Introduction to the Cisco ASA

The Cisco ASA provides advanced stateful firewall and VPN concentrator functionality in one device as well as integrated services with add-on modules. The ASA includes many advanced features, such as multiple security contexts (similar to virtualized firewalls), clustering (combining multiple firewalls into a single firewall), transparent (Layer 2) firewall or routed (Layer 3) firewall operation, advanced inspection engines, IPsec VPN, SSL VPN, and clientless SSL VPN support, and many more features.

Hardware and Software Compatibility

For a complete list of supported hardware and software, see Cisco ASA Compatibility.

VPN Compatibility

See Supported VPN Platforms, Cisco ASA Series.

New Features

This section lists new features for each release.

Note New, changed, and deprecated syslog messages are listed in the syslog message guide.

New Features in ASA 9.7(1.4)

Released: April 4, 2017

Note Verion 9.7(1) was removed from Cisco.com due to bug CSCvd78303.

Feature	Description
Platform Features	
New default configuration for the ASA 5506-X series using Integrated Routing and Bridging	A new default configuration will be used for the ASA 5506-X series. The Integrated Bridging and Routing feature provides an alternative to using an external Layer 2 switch. For users replacing the ASA 5505, which includes a hardware switch, this feature lets you replace the ASA 5505 with an ASA 5506-X or other ASA model without using additional hardware. The new default configuration includes: • outside interface on GigabitEthernet 1/1, IP address from DHCP • inside bridge group BVI 1 with GigabitEthernet ½ (inside1) through 1/8 (inside7), IP address 192.168.1.1 • inside --> outside traffic flow • inside ---> inside traffic flow for member interfaces • (ASA 5506W-X) wifi interface on GigabitEthernet 1/9, IP address 192.168.10.1 • (ASA 5506W-X) wifi <--> inside, wifi --> outside traffic flow • DHCP for clients on inside and wifi. The access point itself and all its clients use the ASA as the DHCP server. • Management 1/1 interface is Up, but otherwise unconfigured. The ASA FirePOWER module can then use this interface to access the ASA inside network and use the inside interface as the gateway to the Internet. • ASDM access—inside and wifi hosts allowed. • NAT—Interface PAT for all traffic from inside, wifi, and management to outside. If you are upgrading, you can either erase your configuration and apply the default using the **configure factory-default** command, or you can manually configure a BVI and bridge group members to suit your needs. Note that to easily allow intra-bridge group communication, you need to enable the **same-security-traffic permit inter-interface** command (this command is already present for the ASA 5506W-X default configuration).

Feature	Description
Alarm ports support on the ISA 3000	The ISA 3000 supports two alarm input interfaces and one alarm out interface. External sensors such as door sensors can be connected to the alarm inputs. External devices like buzzers can be connected to the alarm out interface. Alarms triggered are conveyed through two LEDs, syslogs, SNMP traps, and through devices connected to the alarm out interface.You can configure descriptions of external alarms. You can also specify the severity and trigger, for external and internal alarms. All alarms can be configured for relay, monitoring and logging. We introduced the following commands: **alarm contact description, alarm contact severity, alarm contact trigger, alarm facility input-alarm, alarm facility power-supply rps, alarm facility temperature, alarm facility temperature high, alarm facility temperature low, clear configure alarm, clear facility-alarm output, show alarm settings, show environment alarm-contact**.
Microsoft Azure Security Center support on the ASAv10	Microsoft Azure is a public cloud environment that uses a private Microsoft Hyper V Hypervisor. Microsoft Azure Security Center is a Microsoft orchestration and management layer on top of Azure that simplifies the deployment of a highly secure public cloud infrastructure. Integration of the ASAv into Azure Security Center allows the ASAv to be offered as a firewall option to protect Azure environments.

