Cisco ASA Software Release 9.0

Q. What is Cisco ASA Software Release 9.0?

A. Cisco® Adaptive Security Appliance (ASA) Software Release 9.0 is the latest release of the software that powers the Cisco ASA family. The same core ASA code delivers enterprise-class security capabilities for ASA devices in a variety of form factors, including a wide range of standalone appliances, hardware blades that integrate with the organization's existing network infrastructure, and software that can secure and protect public and private clouds.

Q. What's new in Cisco ASA Software Release 9.0?

A. ASA Software Release 9.0 provides several enhancements. Major new features in this release include:

- The ability to join up to eight Cisco ASA 5585-X or 5580 Series adaptive security appliances in a single cluster, for a linear, predictable increase in performance while providing high availability for always-on data centers
- Integration with Cisco Cloud Web Security (formerly ScanSafe), which allows enterprises to enforce granular web access and web application policy while providing protection from viruses and malware
- Cisco TrustSec® Security Group Tags (SGTs), which integrats security into the network fabric to extend the policy construct on the ASA platform
- Next-Generation Encryption, including the Suite B set of cryptographic algorithms, for much better confidentiality
- IPv6, including critical IPv4-to-IPv6 translation features, enabling ASA to be deployed in a mixed v4/v6 environment
- Dynamic routing and site-to-site VPN on a per-context basis, providing much better segmentation between departments or between customers

Q. What Cisco ASA models are supported by ASA 9.0?

A. Cisco ASA 9.0 will be supported across the ASA product line, including the Cisco ASA 5500 Series, the ASA 5500-X Series, and the Cisco Catalyst® 6500 Series ASA Services Module.

Clustering

Q. Does ASA 9.0 support clustering?

A. Yes. Cisco ASA Release 9.0 enables up to eight Cisco ASA 5585-X or 5580 Adaptive Security Appliance firewall modules to 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. Alternatively, slot 1 of each ASA 5585-X can be populated with an integrated Intrusion Protection System (IPS) module, for up to 60 Gbps of IPS throughput.

Q. What are some of the key features of the clustering architecture in Cisco ASA Release 9.0?

A. At the core of the clustering architecture in ASA 9.0 is the patent-pending Cisco Cluster Link Aggregation Control Protocol (cLACP). The protocol 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 get replicated across all units within the cluster, and the health, performance, and capacity statistics of the entire cluster, as well as individual units within the cluster, can be assessed from the single management console.

Q. What ASA models will support clustering?

A. Initially, Cisco ASA Software Release 9.0 will enable clustering on the ASA 5580 and 5585-X Adaptive Security Appliances.

Q. What ASA modes are supported?

A. Clustered ASA appliances can operate in routed, transparent, or mixed-mode. All members of the cluster must be in the same mode.

Q. Do I have to purchase any license to enable clustering?

A. Yes. A cluster license must be purchased and enabled.

Q. How do feature licenses behave when ASA appliances are clustered?

A. Table 1 provides an explanation of the behavior of key features.

Table 1. Cluster Behavior of Different Cisco ASA Feature License Types

License Type	Behavior in Cluster	Example
Enable/disable feature license	Each unit must have its own feature license.	Security+ license is required on every unit (post 9.0.2). This is unlike the ASA Failover Pair Clustering license required on every unit in the cluster for that unit to be a part of the cluster.
Platform-agnostic licenses	The cluster capacity equals the sum of all licenses installed (subject to the total capacity of each individual appliance).	Example #1: • 4-node cluster • Node 1 = 200 SC • Nodes 2,3, and 4 = 0 • Total capacity = 200 Example #2: • 4-node cluster • Node 1 = 200 SC • Node2 = 100 SC • Nodes 3 and 4 = 0 • Total capacity = 250 SC
Time-based license	If the feature is installed on one unit, it is automatically enabled on the entire cluster. The total duration of the license equals the sum of all remaining license durations.	If the botnet traffic filter is installed on one node, it becomes available to the entire cluster. If Node 1 has 9 months remaining and Node 2 has 7 months remaining, the total remaining duration of the botnet traffic filter feature will be 16 months for the entire cluster.

Q. What is meant by “scaling factor”?

A. Scaling factor is a measurement of expected performance and scale in a clustered environment. For example, if a 4-unit cluster is configured using 20-Gbps firewalls with a scaling factor of 0.8, the expected performance of that cluster will be: 0.8 x 4 x 20 Gbps = 64 Gbps.

