Cisco ASA Next-Generation Firewall Services

Product Overview

Cisco® ASA Next-Generation Firewall Services has reached End of Sale. Please consider consider one of our newer Next-Generation Firewall offerings: the Cisco Firepower NGFW or the Cisco ASA with FirePOWER™ Services. For a similar price, you can get proven firewall protection combined with industry-leading Sourcefire® threat and advanced malware protection (AMP) in a single device.

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.

To Download the Software

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

Cisco Capital

Financing to Help You Achieve Your Objectives

Cisco Capital® financing can help you acquire the technology you need to achieve your objectives and stay competitive. We can help you reduce CapEx, accelerate your growth, and optimize your investment dollars and ROI. Cisco Capital financing gives you flexibility in acquiring hardware, software, services, and complementary third-party equipment. And there's just one predictable payment. Cisco Capital is available in more than 100 countries. Learn more.

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 C78-701659-08 07/16