Cisco Secure Firewall ASA New Features by Release

First Published: 2005-05-31

Last Modified: 2024-01-10

Cisco Secure Firewall ASA New Features

This document lists new features for each release.

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

New Features in Version 9.20

New Features in ASA 9.20(2)/ASDM 7.20(2)

Released: December 13, 2023

Feature	Description
Platform Features	
100GB network module support for the Secure Firewall 3100	You can now use the 100GB network module for the Secure Firewall 3100. This module is also supported for the Secure Firewall 4200.
Increased connection limits for the Secure Firewall 4200	Connection limits have been increased: • 4215: 15M → **40M** • 4225: 30M → **80M** • 4245: 60M → **80M**
ASAv on OCI: Additional instances	ASA Virtual instances on OCI now supports additional shapes to achieve the highest performance and throughput level.
High Availability and Scalability Features	

Feature	Description
ASAv on Azure: Clustering with Gateway Load Balancing	We now support the ASA virtual clustering deployment on Azure using the Azure Resource Manager (ARM) template and then configure the ASAv clusters to use the Gateway Load Balancer (GWLB) for load balancing the network traffic. New/Modified commands: New/Modified screens:
ASAv on AWS: Resiliency for clustering with Gateway Load Balancing	You can configure the Target Failover option in the Target Groups service of AWS, which helps GWLB to forward existing flows to a healthy target in the event of virtual instance failover. In the ASAv clustering, each instance is associated with a Target Group, where the Target Failover option is enabled. It helps GWLB to identify an unhealthy target and redirect or forward the network traffic to a healthy instance identified or registered as a target node in the target group.
Configurable delay to rejoin cluster after chassis heartbeat failure (Firepower 4100/9300)	By default, if the chassis heartbeat fails and then recovers, the node rejoins the cluster immediately. However, if you configure the **health-check chassis-heartbeat-delay-rejoin** command, it will rejoin according to the settings of the **health-check system auto-rejoin** command. New/Modified commands: **health-check chassis-heartbeat-delay-rejoin** New/Modified screens: **Configuration** > **Device Management** > **High Availability and Scalability** > **ASA Cluster** > **Auto Rejoin**
show failover statistics includes client statistics	The failover client packet statistics are now enhanced to improve debuggability. The **show failover statistics** command is enhanced to display **np-clients** (data-path clients) and **cp-clients** (control-plane clients) information. Modified commands: **show failover statistics cp-clients**, **show failover statistics np-clients** *Also in 9.18(4).*
show failover statistics events includes new events	The **show failover statistics events** command is now enhanced to identify the local failures notified by the App agent: failover link uptime, supervisor heartbeat failures, and disk full issues. Modified commands: **show failover statistics events** *Also in 9.18(4).*

New Features in ASA 9.20(1)/ASDM 7.20(1)

Released: September 7, 2023

Note This release is only supported on the Secure Firewall 4200.

Feature	Description
Platform Features	

Feature	Description
Secure Firewall 4200	We introduced the ASA for the Secure Firewall 4215, 4225, and 4245. The Secure Firewall 4200 supports up to 8 units for Spanned EtherChannel clustering. You can hot swap a network module of the same type while the firewall is powered up without having to reboot; making other module changes requires a reboot. Secure Firewall 4200 25 Gbps and higher interfaces support Forward Error Correction as well as speed detection based on the SFP installed. The SSDs are self-encrypting drives (SEDs), and if you have 2 SSDs, they form a software RAID. There are two Management interfaces.
Firewall Features	
ASDM support for the **sysopt connection tcp-max-unprocessed-seg** command	You can set the maximum number of TCP unprocessed segments, from 6 to 24. The default is 6. If you find that SIP phones are not connecting to the call manager, you can try increasing the maximum number of unprocessed TCP segments. New/Modified screens: **Configuration** > **Firewall** > **Advanced** > **TCP Options**.
ASP rule engine compilation offloaded to the data plane.	By default, ASP rule engine compilation is offloaded to the data plane (instead of the control plane) when any rule-based policy (for example, ACL, NAT, VPN) has more than 100 rule updates. The offload leaves more time for the control plane to perform other tasks. We added or modified the following commands: **asp rule-engine compile-offload**, **show asp rule-engine**.
Data plane quick reload	When data plane needs to be restarted, instead of a reboot of the device, you can now reload the data plane process. When data plane quick reload is enabled, it restarts the data plane and other processes. New/Modified commands:**data-plane quick-reload**, **show data-plane quick-reload status**.
High Availability and Scalability Features	
Reduced false failovers for ASA high availability	We now introduced an additional heartbeat module in the data plane of the ASA high availability. This heartbeat module helps to avoid false failovers or split-brain scenarios that can happen due to traffic congestion in the control plain or CPU overload. *Also in 9.18(4).*
Configurable cluster keepalive interval for flow status	The flow owner sends keepalives (clu_keepalive messages) and updates (clu_update messages) to the director and backup owner to refresh the flow state. You can now set the keepalive interval. The default is 15 seconds, and you can set the interval between 15 and 55 seconds. You may want to set the interval to be longer to reduce the amount of traffic on the cluster control link. New/Modified commands: **clu-keepalive-interval** New/Modified screens: **Configuration** > **Device Management** > **High Availability and Scalability** > **ASA Cluster** > **Cluster Configuration**
Routing Features	

Feature	Description
EIGRPv6	You can now configure EIGRP for IPv6 and manage them separately. You must explicitly enable IPv6 when configuring EIGRP on each interface. New/Modified commands: Following are the new commands introduced: **ipv6 eigrp**, **ipv6 hello-interval eigrp**, **ipv6 hold-time eigrp**, **ipv6 split-horizon eigrp**, **show ipv6 eigrp interface** , **show ipv6 eigrp traffic**, **show ipv6 eigrp neighbors** , **show ipv6 eigrp interface**, **ipv6 summary-address eigrp**, **show ipv6 eigrp topology**, **show ipv6 eigrp events** , **show ipv6 eigrp timers**, **clear ipv6 eigrp** , and **clear ipv6 router eigrp** Following commands are modified to support IPv6: **default-metric**, **distribute-list prefix-list**, **passive-interface**, **eigrp log-neighbor-warnings**, **eigrp log-neighbor-changes**, **eigrp router-id**, and **eigrp stub** New/Modified screens: **Configuration** > **Device Setup** > **Routing** > **EIGRPv6** , **Setup**, **Filter Rules**,**Interface**,**Passive Interface**, **Redistribution**, **Static Neighbor** tabs.
Path monitoring through HTTP client	PBR can now use the performance metrics (RTT, jitter, packet-lost, and MOS) collected by path monitoring through HTTP client on the application domain rather than the metrics on a specific destination IP. HTTP-based application monitoring option is enabled by default for the interface. HTTP based path-monitoring can be configured on the interface using Network Service Group objects. You can configure a PBR policy with match ACL having the monitored applications and interface ordering for path determination. New/Modified screens: **Configuration** > **Device Setup** > **Interface Settings** > **Path Monitoring**
Interface Features	
VXLAN VTEP IPv6 support	You can now specify an IPv6 address for the VXLAN VTEP interface. IPv6 is not supported for the ASA virtual cluster control link or for Geneve encapsulation. New/Modified commands: **default-mcast-group**, **mcast-group**, **peer ip** New/Modified screens: • **Configuration** > **Device Setup** > **Interface Settings** > **VXLAN** • **Configuration** > **Device Setup** > **Interface Settings** > **Interfaces** > **Add** > **VNI Interface**
Loopback interface support for DNS, HTTP, ICMP, and IPsec Flow Offload	You can now add a loopback interface and use it for: • DNS • HTTP • ICMP • IPsec Flow Offload
License Features	
IPv6 for Cloud services such as Smart Licensing and Smart Call Home	ASA now supports IPv6 for Cloud services such as Smart Licensing and Smart Call Home.

Feature	Description
Certificate Features	
IPv6 PKI for OCSP and CRL	ASA now supports both IPv4 and IPv6 OCSP and CRL URLs. When using IPv6 in the URLs, it must be enclosed with square brackets. New/Modified commands:**crypto ca trustpointcrl**, **cdp url**, **ocsp url** New/Modified screens: **Configuration** > **Site-to-Site VPN** > **Certificate Management** > **CA Certificates** > **Add**
Administrative, Monitoring, and Troubleshooting Features	
Rate limiting for SNMP syslogs	If you do not set system-wide rate limiting, you can now configure rate limiting separately for syslogs sent to an SNMP server. New/Modified commands: **logging history rate-limit**
Packet Capture for switches	You can now configure to capture egress and ingress traffic packets for a switch. This option is applicable only for Secure Firewall 4200 model devices. New/Modified commands: **capture** *capture_name* **switch interface** *interface_name* [**direction** { **both** | **egress** | **ingress** }] New/Modified screens: **Wizards** > **Packet Capture Wizard** > **Ingress Traffic Selector**and **Wizards** > **Packet Capture Wizard** > **Egress Traffic Selector**
VPN Features	
Crypto debugging enhancements	Following are the enhancements for crypto debugging: • Crypto archive is now available in two formats: text and binary format. • Additional SSL counters. • Stuck encrypt rules can be removed from the ASP table without rebooting the device. New/Modified commands: • **show counters**
Multiple Key Exchanges for IKEv2	ASA supports multiple key exchanges in IKEv2 to secure the IPsec communication from quantum computer attacks. New/Modified commands: **additional-key-exchange**
Secure Client connection authentication using SAML	In a DNS load balancing cluster, when SAML authentication is configured on ASAs, you can specify a local base URL that uniquely resolves to the device on which the configuration is applied. New/Modified screens: **Configuration > Remote Access VPN > Network (Client) Access > Secure Client Connection Profiles > Add/Edit > Basic > SAML Identity Provider > Manage > Add/Edit**
ASDM Features	

Feature	Description
Windows 11 support	ASDM has been verified to operate on Windows 11.

New Features in Version 9.19

New Features in ASDM 7.19(1.95)

Released: July 5, 2023

There are no new features in this release.

New Features in ASDM 7.19(1.90)

Released: February 16, 2023

There are no new features in this release.