Precision Time Protocol (PTP) for the ISA 3000	The ISA 3000 supports PTP, a time synchronization protocol for nodes distributed across a network. It provides greater accuracy than other time synchronization protocols, such as NTP, due to its hardware timestamp feature. The ISA 3000 supports PTP forward mode, as well as the one-step, end-to-end transparent clock. We added the following commands to the default configuration to ensure that PTP traffic is not sent to the ASA FirePOWER module for inspection. If you have an existing deployment, you need to manually add these commands:
	
	`object-group service bypass_sfr_inspect`
	`  service-object udp destination range 319 320`
	`access-list sfrAccessList extended deny object-group bypass_sfr_inspect any any`
	
	We introduced the following commands: **debug ptp, ptp domain, ptp mode e2etransparent, ptp enable, show ptp clock, show ptp internal-info, show ptp port**

Automatic Backup and Restore for the ISA 3000	You can enable auto-backup and/or auto-restore functionality using pre-set parameters in the backup and restore commands. The use cases for these features include initial configuration from external media; device replacement; roll back to an operable state. We introduced the following commands: **backup-package location, backup-package auto, show backup-package status, show backup-package summary**
Firewall Features	
Support for SCTP multi-streaming reordering and reassembly and fragmentation. Support for SCTP multi-homing, where the SCTP endpoints have more than one IP address.	The system now fully supports SCTP multi-streaming reordering, reassembly, and fragmentation, which improves Diameter and M3UA inspection effectiveness for SCTP traffic. The system also supports SCTP multi-homing, where the endpoints have more than one IP address each. For multi-homing, the system opens pinholes for the secondary addresses so that you do not need to write access rules to allow them. SCTP endpoints must be limited to 3 IP addresses each. We modified the output of the following command: **show sctp detail**.

Feature	Description
M3UA inspection improvements.	M3UA inspection now supports stateful failover, semi-distributed clustering, and multihoming. You can also configure strict application server process (ASP) state validation and validation for various messages. Strict ASP state validation is required for stateful failover and clustering. We added or modified the following commands: **clear service-policy inspect m3ua session** [**assocID** *id*], **match port sctp**, **message-tag-validation**, **show service-policy inspect m3ua drop**, **show service-policy inspect m3ua endpoint**, **show service-policy inspect m3ua session**, **show service-policy inspect m3ua table**, **strict-asp-state**, **timeout session**.
Support for TLSv1.2 in TLS proxy and Cisco Unified Communications Manager 10.5.2.	You can now use TLSv1.2 with TLS proxy for encrypted SIP or SCCP inspection with the Cisco Unified Communications Manager 10.5.2. The TLS proxy supports the additional TLSv1.2 cipher suites added as part of the **client cipher-suite** command. We modified the following commands: **client cipher-suite**
Integrated Routing and Bridging	Integrated Routing and Bridging provides the ability to route between a bridge group and a routed interface. A bridge group is a group of interfaces that the ASA bridges instead of routes. The ASA is not a true bridge in that the ASA continues to act as a firewall: access control between interfaces is controlled, and all of the usual firewall checks are in place. Previously, you could only configure bridge groups in transparent firewall mode, where you cannot route between bridge groups. This feature lets you configure bridge groups in routed firewall mode, and to route between bridge groups and between a bridge group and a routed interface. The bridge group participates in routing by using a Bridge Virtual Interface (BVI) to act as a gateway for the bridge group. Integrated Routing and Bridging provides an alternative to using an external Layer 2 switch if you have extra interfaces on the ASA to assign to the bridge group. In routed mode, the BVI can be a named interface and can participate separately from member interfaces in some features, such as access rules and DHCP server. The following features that are supported in transparent mode are not supported in routed mode: multiple context mode, ASA clustering. The following features are also not supported on BVIs: dynamic routing and multicast routing. We modified the following commands: **access-group, access-list ethertype, arp-inspection, dhcpd, mac-address-table static, mac-address-table aging-time, mac-learn, route, show arp-inspection, show bridge-group, show mac-address-table, show mac-learn**
VM Attributes	You can define network objects to filter traffic according to attributes associated with one or more Virtual Machines (VMs) in an VMware ESXi environment managed by VMware vCenter. You can define access control lists (ACLs) to assign policies to traffic from groups of VMs sharing one or more attributes. We added the following command: **show attribute**.
Stale route timeout for interior gateway protocols	You can now configure the timeout for removing stale routes for interior gateway protocols such as OSPF. We added the following command: **timeout igp stale-route**.

