Cisco ASA Next-Generation Firewall Services

Product Overview

Cisco® ASA Next-Generation Firewall Services is a suite of modular security services that run on the Cisco ASA 5500-X Series Next-Generation Firewalls (5512-X, 5515-X, 5525-X, 5545-X, 5555-X, and 5585-X with Security Services Processor SSP-10, SSP-20, SSP-40, and SSP-60).

Cisco ASA Next-Generation Firewall Services include Cisco Application Visibility and Control (AVC), Web Security Essentials (WSE), and Intrusion Prevention System (IPS). They blend a proven stateful inspection firewall with next-generation firewall capabilities and network-based security controls for end-to-end network intelligence and streamlined security operations.

Corporate networks are encountering the highest levels of change in history. Users require anywhere, anytime access to the network from a variety of company-owned and personal mobile devices. In addition, applications have evolved to be highly dynamic and multifaceted, blurring the line between business applications and personal ones that may increase the company's exposure to Internet-based threats. As a result, organizations must take a new approach to that unifies the network's streamlined security operations without abandoning time-tested methods. Cisco ASA Next-Generation Firewall Services enable organizations to rapidly adapt to dynamic business needs while maintaining the highest levels of security.

Features and Benefits

Like most other next-generation firewalls, Cisco ASA Next-Generation Firewalls deliver application awareness and user identity 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 micro applications
- Restrict web and web application use based on the reputation of the site
- Proactively protect against Internet threats
- Enforce differentiated policies based on the user, device, role, application type, and threat profile

Cisco Prime™ Security Manager manages Cisco ASA Next-Generation Firewall Services. It is a comprehensive management solution that delivers increased visibility into the network; provides detailed application, user, behavior, policy, and device control; and employs a flexible architecture that enables significant advances to be introduced in security management. It provides security administrators with end-to-end visibility across the security network, including top-level traffic patterns, detailed logs, and the health and performance of Cisco ASA Next-Generation Firewalls. Users can simplify cost and complexity with Cisco Prime Security Manager to unify core Cisco ASA functions (including firewall and NAT) and Cisco Next-Generation Firewall Services for distributed deployments.

Unprecedented Network Visibility

Cisco ASA Next-Generation Firewall Services gives security administrators greater visibility into the traffic flowing through the network, including the users connecting to the network, the devices used, and the applications and websites that are accessed.

Cisco ASA Next-Generation Firewall Services use Cisco security technologies to provide actionable intelligence to security administrators. For example, Cisco AnyConnect® clients provide information on the type and location of a mobile device before it can access the network. Cisco ASA Next-Generation Firewall Services also use global threat intelligence from Cisco Security Intelligence Operations (SIO) to provide zero-day threat protection. Using these and other Cisco security technologies throughout the network, Cisco ASA Next-Generation Firewall Services deliver end-to-end network visibility for superior security control. These services include:

- **Robust authentication.** In addition to passive authentication methods using Windows Active Directory agent and Lightweight Directory Access Protocol (LDAP), Kerberos and Windows NT LAN Manager are used to provide active authentication.
- **Device information.** Cisco AnyConnect clients provide information on the specific types of user devices attempting to gain access to the network, as well as whether the device is located locally or remotely, enabling administrators to confidently allow devices while maintaining high levels of network protection and control.
- **Reputation-based threat defense.** Threat intelligence feeds from Cisco SIO use the global footprint of Cisco security deployments (more than 2 million devices) to analyze approximately one-third of the world's Internet traffic from email and web threat vectors. Reputation feeds are used by Cisco WSE and IPS to help reduce risk and threat exposure with near-real-time protection from known and zero-day threats.

Precise Application, User, Device, and Threat Control

Cisco ASA Next-Generation Firewall Services with Cisco AVC block port- and protocol-hopping applications such as Skype and other peer-to-peer applications, providing more effective security while requiring fewer policies. It enables policies to be written based on a wide range of contextual elements, including application, user, device, and location. Cisco AVC also employs deep social networking controls. It recognizes more than 1200 applications and 150,000 micro applications, enabling organizations to provide individual or group-based access to specific components of an application (such as Facebook for business use) while disabling other components (such as Facebook games). Specific behaviors can also be blocked within allowed micro applications for an additional layer of control.

Cisco ASA Next-Generation Firewall Services with Cisco WSE is a next-generation web security service that addresses these needs. Cisco WSE provides enterprise-class, context-aware web security capabilities to the industry's most proven stateful inspection firewall for end-to-end network intelligence and streamlined security operations. Cisco WSE blends robust content-based URL filtering with the near-real-time global threat and web reputation analysis from Cisco SIO. Cisco WSE enables organizations to enforce reputation-based web security policies and robust content-based URL filtering to enable differentiated access policies based on user, group, device, and role.

