Cisco Adaptive Security Appliance Software Release 9.0

What Is the Value of Cisco ASA Software Release 9.0?

Cisco ASA Software Release 9.0 is the latest release of software that powers the Cisco ASA family—purpose-built appliances that deliver enforcement of the Cisco SecureX Architecture.™ Release 9.0 delivers enterprise-class security capabilities for Cisco ASA devices in a variety of form factors, including a wide range of standalone appliances; hardware blades that integrate with an organization's existing network infrastructure; and software that can secure and protect both public and private clouds.

What Problems Does Cisco ASA Software Release 9.0 Help Solve?

Organizations that want to harness the power of the web must deal with the consequence of becoming vulnerable to web-based threats that can negatively impact data, brands, and operations. Many current "all-in-one" appliance solutions do not offer the predictable performance and solution flexibility that enterprises need to effectively meet today's security challenges—such as social networking, mobile workers, and the "bring your own device" (BYOD) trend—without sacrificing network performance or undermining workforce productivity.

Cisco ASA Software Release 9.0, integrated with Cisco Cloud Web Security (formerly ScanSafe) and powered by Cisco Security Intelligence Operations (SIO), provides a centralized content security solution combined with localized network security. The result is best-in-class network security integrated with best-in-class web security. All content scanning is offloaded to Cisco's cloud, so there is little to no impact on the performance of ASA devices. Administrators also can choose to perform deep content scanning on a subset of traffic, based on network address, Microsoft Active Directory user or group name, or hosts residing inside a specific security context.

Clustering

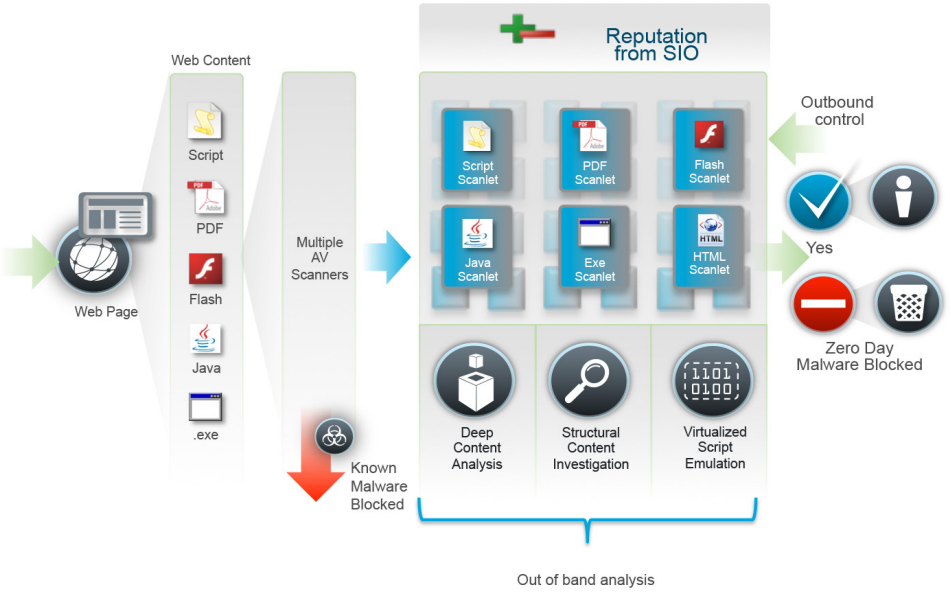
Cisco ASA Software Release 9.0 supports the ability to "cluster" multiple ASAs to deliver much higher capacity and throughput. Up to eight Cisco ASA 5585-X or Cisco ASA 5580 Series firewall modules can be joined in a single cluster to deliver up to 128 Gbps of multiprotocol throughput (300 Gbps max) and more than 50 million concurrent connections.

At the core of the clustering architecture is the patent-pending Cisco Cluster Link Aggregation Control Protocol (cLACP), which enables multiunit ASA clusters to function and be managed as a single entity, identifies the backup unit, and creates the session backup. Policies pushed to the cluster are replicated across all units within the cluster. The health, performance, and capacity statistics of the entire cluster, as well as individual units within it, can be assessed from a single management console.

