 rules over time, when it makes sense to do so.

Q. Can Cisco ASA Next-Generation Firewall Services be used in multicontext mode?

A. Yes, multicontext mode is supported in Cisco ASA CX Software Release 9.2 or later.

Q. Can Cisco ASA Next-Generation Firewall Services be used in transparent mode?

A. Yes. The Cisco ASA firewall can be placed in transparent mode as normal; no configuration is required on Cisco ASA Next-Generation Firewall Services.

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 C67-700607-03 10/13