Feature	Description
Network object limitations for object group search.	You can reduce the memory required to search access rules by enabling object group search with the the **object-group-search access-control** command. When enabled, object group search does not expand network or service objects, but instead searches access rules for matches based on those group definitions. Starting with this release, the following limitation is applied: For each connection, both the source and destination IP addresses are matched against network objects. If the number of objects matched by the source address times the number matched by the destination address exceeds 10,000, the connection is dropped. This check is to prevent performance degradation. Configure your rules to prevent an excessive number of matches.
Routing Features	
31-bit Subnet Mask	For routed interfaces, you can configure an IP address on a 31-bit subnet for point-to-point connections. The 31-bit subnet includes only 2 addresses; normally, the first and last address in the subnet is reserved for the network and broadcast, so a 2-address subnet is not usable. However, if you have a point-to-point connection and do not need network or broadcast addresses, a 31-bit subnet is a useful way to preserve addresses in IPv4. For example, the failover link between 2 ASAs only requires 2 addresses; any packet that is transmitted by one end of the link is always received by the other, and broadcasting is unnecessary. You can also have a directly-connected management station running SNMP or Syslog. This feature is not supported for BVIs for bridge groups or with multicast routing. We modified the following commands: **ip address, http, logging host, snmp-server host, ssh**
High Availability and Scalability Features	
Inter-site clustering improvement for the ASA on the Firepower 4100/9300 chassis	You can now configure the site ID for each Firepower 4100/9300 chassis when you deploy the ASA cluster. Previously, you had to configure the site ID within the ASA application; this new feature eases initial deployment. Note that you can no longer set the site ID within the ASA configuration. Also, for best compatibility with inter-site clustering, we recommend that you upgrade to ASA 9.7(1) and FXOS 2.1.1, which includes several improvements to stability and performance. We modified the following command: **site-id**
Director localization: inter-site clustering improvement for data centers	To improve performance and keep traffic within a site for inter-site clustering for data centers, you can enable director localization. New connections are typically load-balanced and owned by cluster members within a given site. However, the ASA assigns the director role to a member at *any* site. Director localization enables additional director roles: a local director at the same site as the owner, and a global director that can be at any site. Keeping the owner and director at the same site improves performance. Also, if the original owner fails, the local director chooses a new connection owner at the same site. The global director is used if a cluster member receives packets for a connection that is owned on a different site. We introduced or modified the following commands: **director-localization, show asp table cluster chash, show conn, show conn detail**

