Adaptive Security Appliance

Contents

Cisco ASA Software

Q. What is Cisco® Adaptive Security Appliance (ASA) Software?

A. Cisco ASA Software is the core operating system that powers Cisco ASA firewall products. It offers stateful firewalling, VPN capabilities, and clustering capabilities; provides for the scalability of ASA hardware; and integrates with other security solutions like Cisco IPS, Cisco Cloud Web Security, Cisco Identity Services Engine (ISE), and Cisco TrustSec® technology. In addition, it offers next-generation firewall capabilities through the ASA CX software module on ASA5500-X or through a Security Services Processor (SSP) in the ASA 5585-X appliances.

Q. What operating system is the ASA built on?

A. Cisco ASA Software runs on Linux as an ASA OS process. Cisco ASA Software is not forked off Cisco IOS® Software. Its roots are in the Cisco Finesse® OS (an embedded OS), which ran on older Cisco PIX® firewall platforms.

ASA Releases

Q. What's new in the Cisco ASA Software Release 9 train?

A. Please refer to the Cisco ASA 9.0(x) release notes: http://www.cisco.com/c/en/us/td/docs/security/asa/asa90/release/notes/asarn90.html.

Q. Where can I find information on new features introduced in each software release?

A. This information is in the software release notes. A list of all ASA releases and the corresponding release notes can be found at: http://www.cisco.com/c/en/us/td/docs/security/asa/roadmap/asa_new_features.html.

Q. How do I download software for the Cisco ASA 5500-X Series security appliances?

A. The software can be downloaded from the Cisco Download Software page (registered customers only).

Q. How do I migrate from ASA 5500 Series firewalls to ASA 5500-X Series firewalls?

A. Please refer to http://www.cisco.com/c/en/us/products/collateral/security/asa-5500-series-next-generation-firewalls/guide_c07-727453.html for details on how to migrate from ASA 5500 Series appliances to ASA 5500-X Series appliances. The migration tool can also be accessed at: https://fwm.cisco.com.

Q. How can a customer find out about new software defects and software updates?

A. Customer must have an active Cisco SMARTnet™ contract for access to software updates as well as access to the Bug Search Tool (http://tools.cisco.com/Support/BugToolKit/action.do?hdnAction=searchBugs). Customers can also do a quick check with an existing Cisco Adaptive Security Device Manager (ASDM).

Q. Where I can find comparisons of ASA models?

A. Please visit the page at: http://www.cisco.com/c/en/us/products/security/asa-5500-series-next-generation-firewalls/models-comparison.html.

Q. What are the multicontext enhancements in ASA Software Release 9.0?

A. ASA Software now includes support for site-to-site VPN and dynamic routing protocols. It also supports mixed-route and transparent-mode multicontext configurations. Most important, with ASA Software:

- Each firewall context can maintain its own routing table for static and dynamic routes.
- Customers can mix and match routing protocols on a per-context basis.
- Internet Key Exchange IKEv1 and IKEv2 are supported, and single-mode site-to-site VPN features are maintained in in multiple modes. VPN resources can be flexibly allocated in a system context.

Q. Where can I find guidelines on migrating from the Cisco Catalyst® 6500 Series Firewall Services Module (FWSM) to ASA 5585-X appliances?

A. This migration requires a redesign of the network infrastructure. The typical approach is to use the FWSM-to-ASASM migration tool to first sanitize the configuration. Please see the information at: http://topic.cisco.com/news/cisco/cs/cs-asa/msg39419.html.

After that, you can manually replace the VLAN names with physical interfaces and run the configuration through the cloud migration tool for ASA, which can be found at: https://fwm.cisco.com.

You can even skip the first step and use the cloud migration tool directly, but make sure that the source interface names are aligned to match those of an ASA-5550 appliance. Then you have to edit the converted configuration to match that of an ASA 5585-X.

Cisco ASAv Software

Q. What is the Cisco ASAv?

A. The Cisco Adaptive Security Virtual Appliance (ASAv) is a completely reimagined virtual security solution that supports both a fabric-based deployment with the Cisco Application Centric Infrastructure (ACI) and a traditional tiered deployment. The ASAv supports consistent, transparent security across physical, virtual, application-centric, and cloud environments.

Q. Does ASAv support full feature parity with physical ASA?

A. Yes, ASAv is in full sync with physical appliance features, with the exception of multiple contexts, clustering, and EtherChannel.

Q. Does ASAv support Cisco TrustSec® technology: specifically, security group access control lists?

A. Yes, ASAv supports Cisco TrustSec technology and SG-ACLs. The policy rule is integrated into ASA policy and its stateful firewalling.

Q. Considering an ASAv with 1- Gbps, 1-vCPU license, what happens if the traffic passes 1 Gbps?

A. With the Controlled Introduction (9.2.1) ASAv release, 1 Gbps is the maximum performance that a customer can expect from one vCPU. The ASAv software does not do anything special to drop traffic that exceeds the threshold. If the vCPU is running close to close to capacity, incremental traffic will see a drop in speed.

In future software releases a "shaper" in the software will limit traffic to the throughput specification of the product that was purchased. Also keep in mind the underlying virtual switch capacity.

Q. What hypervisors does ASAv support?

A. Following is the list of hypervisors and tentative timelines for support:

- **VMware**: ASAv is currently supported only on VMware as of ASA 9.2(1) software. Note that ASAv is independent of the virtual switch and does not require Cisco Nexus 1000V.
- **KVM**: ASAv on KVM will be supported soon.
- **Microsoft Hyper-V** and **Citrix Xen**: Support for on Hyper-V and Xen is being planned.

Q. What are the system requirements to run ASAv?

A. For a controlled introduction, ASAv requires VMware ESXi 5.x. See the VMware documentation at: http://www.vmware.com/support/pubs/.

Licensing

Q. What are the different types of licenses that exist for an ASA?

A. The ASA supports three basic types of licenses:

- **Perpetual licenses:** The most common ones are “regular” Base licenses, as well as Feature licenses such as the Cisco AnyConnect® 10K Users Premium license (SKU: L-ASA-SSL-10K).
- **Subscription licenses:** These are time-limited licenses for services such as the Botnet Filter (for example, the 1-Year Botnet Filter license for 5585-X devices, SKU: ASA5585-BOT-1YR=).
- **Temporary licenses:** These are usually “regular” licenses with a time limit that is typically no more than a few weeks. Temporary licenses are also known as demo licenses because they are commonly used for product or feature evaluation.

In addition, **ASAv** comes in two flavors: namely, a one-vCPU model and a four-vCPU model. It supports these license tiers:

- **Standard:** Failover, UC Phone Proxy, Botnet Filter, Intercompany Media Engine and GPRS Tunneling Protocol/General Packet Radio Service (GTP/GPRS) Inspection (bundled features have a perpetual license and include no AnyConnect® VPN features)
- **Premium:** AnyConnect Premium (adds a 5-year right-to-use Premium license for AnyConnect and includes the Standard tier)

All licenses are tied to the serial number of a specific device.