New Features in ASA 9.19(1)/ASDM 7.19(1)

Released: November 29, 2022

Feature	Description
Platform Features	
Secure Firewall 3105	We introduced the ASA for the Secure Firewall 3105.
ASA virtual Auto Scale solution with Azure Gateway Load Balancer	You can now deploy the ASA virtual Auto Scale Solution with Gateway Load Balancer on Microsoft Azure. See the Interfaces features for more information.
Firewall Features	
Network service groups support	You can now define a maximum of 1024 network service groups.
High Availability and Scalability Features	
Removal of biased language	Commands, command output, and syslog messages that contained the terms "Master" and "Slave" have been changed to "Control" and "Data." New/Modified commands: **cluster control-node**, **enable as-data-node**, **prompt**, **show cluster history**, **show cluster info**
ASA virtual Amazon Web Services (AWS) clustering	The ASA virtual supports Individual interface clustering for up to 16 nodes on AWS. You can use clustering with or without the AWS Gateway Load Balancer. No ASDM support.
Routing Features	

Feature	Description
BGP graceful restart support for IPv6	We added BGP graceful restart support for IPv6 address family. New/Modified commands: Existing command, extended to support for IPv6 family:**ha-mode graceful-restart** New/Modified screens: **Configuration** > **Device Setup** > **Routing** > **BGP** > **IPv6 Family** > **Neighbour**
ASDM support for loopback interfaces for BGP traffic	ASDM now supports setting a loopback interface as the source interface for BGP neighborship. The loopback interface helps to overcome path failures. New/Modified screens: **Configuration** > **Device Setup** > **Routing** > **BGP** > **IPv4 Family / IPv6 Family** > **Neighbor** > **Add** > **General**
Interface Features	
ASA virtual support for IPv6	ASAv to support IPv6 network protocol on Private and Public Cloud platforms. Users can now: • Enable and configure an IPv6 management address via day0 configuration. • Assign IPv6 addresses using DHCP and static methods.
Paired proxy VXLAN for the ASA virtual for the Azure Gateway Load Balancer	You can configure a paired proxy mode VXLAN interface for the ASA virtual in Azure for use with the Azure Gateway Load Balancer (GWLB). The ASA virtual defines an external interface and an internal interface on a single NIC by utilizing VXLAN segments in a paired proxy. New/Modified commands: **external-port, external-segment-id, internal-port, internal-segment-id, proxy paired** No ASDM support.
Default Forward Error Correction (FEC) on Secure Firewall 3100 fixed ports changed to cl108-rs from cl74-fc for 25 GB+ SR, CSR, and LR transceivers	When you set the FEC to Auto on the Secure Firewall 3100 fixed ports, the default type is now set to cl108-rs instead of cl74-fc for 25 GB SR, CSR, and LR transceivers. New/Modified commands: **fec** New/Modified screens: **Configuration** > **Device Setup** > **Interface Settings** > **Interfaces** > **Edit Interface** > **Configure Hardware Properties** > **FEC Mode**
ASDM support for loopback interfaces	ASDM now supports loopback interfaces. New/Modified screens: **Configuration** > **Device Setup** > **Interface Settings** > **Interfaces** > **Add Loopback Interface**
License Features	
ASA virtual permanent license reservation support for the ASAv5 on KVM and VMware	A new command is available that you can execute to override the default PLR license entitlement and request the Cisco Smart Software Manager (SSM) to issue an ASAv5 PLR license when you are deploying ASAv with 2GB RAM on KVM and VMware. You can modify the same command by adding the <*no*> form to revert the license entitlement from ASAv5 to the default PLR license in correspondence to the RAM configuration.
Administrative, Monitoring, and Troubleshooting Features	

Feature	Description
CiscoSSH stack now default	The Cisco SSH stack is now used by default. New/Modified commands: **ssh stack ciscossh** New/Modified screens: • Single context mode: **Configuration** > **Device Management** > **Management Access** > **ASDM/HTTPS/Telnet/SSH** • Multiple context mode: **Configuration** > **Device Management** > **SSH Stack**
VPN Features	
VTI loopback interface support	You can now set a loopback interface as the source interface for a VTI. Support has also been added to inherit the IP address from a loopback interface instead of a statically configured IP address. The loopback interface helps to overcome path failures. If an interface goes down, you can access all interfaces through the IP address assigned to the loopback interface. New/Modified commands: **tunnel source interface**, **ip unnumbered**, **ipv6 unnumbered** New/Modified screens: **Configuration** > **Device Setup** > **Interface Settings** > **Interfaces** > **Add VTI Interface** > **Advanced**
Dynamic Virtual Tunnel Interface (dynamic VTI) support	The ASA is enhanced with dynamic VTI. A single dynamic VTI can replace several static VTI configurations on the hub. You can add new spokes to a hub without changing the hub configuration. Dynamic VTI supports dynamic (DHCP) spokes. New/Modified commands: **interface virtual-Template, ip unnumbered, ipv6 unnumbered, tunnel protection ipsec policy.** New/Modified screens: **Configuration > Device Setup > Interface Settings > Interfaces > Add > DVTI Interface**
VTI support for EIGRP and OSPF	EIGRP and OSPFv2/v3 routing is now supported on the Virtual Tunnel Interface. You can now use these routing protocol to share routing information and to route traffic flow through VTI-based VPN tunnel between peers
TLS 1.3 in Remote Access VPN	You can now use TLS 1.3 to encrypt remote access VPN connections. TLS 1.3 adds support for the following ciphers: • TLS_AES_128_GCM_SHA256 • TLS_CHACHA20_POLY1305_SHA256 • TLS_AES_256_GCM_SHA384 This feature requires Cisco Secure Client, Version 5.0.01242 and above. New/Modified commands: **sslserver-version, sslclient-version**. New/Modified screens: **Configuration > Device Management > Advanced > SSL Settings**

Feature	Description
Dual Stack support for IKEv2 third-party clients	Secure Firewall ASA now supports dual stack IP request from IKEv2 third-party remote access VPN clients. If the third-party remote access VPN client requests for both IPv4 and IPv6 addresses, ASA can now assign both IP version addresses using multiple traffic selectors. This feature enables third-party remote access VPN clients to send IPv4 and IPv6 data traffic using the single IPsec tunnel. New/Modified commands: **show crypto ikev2 sa, show crypto ipsec sa, show vpn-sessiondb ra-ikev2-ipsec**.
Traffic selector for static VTI interface	You can now assign a traffic selector for a static VTI interface. New/Modified commands: **tunnel protection ipsec policy**.

New Features in Version 9.18

New Features in ASDM 7.18(1.161)

Released: July 3, 2023

There are no new features in this release.

New Features in ASA 9.18(4)/ASDM 7.20(1)

Released: October 3, 2023

Feature	Description
High Availability and Scalability Features	
Reduced false failovers for ASA high availability	We now introduced an additional heartbeat module in the data plane of the ASA high availability. This heartbeat module helps to avoid false failovers or split-brain scenarios that can happen due to traffic congestion in the control plain or CPU overload. *Also in 9.20(1).*
show failover statistics includes client statistics	The failover client packet statistics are now enhanced to improve debuggability. The **show failover statistics** command is enhanced to display **np-clients** (data-path clients) and **cp-clients** (control-plane clients) information. Modified commands: **show failover statistics cp-clients**, **show failover statistics dp-clients** *Also in 9.20(2).*
show failover statistics events includes new events	The **show failover statistics events** command is now enhanced to identify the local failures notified by the App agent: failover link uptime, supervisor heartbeat failures, and disk full issues. Modified commands: **show failover statistics events** *Also in 9.20(2).*

Feature	Description
Interface Features	
FXOS local-mgtm **show** command improvements	See the following additions for interface show commands in FXOS local-mgmt: • Added the **show portmanager switch tail-drop-allocated buffers all** command • Include Ethernet port ID in **show portmanager switch status** command • For the Secure Firewall 3100, added the **show portmanager switch default-rule-drop-counter** command New/Modified FXOS commands: **show portmanager switch tail-drop-allocated buffers all**, **show portmanager switch status**, **show portmanager switch default-rule-drop-counter**
Administrative, Monitoring, and Troubleshooting Features	
show tech support improvements	Added output to **show tech support** for: • **show storage detail**, **show slot expand detail** for the Secure Firewall 3100 in **show tech support brief** • Recent messages from dpdk.log in the flash for the ASA Virtual • Control link state for the Firepower 1010 • **show failover** statistics • FXOS local-mgmt **show portmanager switch tail-drop-allocated buffers all** • **show controller** • DPDK mbuf pool statistics New/Modified commands: **show tech support**

New Features in ASA 9.18(3)/ASDM 7.19(1.90)

Released: February 16, 2023

Feature	Description
Platform Features	
Firepower 1010E	We introduced the Firepower 1010E. This model is the same as the Firepower 1010 except it doesn't have Power Over Ethernet ports. ASDM support in 7.19(1.90) or 7.18(2.1). ASDM 7.19(1) does not support this model. *Also in 9.18(2.218). This model is not supported in 9.19(1).*
Interface Features	

Feature	Description
Default Forward Error Correction (FEC) on Secure Firewall 3100 fixed ports changed to cl108-rs from cl74-fc for 25 GB+ SR, CSR, and LR transceivers	When you set the FEC to Auto on the Secure Firewall 3100 fixed ports, the default type is now set to cl108-rs instead of cl74-fc for 25 GB SR, CSR, and LR transceivers. New/Modified commands: **fec** New/Modified screens: **Configuration** > **Device Setup** > **Interface Settings** > **Interfaces** > **Edit Interface** > **Configure Hardware Properties** > **FEC Mode** *Also in 9.19(1) and 9.18(2.7).*
VPN Features	
AnyConnect connection authentication using SAML	In a DNS load balancing cluster, when SAML authentication is configured on ASAs, you can specify a local base URL that uniquely resolves to the device on which the configuration is applied. New/Modified commands: **local-base-url***url*

New Features in ASA 9.18(2)/ASDM 7.18(1.152)

Released: August 10, 2022

Feature	Description
Interface Features	
Loopback interface support for BGP and management traffic	You can now add a loopback interface and use it for the following features: • AAA • BGP • SNMP • SSH • Syslog • Telnet New/Modified commands: **interface loopback**, **logging host**, **neighbor update-source**, **snmp-server host**, **ssh**, **telnet** No ASDM support.
ping command changes	To support pinging a loopback interface, the **ping** command now has changed behavior. If you specify the interface in the command, the source IP address matches the specified interface IP address, but the actual egress interface is determined by a route lookup using the data routing table. New/Modified commands: **ping**

New Features in ASDM 7.18(1.152)

Released: August 2, 2022

There are no new features in this release.

New Features in ASA 9.18(1)/ASDM 7.18(1)

Released: June 6, 2022

Feature	Description
Platform Features	
ASAv-AWS Security center integration for AWS GuardDuty	You can now integrate Amazon GuardDuty service with ASAv. The integration solution helps you to capture and process the threat analysis data or results (malicious IP addresses) reported by Amazon GuardDuty. You can configure and feed these malicious IP addresses in the ASAv to protect the underlying networks and applications.
Firewall Features	
Forward referencing of ACLs and objects is always enabled. In addition, object group search for access control is now enabled by default.	You can refer to ACLs or network objects that do not yet exist when configuring access groups or access rules. In addition, object group search is now enabled by default for access control for *new* deployments. Upgrading devices will continue to have this command disabled. If you want to enable it (recommended), you must do so manually. **Caution** If you downgrade, the **access-group** command will be rejected because it has not yet loaded the **access-list** commands. This outcome occurs even if you had previously enabled the **forward-reference enable** command, because that command is now removed. Before you downgrade, be sure to copy all **access-group** commands manually, and then after downgrading, re-enter them. We removed the **forward-reference enable** command and changed the default for new deployments for **object-group-search access-control** to enabled.
Routing Features	
Path monitoring metrics in PBR.	PBR uses the metrics to determine the best path (egress interface) for forwarding the traffic. Path monitoring periodically notifies PBR with the monitored interface whose metric got changed. PBR retrieves the latest metric values for the monitored interfaces from the path monitoring database and updates the data path. New/Modified commands: **clear path-monitoring**, **policy-route**, **show path-monitoring** New/Modified screens: **Configuration** > **Device Setup** > **Interface Settings** > **Interfaces**
Interface Features	