Feature	Description
Interface link state monitoring polling for failover now configurable for faster detection	By default, each ASA in a failover pair checks the link state of its interfaces every 500 msec. You can now configure the polling interval, between 300 msec and 799 msec; for example, if you set the polltime to 300 msec, the ASA can detect an interface failure and trigger failover faster. We introduced the following command: **failover polltime link-state**
Bidirectional Forwarding Detection (BFD) support for Active/Standby failover health monitoring on the Firepower 9300 and 4100	You can enable Bidirectional Forwarding Detection (BFD) for the failover health check between two units of an Active/Standby pair on the Firepower 9300 and 4100. Using BFD for the health check is more reliable than the default health check method and uses less CPU. We introduced the following command: **failover health-check bfd**
VPN Features	
Dynamic RRI for IKEv2 static crypto maps	Dynamic Reverse Route Injection occurs upon the successful establishment of IPsec Security Associations (SA's) when **dynamic** is specified for a **crypto map**. Routes are added based on the negotiated selector information. The routes will be deleted after the IPsec SA's are deleted. Dynamic RRI is supported on IKEv2 based static crypto maps only. We modified the following command: **crypto map set reverse-route**.
Virtual Tunnel Interface (VTI) support for ASA VPN module	The ASA VPN module is enhanced with a new logical interface called Virtual Tunnel Interface (VTI), used to represent a VPN tunnel to a peer. This supports route based VPN with IPsec profiles attached to each end of the tunnel. Using VTI does away with the need to configure static crypto map access lists and map them to interfaces. We introduced the following commands: **crypto ipsec profile, interface tunnel, responder-only, set ikev1 transform-set, set pfs, set security-association lifetime, tunnel destination, tunnel mode ipsec, tunnel protection ipsec profile, tunnel source interface**.
SAML 2.0 based SSO for AnyConnect	SAML 2.0-based service provider IdP is supported in a private network. With the ASA as a gateway between the user and services, authentication on IdP is handled with a restricted anonymous webvpn session, and all traffic between IdP and the user is translated. We added the following command: **saml idp** We modified the following commands: **debug webvpn saml, show saml metadata**
CMPv2	To be positioned as a security gateway device in wireless LTE networks, the ASA now supports certain management functions using the Certificate Management Protocol (CMPv2). We modified the following commands: **enrollment url, keypair, auto-update, crypto-ca-trustpoint, show crypto ca server certificates, show crypto key, show tech-support**
Multiple certificate authentication	You can now validate multiple certificates per session with AnyConnect SSL and IKEv2 client protocols. The Aggregate Authentication protocol has been extended to define the protocol exchange for multiple-certificate authentication and utilize this for both session types. We modified the following command: **authentication {[aaa] [certificate | multiple-certificate] | saml}**
Increase split-tunneling routing limit	The limit for split-tunneling routes for AC-SSL and AC-IKEv2 was increased from 200 to 1200. The IKEv1 limit was left at 200.

Feature	Description
Smart Tunnel Support on Chrome	A new method for smart-tunnel support in the Chrome browser on Mac and Windows devices was created. A Chrome Smart Tunnel Extension has replaced Netscape Plugin Application Program Interfaces (NPAPIs) that are no longer supported on Chrome. If you click on the smart tunnel enabled bookmark in Chrome without the extension already being installed, you are redirected to the Chrome Web Store to obtain the extension. New Chrome installations will direct the user to the Chrome Web Store to download the extension. The extension downloads the binaries from ASA that are required to run smart tunnel. Your usual bookmark and application configuration while using smart tunnel is unchanged other than the process of installing the new extension.
Clientless SSL VPN: Session information for all web interfaces	All web interfaces will now display details of the current session, including the user name used to login, and user privileges which are currently assigned. This will help the user be aware of the current user session and will improve user security.
Clientless SSL VPN: Validation of all cookies for web applications' sessions	All web applications will now grant access only after validating all security-related cookies. In each request, each cookie with an authentication token or a session ID will be verified before granting access to the user session. Multiple session cookies in the same request will result in the connection being dropped. Cookies with failed validations will be treated as invalid and the event will be added to the audit log.
AnyConnect: Maximum Connect Time Alert Interval is now supported in the Group Policy for AnyConnect VPN Client connections.	The alert interval is the interval of time before max connection time is reached that a message will be displayed to the user warning them of termination. Valid time interval is 1-30 minutes. Default is 30 minutes. Previously supported for clientless and site-to-site VPN connections. The following command can now be used for AnyConnect connections: **vpn-session-timeout alert-interval**
AAA Features	
IPv6 address support for LDAP and TACACS+ Servers for AAA	You can now use either IPv4 or IPv6 addresses for LDAP and TACACS+ servers used for AAA. We modified the following command: **aaa-server host, test aaa-server**
Administrative Features	
PBKDF2 hashing for all local **username** and **enable** passwords	Local **username** and **enable** passwords of all lengths are stored in the configuration using a PBKDF2 (Password-Based Key Derivation Function 2) hash. Previously, passwords 32 characters and shorter used the MD5-based hashing method. Already existing passwords continue to use the MD5-based hash unless you enter a new password. See the "Software and Configurations" chapter in the General Operations Configuration Guide for downgrading guidelines. We modified the following commands: **enable password, username**
Licensing Features	
Licensing changes for failover pairs on the Firepower 4100/9300 chassis	Only the active unit requests the license entitlements. Previously, both units requested license entitlements. Supported with FXOS 2.1.1.
Monitoring and Troubleshooting Features	