Q. What is the format of an ASA 5500-X license?

A. The ASA 5500-X license consists of a series of five hexadecimal strings, which need to be entered with the activation-key command-line interface or an ASDM license. It will ship preinstalled when ordered with the appliance.

Q. Can I move a license from one ASA to another ASA appliance?

A. No. A license is exclusively tied to the serial number of the ASA appliance. It cannot be transferred.

Q. Do I need a license for a standby appliance?

A. Failover units or standby appliances do not require the same license on each unit.

Older versions of ASA software required that the licenses matched on each unit. Starting with Release 8.3(1), you no longer need to install identical licenses. Typically, you buy a license only for the primary unit; for active/standby failover, the secondary unit inherits the primary license when it becomes active. If you have licenses on both units, they combine into a single running failover Cluster license.

Cluster units do not require the same license on each unit. Typically, you buy a license only for the master unit; slave units inherit the master license. If you have licenses on multiple units, they combine into a single running ASA Cluster license. (Table 1 shows the licensing requirements for cluster units.)

Exceptions

Security Plus license for the ASA 5505 and 5512-X: The Base license does not support failover, so failover cannot be deployed in these systems on a standby unit that has only the Base license.

Both units must have the same **encryption license**.

Both units in an ASA 5512-X through ASA 5555-X system require the **IPS module license**. You also need the IPS signature subscription on the IPS side for both units. See the following guidelines:

- To buy the IPS signature subscription you need the ASA with IPS preinstalled (the part number must include “IPS”: for example, ASA5515-IPS-K9); you cannot buy the IPS signature subscription for a non-“IPS” part number ASA.
- You need the IPS signature subscription on both units; this subscription is not shared in failover because it is not an ASA license.
- The IPS signature subscription requires a unique IPS module license for each unit. Like other ASA licenses, the IPS module license is technically shared in the failover Cluster license. However, because of the IPS signature subscription requirements, you must buy a separate IPS module license for each unit.

For ASAv CPU failover deployments, you must make sure that the standby unit has the same number of virtual CPUs assigned to it as the primary unit (along with matching **vCPU licenses**).

Note: A valid permanent key is required; in rare instances, your authentication key can be removed. If your key consists of all zeros, then you need to reinstall a valid authentication key before failover can be enabled.

Q. What are the licensing requirements for ASA clustering?

A. Please see Table 1.

Table 1. Licensing Requirements for Cisco ASA Cluster Units

Model	License Requirement
Cisco ASA 5585-X	Cluster license supporting up to 16 units. A Cluster license is required on each unit. For other feature licenses, cluster units do not require the same license on each unit. If you have feature licenses on multiple units, they combine into a single running ASA Cluster license. **Note:** Each unit must have the same encryption license and the same 10 GE I/O license
Cisco ASA 5512-X	Security Plus license supporting 2 units. **Note:** Each unit must have the same encryption license.
Cisco ASA 5515-X, **ASA 5525-X,** **ASA 5545-X,** **ASA 5555-X**	Base license supporting 2 units. **Note:** Each unit must have the same encryption license.
All other models	No support.

Q. How do licenses combine for failover pairs or cluster units?

A. For failover pairs or ASA clusters, the licenses on each unit are combined into a single running Cluster license. If you buy separate licenses for each unit, then the combined license uses the following rules:

For licenses that have numerical tiers, such as the number of sessions, the values from each unit’s licenses are combined up to the platform limit. If all licenses in use are time-based, then the licenses count down simultaneously.

Failover Examples

- You have two ASAs with 10 AnyConnect Premium sessions installed on each. The licenses will be combined for a total of 20 AnyConnect Premium sessions.
- You have two ASA 5525-Xs with 500 AnyConnect Premium sessions each. Because the platform limit is 750, the combined license allows 750 AnyConnect Premium sessions.

In the above example, if the AnyConnect Premium licenses are time-based, you might want to disable one of the licenses so that you do not “waste” a 500-session license from which you can use only 250 sessions because of the platform limit.

- You have two ASA 5545-X appliances, one with 20 contexts and the other with 10 contexts. The combined license allows 30 contexts. For active/active failover, the contexts are divided between the two units. One unit can use 18 contexts and the other unit can use 12 contexts, for example, for a total of 30.

Clustering Examples

- You have four ASA 5585-X appliances with SSP-10, three units with 50 contexts each, and one unit with the default 2 contexts. Because the platform limit is 100, the combined license allows a maximum of 100 contexts. Therefore, you can configure up to 100 contexts on the master unit; each slave unit will also have 100 contexts through configuration replication.
- You have four ASA 5585-X appliances with SSP-60, three units with 50 contexts each, and one unit with the default 2 contexts. Because the platform limit is 250, the licenses will be combined for a total of 152 contexts. Therefore, you can configure up to 152 contexts on the master unit; each slave unit will also have 152 contexts through configuration replication.

Only licenses with a status of “enabled” are used. The duration of enabled time-based licenses that do not have numerical tiers is the combined duration of all licenses. The primary or master unit counts down its license first, and when it expires, a secondary or slave unit starts counting down its license, and so on. This rule also applies to active/active failover and ASA clustering, even though all units are actively operating.

For example, if you have 48 weeks left on the Botnet Traffic Filter license on two units, then the combined duration is 96 weeks.

Q. What happens if I enter a wrong license key?
A. License check happens at runtime. A wrong license key will be rejected and the existing license will remain in effect. A license key change does not affect the network traffic flowing through the ASA appliance. Configuration removal and the formatting of internal flash will not remove the license key.

Q. How do I remove the license key from an appliance?
A. Use the command **activation-key <key> deactivate**. This command is applicable only to time-based licenses.

Q. Can I “ turn back the clock” to get around expiring licenses?
A. No. ASA licenses fall into three categories. Perpetual licenses are always in effect and are tied to the serial number of the appliance. Count-based licenses can float between active and standby appliances, and time-based licenses are not dependent on the ASA clock settings.

Q. Is there a license to enable the Botnet Traffic Filter?
A. Yes, an annual license is required to enable this feature.

Certifications

Q. Has ASA Software received Common Criteria and Federal Information Processing Standards (FIPS) certification?
A. Please see the certification for the Cisco Adaptive Security Appliances (ASA) Firewall and Virtual Private Network (VPN) Platform.

Q. Is the ASA 5500-X appliance Common Criteria certified?

A. The following currently orderable models are certified: ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X, ASA 5585-X, and ASA-SM. In addition, Cisco IPS on ASA is also Common Criteria certified on currently orderable ASA models with IPS: ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X, and ASA 5585-X.