Q. What is the expected performance and capacity with a 2-, 4-, and 8-unit cluster?

A. Cisco currently offers a scaling factor of between 0.7 and 1.0, depending on the traffic profile. Table 2 shows the expected performance of a 2-unit cluster with a multiprotocol traffic profile (the expected performance of 4- and 8-unit clusters can be calculated by multiplying the 2-unit cluster results by 2 and 4, respectively).

Table 2. Sample Data for a Two-Node Cluster

Platform	Single-Unit Throughput	2-Unit Cluster
ASA5585-S10	2 G	3.2 G
ASA5585-S20	5 G	8 G

Platform	Single-Unit Throughput	2-Unit Cluster
ASA5585-S40	10 G	16 G
ASA5585-S60	20 G	32 G

Q. What is the expected behavior if the cluster uses an integrated IPS module in slot 1 of each unit?

A. All IPS modules in the cluster are configured as independent IPSs, so no configuration sync is required. However, Cisco Security Manager and Cisco IPS Manager Express can be used to simplify configuration management across the IPS modules in the cluster. When the traffic enters the cluster, one specific unit becomes the owner for that specific session. When a policy dictates that traffic be redirected to an IPS for further analysis, the IPS module physically associated with that “owner” unit will be utilized. In other words, traffic from one firewall cannot be redirected to an IPS that is integrated with a different firewall in the cluster.

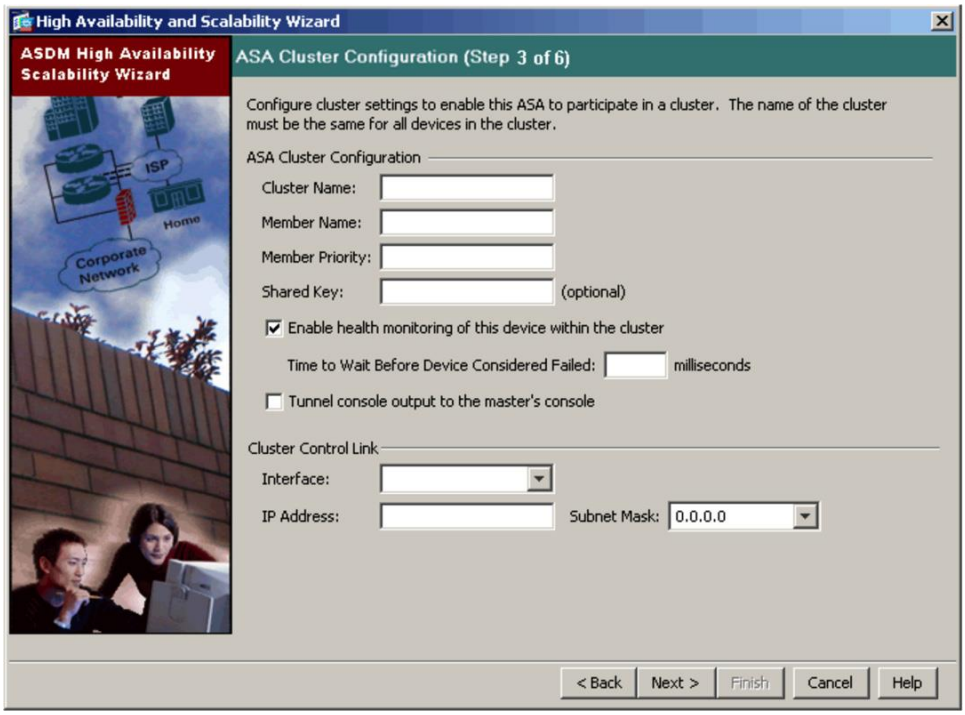
Q. How is session and configuration information synchronized across the cluster members?

A. Cisco ASA Software Release 9.0 uses Cluster Control Link (CCL) to synchronize all state information across the cluster.

Q. How is the cluster managed?

A. The clustered ASA appliances behave as a single firewall instance, so a single instance of Cisco Application Security Device Manager (ASDM) is capable of managing an 8-unit cluster as a single ASA unit. To simplify the configuration phase, cluster configuration steps have been added to the ASDM High Availability and Scalability wizard (Figure 1).