Feature	Description
IPv6 address support for traceroute	The **traceroute** command was modified to accept an IPv6 address. We modified the following command: **traceroute**
Support for the packet tracer for bridge group member interfaces	You can now use the packet tracer for bridge group member interfaces. We added two new options to the **packet-tracer** command; **vlan-id** and **dmac**
IPv6 address support for syslog servers	You can now configure syslog servers with IPv6 addresses to record and send syslogs over TCP and UDP. We modified the following commands: **logging host, show running config, show logging**
SNMP OIDs and MIBs	The ASA now supports SNMP MIB objects corresponding to the end-to-end transparent clock mode as part of the Precision Time Protocol (PTP) for the ISA 3000. The following SNMP MIB objects are supported: • ciscoPtpMIBSystemInfo • cPtpClockDefaultDSTable • cPtpClockTransDefaultDSTable • cPtpClockPortTransDSTable
Manually stop and start packet captures	You can now manually stop and start the capture. Added/Modified commands: **capture stop**

Firewall Functional Overview

Firewalls protect inside networks from unauthorized access by users on an outside network. A firewall can also protect inside networks from each other, for example, by keeping a human resources network separate from a user network. If you have network resources that need to be available to an outside user, such as a web or FTP server, you can place these resources on a separate network behind the firewall, called a *demilitarized zone* (DMZ). The firewall allows limited access to the DMZ, but because the DMZ only includes the public servers, an attack there only affects the servers and does not affect the other inside networks. You can also control when inside users access outside networks (for example, access to the Internet), by allowing only certain addresses out, by requiring authentication or authorization, or by coordinating with an external URL filtering server.

When discussing networks connected to a firewall, the *outside* network is in front of the firewall, the *inside* network is protected and behind the firewall, and a *DMZ*, while behind the firewall, allows limited access to outside users. Because the ASA lets you configure many interfaces with varied security policies, including many inside interfaces, many DMZs, and even many outside interfaces if desired, these terms are used in a general sense only.

Security Policy Overview

A security policy determines which traffic is allowed to pass through the firewall to access another network. By default, the ASA allows traffic to flow freely from an inside network (higher security level) to an outside network (lower security level). You can apply actions to traffic to customize the security policy.

Permitting or Denying Traffic with Access Rules

You can apply access rules to limit traffic from inside to outside, or allow traffic from outside to inside. For bridge group interfaces, you can also apply an EtherType access rule to allow non-IP traffic.

Applying NAT

Some of the benefits of NAT include the following:

- You can use private addresses on your inside networks. Private addresses are not routable on the Internet.
- NAT hides the local addresses from other networks, so attackers cannot learn the real address of a host.
- NAT can resolve IP routing problems by supporting overlapping IP addresses.

Protecting from IP Fragments

The ASA provides IP fragment protection. This feature performs full reassembly of all ICMP error messages and virtual reassembly of the remaining IP fragments that are routed through the ASA. Fragments that fail the security check are dropped and logged. Virtual reassembly cannot be disabled.

Applying HTTP, HTTPS, or FTP Filtering

Although you can use access lists to prevent outbound access to specific websites or FTP servers, configuring and managing web usage this way is not practical because of the size and dynamic nature of the Internet.

You can configure Cloud Web Security on the ASA, or install an ASA module that provides URL and other filtering services, such as ASA CX or ASA FirePOWER. You can also use the ASA in conjunction with an external product such as the Cisco Web Security Appliance (WSA).

Applying Application Inspection

Inspection engines are required for services that embed IP addressing information in the user data packet or that open secondary channels on dynamically assigned ports. These protocols require the ASA to do a deep packet inspection.

Sending Traffic to Supported Hardware or Software Modules

Some ASA models allow you to configure software modules, or to insert hardware modules into the chassis, to provide advanced services. These modules provide additional traffic inspection and can block traffic based on your configured policies. You can send traffic to these modules to take advantage of these advanced services.