Feature	Description
Pause Frames for Flow Control for the Secure Firewall 3100	If you have a traffic burst, dropped packets can occur if the burst exceeds the buffering capacity of the FIFO buffer on the NIC and the receive ring buffers. Enabling pause frames for flow control can alleviate this issue. New/Modified commands: **flowcontrol send on** New/Modified screens: **Configuration** > **Device Settings** > **Interfaces** > **General**
Breakout ports for the Secure Firewall 3130 and 3140	You can now configure four 10GB breakout ports for each 40GB interface on the Secure Firewall 3130 and 3140. New/Modified commands: **breakout** New/Modified screens: **Configuration** > **Device Management** > **Advanced** > **EPM**
License Features	
Secure Firewall 3100 support for the Carrier license	The Carrier license enables Diameter, GTP/GPRS, SCTP inspection. New/Modified commands: **feature carrier** New/Modified screens: **Configuration** > **Device Management** > **Licensing** > **Smart Licensing**.
Certificate Features	
Mutual LDAPS authentication.	You can configure a client certificate for the ASA to present to the LDAP server when it requests a certificate to authenticate. This feature applies when using LDAP over SSL. If an LDAP server is configured to require a peer certificate, the secure LDAP session will not complete and authentication/authorization requests will fail. New/Modified commands: **ssl-client-certificate**. New/Modified screens: **Configuration** > **Device Management** > **Users/AAA** > > **AAA Server Groups**, Add/Edit LDAP server.
Authentication: Validate certificate name or SAN	When a feature specific reference-identity is configured, the peer certificate identity is validated with the matching criteria specified under **crypto ca reference-identity** <*name*> submode commands. If there is no match found in the peer certificate Subject Name/SAN or if the FQDN specified with reference-identity submode command fail to resolve, the connection is terminated The reference-identity CLI is configured as a submode command for aaa-server host configuration and ddns configuration. New/Modified commands: **ldap-over-ssl**, **ddns update method** , and **show update method**. New/Modified screens: • **Configuration** > **Device Management** > **Users/AAA** > > **AAA Server Groups** > **LDAP Parameters for authentication/authorization** • **Configuration** > **Device Management** > **DNS** > **Dynamic DNS** > **Update Methods**
Administrative, Monitoring, and Troubleshooting Features	

Feature	Description
Multiple DNS server groups	You can now use multiple DNS server groups: one group is the default, while other groups can be associated with specific domains. A DNS request that matches a domain associated with a DNS server group will use that group. For example, if you want traffic destined to inside eng.cisco.com servers to use an inside DNS server, you can map eng.cisco.com to an inside DNS group. All DNS requests that do not match a domain mapping will use the default DNS server group, which has no associated domains. For example, the DefaultDNS group can include a public DNS server available on the outside interface. New/Modified commands: **dns-group-map**, **dns-to-domain** New/Modified screens: **Configuration** > **Device Management** > **DNS** > **DNS Client**
Dynamic Logging Rate-limit	A new option to limit logging rate when block usage exceeds a specified threshold value was added. It dynamically limits the logging rate as the rate limiting is disabled when the block usage returns to normal value. New/Modified commands: **logging rate-limit** New/Modified screens: **Configuration** > **Device Management** > **Logging** > **Rate Limit**
Packet Capture for Secure Firewall 3100 devices	The provision to capture switch packets was added. This option can be enabled only for Secure Firewall 3100 devices. New/Modified commands: **capture real-time** New/Modified screens: **Wizards** > **Packet Capture Wizard** > **Buffers & Captures**
VPN Features	
IPsec flow offload.	On the Secure Firewall 3100, IPsec flows are offloaded by default. After the initial setup of an IPsec site-to-site VPN or remote access VPN security association (SA), IPsec connections are offloaded to the field-programmable gate array (FPGA) in the device, which should improve device performance. New/Modified commands: **clear flow-offload-ipsec**, **flow-offload-ipsec**, **show flow-offload-ipsec** New/Modified screens: **Configuration** > **Firewall** > **Advanced** > **IPsec Offload**
Certificate and SAML for Authentication	You can configure remote access VPN connection profiles for certificate and SAML authentication. Users can configure VPN settings to authenticate a machine certificate or user certificate before a SAML authentication/authorization is initiated. This can be done using DAP certificate attributes along with user specific SAML DAP attributes. New/Modified commands: **authentication saml certificate**, **authentication certificate saml** , **authentication multiple-certificate saml** New/Modified screens: **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **IPsec(IKEv1) Connection Profiles** > **Add/Edit > Basic**

New Features in Version 9.17

New Features in ASDM 7.17(1.155)

Released: June 28, 2022

There are no new features in this release.

New Features in ASDM 7.17(1.152)

Released: February 8, 2022

There are no new features in this release.

New Features in ASA 9.17(1)/ASDM 7.17(1)

Released: December 1, 2021

Feature	Description
Platform Features	
Secure Firewall 3100	We introduced the ASA for the Secure Firewall 3110, 3120, 3130, and 3140. The Secure Firewall 3100 supports up to 8 units for Spanned EtherChannel clustering. You can hot swap a network module of the same type while the firewall is powered up without having to reboot; making other module changes requires a reboot. Secure Firewall 3100 25 Gbps interfaces support Forward Error Correction as well as speed detection based on the SFP installed. The SSDs are self-encrypting drives (SEDs), and if you have 2 SSDs, they form a software RAID. New/Modified commands: **fec, netmod, speed sfp-detect, raid, show raid, show ssd** New/Modified screens: • **Configuration** > **Device Management** > **Advanced** > **EPM** • **Configuration** > **Device Settings** > **Interfaces** > **Edit Interface** > **Configure Hardware Properties**
ASA virtual support for Autoscale	The ASA virtual now supports Autoscale for the following Public Cloud offerings: • Google Cloud Platform (GCP) • Oracle Cloud Infrastructure (OCI) Autoscaling increases or decreases the number of ASA virtual application instances based on capacity requirements.

Feature	Description
ASA virtual for AWS expanded instance support	The ASA virtual on the AWS Public Cloud now supports AWS Nitro System instances from different Nitro instance families. ASA virtual for AWS adds support for these instances: • c5a.large, c5a.xlarge, c5a.2xlarge, c5a.4xlarge • c5d.large, c5d.xlarge, c5d.2xlarge, c5d.4xlarge • c5ad.large, c5ad.xlarge, c5ad.2xlarge, c5ad.4xlarge • m5n.large, m5n.xlarge, m5n.2xlarge, m5n.4xlarge • m5zn.large, m5zn.xlarge, m5zn.2xlarge For a detailed list of supported instances, see the Cisco Adaptive Security Virtual Appliance (ASAv) Data Sheet.
ASA virtual for Azure expanded instance support	ASA virtual on the Azure Public Cloud now supports these instances: • Standard_D8s_v3 • Standard_D16s_v3 • Standard_F8s_v2 • Standard_F16s_v2 For a detailed list of supported instances, see the Cisco Adaptive Security Virtual Appliance (ASAv) Data Sheet.
Intel QuickAssist Technology (QAT) on ASA virtual	The ASA virtual supports hardware crypto acceleration for ASA virtual deployments that use the Intel QuickAssist (QAT) 8970 PCI adapter. Hardware crypto acceleration for the ASA virtual using QAT is supported on VMware ESXi and KVM only.
Single Root I/O Virtualization (SR-IOV) support for ASA virtual on OCI.	You can now implement Single Root Input/Output Virtualization (SR-IOV) for ASA virtual on OCI. SR-IOV can provide performance improvements for ASA virtual. Mellanox 5 as vNICs are not supported in SR-IOV mode.
Firewall Features	
Twice NAT support for fully-qualified domain name (FQDN) objects as the translated (mapped) destination	You can use an FQDN network object, such as one specifying www.example.com, as the translated (mapped) destination address in twice NAT rules. The system configures the rule based on the IP address returned from the DNS server.

Feature	Description
Network-service objects and their use in policy-based routing and access control	You can configure network-service objects and use them in extended access control lists for use in policy-based routing route maps and access control groups. Network-service objects include IP subnet or DNS domain name specifications, and optionally protocol and port specifications, that essentially combine network and service objects. This feature also includes the ability to define trusted DNS servers, to ensure that any DNS domain name resolutions acquire IP addresses from trusted sources. We added or modified the following commands: **access-list extended**, **app-id**, **clear configure object network-service**, **clear configure object-group network-service**, **clear dns ip-cache**, **clear object**, **clear object-group**, **debug network-service**, **description**, **dns trusted-source**, **domain**, **network-service-member**, **network-service reload**, **object-group network-service**, **object network-service**, **policy-route cost**, **set adaptive-interface cost**, **show asp table classify**, **show asp table network-service**, **show dns trusted-source**, **show dns ip-cache**, **show object**, **show object-group**, **show running-config**, **subnet**. We added or modified the following screens. • **Configuration** > **Device Setup** > **Routing** > **Route Maps**, Add/Edit dialog boxes. • **Configuration** > **Device Setup** > **Interface Settings** > **Interfaces**, Add/Edit dialog boxes. • **Configuration** > **Firewall** > **Objects** > **Network Services Objects/Groups**. • **Configuration** > **Device Management** > **DNS** > **DNS Client**.
High Availability and Scalability Features	
ASAv30, ASAv50, and ASAv100 clustering for VMware and KVM	ASA virtual clustering lets you group up to 16 ASA virtuals 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. ASA virtual clustering supports Individual Interface mode in routed firewall mode; Spanned EtherChannels are not supported. The ASA virtual uses a VXLAN virtual interface (VNI) for the cluster control link. New/Modified commands: **cluster-interface vni**, **nve-only cluster**, **peer-group**, **show cluster info**, **show cluster info instance-type**, **show nve 1** New/Modified screens: • **Configuration** > **Device Setup** > **Interface Settings** > **Interfaces** • **Configuration** > **Device Management** > **High Availability and Scalability** > **ASA Cluster**
Clearing routes in a high availability group or cluster	In previous releases, the **clear route** command cleared the routing table on the unit only. Now, when operating in a high availability group or cluster, the command is available on the active or control unit only, and clears the routing table on all units in the group or cluster. We changed the **clear route** command.
Interface Features	

Feature	Description
Geneve interface support for the ASA virtual	Geneve encapsulation support was added for the ASAv30, ASAv50, and ASAv100 to support single-arm proxy for the AWS Gateway Load Balancer. New/Modified commands: **debug geneve**, **debug nve**, **debug vxlan**, **encapsulation**, **packet-tracer geneve**, **proxy single-arm**, **show asp drop**, **show capture**, **show interface**, **show nve** New/Modified screens: • **Configuration** > **Device Setup** > **Interface Settings** > **Interfaces** > **Add** > **VNI Interface** • **Configuration** > **Device Setup** > **Interface Settings** > **VXLAN**
Secure Firewall 3100 auto-negotiation can be enabled or disabled for 1Gigabit and higher interfaces.	Secure Firewall 3100 auto-negotiation can be enabled or disabled for 1Gigabit and higher interfaces. For other model SFP ports, the **no speed nonegotiate** option sets the speed to 1000 Mbps; the new command means you can set auto-negotiation and speed independently. New/Modified commands: **negotiate-auto** New/Modified screens: **Configuration** > **Device Setup** > **Interface Settings** > **Interfaces** > **Advanced**
Administrative and Troubleshooting Features	
Startup time and tmatch compilation status	The **show version** command now includes information on how long it took to start (boot) up the system. Note that the larger the configuration, the longer it takes to boot up the system. The new **show asp rule-engine** command shows status on tmatch compilation. Tmatch compilation is used for an access list that is used as an access group, the NAT table, and some other items. It is an internal process that can consume CPU resources and impact performance while in progress, if you have very large ACLs and NAT tables. Compilation time depends on the size of the access list, NAT table, and so forth.
Enhancements to **show access-list element-count** output and **show tech-support** content	The output of the **show access-list element-count** has be enhanced to show the following: • When used in the system context in multiple-context mode, the output shows the element count for all access lists across all the contexts. • When used with object-group search enabled, the output includes details about the number of object groups in the element count. In addition, the **show tech-support** output now includes the output **show access-list element-count** and **show asp rule-engine**.