Integration with Cisco Cloud Web Security

Cisco ASA Software Release 9.0 integrates with Cisco Cloud Web Security, providing the best way to enhance an organization's investment in Cisco data centers, networks, and branches. Real-time, cloud-based scanning blocks malware and inappropriate content before it reaches the network (Figure 1). In addition, management is simplified because acceptable use policies can be applied to all users, regardless of location.

Figure 1: Overview of Cisco Cloud Web Security



Cisco's cloud infrastructure, built on high-availability and high-performance data centers spread throughout the globe, has a proven track record for availability and provides visibility and security without the need for on-premise devices. Cisco's global network processes high volumes of web content at high speeds, everywhere, for a true global solution that is always available.

Cisco Cloud Web Security also integrates with Cisco branch office routers and Cisco AnyConnect® to enable flexible deployments. Organizations can avoid costs associated with deployment and maintenance of on-premise software and hardware.

What Other Benefits Does Cisco ASA Software Release 9.0 Provide?

In addition to the ability to cluster ASA devices and seamless integration with Cisco Cloud Web Security, Cisco ASA Software Release 9.0 provides:

- **Next-generation encryption**—The Suite B set of cryptographic algorithms is included. These cryptographic standards for remote access and site-to-site connections use an IPsec tunnel, providing greater confidentiality.
- **Cisco TrustSec® integration**—Cisco TrustSec security group tags (SGTs) integrate security into the network fabric to extend the policy construct on the ASA platform. Cisco TrustSec policy-based access control, identity-aware networking, and data integrity and confidentiality services help secure networks and resources.
- **IPv6**—Cisco ASA Software Release 9.0 enables IPv6 clientless support. This includes critical IPv4-to-IPv6 translation features, enabling ASA appliances to be deployed in a mixed IPv4/IPv6 environment.
- **Dynamic routing and site-to-site VPN**—This capability is provided on a per-context basis, providing better segmentation between departments or between customers.

Why Cisco?

Security is more critical to your network than ever before. As threats and risks persist, security is necessary to provide business continuity, protect valuable information, maintain brand reputation, and adopt new technology. A secure network enables your employees to embrace mobility and securely connect to the right information. It also allows your customers and partners to conduct business with you more easily.

No organization understands network security like Cisco. Our market leadership, unmatched threat protection and prevention, innovative products, and longevity make us the right vendor for your security needs.

For more information, please visit: http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5708/ps5709/ps12726/qa_c67-712934.html

Cisco ASA Software Release 9.0: FAQs

Q. What Cisco ASA models support Cisco ASA Software Release 9.0?

A. Cisco ASA Software Release 9.0 will be supported across the ASA product line, including Cisco ASA 5500 Series Adaptive Security Appliances, Cisco ASA 5500-X Series Adaptive Security Appliances, and Cisco Catalyst® 6500 Series ASA Services Modules.

Q. How can Cisco Cloud Web Security capabilities be extended to remote users?

A. Cisco Cloud Web Security capabilities are extended to remote users via the Cisco AnyConnect Secure Mobility Client, which performs split-tunneling of web and VPN traffic. This eliminates the need to backhaul Internet traffic to company headquarters, thereby enabling complex remote access use cases.

Q. How does Cisco ASA redirect traffic to Cisco Cloud Web Security?

A. The Cisco ASA Modular Policy Framework (MPF) allows flexible policies to be created to serve a wide range of needs. Outbound traffic can be classified based on user name, user group, source, or destination. The destination aspect can be further classified into three broad categories:

- **Approved traffic:** Traffic from known, safe websites that is automatically approved by corporate policy
- **VPN traffic:** Traffic flowing through a site-to-site VPN tunnel
- **Traffic redirected to Cisco Cloud Web Security:** Traffic sent to Cisco Cloud Web Security for granular web policy control, including URL filtering, antivirus scanning, web content scanning, and web application visibility and control

C45-715175-00 09/12