ASA Hardware

Physical Appliances

Q. What is the Cisco ASA 5585-X?

A. Designed for mission-critical data centers that require exceptional flexibility and security, the new Cisco ASA 5585-X Adaptive Security Appliance delivers superior technology that spans multiple platforms and deployment scenarios. The Cisco ASA 5585-X scales to the highest VPN session counts, throughput, and connection speed and capacity to meet the growing needs of today's most dynamic organizations, all in a compact 2-RU footprint. Offering protocol-agnostic client and clientless access for a broad spectrum of desktop and mobile platforms, the Cisco ASA 5585-X delivers versatile, always-on remote access integrated with IPS and web security for highly secure mobility and enhanced productivity.

Q. What are the rails that come with an ASA 5585-X?

A. ASA 5585-X has two types of rails: An internal rail is attached to the chassis at the time of manufacturing (this is not orderable except with the chassis). An external rail ships with ASA 5585-X and is also orderable (part number ASA5585-RAILS=).

Q. What are the SKUs (aka product identification numbers, or PIDs) for the rails and rack mounts that can be ordered along with an ASA 5585-X?

A. These are the SKUs related to ASA 5585-X rails and rack mounts:

- ASA5585-RACK-KIT= (This kit comprises both front and rear rack mounts; it is typically used for 4-post racks)
- ASA5585-REAR-RACK= (Use only if customer has only the front rack mounts and wants rear rack mounts in addition to the front)
- ASA5585-RAILS= (Use if customer wants rails instead of rack mounts)

Cable management brackets ship with rail and rack-mount kits but cannot be ordered separately.

Performance and Scalability

Q. What is the maximum performance of ASA appliances?

A. The performance of ASA 5500-X appliances, referred to as the firewall throughput, is measured in 1500-byte User Datagram Protocol (UDP) packets traversing the firewall. Please refer to the ASA 5500-X at-a-glance brochure for individual appliance performance numbers: http://www.cisco.com/c/dam/en/us/products/collateral/security/asa-5500-series-next-generation-firewalls/at_a_glance_c45-701635.pdf.

Firewall throughput is measured by configuring a simple “permit all” ACL on the ASA platform running in a single-route mode and with two configured interfaces (inside and outside). The 1500-byte UDP traffic is sent through the firewall in both directions across 1000 flows for 60 seconds.

Q. What features affect performance on ASA Software?

A. All computation-intensive features such as deep packet inspections and logging will have a direct impact on the performance of ASA Software. For detailed information, watch the presentation .

Q. How many logs per second can ASA Software generate on the ASA 5500-X appliances?

A. The data in Table 2 is based on internal tests done on non-Fabric Configuration Server (FCS) builds. (It is subject to change.)

Table 2. Maximum Logs per Second on Cisco ASA 5500-X Appliances

Model	Maximum Logs per Second
Cisco ASA 5512-X	10,000
Cisco ASA 5515-X	15,000
Cisco ASA 5525-X	20,000
Cisco ASA 5545-X	28,000
Cisco ASA 5555-X	35,000

Q. Does performance vary from one software release to another?

A. New features result in a minor variance in performance from one software release to another across all ASA platforms.

Q. What indicates that an ASA 5500-X appliance is over its maximum capacity?

A. Prolonged high CPU use (anything over 90 percent), less than 10 percent of available memory, and interface packet drops due to high numbers of packets per second are all signs of appliance reaching its capacity limits.

Q. Is there a third-party performance report for ASA 5500-X appliances?

A. Please view the Miercom report at: http://www.miercom.com/pdf/reports/20120514.pdf.

Q. Is it possible to set artificial limits on certain resources?

A. Yes. Resource management is available in the multicontext mode. More details are provided in the configuration guide under the subheading Information for Resource Management.

Q. Where can I find performance results for ASA 5500-X appliances?

A. Please refer to the FAQ at: http://www.cisco.com/c/en/us/products/collateral/security/asa-5500-series-next-generation-firewalls/qa_c67-700608.html.

Q. What is the average latency on the base I/O ports of an ASA 5500-X appliance? Is it different for I/O modules?

A. Average latency on the new appliances varies between 15 to 30 microseconds. These are early results. There is no difference in latency values between native ports and expansion I/O ports.

Q. How does the latency compare to that of the ASA 5500 series of appliances?

A. Cisco ASA 5500-X appliances exhibit lower latency than ASA 5500 appliances, especially at higher throughput. With a multicore CPU and more memory, they are able to scale better than the ASA 5500 appliances. For example, average latency on the ASA 5550 is close to 70 microseconds. ASA 5555-X exhibits latencies closer to 40 microseconds.

Q. Where I can find information about the different ASA models in terms of the following?

- Performance
- Supported VLAN count
- Supported context count

- Interface count and types

A. Please see the following documents.

- For the Cisco ASA 5500 Series (Including the 5585-X models): http://www.cisco.com/c/dam/en/us/products/collateral/security/asa-5500-series-next-generation-firewalls/prod_brochure0900aecd80285492.pdf
- For the Cisco ASA 5500-X Series (which replaces the 5500 series): http://www.cisco.com/c/dam/en/us/products/collateral/security/asa-5500-series-next-generation-firewalls/at_a_glance_c45-701635.pdf

Q. Why were the minimum memory requirements increased for the Cisco ASA Adaptive Security Appliances running Release 8.3 and later?

A. Feature enhancements require additional RAM.

Q. What is the port density (number of supported ports) for an ASA 5585-X?

A. The ASA 5585-X is a 2RU appliance with two slots. The base slot (slot 0) should have a firewall SSP. The second slot (slot 1) can be an additional firewall SSP, an IPS SSP, or a CX (NGFW) SSP or two network modules (half-slot modules). The firewall SSP comes in four flavors (SSP-10, SSP-20, SSP-40, and SSP-60). The number of supported ports varies depending on the model (see Table 4).

Table 3. Supported Ports in the Cisco ASA 5585-X

Cisco ASA 5585-X Model	Number of 1 GE Ports	Number of 10 GE Ports	Total Number of Ports
SSP-10	8	2 SFP/SFP+ (require optional Security Plus license to operate in 10GE I/O mode)	10
SSP-20	8	2 SFP/SFP+ (require optional Security Plus license to operate in 10GE I/O mode)	10
SSP-40	6	4 SFP/SFP+	10
SSP-60	6	4 SFP/SFP+	10

Slot 1 can be installed with network modules to increase the port density. The network modules are half slot cards, so any two-network modules can be installed in the ASA 5585-X.

The network modules are:

- Cisco ASA 5585-X 4-port 10 Gigabit Ethernet Network Module
- Cisco ASA 5585-X 8-port 10 Gigabit Ethernet Network Module
- Cisco ASA 5585-X 20-port 1 Gigabit Ethernet Network Module

Details of the supported network modules and the number of ports can be found at: http://www.cisco.com/c/en/us/products/collateral/security/asa-5585-x-adaptive-security-appliance/product_bulletin_c25-711904.html.