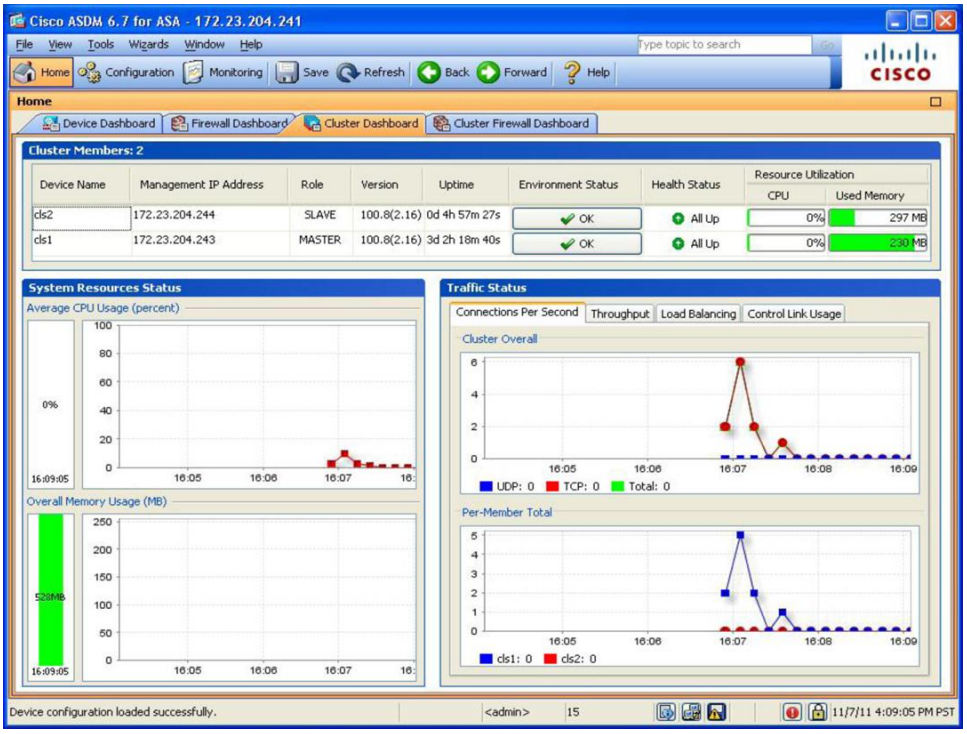
Figure 1. Cluster Configuration Steps in ASDM High Availability and Scalability Wizard



Once the cluster has been deployed, the ASDM Cluster Dashboard (Figure 2) shows the entire cluster on a single screen. The dashboard displays following information:

- Devices information (IP addresses, version, role, and so on)
- Health status: CPU and memory utilizations
- Average CPU and memory status across the cluster
- Control link usage
- Performance statistics: Connections per second and throughput
- Capacity information (number of connections)

Figure 2. ASDM Cluster Dashboard



Cloud Web Security Integration

Q. What are the advantages of cloud web security being integrated with the firewall?

A. Now that Cisco Cloud Web Security is integrated with Cisco ASA Software Release 9.0, organizations gain a centralized content security solution combined with localized network security. However, in contrast to Unified Threat Management appliances (UTMs), which suffer significant performance degradation when web security services are enabled, there is little to no impact on ASA performance because the content scanning is offloaded to the Cisco web security cloud. Administrators 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.

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. The 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 approved by corporate policy
- **VPN traffic:** Traffic flowing through a site-to-site VPN tunnel
- **Traffic redirected to Cisco Cloud Web Security:** Traffic is sent to Cisco Cloud Web Security for granular web policy control, including URL filtering, antivirus scanning, web content scanning scansafe-scanlets, and web application visibility and control

The traffic classification criteria can also be mixed and matched (for example, a group of users such as guests, vendors, or interns can be selected for Cisco Cloud Web Security inspection).

Q. How does integrated Cisco Cloud Web Security compare with web security functionalities that are offered on-box from other firewall vendors?

A. The key challenge with all-in-one approaches to security is that all security functionalities (firewall, network access control, web, antivirus, VPN, and so on) compete for fixed computing resources (for example, CPU, Regex, and crypto). As a result, performance can drop significantly as more services are enabled. In contrast, with Cisco Cloud Web Security integrated into ASA 9.0, the antivirus and web security component is executed on the scalable Cisco Cloud Web Security cloud, while the network security component is executed on the Cisco ASA. As a result, both services achieve maximum security efficacy, with little or no performance impact.

Q. My deployment is not yet ready for identity enablement. Can I still use the Cisco Cloud Web Security Connector in Cisco ASA Software Release 9.0?

A. Yes. Traffic can be redirected to Cisco Cloud Web Security based on 5-tuples, or by using a cut-through-proxy and local database users on the Cisco ASA. However, either of these methods will disable user-level and group-level reporting, as well as policy control on both the ASA and Cisco Cloud Web Security.

Q. Is Cisco Cloud Web Security available when the Cisco ASA appliance is in multicontext mode?

A. Yes. When the ASA is configured for multicontext mode, managed security providers can enable Cisco Cloud Web Security on a per-context basis. Note, however, that Cisco Cloud Web Security is **not** supported when Cisco ASA is in transparent mode.