Feature	Description
CiscoSSH stack	The ASA uses a proprietary SSH stack for SSH connections. You can now choose to use the CiscoSSH stack instead, which is based on OpenSSH. The default stack continues to be the ASA stack. Cisco SSH supports: • FIPS compliance • Regular updates, including updates from Cisco and the open source community Note that the CiscoSSH stack does not support: • SSH to a different interface over VPN (management-access) • EdDSA key pair • RSA key pair in FIPS mode If you need these features, you should continue to use the ASA SSH stack. There is a small change to SCP functionality with the CiscoSSH stack: to use the ASA **copy** command to copy a file to or from an SCP server, you have to enable SSH access on the ASA for the SCP server subnet/host using the **ssh** command. New/Modified commands: **ssh stack ciscossh** New/Modified screens: • Single context mode: **Configuration** > **Device Management** > **Management Access** > **ASDM/HTTPS/Telnet/SSH** • Multiple context mode: **Configuration** > **Device Management** > **SSH Stack**
PCAP support in packet tracer	You can replay a PCAP file in packet tracer tool and obtain the trace results. **pcap** and **force** are two new keywords that is used to support the usage of PCAP in packet tracer. New/Modified commands: **packet-tracer input** and **show packet-tracer**

Feature	Description
Stronger local user and enable password requirements	For local users and the enable password, the following password requirements were added: • Password length—Minimum 8 characters. Formerly, the minimum was 3 characters. • Repetitive and sequential characters—Three or more consecutive sequential or repetitive ASCII characters are disallowed. For example, the following passwords will be rejected: • **abc**user1 • user**543** • user**aaaa** • user2**666** New/Modified commands: **enable password**, **username** New/Modified screens: • **Configuration** > **Device Management** > **Users/AAA** > **User Accounts** • **Configuration** > **Device Setup** > **Device Name/Password**
Local user lockout changes	The ASA can lock out local users after a configurable number of failed login attempts. This feature did not apply to users with privilege level 15. Also, a user would be locked out indefinitely until an admin unlocked their account. Now, users will be unlocked after 10 minutes unless an admin uses the **clear aaa local user lockout** command before then. Privilege level 15 users are also now affected by the lockout setting. New/Modified commands: **aaa local authentication attempts max-fail** , **show aaa local user**
SSH and Telnet password change prompt	The first time a local user logs into the ASA using SSH or Telnet, they are prompted to change their password. They will also be prompted for the first login after an admin changes their password. If the ASA reloads, however, users will not be prompted even if it is their first login. Note that any service that uses the local user database, such as VPN, will also have to use the new password if it was changed during an SSH or Telnet login. New/Modified commands: **show aaa local user**
Monitoring Features	
SNMP now supports IPv6 when grouping multiple hosts in the form of a network object	The **host-group** command of **snmp-server** now supports IPv6 host, range, and subnet objects. New/Modified commands: **snmp-server host-group**
VPN Features	
Local tunnel id support for IKEv2	Support has been added for local Tunnel id configuration for IKEv2. New/Modified commands: **set ikev2 local-identity**

Feature	Description
Support for SAML Attributes with DAP constraint	Support has been added for SAML assertion attributes which can be used to make DAP policy selections. It also introduces the ability for a group-policy to be specified by the *cisco_group_policy* attribute.
Multiple SAML trustpoints in IDP configuration	This feature supports adding multiple IDP trustpoints per SAML IDP configuration for applications that support multiple applications for the same Entity ID. New/Modified commands: **saml idp-trustpoint <trustpoint-name>**
Secure Client VPN SAML External Browser	You can now configure VPN SAML External Browser to enable additional authentication choices, such as passwordless authentication, WebAuthN, FIDO2, SSO, U2F, and an improved SAML experience due to the persistence of cookies. When you use SAML as the primary authentication method for a remote access VPN connection profile, you can elect to have the Secure Client use the client's local browser instead of the Secure Client embedded browser to perform the web authentication. This option enables single sign-on (SSO) between your VPN authentication and other corporate logins. Also choose this option if you want to support web authentication methods, such as biometric authentication and Yubikeys, that cannot be performed in the embedded browser. New/Modified commands: **external-browser** New/Modified screens: **Remote Access VPN connection profile wizard** > **SAML Login Experience**.
VPN Load balancing with SAML	ASA now supports VPN load balancing with SAML authentication.

New Features in Version 9.16

New Features in ASA 9.16(4)

Released: October 13, 2022

There are no new features in this release.

New Features in ASA 9.16(3)

Released: April 6, 2022

There are no new features in this release.

New Features in ASA 9.16(2)

Released: August 18, 2021

There are no new features in this release.

New Features in ASDM 7.16(1.150)

Released: June 15, 2021

There are no new features in this release.

New Features in ASA 9.16(1)/ASDM 7.16(1)

Released: May 26, 2021

Feature	Description
Firewall Features	
New Section 0 for system-defined NAT rules.	A new Section 0 has been added to the NAT rule table. This section is exclusively for the use of the system. Any NAT rules that the system needs for normal functioning are added to this section, and these rules take priority over any rules you create. Previously, system-defined rules were added to Section 1, and user-defined rules could interfere with proper system functioning. You cannot add, edit, or delete Section 0 rules, but you will see them in **show nat detail** command output.
The default SIP inspection policy map drops non-SIP traffic.	For SIP-inspected traffic, the default is now to drop non-SIP traffic. The previous default was to allow non-SIP traffic on ports inspected for SIP. We changed the default SIP policy map to include the **no traffic-non-sip** command.
Ability to specify the IMSI prefixes to be dropped in GTP inspection.	GTP inspection lets you configure IMSI prefix filtering, to identify the Mobile Country Code/Mobile Network Code (MCC/MNC) combinations to allow. You can now do IMSI filtering on the MCC/MNC combinations that you want to drop. This way, you can list out the unwanted combinations, and default to allowing all other combinations. We added the following command: **drop mcc**. We changed the following screens: The Drop option was added to the IMSI Prefix Filtering tab for GTP inspection maps.
Configure the maximum segment size (MSS) for embryonic connections	You can configure a service policy to set the server maximum segment size (MSS) for SYN-cookie generation for embryonic connections upon reaching the embryonic connections limit. This is meaningful for service policies where you are also setting embryonic connection maximums. New/Modified commands: **set connection syn-cookie-mss**. New/Modified screens: **Connection Settings** in the Add/Edit Service Policy wizard.
Improved CPU usage and performance for many-to-one and one-to-many connections.	The system no longer creates local host objects and locks them when creating connections, except for connections that involve dynamic NAT/PAT and scanning threat detection and host statistics. This improves performance and CPU usage in situations where many connections are going to the same server (such as a load balancer or web server), or one endpoint is making connections to many remote hosts. We changed the following commands: **clear local-host** (deprecated), **show local-host**
Platform Features	

Feature	Description
ASA Virtual support for VMware ESXi 7.0	The ASA virtual virtual platform supports hosts running on VMware ESXi 7.0. New VMware hardware versions have been added to the vi.ovf and esxi.ovf files to enable optimal performance and usability of the ASA virtual on ESXi 7.0. No modified commands. No modified screens.
Intel QuickAssist Technology (QAT) on ASA virtual	The ASA virtual supports hardware crypto acceleration for ASA virtual deployments that use the Intel QuickAssist (QAT) 8970 PCI adapter. Hardware crypto acceleration for the ASA virtual using QAT is supported on VMware ESXi and KVM only. No modified commands. No modified screens.
ASA Virtual on OpenStack	The ASA virtual virtual platform has added support for OpenStack. No modified commands. No modified screens.
High Availability and Scalability Features	
Improved PAT port block allocation for clustering on the Firepower 4100/9300	The improved PAT port block allocation ensures that the control unit keeps ports in reserve for joining nodes, and proactively reclaims unused ports. To best optimize the allocation, you can set the maximum nodes you plan to have in the cluster using the **cluster-member-limit** command. The control unit can then allocate port blocks to the planned number of nodes, and it will not have to reserve ports for extra nodes you don't plan to use. The default is 16 nodes. You can also monitor syslog 747046 to ensure that there are enough ports available for a new node. New/Modified commands: **cluster-member-limit**, **show nat pool cluster** [**summary**], **show nat pool ip detail** New/Modified screens: **Configuration** > **Device Management** > **High Availability and Scalability** > **ASA Cluster** > **Cluster Configuration** > **Cluster Member Limit** field
show cluster history command improvements	We have added additional outputs for the **show cluster history** command. New/Modified commands: **show cluster history brief**, **show cluster history latest**, **show cluster history reverse**, **show cluster history time**
Firepower 1140 maximum contexts increased from 5 to 10	The Firepower 1140 now supports up to 10 contexts.
Certificate Features	

Feature	Description
Enrollment over Secure Transport (EST) for certification	ASA supports certificate enrollment using the Enrollment over Secure Transport (EST). However, you can configure to use EST enrollments only with RSA and ECDSA keys. You cannot use EdDSA keypair for a trustpoint configured for EST enrollment. New/Modified commands: **enrollment protocol**, **crypto ca authenticate**, and **crypto ca enroll** New/Modified screens: **Configuration** > **Device Management** > **Certificate Management** > **Identity Certificate** > **Advanced**.
Support for new EdDSA key	The new key option, EdDSA, was added to the existing RSA and ECDSA options. New/Modified commands: **crypto key generate**, **crypto key zeroize**, **show crypto key mypubkey** New/Modified screens: **Configuration** > **Device Management** > **Certificate Management** > **Identity Certificate** > **Add Identity Certificates** > **Add Key Pair**.
Command to override restrictions on certificate keys	Support to use SHA1with RSA Encryption algorithm for certification and support for certificates with RSA key sizes smaller than 2048 were removed. You can use **crypto ca permit-weak-crypto** command to override these restrictions. New/Modified commands: **crypto ca permit-weak-crypto** New/Modified screens: **Configuration** > **Device Management** > **Certificate Management** > **Identity Certificate**, **Configuration** > **Remote Access VPN** > **Certificate Management** > **Identity Certificate**, and **Configuration** > **Remote Access VPN** > **Certificate Management** > **Code Signer**
Administrative and Troubleshooting Features	

Feature	Description
SSH security improvements	SSH now supports the following security improvements: • Host key format—**crypto key generate** {**eddsa** | **ecdsa**}. In addition to RSA, we added support for the EdDSA and ECDSA host keys. The ASA tries to use keys in the following order if they exist: EdDSA, ECDSA, and then RSA. If you explicitly configure the ASA to use the RSA key with the **ssh key-exchange hostkey rsa** command, you must generate a key that is 2048 bits or higher. For upgrade compatibility, the ASA will use smaller RSA host keys only when the default host key setting is used. RSA support will be removed in a later release. • Key exchange algorithms—**ssh key-exchange group** {**ecdh-sha2-nistp256** | **curve25519-sha256**} • Encryption algorithms—**ssh cipher encryption chacha20-poly1305@openssh.com** • SSH version 1 is no longer supported—The **ssh version** command is removed. New/Modified commands: **crypto key generate eddsa**, **crypto key zeroize eddsa** , **show crypto key mypubkey**, **ssh cipher encryption chacha20-poly1305@openssh.com**, **ssh key-exchange group** {**ecdh-sha2-nistp256** | **curve25519-sha256**}, **ssh key-exchange hostkey**, **ssh version** New/Modified screens: • **Configuration** > **Device Management** > **Management Access** > **ASDM/HTTPS/Telnet/SSH** • **Configuration** > **Device Management** > **Certificate Management** > **Identity Certificates** • **Configuration** > **Device Management** > **Advanced** > **SSH Ciphers**
Monitoring Features	
SNMPv3 Authentication	You can now use SHA-224 and SHA-384 for user authentication. You can no longer use MD5 for user authentication. You can no longer use DES for encryption. New/Modified commands: **snmp-server user** New/Modified screens: **Configuration** > **Device Management** > **Management Access** > **SNMP**
VPN Features	