I have 5585-X SSP-20 appliances in active/active mode running multiple contexts. In this network, video endpoints sometimes send a massive amount of UDP traffic, around 75,000 small packets per second, causing ASA to fail the forwarding packets. During this UDP flood, the ASA is dropping packets due to CPU exhaustion. We see that some ICMP echo requests are dropped whereas others are successful.

Q. The traffic hits one context where it is allowed, then hits a second context where the traffic is dropped. Any idea how to improve the performance?

A. In cascaded contexts, 75,000 pps of small packets becomes 150,000 pps. Much of the performance depends on how this traffic arrives at the ASA (the number of flows, the uniformity, and so on).

You will need ASA Software Release 9.1(4) or later, along with the “asp load-balance per-packet” command. Please see the discussion at: https://techzone.cisco.com/t5/ASA-Firewall/ASA-5585-and-ASA-SM-Interface-Architecture-Information-and/ta-p/87044#anc10.

Advanced Protection

Botnet Traffic Filter

Q. What advanced protection is provided by the new Botnet Traffic Filter feature in the Cisco ASA Software?

A. The Cisco ASA 5500 Series Botnet Traffic Filter was introduced in the Cisco ASA Software Release 8.2. The Botnet Traffic Filter monitors the network across all ports and protocols for rogue activity. It detects infected internal endpoints and bots sending command-and-control traffic back to a host on the Internet. The command-and-control hosts receiving the information are identified using the Botnet Traffic Filter database. With updates from Cisco Security Intelligence Operations (SIO), this feature can provide fast and accurate protection against botnet threats. A license is required to deploy this feature on the Cisco ASA 5500 Series.

Q. How do I use the Botnet Traffic Filter with my organization's existing Cisco Content Security Management Appliance and IPS solutions?

A. The Botnet Traffic Filter is complementary to existing Cisco security solutions. Cisco Content Security and IPS solutions protect endpoints and servers by identifying and blocking malware. The Botnet Traffic Filter assists in identifying endpoints that have already been infected or have bypassed existing endpoint prevention solutions.

Q. Is the Botnet Traffic Filter's database the same as the one used by the IronPort® S-Series?

A. No, the databases are not the same. Although both databases are powered by Cisco SIO, the Botnet Traffic Filter relies on a separate, unique database.

Q. What reports are available with the Botnet Traffic Filter?

A. The Botnet Traffic Filter offers reports on top infected hosts, top botnet domains (or "sites"), and top malware ports.

Cisco IPS

Q. Is there any guide to the ASA IPS module?

A. Please refer to the quick-start guide at: http://www.cisco.com/en/US/docs/security/asa/quick_start/ips/ips_qsg.html.

Next-Generation Firewalls (CX)

Q. What software is supported on the Cisco ASA 5500-X Series Next-Generation Firewalls?

A. The Cisco ASA 5500-X Series supports Cisco ASA Software Release 8.6.1 and later. Cisco Cloud Web Security requires ASA Software Release 9.0.1 or later. The IPS service on the ASA 5500-X Series requires Cisco IPS Sensor Software Release 7.1.4 or later. The next-generation firewall service (application visibility, monitoring, and reporting) requires ASA CX Software Release 9.1.1 (the Cisco ASA Software Release must be 9.1.1).

Q. Does the ASA CX Sensor Software Release 9.1.1 include 64-bit support?

A. Yes.

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 all-in-one offerings, 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 according to 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 is approved by corporate policy.
- **VPN traffic:** Traffic flows through a site-to-site VPN tunnel.
- **Traffic redirected to Cisco Cloud Web Security:** Traffic is sent to Cisco Cloud Web Security for precise 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 functions that are offered on-box from other firewall vendors?

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

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 you can use a cut-through proxy or local database users on the Cisco ASHowever, either of these methods will disable user-level and group-level reporting.

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

A. Yes. When the ASA is configured for the multicontext mode, managed security providers can deploy 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. Configuring Cisco ASA for integration with Cloud Web Security has two broad components: Cisco Cloud Web Security information classification, and traffic classification. Traffic classifications are performed using the Cisco ASA Modular Policy Framework (MPF). Cisco Cloud Web Security classifications require the following information:

- Fully qualified domain name (FQDN) or IP address of the primary or backup Cloud Web Security proxy servers
- License hex keys

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 through the Cisco AnyConnect Secure Mobility Client. The AnyConnect client performs a split tunneling of web and VPN traffic to eliminate the need to backhaul Internet traffic to company headquarters, thereby supporting 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 such as iPhone and iPad devices?

A. The Cisco AnyConnect Secure Mobility Client launches the tunnel to the Cisco ASA head end. The ASA redirects part of tunnel traffic (ports 80 and 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, the Cisco ASA 5585-X platform, 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): the Cisco Cloud Web Security Tower HA and Cisco ASA HWhen 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 (because Internet connectivity is lost, for example), 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 application visibility and control can be found at: http://www.cisco.com/c/en/us/products/security/asa-next-generation-firewall-services/index.html.

Management

Q. How do I manage Cisco ASA 5500-X Series and 5585-X Next-Generation Firewalls?

A. You have several options for managing the Cisco ASA 5500-X Series firewalls:

- Cisco Security Manager 4.3 or later, an off-box GUI management application, is available for managing most of your physical network security infrastructure. The upgrade path from Cisco Security Manager 3.x to 4.3 and later is discussed here.
- Command-line interface (CLI)
- Cisco Adaptive Security Device Manager (ASDM), the ASA on-box management application

- Cisco Prime™ Security Manager, the Cisco ASA Next-Generation Firewall Services management application for both on- and off-box deployments

For more information on Cisco ASDM, visit: http://www.cisco.com/go/asdm.

For more information on Cisco Security Manager, visit: http://www.cisco.com/c/en/us/products/security/security-manager/index.html.

For more information on Cisco Prime Security Manager, visit http://www.cisco.com/c/en/us/products/security/prime-security-manager/index.html.

Q. What version of ASDM is used to manage the Cisco ASA 5500-X Series?

A. The Cisco ASA 5500-X Series can be managed using ASDM 6.6.1 or later. Previous releases of ASDM are not supported.

Q. What AAA or remote authentication model does your solution support (for example, RADIUS, Active Directory, etc.)?

A. Please see http://www.cisco.com/c/en/us/td/docs/security/asa/asa90/configuration/guide/asa_90_cli_config/aaa_servers.html.

Q. Can management access to your solution be restricted by an access control list or other method?

A. Yes. Please see the configuration guide at: http://www.cisco.com/en/US/docs/security/asa/asa91/configuration/general/admin_management.html.