Cisco ASA Next-Generation Firewalls with IPS provide context-driven threat detection and mitigation. The simplified operation puts focus on threat prevention rather than on detection parameters. Inputs from the Cisco AVC and WSE security services optimize the Cisco IPS's operation and efficacy to provide holistic threat prevention.

Comprehensive Security Architecture

Cisco ASA Next-Generation Firewall Services extend the Cisco ASA platform to provide unprecedented visibility and control. Support for Layer 3 and Layer 4 stateful firewall features, including access control, network address translation, and stateful inspection, enables organizations to keep existing stateful inspection firewall policies that are essential for a host of compliance regulations, while adding Layer 7 context-aware rules that can act intelligently on contextual information. Cisco ASA Next-Generation Firewall Services pull in local intelligence from the Cisco AnyConnect Secure Mobility Client and near-real-time global threat intelligence from Cisco SIO. A proven firewall platform, combined with the power of local and global threat intelligence, provides a comprehensive, dynamic security architecture that is capable of addressing an organization's evolving security needs to enable growth, extensibility, and ongoing innovation.

Table 1 lists the features and benefits of Cisco ASA Next-Generation Firewall Services.

Table 1. Features and Benefits of Cisco ASA Next-Generation Firewall Services

Feature	Benefits
Application awareness	Enforces access policy based on more than 1200 commonly used applications and 150,000 micro applications; provides access control based on "behavior" (for example, a file upload or a post on a social networking site) to further control user activity related to applications; controls port- and protocol-hopping applications that can evade classic security controls.
Identity-based firewalling	Provides differentiated access control based on user and user role; supports common identity mechanisms such as Windows Active Directory agent, LDAP, Kerberos, and Windows NT LAN Manager.
Device-type-based enforcement	Uses Cisco AnyConnect clients to identify the types of devices (such as iPads, iPhones, and Android devices) that are accessing the network, and controls which devices will be permitted or denied.
URL filtering	Enables precise control of Internet traffic with an enterprise-class, full-featured URL filtering solution.
Intrusion prevention	Detects and blocks Internet-born threats that target end users and their personal devices. Cisco ASA Next-Generation Firewalls with IPS protect the Internet edge and reduce complexity through simplified policies integrated with Cisco ASA Next-Generation Firewall Services.
Global threat intelligence	Uses the global footprint of Cisco security deployments for more comprehensive network protection. Cisco SIO delivers regularly updated threat intelligence feeds for near-real-time protection from zero-day malware.
Stateful firewall capabilities	In addition to enabling Layer 7 context-aware rules, provides extensive support for Layer 3 and Layer 4 stateful firewall features, including access control, network address translation, and stateful inspection.
Intuitive management solution	Comes preloaded with Cisco Prime Security Manager, a powerful, intuitive management solution that simplifies the management of context-aware firewalls.

Product Performance

Table 2 lists the capabilities and capacities of the Cisco ASA Next-Generation Firewall Services for the Cisco ASA 5500-X midrange firewalls.

For more information about the capabilities and capacities of Cisco ASA Next-Generation Firewall software on the Cisco ASA 5500-X platform, please see the data sheets for Cisco ASA 5500-X Series appliances for small and branch offices or for the Internet edge.

Table 2. Cisco ASA 5500-X Series Midrange Next-Generation Firewall Capabilities and Capacities

Feature	Cisco ASA 5512-X	Cisco ASA 5515-X	Cisco ASA 5525-X	Cisco ASA 5545-X	Cisco ASA 5555-X
Throughput with Cisco AVC and WSE	200 Mbps (multiprotocol)	350 Mbps (multiprotocol)	650 Mbps (multiprotocol)	1 Gbps (multiprotocol)	1.4 Gbps (multiprotocol)
Maximum concurrent sessions	100,000	250,000	500,000	750,000	1,000,000
Connections per second	10,000	15,000	20,000	30,000	50,000
Supported applications	More than 1200				

Feature	Cisco ASA 5512-X	Cisco ASA 5515-X	Cisco ASA 5525-X	Cisco ASA 5545-X	Cisco ASA 5555-X
Supported micro-applications	More than 150,000				
URL categories	78				
Number of URLs categorized	More than 20 million				
Languages for URL filtering	More than 60				
Web requests analyzed by Cisco SIO every day	30 billion				
Configuration, logging, and monitoring	On-device Cisco Prime Security Manager				
Reporting	On-device Cisco Prime Security Manager				
Centralized configuration, logging, monitoring, and reporting	Multi device Cisco Prime Security Manager				

Hardware Product Specifications

Table 3 provides a comparison of the Cisco ASA 5585-X CX Security Services Processor (SSP) 10, 20, 40, and 60 hardware blades.