Feature	Description
Support for IPv6 on Static VTI	ASA supports IPv6 addresses in Virtual Tunnel Interfaces (VTI) configurations. A VTI tunnel source interface can have an IPv6 address, which you can configure to use as the tunnel endpoint. If the tunnel source interface has multiple IPv6 addresses, you can specify which address to be used, else the first IPv6 global address in the list is used by default. The tunnel mode can be either IPv4 or IPv6, but it must be the same as IP address type configured on VTI for the tunnel to be active. An IPv6 address can be assigned to the tunnel source or the tunnel destination interface in a VTI. New/Modified commands: **tunnel source interface**, **tunnel destination**, **tunnel mode**
Support for 1024 VTI interfaces per device	The number of maximum VTIs to be configured on a device has been increased from 100 to 1024. Even if a platform supports more than 1024 interfaces, the VTI count is limited to the number of VLANs configurable on that platform. For example, ASA 5510 supports 100 VLANs, the tunnel count would be 100 minus the number of physical interfaces configured. New/Modified commands: None New/Modified screens: None
Support for DH group 15 in SSL	Support has been added for DH group 15 for SSL encryption. New/Modified commands: **ssl dh-group group15**
Support for DH group 31 for IPsec encryption	Support has been added for DH group 31 for IPsec encryption. New/Modified commands: **set pfs**
Support to limit the SA in IKEv2 queue	Support has been added to limit the number of queues in SA-INIT packets. New/Modified commands: **crypto ikev2 limit queue sa_init**
Option to clear IPsec statistics	CLIs have been introduced to clear and reset IPsec statistics. New/Modified commands: **clear crypto ipsec stats** and **clear ipsec stats**

New Features in Version 9.15

New Features in ASDM 7.15(1.150)

Released: February 8, 2021

There are no new features in this release.

New Features in ASA 9.15(1)/ASDM 7.15(1)

Released: November 2, 2020

Feature	Description
Platform Features	
ASAv for the Public Cloud	We introduced the ASAv for the following Public Cloud offerings: • Oracle Cloud Infrastrucure (OCI) • Google Cloud Platform (GCP) No modified commands. No modified screens.
ASAv support for Autoscale	The ASAv now supports Autoscale for the following Public Could offerings: • Amazon Web Services (AWS) • Miscrosoft Azure Autoscaling increases or decreases the number of ASAv application instances based on capacity requirements. No modified commands. No modified screens.
ASAv for Microsoft Azure support for Accelerated Networking (SR-IOV).	The ASAv on the Microsoft Azure Public Cloud now supports Azure's Accelerated Networking (AN), which enables single root I/O virtualization (SR-IOV) to a VM, greatly improving its networking performance. No modified commands. No modified screens.
Firewall Features	

Feature	Description
Changes to PAT address allocation in clustering. The PAT pool **flat** option is now enabled by default and it is not configurable.	The way PAT addresses are distributed to the members of a cluster is changed. Previously, addresses were distributed to the members of the cluster, so your PAT pool would need a minimum of one address per cluster member. Now, the master instead divides each PAT pool address into equal-sized port blocks and distributes them across cluster members. Each member has port blocks for the same PAT addresses. Thus, you can reduce the size of the PAT pool, even to as few as one IP address, depending on the amount of connections you typically need to PAT. Port blocks are allocated in 512-port blocks from the 1024-65535 range. You can optionally included the reserved ports, 1-1023, in this block allocation when you configure PAT pool rules. For example, in a 4-node cluster, each node gets 32 blocks with which it will be able to handle 16384 connections per PAT pool IP address compared to a single node handling all 65535 connections per PAT pool IP address. As part of this change, PAT pools for all systems, whether standalone or operating in a cluster, now use a flat port range of 1023 - 65535. Previously, you could optionally use a flat range by including the **flat** keyword in a PAT pool rule. The **flat** keyword is no longer supported: the PAT pool is now always flat. The **include-reserve** keyword, which was previously a sub-keyword to **flat**, is now an independent keyword within the PAT pool configuration. With this option, you can include the 1 - 1023 port range within the PAT pool. Note that if you configure port block allocation (the **block-allocation** PAT pool option), your block allocation size is used rather than the default 512-port block. In addition, you cannot configure extended PAT for a PAT pool for systems in a cluster. New/Modified commands: **nat**, **show nat pool** New/Modified screens: NAT PAT Pool configuration.
XDMCP inspection disabled by default in new installations.	Previously, XDMCP inspection was enabled by default for all traffic. Now, on new installations, which includes new systems and reimaged systems, XDMCP is off by default. If you need this inspection, please enable it. Note that on upgrades, your current settings for XDMCP inspection are retained, even if you simply had it enabled by way of the default inspection settings.
High Availability and Scalability Features	
Disable failover delay	When you use bridge groups or IPv6 DAD, when a failover occurs the new active unit waits up to 3000 ms for the standby unit to finish networking tasks and transition to the standby state. Then the active unit can start passing traffic. To avoid this delay, you can disable the waiting time, and the active unit will start passing traffic before the standby unit transitions. New/Modified commands: **failover wait-disable** New/Modified screens: **Configuration** > **Device Management** > **High Availability and Scalability** > **Failover** > **Enable switchover waiting for peer state**
Routing Features	
Multicast IGMP interface state limit raised from 500 to 5000	The multicast IGMP state limit per interface was raised from 500 to 5000. New/Modified commands: **igmp limit** No ASDM support. *Also in 9.12(4).*

Feature	Description
Interface Features	
ASDM support for unique MAC address generation for single context mode	You can now enable unique MAC address generation for VLAN subinterfaces in single context mode in ASDM. Normally, subinterfaces share the same MAC address with the main interface. Because IPv6 link-local addresses are generated based on the MAC address, this feature allows for unique IPv6 link-local addresses. CLI support was added in ASA 9.8(3), 9.8(4), and 9.9(2) and later. New/Modified screen: **Configuration** > **Device Setup** > **Interface Settings** > **Interfaces**
DDNS support for the web update method	You can now configure an interface to use DDNS with the web update method. New/Modified commands: **show ddns update interface**, **show ddns update method**, **web update-url**, **web update-type** New/Modified screens: **Configuration** > **Device Management** > **DNS** > **Dynamic DNS**
Certificate Features	
Modifications to Match Certificate commands to support static CRL Distribution Point URL	The static CDP URL configuration commands allowed CDPs to be mapped uniquely to each certificate in a chain that is being validated. However, only one such mapping was supported for each certificate. This modification allows statically configured CDPs to be mapped to a chain of certificates for authentication. New/Modified commands: **match certificate override cdp**,
Administrative and Troubleshooting Features	
Manual import of node secret file from the RSA Authentication Manager for SDI AAA server groups.	You can import the node secret file that you export from the RSA Authentication Manager for use with SDI AAA server groups. We added the following commands: **aaa sdi import-node-secret**, **clear aaa sdi node-secret**, **show aaa sdi node-secrets**. We added the following screen: **Configuration** > **Device Management** > **Users/AAA** > **AAA SDI**.
show fragment command output enhanced	The output for **show fragment** command was enhanced to include IP fragment related drops and error counters. No modified commands. No modified screens
show tech-support command output enhanced	The output for **show tech-support** command was enhanced to include the bias that is configured for the crypto accelerator. The bias value can be ssl, ipsec, or balanced. No modified commands. No modified screens
Monitoring Features	

Feature	Description
Support to configure cplane keepalive holdtime values	Due to communication delays caused by high CPU usage, the response to the keepalive event fails to reach ASA, resulting in trigerring failover due to card failure. You can now configure the keepalive timeout period and the maximum keepalive counter value to ensure sufficient time and retries are given. New/Modified commands: **service-module** We added the following screen: **Configuration** > **Device Management** > **Service Module Settings**.
VPN Features	
Support for configuring the maximum in-negotiation SAs as an absolute value	You can now configure the maximum in-negotiation SAs as an absolute value up to 15000 or a maximum value derived from the maximum device capacity; formerly, only a percentage was allowed. New/Modified commands: **crypto ikev2 limit max-in-negotiation-sa value** No ASDM support. *Also in 9.12(4).*
Cross-Site Request Forgery (CSRF) Vulnerabilities Prevention for WebVPN Handlers	ASA provides protection against CSRF attacks for WebVPN handlers. If a CSRF attack is detected, a user is notified by warning messages. This feature is enabled by default.
Kerberos server validation for Kerberos Constrained Delegation (KCD).	When configured for KCD, the ASA initiates an AD domain join with the configured server in order to acquire Kerberos keys. These keys are required for the ASA to request service tickets on behalf of clientless SSL VPN users. You can optionally configure the ASA to validate the identity of the server during domain join. We modified the **kcd-server** command to add the **validate-server-certificate** keyword. We changed the following screens: **Configuration** > **Remote Access VPN** > **Clientless SSL VPN Access** > **Advanced** > **Microsoft KCD Server**

New Features in Version 9.14

New Features in ASA 9.14(4)/ASDM 7.17(1)

Released: February 2, 2022

There are no new features in this release.

New Features in ASA 9.14(3)/ASDM 7.15(1.150)

Released: June 15, 2021

There are no new features in this release.

New Features in ASA 9.14(2)

Released: November 9, 2020

Feature	Description
SNMP Features	
SNMP polling over site-to-site VPN	For secure SNMP polling over a site-to-site VPN, include the IP address of the outside interface in the crypto map access-list as part of the VPN configuration.

New Features in ASA 9.14(1.30)

Released: September 23, 2020

Feature	Description
Licensing Features	
ASAv100 permanent license reservation	The ASAv100 now supports permanent license reservation using product ID L-ASAV100SR-K9=. **Note:** Not all accounts are approved for permanent license reservation.

New Features in ASDM 7.14(1.48)

Released: April 30, 2020

Feature	Description
Platform Features	
Restore support for the ASA 5512-X, 5515-X, 5585-X, and ASASM for ASA 9.12 and earlier	This ASDM release restores support for the ASA 5512-X, 5515-X, 5585-X, and ASASM when they are running 9.12 or earlier. The final ASA version for these models is 9.12. The original 7.13(1) and 7.14(1) releases blocked backwards compatibility with these models; this version has restored compatibility.

New Features in ASA Virtual 9.14(1.6)

Released: April 30, 2020

Note This release is only supported on the ASA virtual.

Feature	Description
Platform Features	

Feature	Description
ASAv100 platform	The ASA virtual virtual platform has added the ASAv100, a high-end performance model that provides 20 Gbps Firewall throughput levels. The ASAv100 is a subscription-based license, available in terms of 1 year, 3 years, or 5 years. The ASAv100 is supported on VMware ESXi and KVM only.