Q. Does your solution support certificate-based authentication for management access?

A. Yes, it does, using the HTTPS protocol.

Q. What version of Cisco Security Manager is used to manage the Cisco ASA 5500-X Series?

A. The Cisco ASA 5500-X Series can be managed using Cisco Security Manager 4.3 and later. Previous releases do not support the Cisco ASA 5500-X Series.

Q. How do I manage IPS on the Cisco ASA 5500-X Series and Cisco ASA 5585-X?

A. There are several options, depending on your specific configuration. Cisco Security Manager is an off-box GUI management solution that provides enterprise-class policy control and visibility for the entire feature set (including IPS) of the Cisco ASA 5500-X Series. Cisco IPS Manager Express is an off-box GUI management application that provides policy, configuration, reporting, and event management for fewer than 10 appliances running IPS. Cisco IPS Device Manager (IDM) is the on-box GUI management application for Cisco IPS.

For more information on Cisco IPS Manager Express, visit http://www.cisco.com/go/ime.

For more information on Cisco Security Manager, visit http://www.cisco.com/c/en/us/products/security/security-manager/index.html.

Q. How do I manage the ASA Next-Generation Firewall Services (ASA CX) on the Cisco ASA 5500-X Series?

A. ASA CX is managed by the Cisco Prime Security Manager, which can be used either in an on-box or an off-box mode.

Q. What version of Cisco IPS Manager Express is used to manage the Cisco ASA 5585-X?

A. The Cisco ASA 5585-X Series can be managed with IPS Manager Express 7.2.1 or later. Previous releases do not support these next-generation firewalls.

Q. Does ASA software fully support IPv4 for management?
A. Yes.

Q. Do you provide an enterprise management tool with the capability to manage multiple instances of your solution?
A. Yes, the Cisco Content Switching Module delivers this capability.

Q. Can your enterprise management tool access the local logs of an instance of your solution?
A. Yes. The enterprise management tool for ASA is the Cisco Security Manager. It does not access local logs from the individual devices but receives events from them and correlates them.

Q. What versions of Simple Network Management Protocol (SNMP) does Cisco ASA Software support?
A. Cisco ASA Software supports SNMPv1, SNMPv2 and SNMPv3. With SNMPv3, customers can configure highly secure telemetry with supported SNMP managers and gateways.

Q. What are the details of SNMPv3 implementation on Cisco ASA Software?
A. The SNMPv3 implementation for Cisco ASA Software Release 8.2 supports the user-based security model described in RFC 3414 and the view-based access control model described in RFC 3415.

Q. Does Cisco ASA Software support Cisco NetFlow?
A. Cisco ASA Software Release 8.2 or later supports the NetFlow Secure Event Logging feature, which uses templates from NetFlow version 9. This feature is particularly useful for connection logging in high-performance environments.

Q. On an ASA, can you take a packet capture and export the file to the administrator context? Basically, can you move files between contexts? Or do they have to move the files through the network?
A. From the system space you can use this command: copy /pcap capture:<context_name>/<capture_name> tftp:

This command uses the network connectivity of the administrator context to reach the TFTP server.

Q. In my network, systems outside the firewall need to talk to systems inside the firewall, and the firewall itself needs to talk to the same systems, but needs to do it through the management interface instead of the inside interface. How is this generally handled when the management interface and the inside interface are in the same routing table?
A. When you configure the interface as "management only," it will not accept transit traffic and will be dedicated only to traffic "to the box." For example: If you want to reach the servers from the network 192.168.12.0/24 behind the management interface, then you have to remove the "management only" keyword.

Deployment Modes

Routed Mode

Q. What is ASA routed mode?
A. In the routed mode, the ASA is considered to be a router hop in the network. In single-context mode, it can use the Open Shortest Path First (OSPF) protocol or the Routing Information Protocol (RIP). The routed mode supports many interfaces. Each interface is on a different subnet. You can share interfaces between contexts.

The ASA acts as a router between connected networks, and each interface requires an IP address on a different subnet. In single-context mode, the routed firewall supports Enhanced Interior Gateway Routing Protocol (EIGRP), OSPF, and RIP. The multiple-context mode supports static routes only. We recommend

using the advanced routing capabilities of the upstream and downstream routers instead of relying on the ASA for extensive routing needs.

Transparent Mode

Q. What is the ASA firewall transparent mode?

A. Traditionally, a firewall is a routed hop and acts as a default gateway for hosts that connect to one of its screened subnets. A transparent firewall, on the other hand, is a Layer 2 firewall that acts like a "bump in the wire," or a "stealth firewall," and is not seen as a router hop to connected devices.

Q. What are the benefits of deploying a firewall in transparent mode?

A. The security appliance connects the same network on its inside and outside ports in transparent mode. Following are some of the benefits:

- Because the firewall is not a routed hop, you can easily introduce a transparent firewall into an existing network; it is unnecessary to readdress the IP.
- Maintenance is facilitated because there are no complicated routing patterns to troubleshoot and no NAT configuration.
- In routed mode, some types of traffic cannot pass through the security appliance even if you allow it in an access list. Alternatively, the transparent firewall can allow any traffic through with either an extended access list (for IP traffic) or an EtherType access list (for non-IP traffic).For example, you can establish routing protocol adjacencies through a transparent firewall; you can allow VPN (IPsec), OSPF, RIP, EIGRP, or Border Gateway Protocol (BGP) traffic through based on an extended access list.
- Likewise, protocols such as Hot Standby Router Protocol (HSRP) or Virtual Router Redundancy Protocol (VRRP) can pass through the security appliance. Non-IP traffic (for example, AppleTalk, Internet Packet Exchange, Bridge Protocol Data Units, and Multiprotocol Label Switching) can be configured to go through with an EtherType access list.
- For features that are not directly supported on the transparent firewall, you can allow traffic to pass through so that upstream and downstream routers can support those features. For example, with an extended access list, you can allow Dynamic Host Configuration Protocol (DHCP) traffic (instead of the unsupported DHCP relay feature) or multicast traffic, such as that created by IPTV.

Q. What features are not supported in transparent mode?

A. These features are not supported in transparent mode:

- Dynamic routing protocols such as RIP, EIGRP, and OSPF
- DHCP relay
- Quality of service (QoS)
- Multicast
- VPN termination for through traffic

Q. How does ASA in transparent mode populate the Address Resolution Protocol (ARP) table for directly connected hosts?

A. An ASA operating in transparent mode does not rely on the ARP table for transit communication; it is only for to-the-box and from-the-box traffic. The ARP table is populated using the Bridge Group Virtual Interface (BVI) IP address of the group.

Q. How does interface monitoring work when the failover link is up in transparent mode?

A. ASA uses the MAC and IP addresses of the peer to generate the probes; these are exchanged outside the ARP table based on the configuration and failover data structures.