Applying QoS Policies

Some network traffic, such as voice and streaming video, cannot tolerate long latency times. QoS is a network feature that lets you give priority to these types of traffic. QoS refers to the capability of a network to provide better service to selected network traffic.

Applying Connection Limits and TCP Normalization

You can limit TCP and UDP connections and embryonic connections. Limiting the number of connections and embryonic connections protects you from a DoS attack. The ASA uses the embryonic limit to trigger TCP Intercept, which protects inside systems from a DoS attack perpetrated by flooding an interface with TCP SYN packets. An embryonic connection is a connection request that has not finished the necessary handshake between source and destination.

TCP normalization is a feature consisting of advanced TCP connection settings designed to drop packets that do not appear normal.

Enabling Threat Detection

You can configure scanning threat detection and basic threat detection, and also how to use statistics to analyze threats.

Basic threat detection detects activity that might be related to an attack, such as a DoS attack, and automatically sends a system log message.

A typical scanning attack consists of a host that tests the accessibility of every IP address in a subnet (by scanning through many hosts in the subnet or sweeping through many ports in a host or subnet). The scanning threat detection feature determines when a host is performing a scan. Unlike IPS scan detection that is based on traffic signatures, the ASA scanning threat detection feature maintains an extensive database that contains host statistics that can be analyzed for scanning activity.

The host database tracks suspicious activity such as connections with no return activity, access of closed service ports, vulnerable TCP behaviors such as non-random IPID, and many more behaviors.

You can configure the ASA to send system log messages about an attacker or you can automatically shun the host.

Firewall Mode Overview

The ASA runs in two different firewall modes:

- Routed
- Transparent

In routed mode, the ASA is considered to be a router hop in the network.

In transparent mode, the ASA acts like a “bump in the wire,” or a “stealth firewall,” and is not considered a router hop. The ASA connects to the same network on its inside and outside interfaces in a "bridge group".

You might use a transparent firewall to simplify your network configuration. Transparent mode is also useful if you want the firewall to be invisible to attackers. You can also use a transparent firewall for traffic that would otherwise be blocked in routed mode. For example, a transparent firewall can allow multicast streams using an EtherType access list.

Routed mode supports Integrated Routing and Bridging, so you can also configure bridge groups in routed mode, and route between bridge groups and regular interfaces. In routed mode, you can replicate transparent mode functionality; if you do not need multiple context mode or clustering, you might consider using routed mode instead.

Stateful Inspection Overview

All traffic that goes through the ASA is inspected using the Adaptive Security Algorithm and either allowed through or dropped. A simple packet filter can check for the correct source address, destination address, and ports, but it does not check that the packet sequence or flags are correct. A filter also checks *every* packet against the filter, which can be a slow process.

Note The TCP state bypass feature allows you to customize the packet flow.

A stateful firewall like the ASA, however, takes into consideration the state of a packet:

- Is this a new connection?

  If it is a new connection, the ASA has to check the packet against access lists and perform other tasks to determine if the packet is allowed or denied. To perform this check, the first packet of the session goes through the "session management path," and depending on the type of traffic, it might also pass through the "control plane path."

  The session management path is responsible for the following tasks:

  - Performing the access list checks
  - Performing route lookups
  - Allocating NAT translations (xlates)
  - Establishing sessions in the "fast path"

  The ASA creates forward and reverse flows in the fast path for TCP traffic; the ASA also creates connection state information for connectionless protocols like UDP, ICMP (when you enable ICMP inspection), so that they can also use the fast path.

  

  Note For other IP protocols, like SCTP, the ASA does not create reverse path flows. As a result, ICMP error packets that refer to these connections are dropped.

  Some packets that require Layer 7 inspection (the packet payload must be inspected or altered) are passed on to the control plane path. Layer 7 inspection engines are required for protocols that have two or more channels: a data channel, which uses well-known port numbers, and a control channel, which uses different port numbers for each session. These protocols include FTP, H.323, and SNMP.

- Is this an established connection?