New Features in ASA 9.14(1)/ASDM 7.14(1)

Released: April 6, 2020

Feature	Description
Platform Features	
ASA for the Firepower 4112	We introduced the ASA for the Firepower 4112. No modified commands. No modified screens. **Note** Requires FXOS 2.8(1).
Firewall Features	
Ability to see port numbers in show access-list output.	The **show access-list** command now has the numeric keyword. You can use this to view port numbers in the access control entries rather than names, for example, 80 instead of www.
The **object-group icmp-type** command is deprecated.	Although the command remains supported in this release, the **object-group icmp-type** command is deprecated and might be removed in a future release. Please change all ICMP-type objects to service object groups (**object-group service**) and specify **service icmp** within the object.
Kerberos Key Distribution Center (KDC) authentication.	You can import a keytab file from a Kerberos Key Distribution Center (KDC), and the system can authenticate that the Kerberos server is not being spoofed before using it to authenticate users. To accomplish KDC authentication, you must set up a **host**/*ASA_hostname* service principal name (SPN) on the Kerberos KDC, then export a keytab for that SPN. You then must upload the keytab to the ASA, and configure the Kerberos AAA server group to validate the KDC. New/Modified commands: **aaa kerberos import-keytab**, **clear aaa kerberos keytab**, **show aaa kerberos keytab**, **validate-kdc**. New/Modified screens: **Configuration** > **Device Management** > **Users/AAA** > **AAA Kerberos**, **Configuration** > **Device Management** > **Users/AAA** > **AAA Server Groups** Add/Edit dialog box for Kerberos server groups.
High Availability and Scalability Features	

Feature	Description
Configuration sync to data units in parallel	The control unit now syncs configuration changes with data units in parallel by default. Formerly, synching occurred sequentially. New/Modified commands: **config-replicate-parallel** New/Modified screens: **Configuration** > **Device Management** > **High Availability and Scalability** > **ASA Cluster** > **Cluster Configuration** > **Enable parallel configuration replicate** check box
Messages for cluster join failure or eviction added to **show cluster history**	New messages were added to the **show cluster history** command for when a cluster unit either fails to join the cluster or leaves the cluster. New/Modified commands: **show cluster history** No modified screens.
Interface Features	
Speed auto-negotation can be disabled on 1GB fiber interfaces on the Firepower 1000 and 2100	You can now configure a Firepower 1100 or 2100 SFP interface to disable auto-negotiation. For 10GB interfaces, you can configure the speed down to 1GB without auto-negotiation; you cannot disable auto-negotiation for an interface with the speed set to 10GB. New/Modified commands: **speed nonegotiate** New/Modified screens: **Configuration** > **Device Settings** > **Interfaces** > **Edit Interface** > **Configure Hardware Properties** > **Speed**
Administrative and Troubleshooting Features	
New **connection-data-rate** command	The **connection-data-rate** command was introduced to provide an overview on data rate of individual connections on the ASA. When this command is enabled, per-flow data rate along with the existing connection information are provided. This information helps to identify and block unwanted connections with high data rates, thereby, ensuring an optimized CPU utilization. New/Modified commands: **conn data-rate**,**show conn data-rate**, **show conn detail**, **clear conn data-rate** No modified screens.
HTTPS idle timeout setting	You can now set the idle timeout for all HTTPS connections to the ASA, including ASDM, WebVPN, and other clients. Formerly, using the **http server idle-timeout** command, you could only set the ASDM idle timeout. If you set both timeouts, the new command takes precendence. New/Modified commands: **http connection idle-timeout** New/Modified screens: **Configuration** > **Device Management** > **Management Access** > **ASDM/HTTPS/Telnet/SSH** > **HTTP Settings** > **Connection Idle Timeout** check box.
NTPv4 support	The ASA now supports NTPv4. No modified commands. No modified screens.

Feature	Description
New **clear logging counter** command	The **show logging** command provides statistics of messages logged for each logging category configured on the ASA. The **clear logging counter** command was introduced to clear the logged counters and statistics. New/Modified commands: **clear logging counter** No modified screens.
Debug command changes for FXOS on the Firepower 1000 and 2100 in Appliance mode	The **debug fxos_parser** command has been simplified to provide commonly-used troubleshooting messages about FXOS. Other FXOS debug commands have been moved under the **debug menu fxos_parser** command. New/Modified commands: **debug fxos_parser**, **debug menu fxos_parser** No modified screens.
show tech-support command enhanced	The **show ssl objects** and **show ssl errors** command was added to the output of the **show tech-support** command. New/Modified commands: **show tech-support** No modified screens. *Also in 9.12(4).*
Monitoring Features	
Net-SNMP version 5.8 Support	The ASA is using Net-SNMP, a suite of applications used to implement SNMP v1, SNMP v2c, and SNMP v3 using both IPv4 and IPv6. No modified commands. New/Modified screens: **Configuration** > **Device Management** > **Management Access** > **SNMP**
SNMP OIDs and MIBs	The ASA enhances support for the CISCO-REMOTE-ACCESS-MONITOR-MIB to track rejected/failed authentications from RADIUS over SNMP. This feature implements three SNMP OIDs: • crasNumTotalFailures (total failures) • crasNumSetupFailInsufResources (AAA and other internal failures) • crasNumAbortedSessions (aborted sessions) objects The ASA provides support for the Advanced Encryption Standard (AES) Cipher Algorithm. This feature implements the following SNMP OIDs: • usmAesCfb128Protocol • usmNoPrivProtocol
SNMPv3 Authentication	You can now use SHA-256 HMAC for user authentication. New/Modified commands: **snmp-server user** New/Modified screens: **Configuration** > **Device Management** > **Management Access** > **SNMP**

Feature	Description
debug telemetry command.	You can use the **debug telemetry** command, debug messages related to telemetry are displayed. The debugs help to identify the cause for errors when generating the telemetry report. New/Modified commands: **debug telemetry**, **show debug telemetry** No modified screens.
VPN Features	
DHCP Relay Server Support on VTI	You can now configure DHCP relay server to forward DHCP messages through VTI tunnel interface. New/Modified commands: **dhcprelay server** New/Modified screens: **Configuration** > **Device Management** > **DHCP** > **DHCP Relay**
IKEv2 Support for Multiple Peer Crypto Map	You can now configure IKEv2 with multi-peer crypto map—when a peer in a tunnel goes down, IKEv2 attempts to establish the SA with the next peer in the list. No modified commands. New/Modified screens: **Configuration** > **Site-to-Site VPN** > **Advanced** > **Crypto Maps** > **Create / Edit IPsec Rule** > **Tunnel Policy (Crypto Map) - Basic**
Username Options for Multiple Certificate Authentication	In multiple certificate authentication, you can now specify from which certificate, first (machine certificate) or second (user certificate), you want the attributes to be used for aaa authentication. New/Modified commands: **username-from-certificate-choice**, **secondary-username-from-certificate-choice** New/Modified screens: • **Connection Profile** > **Advanced** > **Authentication** • **Connection Profile** > **Advanced** > **Secondary Authentication**

New Features in Version 9.13

New Features in ASDM 7.13(1.101)

Released: May 7, 2020

Feature	Description
Platform Features	
Restore support for the ASA 5512-X, 5515-X, 5585-X, and ASASM for ASA 9.12 and earlier	This ASDM release restores support for the ASA 5512-X, 5515-X, 5585-X, and ASASM when they are running 9.12 or earlier. The final ASA version for these models is 9.12. The original 7.13(1) and 7.14(1) releases blocked backwards compatibility with these models; this version has restored compatibility.

New Features in ASA 9.13(1)/ASDM 7.13(1)

Released: September 25, 2019

Feature	Description
Platform Features	
ASA for the Firepower 1010	We introduced the ASA for the Firepower 1010. This desktop model includes a built-in hardware switch and Power-Over-Ethernet+ (PoE+) support. New/Modified commands: **boot system**, **clock timezone**, **connect fxos admin**, **forward interface**, **interface vlan**, **power inline**, **show counters**, **show environment**, **show interface**, **show inventory**, **show power inline**, **show switch mac-address-table**, **show switch vlan**, **switchport**, **switchport access vlan**, **switchport mode**, **switchport trunk allowed vlan** New/Modified screens: • **Configuration** > **Device Setup** > **Interface Settings** > **Interfaces** > **Edit** > **Switch Port** • **Configuration** > **Device Setup** > **Interface Settings** > **Interfaces** > **Edit** > **Power Over Ethernet** • **Configuration** > **Device Setup** > **Interface Settings** > **Interfaces** > **Add VLAN Interface** • **Configuration** > **Device Management** > **System Image/Configuration** > **Boot Image/Configuration** • **Configuration** > **Device Setup** > **System Time** > **Clock** • **Monitoring** > **Interfaces** > **L2 Switching** • **Monitoring** > **Interfaces** > **Power Over Ethernet**
ASA for the Firepower 1120, 1140, and 1150	We introduced the ASA for the Firepower 1120, 1140, and 1150. New/Modified commands: **boot system**, **clock timezone**, **connect fxos admin**, **show counters**, **show environment**, **show interface**, **show inventory** New/Modified screens: • **Configuration** > **Device Management** > **System Image/Configuration** > **Boot Image/Configuration** • **Configuration** > **Device Setup** > **System Time** > **Clock**

Feature	Description
Firepower 2100 Appliance mode	The Firepower 2100 runs an underlying operating system called the Firepower eXtensible Operating System (FXOS). You can run the Firepower 2100 in the following modes: • Appliance mode (now the default)—Appliance mode lets you configure all settings in the ASA. Only advanced troubleshooting commands are available from the FXOS CLI. • Platform mode—When in Platform mode, you must configure basic operating parameters and hardware interface settings in FXOS. These settings include enabling interfaces, establishing EtherChannels, NTP, image management, and more. You can use the chassis manager web interface or FXOS CLI. You can then configure your security policy in the ASA operating system using ASDM or the ASA CLI. If you are upgrading to 9.13(1), the mode will remain in Platform mode. New/Modified commands: **boot system**, **clock timezone**, **connect fxos admin**, **fxos mode appliance**, **show counters**, **show environment**, **show fxos mode**, **show interface**, **show inventory** New/Modified screens: • **Configuration** > **Device Management** > **System Image/Configuration** > **Boot Image/Configuration** • **Configuration** > **Device Setup** > **System Time** > **Clock**
DHCP reservation	The ASA DHCP server now supports DHCP reservation. You can assign a static IP address from the defined address pool to a DHCP client based on the client's MAC address. New/Modified commands: **dhcpd reserve-address** No modified screens.
ASA Virtual minimum memory requirement	The minimum memory requirement for the ASA virtual is now 2GB. If your current ASA virtual runs with less than 2GB of memory, you cannot upgrade to 9.13(1) from an earlier version without increasing the memory of your ASA virtual VM. You can also redeploy a new ASA virtual VM with version 9.13(1). No modified commands. No modified screens.
ASA Virtual MSLA Support	The ASA virtual supports Cisco's Managed Service License Agreement (MSLA) program, which is a software licensing and consumption framework designed for Cisco customers and partners who offer managed software services to third parties. MSLA is a new form of Smart Licensing where the licensing Smart Agent keeps track of the usage of licensing entitlements in units of time. New/Modified commands: **license smart**, **mode**, **utility**, **custom-id**, **custom-info**, **privacy**, **transport type**, **transport url**, **transport proxy** New/Modified screens: **Configuration** > **Device Management** > **Licensing** > **Smart Licensing**.