Q. What are some of the configuration steps required to integrate Cisco Cloud Web Security with Cisco ASA?

A. Cisco ASA configuration has two broad components: Cisco Cloud Web Security information and traffic classification. Traffic classifications are performed using the Cisco ASA Modular Policy Framework (MPF), while Cisco Cloud Web Security classifications require the following information:

- IP address of the Cisco Cloud Web Security tower (primary and backup)
- A valid license
- A designated “retry count” before declaring a tower “dead”

Q. Up to 10 percent of the employees in my organization are remote. How can I extend Cisco Cloud Web Security capabilities to those remote users?

A. Cisco Cloud Web Security capabilities are extended to remote users via the Cisco AnyConnect® Secure Mobility Client. The AnyConnect client performs split-tunneling of web and VPN traffic to eliminate the need to backhaul Internet traffic to company headquarters, thereby enabling complex remote access use cases. For example, if a user is traveling from the United States to Japan, AnyConnect will automatically find the closest Cisco Cloud Web Security tower in Japan, even if the VPN tunnel is terminated to the U.S. headquarters location.

Q. How can I enforce Web 2.0 policies on personal handhelds (iPhone and iPads)?

A. The Cisco AnyConnect Secure Mobility Client launches the tunnel to the Cisco ASA headend. The ASA redirects part of tunnel traffic (port 80 and port 443) to the Cisco web security cloud for Web 2.0 application enforcement. This entire process is transparent to the end user.

Q. Is Cisco Cloud Web Security integration available on all Cisco ASA platforms?

A. Yes. Cisco Cloud Web Security integration is available on all currently shipping Cisco ASA appliance platforms, including the Cisco ASA 5500 Series, the Cisco ASA 5500-X Series, and the Cisco Catalyst 6500 Series ASA Services Module. It is not yet available on the Cisco ASA 1000V Cloud Firewall.

Q. How does this integration achieve high availability?

A. There are two pieces to high availability (HA): Cisco Cloud Web Security Tower HA and Cisco ASA HA. When you configure Cisco Cloud Web Security tower information, you can configure a backup Cisco Cloud Web Security tower, which automatically redirects web traffic to the secondary tower if the primary tower goes down. If you are using Cisco ASA HA, the entire system - including the ASA and the Cisco Cloud Web Security tower - can achieve full redundancy in either active/passive or active/active mode. In exceptional circumstances, if both Cisco Cloud Web Security towers are unavailable (e.g., due to the loss of Internet connectivity), the ASA can be configured to either fail-open or fail-close.

Q. Where do I go for more information on the integrated Cisco Cloud Web Security?

A. More information on Cisco Cloud Web Security web AVC can found at Application Visibility and Control now available in Cisco Cloud Web Security.

Secure Remote Access

Q. Does ASA support IPv6 remote access connections?

A. Yes. IPv4/IPv6 dual stack has been supported inside SSL tunnels since ASA 8.4. ASA 9.0 expands this support to enable IPv4 and IPv6 on the public interface when used in conjunction with Cisco AnyConnect 3.1 or greater. ASA 9.0 also enables IPv6 clientless support.

Q. Does ASA 9.0 support Suite B cryptographic standards?

A. Yes. ASA 9.0 provides comprehensive next-generation encryption capabilities, which includes the Suite B cryptographic standards for remote access and site-to-site connections using an IPsec tunnel. For more information, see the “AnyConnect VPN - Next Generation Encryption” section of this document.

Q. Is next generation encryption available on all ASA platforms?

A. No. Next Generation Encryption is fully supported on the ASA 5585-X, 5500-X Series, and 5580, as well as on the Catalyst 6500 Series ASA Services Module. It can only be partially supported on the ASA 5505, 5510, 5520, 5540, and 5550 due to hardware limitations. AnyConnect 3.1 or greater and an AnyConnect Premium License are also required to use next generation encryption for remote access connections.

Q. Can we use the Cisco AnyConnect Secure Mobility Client with ASA 9.0?

A. Yes. The Cisco AnyConnect Secure Mobility Client is fully supported in ASA 9.0. Customers are encouraged to migrate to AnyConnect for VPN remote access as soon as possible.

Q. Does ASA 9.0 support Virtual Desktop Infrastructure (VDI)?

A. Yes. ASA native clientless support for Citrix VDI deployments has been updated in ASA 9.0 to include XenApp 6.5 and the latest versions of XenDesktop (up to 5.5) both laptops, desktops, and mobile devices (Citrix Mobile Receiver). Support for VMware VDI deployments is also offered (via SmartTunnels). As in past releases, Cisco AnyConnect supports Citrix and VMWare VDI deployments.

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 C67-712934-01 03/14