Miscellaneous

Q. Does ASA act as a traditional load balancer?

A. No. For compatible solutions, please see the configuration guide at: http://www.cisco.com/en/US/docs/security/asa/asa90/configuration/guide/ha_cluster.html.

Q. Are there any best-practice documents for ASA deployment in the data center?

A. Please see the following documents:

- Design guide for the Cisco ASA 5585-X in the data center: http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6032/ps6094/ps6120/design_guide_c22-624431.html
- Data center deployment guide: http://www.cisco.com/en/US/docs/solutions/Enterprise/Borderless_Networks/Smart_Business_Architecture/February2012/SBA_Mid_DC_DataCenterDeploymentGuide-February2012.pdf.
- Configuration guide for Cisco ASA firewalls in the data center: http://docwiki.cisco.com/wiki/Cisco_ASA_Firewall_Configuration_for_Data_Center.
- Firewall and IPS Design Guide: http://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Aug2013/CVD-FirewallAndIPSDesignGuide-AUG13.pdf
- VPN Using Cisco ASA 5505 Design Guide: http://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Aug2013/CVD-VPNUsingCiscoASA5505DesignGuide-AUG13.pdf
- ASA Clustering within VMDC: http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Data_Center/VMDC/ASA_Cluster/ASA_Cluster/ASA_Cluster.pdf

Access Control

Q. What is the maximum ACL limit on ASA?

A. There is no hard-coded limit on the number of elements (access control entries) in an ACL, which is bound only by memory. Each ACE uses a minimum of 212 bytes of RAM. However maximum performance may decrease (typically by 10 to 15 percent as you reach or exceed the recommended maximum number of ACEs. The Table 5indicates the recommended maximum ACE limit per ASA platform. (See Table 3 above for throughputs.)

Table 4. Maximum Access Control Entries for Cisco ASA Models

	5505	5510	5512-X	5515-X	5520	5525-X	5540	5545-X	5550	5555-X	5580	5585 10/20/40/60	ASASM
Max Recommended ACEs	25K	80K	100K	100K	200K	200K	500K	300K	700K	500K	750K	500K/750K 1 - 2 million	2 million
Tested ACEs		80K			300K		700K		700K		1 million+	500K/750K 1-2 million	2 million
Max Observed (from customers)									2.74 million		15.959 million	3.5 million (SSP-40)	

Q. What are the limits for policy maps, class maps, and classes in ASA?

A. Here are the limits:

1. The maximum number of policy maps per device or context: 64
2. The maximum number of maps per device or context: 255
3. The maximum number of classes per policy map: 63

Q. Does ASA offer traffic-policing capabilities? If yes, how is this done?

A. ASA does have traffic-policing capabilities to restrict the bandwidth of an inbound flow, but if you are planning on doing this as a distributed denial-of-service (DDoS) defense, then do not expect fantastic results, because the DDoS could fill up the pipe with traffic before the ASA drops the offending packets. If the inside address is configured by Port Address Translation (PAT), then there are additional things to consider. More information is available here: https://supportforums.cisco.com/document/7011/asa-qos.

A best practice would be to authenticate against the Cisco ISE and then use security group tags (SGTs) to match the user to the traffic policing policy.

Q. If a given source or destination flow is configured for TCP state bypass, and the ACL on inside interface allows it, do I need to create an ACL for return traffic on the outside interface?

A. You do not need an ACL for the return traffic, since a TCP-state-bypassed connection behaves just like a UDP one.

Security Group Tags

Q. How does Cisco ASA software integration work with the Cisco TrustSec architecture?

A. The ASA Software is integrated into the Cisco TrustSec architecture, which augments the ASA Software 5-tuple and identity-based firewall policy elements with SGTs and security group names. Most Cisco devices can transport this security group information with the user's traffic.

- Security devices can use SGTs as a consistent enforcement element. The SGT is 16-bit value, which is embedded in each frame associated with the user device. The SGT can be transported over LAN, WAN, and data center networks so that it is available for inspection and policy enforcement wherever appropriate.
- Customers can use ASA Software to create and enforce policies based on SGTs. The ASA reads the source SGT (denoting a Retail-Manager role, for example). It then evaluates the retail manager's privileges to access the destination resource, which would also have an assigned SGT, such as “PCI-Compliant Server” or “HR Database.” It then determines whether the traffic should be allowed or denied.

  The ASA will perform stateful firewall processing using the source and destination SGTs. The Cisco ASA Software can also make additional inspection decisions based on the source and destination SGT values. For example, it can selectively pass traffic through additional intrusion prevention analysis or direct traffic to Cisco Cloud Web Security services according to SGT values.

Q. I like to know what the advantage may be in using the Cisco ISE with ASA firewalls. I am planning to have a VPN user who will use AnyConnect and connect through ASA.

A. While ASA can act as a VPN termination point, it can only filter traffic or inspect the content passing through it. Cisco ISE can do much more in conjunction with ASCisco ISE allows ASA to apply precise security rules based on posture assessment, posture remediation, and SGTs. The administrator can allow or block access for a user to corporate resources based on certain attributes.

For example, upon connecting to the ASA from IPsec or Any Connect VPN, Cisco ISE can tell ASA if the user's antivirus function is turned off and can therefore allow limited access to the network. This capability is much greater than doing user authentication and authorization. You are actually limiting the user access based on the antivirus protection, software patches, and so on.

Protocol Inspection

Q. Can your firewall solution perform protocol inspection for standards compliance and to facilitate the opening of dynamic ports (for example, H.323, SIP, and AS-SIP)? If so, please list them.

A. Yes. Please see the guide at: http://www.cisco.com/en/US/docs/security/asa/asa91/configuration/firewall/inspect_overview.html.

Network Address Translation

Q. Are there any latency numbers (for smaller packet sizes) when doing NAT64 on the Cisco ASA Services Module with the Cisco Catalyst 6500 Series Supervisor Engine 2T?

A. We do not measure latency for NAT specifically, but there should be no difference between NAT64, NAT46, NAT44, or NAT66.

IPv4 and IPv6

Q. Is ASA software capable of being deployed in a mixed IPv4 and IPv6 environment?

A. ASA can be deployed in mixed IPv4 and IPv6 deployments, and it prepares customers for this imminent migration. ASA capability helps customers prepare for migrating to IPv6 by delivering critical v4 to v6 translation. It provides stateful NAT64 and NAT66, DHCPv6 relay, DNS64, and Unified ACL to simplify policy configuration in a mixed v4 and v6 environment. ASA delivers IPv6 remote access connections with less than a 15 percent performance impact compared with IPv4 traffic. In contrast, other offerings experience an average of 80 percent degradation in performance when transitioning from an IPv4 to an IPv6 traffic pattern.