Table 3. Cisco ASA 5585-X Next-Generation Firewall Hardware Blade Capabilities and Capacities

Feature	Cisco ASA 5585-X CX SSP-10	Cisco ASA 5585-X CX SSP-20	Cisco ASA 5585-X CX SSP-40	Cisco ASA 5585-X CX SSP-60
Throughput with Cisco AVC and WSE	2 Gbps (multiprotocol)	5 Gbps (multiprotocol)	9 Gbps (multiprotocol)	13 Gbps (multiprotocol)
Maximum number of concurrent sessions	500,000	1,000,000	1,800,000	4,000,000
Connections per second	40,000	75,000	120,000	160,000
Supported applications	More than 1200			
Supported micro applications	More than 150,000			
URL categories	78			
Number of URLs categorized	More than 20 million			
Languages for URL filtering	More than 60			
Number of web requests analyzed by Cisco SIO every day	30 billion			
Configuration, logging, and monitoring	On-device Cisco Prime Security Manager			
Reporting	On-device Cisco Prime Security Manager			
Centralized configuration, logging, monitoring, and reporting	Multi device Cisco Prime Security Manager			

Product Model	Cisco ASA 5585-X CX SSP-10	Cisco ASA 5585-X CX SSP-20	Cisco ASA 5585-X CX SSP-40	Cisco ASA 5585-X CX SSP-60
Technical Specifications				
Memory	12 GB	24 GB	24 GB	48 GB
Minimum flash	8 GB			
Management and monitoring interface	2 Ethernet 10/100/1000 ports			

Platform Support/Compatibility

The Cisco ASA 5585-X CX SSP-10, SSP-20, SSP-40, and SSP-60 hardware blades are supported on the Cisco ASA 5585-X platform. Cisco ASA 5585-X SSP-10 and SSP-20 firewalls require Cisco ASA Software Release 8.4.4 and later. Cisco ASA 5585-X SSP-40 and SSP-60 firewalls require Cisco ASA Software Release 9.1.3 and later. Cisco ASA Next-Generation Firewall Services software is supported on the Cisco ASA 5500-X Series of next-generation midrange security appliances running Cisco ASA Software Release 9.1 and later. Regardless of form factor, Cisco ASA Next-Generation Firewall Services are managed by Cisco Prime Security Manager.

Ordering Information

To place an order, visit the Cisco ordering homepage. Table 4 provides ordering information for Cisco ASA Next-Generation Firewall Services.

Table 4. Cisco ASA Next-Generation Firewall Services Ordering Information

Product Name	Part Number
Cisco ASA 5500-X Series Midrange Appliances (Hardware)	
ASA 5512-X with software, 6GE data, 1GE mgmt, AC, DES, 120GB SSD	ASA5512-SSD120-K8
ASA 5512-X with software, 6GE data, 1GE mgmt, AC, 3DES/AES, 120GB SSD	ASA5512-SSD120-K9
ASA 5515-X with software, 6GE data, 1GE mgmt, AC, DES, 120GB SSD	ASA5515-SSD120-K8
ASA 5515-X with software, 6GE data, 1GE mgmt, AC, 3DES/AES, 120GB SSD	ASA5515-SSD120-K9
ASA 5525-X with software, 8 GE data, 1GE mgmt, AC, DES, 120GB SSD	ASA5525-SSD120-K8
ASA 5525-X with software, 8 GE data, 1GE mgmt, AC, 3DES/AES, 120GB SSD	ASA5525-SSD120-K9
ASA 5545-X with software, 8 GE data, 1GE mgmt, AC, DES, 2 120GB SSD	ASA5545-2SSD120-K8
ASA 5545-X with software, 8 GE data, 1GE mgmt, AC, 3DES/AES, 2 120GB SSD	ASA5545-2SSD120-K9
ASA 5555-X with software, 8 GE data, 1GE mgmt, AC, DES, 2 120GB SSD	ASA5555-2SSD120-K8
ASA 5555-X with software, 8 GE data, 1GE mgmt, AC, 3DES/AES, 2 120GB SSD	ASA5555-2SSD120-K9
Cisco ASA 5585-X Appliances (Hardware)	
ASA 5585-X chassis with SSP-10, CX SSP-10, 16GE, 4GE mgmt, 1 AC, DES	ASA5585-S10C10-K8
ASA 5585-X chassis with SSP-10, CX SSP-10, 16GE, 4GE mgmt, 1 AC, 3DES/AES	ASA5585-S10C10-K9
ASA 5585-X chassis with SSP-10, CX SSP-10, 16GE, 4 SFP+, 2 AC, 3DES/AES	ASA5585-S10C10XK9
ASA 5585-X chassis with SSP-20, CX SSP-20, 16GE, 4GE mgmt, 1 AC, DES	ASA5585-S20C20-K8
ASA 5585-X chassis with SSP-20, CX SSP-20, 16GE, 4GE mgmt, 1 AC, 3DES/AES	ASA5585-S20C20-K9
ASA 5585-X chassis with SSP-20, CX SSP-20, 16GE, 4 SFP+, 2 AC, 3DES/AES	ASA5585-S20C20XK9
ASA 5585-X chassis with SSP-40, CX SSP-40, 12GE, 8 SFP+, 2 AC, DES	ASA5585-S40C40-K8
ASA 5585-X chassis with SSP-40, CX SSP-40, 12GE,8 SFP+, 2 AC, 3DES/AES	ASA5585-S40C40-K9
ASA 5585-X chassis with SSP-60, CX SSP-60, 12GE, 8 SFP+, 2 AC, DES	ASA5585-S60C60-K8
ASA 5585-X chassis with SSP-60, CX SSP-60, 12GE,8 SFP+, 2 AC, 3DES/AES	ASA5585-S60C60-K9
ASA 5585-X CX SSP-40 with 6GE, 4SFP+	ASA5585-SSP-CX40
ASA 5585-X CX SSP-60 with 6GE, 4SFP+	ASA5585-SSP-CX60
ASA Next-Generation Firewall Services Software Subscriptions: 3-year term (1-year and 5-year service software bundle subscriptions can be purchased as well as individual Cisco AVC, WSE, and Next-Generation Firewall IPS service software subscriptions with 1-year, 3-year, and 5-year terms)	
ASA 5512-X with Cisco AVC, WSE, and IPS, 3-year	ASA5512-AWI3Y
ASA 5515-X AVC, WSE, and IPS, 3-year	ASA5515-AWI3Y
ASA 5525-X AVC, WSE, and IPS, 3-year	ASA5525-AWI3Y
ASA 5545-X AVC, WSE, and IPS, 3-year	ASA5545-AWI3Y