Feature	Description
ASA Virtual Flexible Licensing	Flexible Licensing is a new form of Smart Licensing where any ASA virtual license now can be used on any supported ASA virtual vCPU/memory configuration. Session limits for Secure Client and TLS proxy will be determined by the ASA virtual platform entitlement installed rather than a platform limit tied to a model type. New/Modified commands: **show version**, **show vm**, **show cpu**, **show license features** New/Modified screens: **Configuration** > **Device Management** > **Licensing** > **Smart Licensing**.
ASA Virtual for AWS support for the C5 instance; expanded support for C4, C3, and M4 instances	The ASA virtual on the AWS Public Cloud now supports the C5 instance (c5.large, c5.xlarge, and c5.2xlarge). In addition, support has been expanded for the C4 instance (c4.2xlarge and c4.4xlarge); C3 instance (c3.2xlarge, c3.4xlarge, and c3.8xlarge); and M4 instance (m4.2xlarge and m4.4xlarge). No modified commands. No modified screens.
ASA Virtual for Microsoft Azure support for more Azure virtual machine sizes	The ASA virtual on the Microsoft Azure Public Cloud now supports more Linux virtual machine sizes: • Standard_D4, Standard_D4_v2 • Standard_D8_v3 • Standard_DS3, Standard_DS3_v2 • Standard_DS4, Standard_DS4_v2 • Standard_F4, Standard_F4s • Standard_F8, Standard_F8s Earlier releases only supported the Standard_D3 and Standard_D3_v2 sizes. No modified commands. No modified screens.
ASA Virtual enhanced support for DPDK	The ASA virtual supports enhancements to the Data Plane Development Kit (DPDK) to enable support for multiple NIC queues, which allow multi-core CPUs to concurrently and efficiently service network interfaces. This applies to all ASA virtual hypervisors except Microsoft Azure and Hyper-V. **Note** DPDK support was introduced in release ASA 9.10(1)/ASDM 7.13(1). No modified commands. No modified screens.

Feature	Description
ASA Virtual support for VMware ESXi 6.7	The ASA virtual virtual platform supports hosts running on VMware ESXi 6.7. New VMware hardware versions have been added to the *vi.ovf* and *esxi.ovf* files to enable optimal performance and usability of the ASA virtual on ESXi 6.7. No modified commands. No modified screens.
Increased VLANs for the ISA 3000	The maximum VLANs for the ISA 3000 with the Security Plus license increased from 25 to 100.
Firewall Features	
Location logging for mobile stations (GTP inspection).	You can configure GTP inspection to log the initial location of a mobile station and subsequent changes to the location. Tracking location changes can help you identify possibly fraudulent roaming charges. New/Modified commands: **location-logging**. New/Modified screens: **Configuration** > **Firewall** > **Objects** > **Inspect Maps** > **GTP**.
GTPv2 and GTPv1 release 15 support.	The system now supports GTPv2 3GPP 29.274 V15.5.0. For GTPv1, support is up to 3GPP 29.060 V15.2.0. The new support includes recognition of 2 additional messages and 53 information elements. No modified commands. No modified screens.
Mapping Address and Port-Translation (MAP-T)	Mapping Address and Port (MAP) is primarily a feature for use in service provider (SP) networks. The service provider can operate an IPv6-only network, the MAP domain, while supporting IPv4-only subscribers and their need to communicate with IPv4-only sites on the public Internet. MAP is defined in RFC7597, RFC7598, and RFC7599. New/Modified commands: **basic-mapping-rule**, **default-mapping-rule**, **ipv4-prefix**, **ipv6-prefix**, **map-domain**, **share-ratio**, **show map-domain**, **start-port**. New/Modified commands: **Configuration** > **Device Setup** > **CGNAT Map**, **Monitoring** > **Properties** > **MAP Domains**.
Increased limits for AAA server groups and servers per group.	You can configure more AAA server groups. In single context mode, you can configure 200 AAA server groups (the former limit was 100). In multiple context mode, you can configure 8 (the former limit was 4). In addition, in multiple context mode, you can configure 8 servers per group (the former limit was 4 servers per group). The single context mode per-group limit of 16 remains unchanged. We modified the following commands to accept these new limits: **aaa-server**, **aaa-server host**. We modified the AAA screens to accept these new limits.
TLS proxy deprecated for SCCP (Skinny) inspection.	The **tls-proxy** keyword, and support for SCCP/Skinny encrypted inspection, was deprecated. The keyword will be removed from the **inspect skinny** command in a future release.
VPN Features	

Feature	Description
HSTS Support for WebVPN as Client	A new CLI mode under WebVPN mode called http-headers was added so that WebVPN could transform HTTP references to HTTPS references for hosts that are HSTS. Configures whether the user agent should allow the embedding of resources when sending this header for WebVPN connections from the ASA to browsers. You can choose to configure the http-headers as: **x-content-type-options**, **x-xss-protection**, **hsts-client** (HSTS support for WebVPN as client), **hsts-server**, or **content-security-policy**. New/Modified commands: **webvpn**, **show webvpn hsts host (name <hostname&s{253}> | all)**and **clear webvpn hsts host (name <hostname&s{253}> | all)**. New/Modified screens: **Configuration** > **Remote Access VPN** > **Clientless SSL VPN Access** > **Advanced** > **Proxies**.
Diffie-Hellman groups 15 and 16 added for key exchange	To add support for Diffie-Hellman groups 15 and 16, we modified few **crypto** commands to accept these new limits. **crypto ikev2 policy <index> group <number>** and **crypto map <map-name> <map-index> set pfs <group>.**
show asp table vpn-context enhancement to output	To enhance debug capability, these vpn context counters were added to the output: Lock Err, No SA, IP Ver Err, and Tun Down. New/Modified commands: **show asp table vpn-context** (output only).
Immediate session establishment when the maximum remote access VPN session limit is reached.	When a user reaches the maximum session (login) limit, the system deletes the user's oldest session and waits for the deletion to complete before establishing the new session. This can prevent the user from successfully connecting on the first attempt. You can remove this delay and have the system establish the new connection without waiting for the deletion to complete. New/Modified commands: **vpn-simultaneous-login-delete-no-delay**. New/Modified screens: **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **Group Policies** Add/Edit dialog box, **General** tab.
High Availability and Scalability Features	
Initiator and responder information for Dead Connection Detection (DCD), and DCD support in a cluster.	If you enable Dead Connection Detection (DCD), you can use the **show conn detail** command to get information about the initiator and responder. Dead Connection Detection allows you to maintain an inactive connection, and the **show conn** output tells you how often the endpoints have been probed. In addition, DCD is now supported in a cluster. New/Modified commands: **show conn** (output only). No modified screens.

Feature	Description
Monitor the traffic load for a cluster	You can now monitor the traffic load for cluster members, including total connection count, CPU and memory usage, and buffer drops. If the load is too high, you can choose to manually disable clustering on the unit if the remaining units can handle the load, or adjust the load balancing on the external switch. This feature is enabled by default. New/Modified commands: **debug cluster load-monitor**, **load-monitor**, **show cluster info load-monitor** New/Modified screens: • **Configuration** > **Device Management** > **High Availability and Scalability** > **ASA Cluster** > **Cluster Configuration** > **Enable Cluster Load Monitor** check box • **Monitoring** > **ASA Cluster** > **Cluster Load-Monitoring**
Accelerated cluster joining	When a data unit has the same configuration as the control unit, it will skip syncing the configuration and will join faster. This feature is enabled by default. This feature is configured on each unit, and is not replicated from the control unit to the data unit. **Note** Some configuration commands are not compatible with accelerated cluster joining; if these commands are present on the unit, even if accelerated cluster joining is enabled, configuration syncing will always occur. You must remove the incompatible configuration for accelerated cluster joining to work. Use the **show cluster info unit-join-acceleration incompatible-config** to view incompatible configuration. New/Modified commands: **unit join-acceleration**, **show cluster info unit-join-acceleration incompatible-config** New/Modified screens: **Configuration** > **Device Management** > **High Availability and Scalability** > **ASA Cluster** > **Cluster Configuration** > **Enable config sync accelleration** check box
Routing Features	
SMTP configuration enhancement	You can optionally configure the SMTP server with primary and backup interface names to enable ASA for identifying the routing table to be used for logging—management routing table or data routing table. If no interface is provided, ASA would refer to management routing table lookup, and if no proper route entry is present, it would look at the data routing table. New/Modified commands: **smtp-server [primary-interface][backup-interface]**
Support to set NSF wait timer	OSPF routers are expected to set the RS-bit in the EO-TLV attached to a Hello packet when it is not known whether all neighbors are listed in the packet, and the restarting router require to preserve their adjacencies. However, the RS-bit value must not be longer than the RouterDeadInterval seconds. The **timers nsf wait**command is introduced to set the the RS-bit in Hello packets lesser than RouterDeadInterval seconds. New/Modified commands: **timers nsf wait**

Feature	Description
Support to set tftp blocksize	The typical blocksize fixed for tftp file transfer is 512-octets. A new command, **tftp blocksize**, is introduced to configure a larger blocksize and thereby enhance the tftp file transfer speed. You can set a blocksize varying from 513 to 8192 octets. The new default blocksize is 1456 octets. The **no** form of this command will reset the blocksize to the older default value—512 octets. The **timers nsf wait**command is introduced to set the the RS-bit in Hello packets lesser than RouterDeadInterval seconds. New/Modified commands: **tftp blocksize**
Certificate Features	
Support to view FIPS status	The **show running-configuration fips** command displayed the FIPS status only when fips was enabled. In order to know the operational state, the **show fips** command was introduced where, it displays the fips status when an user enables or disables fips that is in disabled or enabled state. This command also displays the status for rebooting the device after an enable or disable action. New/Modified commands: **show fips**
CRL cache size increased	To prevent failure of large CRL downloads, the cache size was increased, and the limit on the number of entries in an individual CRL was removed. • Increased the total CRL cache size to 16 MB per context for multi-context mode. • Increased the total CRL cache size to 128 MB for single-context mode.
Modifications to the CRL Distribution Point commands	The static CDP URL configuration commands are removed and moved to the match certificate command. New/Modified commands: **crypto-ca-trustpoint crl** and **crl url** were removed with other related logic. **match-certificate override-cdp** was introduced. New/Modified screens: **Configuration** > **Device Management** > **Certificate Management** > **CA Certificates** The static CDP URL was re-introduced in 9.13(1)12 to the match certificate command.
Administrative and Troubleshooting Features	

Feature	Description
Management access when the Firepower 1000, Firepower 2100 Appliance mode is in licensing evaluation mode	The ASA includes 3DES capability by default for management access only, so you can connect to the Smart Software Manager and also use ASDM immediately. You can also use SSH and SCP if you later configure SSH access on the ASA. Other features that require strong encryption (such as VPN) must have Strong Encryption enabled, which requires you to first register to the Smart Software Manager. **Note** If you attempt to configure any features that can use strong encryption before you register—even if you only configure weak encryption—then your HTTPS connection will be dropped on that interface, and you cannot reconnect. The exception to this rule is if you are connected to a management-only interface, such as Management 1/1. SSH is not affected. If you lose your HTTPS connection, you can connect to the console port to reconfigure the ASA, connect to a management-only interface, or connect to an interface not configured for a strong encryption feature. No modified commands. No modified screens.
Additional NTP authentication algorithms	Formerly, only MD5 was supported for NTP authentication. The ASA now supports the following algorithms: • MD5 • SHA-1 • SHA-256 • SHA-512 • AES-CMAC New/Modified commands: **ntp authentication-key** New/Modified screens: **Configuration** > **Device Setup** > **System Time** > **NTP** > **Add** button **> Add NTP Server Configuration** dialog box **> Key Algorithm** drop-down list
ASA Security Service Exchange (SSE) Telemetry Support for the Firepower 4100/9300	With Cisco Success Network enabled in your network, device usage information and statistics are provided to Cisco which is used to optimize technical support. The telemetry data that is collected on your ASA devices includes CPU, memory, disk, or bandwidth usage, license usage, configured feature list, cluster/failover information and the like. New/Modified commands: **service telemetry**and **show telemetry** New/Modified screens: • **Configuration** > **Device Management** > **Telemetry** • **Monitoring** > **Properties** > **Telemetry**