Q. How do I configure IPv6 neighbor discovery on ASA?

A. Please see the configuration guide at: http://www.cisco.com/c/en/us/td/docs/security/asa/asa90/configuration/guide/asa_90_cli_config/route_ipv6_neighbor.html.

VPN

Cisco AnyConnect

Q. Can the ASA 5545-X be used simultaneously as a firewall and a remote access appliance?

A. Yes. The ASA 5500-X Series has been designed to run multiple simultaneous services without sacrificing performance.

Q. How does ASA Software provide highly secure remote access?

A. ASA Software enables IPv4 and IPv6 dual stack on the inside SSL tunnels, as well as on the public interface when used in conjunction with Cisco AnyConnect 3.1 or later. IPv6 clientless support is also provided. While most other offerings experience an average of 80 percent degradation in performance when transitioning from an IPv4 to an IPv6 traffic pattern, ASA Software supports IPv6 remote access connections with less than a 15 percent performance impact. ASA Software also provides comprehensive next-generation encryption capability, which includes Suite B cryptography standards for remote access and site -to-site connections using an IPsec tunnel.

Q. Does ASA support IPv6 remote access connections?

A. Yes. The IPv4 and 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 later. ASA 9.0 also enables IPv6 clientless support.

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.

Clientless VPN

Q. What are the clientless VPN enhancements in ASA 9.0 and later?

A. The clientless VPN enhancements include:

- Templates and tools for automatic sign-on configuration
- Rewriter enhancements
- Microsoft SharePoint 2010
- Server certificate validation
- Citrix Mobile Receiver
- Java file browser
- Java rewrite proxy
- HTML5

Q. What do the clientless VPN enhancements bring to users?

A. Benefits of the clientless VPN enhancements include the following:

- Easier and faster configuration of the clientless portal for single sign-on with various applications
- Standardized templates for multiple applications
- Customer access to shared files through the clientless portal using the new Java- based fill browser
- Customer access to TCP/IP applications using Java plug-ins, even when the end user is behind a proxy server

Q. Does the Cisco ASA Software clientless VPN allow interoperability with Citrix solutions?

A. End users can access the Citrix Xen infrastructure through the clientless portal. the ASA Software has eliminated the need for the Citrix Access Gateway.

SSL Decryption

Q. Does the ASA 5525-X offer a separate hardware cryptographic module like other offerings in the market?

A. Hardware cryptographic acceleration is already built into the ASA 5525-X, so there is no need for an optional hardware cryptographic module.

Q. Does ASA 9.0 support Suite B cryptography standards?

A. Yes. ASA 9.0 provides comprehensive next-generation encryption capabilities, which includes the Suite B cryptography standards for remote access and site-to-site connections using an IPsec tunnel.

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

A. No. Next-generation encryption is fully supported on the ASA 5500-X Series, the ASA 5585-X, and the ASA 5580, as well as on the Catalyst 6500 Series ASA Services Module. It is partially supported on the ASA 5505,

5510, 5520, 5540, and 5550 models. Cisco AnyConnect 3.1 or later and an AnyConnect Premium license are also required to use next-generation encryption for remote access connections.

Q. What is the next-generation encryption support on Cisco ASA Software?

A. ASA Software supports the Suite B set of cryptography algorithms, including elliptical curve and the SHA-2 family of hashes (256, 384, and 512 bits). It also includes IPsecv3 and enhanced IPsecv3 features, which are defined as Encapsulated Security Payload (ESPv3). This capability helps deliver confidentiality and integrity with a smaller key size with NSA-approved Suite B encryption specifications.

Support for Suite B cryptography in the ASA Next-Generation Firewalls can be summarized as follows:

- Advanced Encryption Standard using Galois/Counter Mode (**AES-GCM**) and Galois Message Authentication Code (**GMAC**) support (128-, 192-, and 256-bit keys): Internet Key Exchange (IKEv2) payload encryption and authentication; ESP packet encryption and authentication
- **SHA-2** (Phase 3a) support (256-, 384-, and 512-bit hashes): ESP packet authentication
- Elliptic Curve Diffie-Hellman (**ECDH**) support (groups 19, 20, and 21): IKEv2 key exchange; IKEv2 perfect forward secrecy (PFS)
- Elliptic Curve Digital Signature Algorithm (**ECDSA**) support (256-, 384-, and 521-bit elliptic curves):IKEv2 user authentication; public key infrastructure (PKI) certificate enrollment; PKI certificate generation and verification

Miscellaneous

Q. Can ASA lock SSL VPN users with "Device certification authentication" and "user Radius authentication"?

A. Yes, you can apply “cert + OTP (RADIUS).” Please note that access to machine certification is not permitted by default and must explicitly be enabled by a file change in Cisco AnyConnect by a user with system privileges.

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 XenApp6.5 and the latest releases of XenDesktop (up to 5.5) for laptops, desktops, and mobile devices (Citrix Mobile Receiver). Support for VMware VDI deployments is also offered (through smart tunnels). As in past releases, Cisco AnyConnect supports Citrix and VMware VDI deployments.

High Availability

Failover

Q. How many members are allowed within one failover group for ASA?

A. Members can be included in one group up to the group’s maximum platform context count.

Q. As soon as the failover command is executed, there is a 30- to 45-second loss of connectivity through the firewall. Is this expected?

A. This is expected behavior. Upon enabling failover, the unit will wait for 45 seconds before going active in case another active unit already exists.

Q. If I have two ASA Services Modules configured as a failover pair, and then for some reason they go to active/active mode (split brain) for a couple of minutes, what will happen to the sessions if they merge again? For a few seconds, the two blades will see different sessions. Will the primary ASA's session table be replicated to the secondary services module?

A. The primary unit always wins the active role when the split failover pair is reconnected. The secondary standby will clear its configuration and connections and perform the complete bulk sync from the active unit.

Q. Is ASA HA supported over Overlay Transport Virtualization?

A. ASA does not impose any specific limitations on the intersite transport with failover, because the IP addresses between the active and standby members are unique. You just need to make sure that the latency on the state link is within 10 milliseconds (best case) or 200 milliseconds (maximum acceptable case).

Clustering

Q. Does ASA 9.x support clustering?

A. Yes. Cisco ASA Release 9.0 supports up to eight Cisco ASA 5585-X or ASA 5580 firewall modules to be joined in a single cluster to deliver up to 128 Gbps of multiprotocol throughput (300 Gbps maximum) and more than 50 million concurrent connections. Alternatively, slot 1 of each ASA 5585-X can be populated with an integrated Cisco IPS module. With ASA 9.2.1, you can now place cluster members at different geographical locations when using the spanned EtherChannel mode in a transparent firewall mode. Intersite clustering with spanned EtherChannels in the routed firewall mode is not supported. ASA Release 9.2.1 now supports 16-unit clusters as well. What this means is that a maximum of 16 nodes are supported in a single cluster. All these nodes are managed as a single logical firewall. Moreover, the ability to look at the statistics of the individual nodes in a cluster is also available. The cluster upgrade is achieved without any disruption in traffic because the nodes in the cluster can be at different minor versions during the upgrade.