Product Name	Part Number
ASA 5555-X AVC, WSE, and IPS, 3-year	ASA5555-AWI3Y
ASA 5585-X SSP-10 AVC, WSE, and IPS, 3-year	ASA5585-10-AWI3Y
ASA 5585-X SSP-20 AVC, WSE, and IPS, 3-year	ASA5585-20-AWI3Y
ASA 5585-X SSP-40 AVC, WSE, and IPS, 3-year	ASA5585-40-AWI3Y
ASA 5585-X SSP-60 AVC, WSE, and IPS, 3-year	ASA5585-60-AWI3Y
ASA 5512-X AVC and WSE, 3-year	ASA5512-AW3Y
ASA 5515-X AVC and WSE, 3-year	ASA5515-AW3Y
ASA 5525-X AVC and WSE, 3-year	ASA5525-AW3Y
ASA 5545-X AVC and WSE, 3-year	ASA5545-AW3Y
ASA 5555-X AVC and WSE, 3-year	ASA5555-AW3Y
ASA 5585-X SSP-10 AVC and WSE, 3-year	ASA5585-10-AW3Y
ASA 5585-X SSP-20 AVC and WSE, 3-year	ASA5585-20-AW3Y
ASA 5585-X SSP-40 AVC and WSE, 3-year	ASA5585-40-AW3Y
ASA 5585-X SSP-60 AVC and WSE, 3-year	ASA5585-60-AW3Y
ASA 5515-X AVC and NGFW IPS, 3-year	ASA5515-AI3Y
ASA 5525-X AVC and NGFW IPS, 3-year	ASA5525-AI3Y
ASA 5545-X AVC and NGFW IPS, 3-year	ASA5545-AI3Y
ASA 5555-X AVC and NGFW IPS, 3-year	ASA5555-AI3Y
ASA 5585-X SSP-10 AVC and NGFW IPS, 3-year	ASA5585-10-AI3Y
ASA 5585-X SSP-20 AVC and NGFW IPS, 3-year	ASA5585-20-AI3Y
ASA 5585-X SSP-40 AVC and NGFW IPS, 3-year	ASA5585-40-AI3Y
ASA 5585-X SSP-60 AVC and NGFW IPS, 3-year	ASA5585-60-AI3Y

To Download the Software

Visit the Cisco Software Center to download Cisco ASA Next-Generation Firewall Services Software.

For More Information

For more information, please visit the following links:

- Cisco ASA Next-Generation Firewall Services: http://www.cisco.com/go/asacx.
- Cisco ASA 5500-X Series Next-Generation Firewalls: http://www.cisco.com/go/asa.
- Cisco Prime Security Manager: http://www.cisco.com/go/prsm.
- Cisco Security Services: http://www.cisco.com/en/US/products/svcs/ps2961/ps2952/serv_group_home.html.

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 C78-701659-05 01/14