  If the connection is already established, the ASA does not need to re-check packets; most matching packets can go through the "fast" path in both directions. The fast path is responsible for the following tasks:

- IP checksum verification
- Session lookup
- TCP sequence number check
- NAT translations based on existing sessions
- Layer 3 and Layer 4 header adjustments

Data packets for protocols that require Layer 7 inspection can also go through the fast path.

Some established session packets must continue to go through the session management path or the control plane path. Packets that go through the session management path include HTTP packets that require inspection or content filtering. Packets that go through the control plane path include the control packets for protocols that require Layer 7 inspection.

VPN Functional Overview

A VPN is a secure connection across a TCP/IP network (such as the Internet) that appears as a private connection. This secure connection is called a tunnel. The ASA uses tunneling protocols to negotiate security parameters, create and manage tunnels, encapsulate packets, transmit or receive them through the tunnel, and unencapsulate them. The ASA functions as a bidirectional tunnel endpoint: it can receive plain packets, encapsulate them, and send them to the other end of the tunnel where they are unencapsulated and sent to their final destination. It can also receive encapsulated packets, unencapsulate them, and send them to their final destination. The ASA invokes various standard protocols to accomplish these functions.

The ASA performs the following functions:

- Establishes tunnels
- Negotiates tunnel parameters
- Authenticates users
- Assigns user addresses
- Encrypts and decrypts data
- Manages security keys
- Manages data transfer across the tunnel
- Manages data transfer inbound and outbound as a tunnel endpoint or router

The ASA invokes various standard protocols to accomplish these functions.

Security Context Overview

You can partition a single ASA into multiple virtual devices, known as security contexts. Each context is an independent device, with its own security policy, interfaces, and administrators. Multiple contexts are similar to having multiple standalone devices. Many features are supported in multiple context mode, including routing tables, firewall features, IPS, and management; however, some features are not supported. See the feature chapters for more information.

In multiple context mode, the ASA includes a configuration for each context that identifies the security policy, interfaces, and almost all the options you can configure on a standalone device. The system administrator adds and manages contexts by configuring them in the system configuration, which, like a single mode configuration, is the startup configuration. The system configuration identifies basic settings for the ASA. The system configuration does not include any network interfaces or network settings for itself; rather, when the system needs to access network resources (such as downloading the contexts from the server), it uses one of the contexts that is designated as the admin context.

The admin context is just like any other context, except that when a user logs into the admin context, then that user has system administrator rights and can access the system and all other contexts.

ASA Clustering Overview

ASA Clustering lets you group multiple ASAs together as a single logical device. A cluster provides all the convenience of a single device (management, integration into a network) while achieving the increased throughput and redundancy of multiple devices.

You perform all configuration (aside from the bootstrap configuration) on the control unit only; the configuration is then replicated to the member units.

Special and Legacy Services

For some services, documentation is located outside of the main configuration guides and online help.

Special Services Guides

Special services allow the ASA to interoperate with other Cisco products; for example, by providing a security proxy for phone services (Unified Communications), or by providing Botnet traffic filtering in conjunction with the dynamic database from the Cisco update server, or by providing WCCP services for the Cisco Web Security Appliance. Some of these special services are covered in separate guides:

- Cisco ASA Botnet Traffic Filter Guide
- Cisco ASA NetFlow Implementation Guide
- Cisco ASA Unified Communications Guide
- Cisco ASA WCCP Traffic Redirection Guide
- SNMP Version 3 Tools Implementation Guide

Legacy Services Guide

Legacy services are still supported on the ASA, however there may be better alternative services that you can use instead. Legacy services are covered in a separate guide:

Cisco ASA Legacy Feature Guide

This guide includes the following chapters:

- Configuring RIP
- AAA Rules for Network Access

- Using Protection Tools, which includes Preventing IP Spoofing (**ip verify reverse-path**), Configuring the Fragment Size (**fragment**), Blocking Unwanted Connections (**shun**), Configuring TCP Options (for ASDM), and Configuring IP Audit for Basic IPS Support (**ip audit**).
- Configuring Filtering Services