With Cisco ASA Release 9.2.1, we support up to 16 ASA nodes in a cluster and can scale up to 640 Gbps HTTP/TCP throughput or 320 GB EMIX throughputs.

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 (CHASH). 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 are 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 support clustering?

A. Initially, Cisco ASA Software Release 9.0 supports clustering on the ASA 5580 and ASA 5585-X 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 activated.

Q. What does “scaling factor” mean?

A. Scaling factor is a measurement of expected performance and scale in a cluster 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, or 64 Gbps.

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 IPS modules. However, Cisco Security Manager and Cisco IPS Manager Express can be used to simplify the 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 used. 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 do feature licenses behave when ASA appliances are clustered?

A. Table 6 provides an explanation of the behavior of key features.

Table 5. Cluster Behavior of Cisco ASA Feature License Types

License Type	Behavior in Cluster	Example
Enable or disable feature	Only one unit in the cluster is required to have a license.	Security Plus license on the Cisco ASA 5585-X: license is required on only one unit
Platform agnostic	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 security contexts Nodes 2, 3, and 4 = 2 SCs Total capacity = 206 Example 2: 4-node cluster Node 1 = 200 SCs Node 2 = 100 SCs Nodes 3 and 4 = 2 SCs Total capacity = 250 SCs
Time based	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. How is session and configuration information synchronized across the cluster members?

A. Cisco ASA Software uses a cluster control link (CCL) to synchronize all state information across the cluster.

Q. How can I activate clustering on ASA?

A. Customers can activate clustering by applying product identification numbers (PIDs). The PIDs give you a license, which in turn can be activated on the units. The PIDS for the ASA 5585-X models are as follows:

Product ID	Product Description
L-ASA5585-CL-S10=	Cluster license for Cisco ASA 5585-X with SSP-10
L-ASA5585--CL-S20=	Cluster license for Cisco ASA 5585-X with SSP-20
L-ASA5585-CL-S40=	Cluster license for Cisco ASA 5585-X with SSP-40
L-ASA5585-CL-S60=	Cluster license for Cisco ASA 5585-X with SSP-60
L-ASA5580-CL-20=	Cluster license for Cisco ASA 5580-20
L-ASA5580-CL-40=	Cluster license for Cisco ASA 5580-40

Q. How is the cluster managed?

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

Q. Is routing supported in the cluster mode?

A. Yes. Routing in single-context and multicontext mode is supported when appliances are clustered.

Q. Can the cluster be attached to Cisco Nexus 7000 Series Switches running a fabric path?

A. The ASA cluster cannot participate in fabric path, but it can run in conjunction with the path.

Q. Is the cluster control link a hardware port or user port reuse?

A. The CCL is a hardware port or an EtherChannel that overlaps multiple physical ports.

Q. With a single-port channel with a Layer 2 firewall, can I have only one logical segment (pair of VLANs) or can I have multiple pairs?

A. You can have bridge groups to combine multiple VLANs.

Q. What are the different modes in which ASA clustering can be achieved?

A. Cisco ASA Clustering is supported in two modes: spanned and Individual interface. In spanned mode, the firewall's interfaces are bundled into port channel(s) statically or with Cluster Link Aggregation Control Protocol (cLACP). In individual interface mode, the traffic is to be load balanced by Layer 3 devices before the firewall (Cisco Application Control Engine, a router, etc.), and each cluster member has its interfaces with routable IP addresses.

Q. Is there a specific license required for ASA clustering? If yes, is it per firewall or only for the master unit?

A. Yes, Cisco ASA requires the Cluster license for each node that will be a part of the cluster.

Q. Is service-level agreement monitoring supported in an ASA cluster? From the configuration guide, I see that static route-object tracking is a centralized function and can be activated on the master device only. I would like to confirm whether it is supported on transparent mode running multiple contexts.

A. SLA monitoring is supported only with floating static routes, so it cannot be used for cluster health monitoring or in transparent mode.

Q. Does Cisco ASA support clustering over Cisco FabricPath or IETF TRILL? Does ASA support clustering over OTV?

A. ASA supports “dark media” CCL extension regardless of the specific transport. Keep in mind that this does not imply data interface support with OTV, only CCL.

Q. Is ASA clustering supported by the Cisco Nexus 2000 Series, or just Cisco Nexus 5000?

A. Table 7 lists the external hardware and software supported for interoperation with ASA clustering.

Table 6. Cisco External Hardware and Software for Interoperation with Cisco ASA Software

External Hardware	External Software	Cisco ASA Software Release
Cisco Nexus 9300	Cisco NX-OS Software 6.1(2)I2(1) and later	9.2(1) or later
Cisco Nexus 7000	Cisco NX-OS Software 5.2(5) and later	9.0(1) or later
Cisco Nexus 5000	Cisco NX-OS Software 7.0(1) and later	9.1(4) or later
Cisco Catalyst 6500 with Sup 32,720 and 720-10GE	Cisco IOS Software Release 12.2(33)SXI7, SXI8, - SXI9 or later	9.0(1) or later
Cisco Catalyst 3750-X	Cisco IOS Software Release 15.0(2) or later	9.1(4) or later

Q. How do we transport the CCL between two data centers? Do we have to use dark fiber (a dedicated link), or can we use a VLAN that can be extended between the two data centers?

A. This is a “dark media” connection through some switched infrastructure. The requirements include unimpeded unicast and broadcast connectivity at Layer 2, no packet loss or reordering, and less than 20 milliseconds of round-trip time.

Q. Is there a migration path or best practice to migrate from ASA in failover mode to ASA in cluster mode?

A. The best approach to a successful migration would be to clear all configurations, set the interface mode, configure clustering, and then restore the various elements from a backup to the master. Failover and clustering are different enough that there is no “easy” migration path.

Ordering

Q. Is the Cisco ASA 5500-X Series currently orderable?

A. Yes. Use the Cisco Ordering Tool to place your order.

Q. Where can I get pricing information?

A. Check the current Cisco Product Price List (requires a Cisco.com username and password), or contact your Cisco account representative.

Q. How do I build and verify a Cisco ASA 5500-X Series configuration?

A. Use the dynamic configuration tool (DCT) and enter the respective part number(s).

Q. What product service and support options are available?

A. Please visit the Cisco Service Finder for available support options.

Q. Is the Botnet Traffic Filter considered an IPS service, or do we need a separate license for it? Can we order both the Botnet Traffic Filter and IPS in a box?

A. These are independent features, so you need to order the BTF license separately from the IPS package. You can order both the botnet filter and IPS in a box.

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 C67-731962-01 10/14