Feature	Description
SSH encryption ciphers are now listed in order from highest to lowest security for pre-defined lists	SSH encryption ciphers are now listed in order from highest security to lowest security for pre-defined lists (such as medium or high). In earlier releases, they were listed from lowest to highest, which meant that a low security cipher would be proposed before a high security cipher. New/Modified commands: **ssh cipher encryption** New/Modified screens: **Configuration** > **Device Management** > **Advanced** > **SSH Ciphers**
show tech-support includes additional output	The output of **show tech-support** is enhanced to display the output of the following: **show flow-offload info detail** **show flow-offload statistics** **show asp table socket** New/Modified commands: **show tech-support** (output only).
Enhancement to **show-capture asp_drop** output to include drop location information	While troubleshooting using ASP drop counters, the exact location of the drop is unknown, especially when the same ASP drop reason is used in many different places. This information is critical in finding root cause of the drop. With this enhancement, the ASP drop details such as the build target, ASA release number, hardware model, and ASLR memory text region (to facilitate the decode of drop location) are shown. New/Modified commands: **show-capture asp_drop**
Modifications to **debug crypto ca**	The **debug crypto ca transactions** and **debug crypto ca messages** options are consolidated to provide all applicable content into the **debug crypto ca** command itself. Also, the number of available debugging levels are reduced to 14. New/Modified commands: **debug crypto ca**
FXOS Features for the Firepower 1000 and 2100	
Secure Erase	The secure erase feature erases all data on the SSDs so that data cannot be recovered even by using special tools on the SSD itself. You should perform a secure erase in FXOS when decomissioning the device. New/Modified FXOS commands: **erase secure** (local-mgmt) Supported models: Firepower 1000 and 2100
Configurable HTTPS protocol	You can set the SSL/TLS versions for FXOS HTTPS acccess. New/Modified FXOS commands: **set https access-protocols** Supported models: Firepower 2100 in Platform Mode

Feature	Description
FQDN enforcement for IPSec and Keyrings	For FXOS, you can configure FQDN enforcement so that the FDQN of the peer needs to match the DNS Name in the X.509 Certificate presented by the peer. For IPSec, enforcement is enabled by default, except for connections created prior to 9.13(1); you must manually enable enforcement for those old connections. For keyrings, all hostnames must be FQDNs, and cannot use wild cards. New/Modified FXOS commands: **set dns**, **set e-mail**, **set fqdn-enforce**, **set ip**, **set ipv6**, **set remote-address**, **set remote-ike-id** Removed commands: **fi-a-ip**, **fi-a-ipv6**, **fi-b-ip**, **fi-b-ipv6** Supported models: Firepower 2100 in Platform Mode
New IPSec ciphers and algorithms	We added the following IKE and ESP ciphers and algorithms to configure an IPSec tunnel to encrypt FXOS management traffic: • Ciphers—aes192. Existing ciphers include: aes128, aes256, aes128gcm16. • Pseudo-Random Function (PRF) (IKE only)—prfsha384, prfsha512, prfsha256. Existing PRFs include: prfsha1. • Integrity Algorithms—sha256, sha384, sha512, sha1_160. Existing algorithms incldue: sha1. • Diffie-Hellman Groups—curve25519, ecp256, ecp384, ecp521,modp3072, modp4096. Existing groups include: modp2048. No modified FXOS commands. Supported models: Firepower 2100 in Platform Mode
SSH authentication enhancements	We added the following SSH server encryption algoritghms for FXOS: • aes128-gcm@openssh.com • aes256-gcm@openssh.com • chacha20-poly@openssh.com We added the following SSH server key exchange methods for FXOS: • diffie-hellman-group14-sha256 • curve25519-sha256 • curve25519-sha256@libssh.org • ecdh-sha2-nistp256 • ecdh-sha2-nistp384 • ecdh-sha2-nistp521 New/Modified FXOS commands: **set ssh-server encrypt-algorithm**, **set ssh-server kex-algorithm** Supported models: Firepower 2100 in Platform Mode

Feature	Description
EDCS keys for X.509 Certificates	You can now use EDCS keys for FXOS certificates. Formerly, only RSA keys were supported. New/Modified FXOS commands: **set elliptic-curve**, **set keypair-type** Supported models: Firepower 2100 in Platform Mode
User password improvements	We added FXOS password security improvements, including the following: • User passwords can be up to 127 characters. The old limit was 80 characters. • Strong password check is enabled by default. • Prompt to set admin password. • Password expiration. • Limit password reuse. • Removed the **set change-during-interval** command, and added a **disabled** option for the **set change-interval**, **set no-change-interval**, and **set history-count** commands. New/Modified FXOS commands: **set change-during-interval**, **set expiration-grace-period**, **set expiration-warning-period**, **set history-count**, **set no-change-interval**, **set password**, **set password-expiration**, **set password-reuse-interval** New/Modified Firepower Chassis Manager screens: • **System** > **User Management** > **Local Users** • **System** > **User Management** > **Settings** Supported models: Firepower 2100 in Platform Mode

New Features in Version 9.12

New Features in ASA 9.12(4)

Released: May 26, 2020

Feature	Description
Routing Features	
Multicast IGMP interface state limit raised from 500 to 5000	The multicast IGMP state limit per interface was raised from 500 to 5000. New/Modified commands: **igmp limit** No ASDM support.
Troubleshooting Features	

Feature	Description
show tech-support command enhanced	The **show ssl objects** and **show ssl errors** command was added to the output of the **show tech-support** command. New/Modified commands: **show tech-support** No modified screens.
VPN Features	
Support for configuring the maximum in-negotiation SAs as an absolute value	You can now configure the maximum in-negotiation SAs as an absolute value up to 15000 or a maximum value derived from the maximum device capacity; formerly, only a percentage was allowed. New/Modified commands: **crypto ikev2 limit max-in-negotiation-sa value** No ASDM support.

New Features in ASA 9.12(3)

Released: November 25, 2019

There are no new features in this release.

New Features in ASA 9.12(2)/ASDM 7.12(2)

Released: May 30, 2019

Feature	Description
Platform Features	
Firepower 9300 SM-56 support	We introduced the following security modules: SM-56. Requires FXOS 2.6.1.157 No modified commands. No modified screens.
Administration Features	
Setting the SSH key exchange mode is restricted to the Admin context	You must set the SSH key exchange in the Admin context; this setting is inherited by all other contexts. New/Modified commands: **ssh key-exchange** New/Modified screen: **Configuration** > **Device Management** > **Management Access** > **ASDM/HTTPS/Telnet/SSH** > **SSH Settings** > **DH Key Exchange**
ASDM Features	
OpenJRE version of ASDM	You can install a version of ASDM that uses OpenJRE 1.8.x instead of Oracle JRE. The filename of the OpenJRE version is **asdm-openjre-***version***.bin**.

Feature	Description
Tools > **Preferences** option to specify the ASA FirePOWER module local management file folder	You can now specify the location to install ASA FirePOWER module local management files. You must have read/write privileges to the configured location. New/Modified screen: **Tools** > **Preferences** > **SFR Location Wizard** area

New Features in ASA 9.12(1)/ASDM 7.12(1)

Released: March 13, 2019

Feature	Description
Platform Features	
ASA for the Firepower 4115, 4125, and 4145	We introduced the Firepower 4115, 4125, and 4145. Requires FXOS 2.6.1. No modified commands. No modified screens.
Support for ASA and threat defense on separate modules of the same Firepower 9300	You can now deploy ASA and threat defense logical devices on the same Firepower 9300. Requires FXOS 2.6.1. No modified commands. No modified screens.
Firepower 9300 SM-40 and SM-48 support	We introduced the following two security modules: SM-40 and SM-48. Requires FXOS 2.6.1. No modified commands. No modified screens.
Firewall Features	
GTPv1 release 10.12 support.	The system now supports GTPv1 release 10.12. Previously, the system supported release 6.1. The new support includes recognition of 25 additional GTPv1 messages and 66 information elements. In addition, there is a behavior change. Now, any unknown message IDs are allowed. Previously, unknown messages were dropped and logged. No modified commands. No modified screens.

Feature	Description
Cisco Umbrella Enhancements.	You can now identify local domain names that should bypass Cisco Umbrella. DNS requests for these domains go directly to the DNS servers without Umbrella processing. You can also identify which Umbrella servers to use for resolving DNS requests. Finally, you can define the Umbrella inspection policy to fail open, so that DNS requests are not blocked if the Umbrella server is unavailable. New/Modified commands: **local-domain-bypass**, **resolver**, **umbrella fail-open**. New/Modified screens: **Configuration** > **Firewall** > **Objects** > **Umbrella**, **Configuration** > **Firewall** > **Objects** > **Inspect Maps** > **DNS**.
The object group search threshold is now disabled by default.	If you enabled object group search, the feature was subject to a threshold to help prevent performance degradation. That threshold is now disabled by default. You can enable it by using the **object-group-search threshold** command. New/Modified command: **object-group-search threshold**. We changed the following screen: **Configuration** > **Access Rules** > **Advanced**.
Interim logging for NAT port block allocation.	When you enable port block allocation for NAT, the system generates syslog messages during port block creation and deletion. If you enable interim logging, the system generates message 305017 at the interval you specify. The messages report all active port blocks allocated at that time, including the protocol (ICMP, TCP, UDP) and source and destination interface and IP address, and the port block. New/Modified command: **xlate block-allocation pba-interim-logging** *seconds*. New/Modified screen: **Configuration** > **Firewall** > **Advanced** > **PAT Port Block Allocation**.
VPN Features	
New **condition** option for **debug aaa**.	The **condition** option was added to the **debug aaa** command. You can use this option to filter VPN debugging based on group name, user name, or peer IP address. New/Modified commands: **debug aaa condition** No modified screens.
Support for RSA SHA-1 in IKEv2	You can now generate a signature using the RSA SHA-1 hashing algorithm for IKEv2. New/Modified commands: **rsa-sig-sha1** New/Modified screens:
View the default SSL configuration for both DES and 3DES encryption licenses as well as available ciphers	You can now view the default SSL configuration with and without the 3DES encryption license. In addition, you can view all the ciphers supported on the device. New/Modified commands: **show ssl information** No modified screens.

Feature	Description
Add subdomains to webVPN HSTS	Allows domain owners to submit what domains should be included in the HSTS preload list for web browsers. New/Modified commands: **hostname(config-webvpn) includesubdomains** New/Modified screens: **Configuration** > **Remote Access VPN** > **Clientless SSL VPN Access** > **Advanced** > **Proxies** > **Enable HSTS Subdomains**field
High Availability and Scalability Features	
Per-site gratuitous ARP for clustering	The ASA now generates gratuitous ARP (GARP) packets to keep the switching infrastructure up to date: the highest priority member at each site periodically generates GARP traffic for the global MAC/IP addresses. When using per-site MAC and IP addresses, packets sourced from the cluster use a site-specific MAC address and IP address, while packets received by the cluster use a global MAC address and IP address. If traffic is not generated from the global MAC address periodically, you could experience a MAC address timeout on your switches for the global MAC address. After a timeout, traffic destined for the global MAC address will be flooded across the entire switching infrastructure, which can cause performance and security concerns. GARP is enabled by default when you set the site ID for each unit and the site MAC address for each Spanned EtherChannel. New/Modified commands: **site-periodic-garp interval** New/Modified screens: **Configuration** > **Device Management** > **High Availability and Scalability** > **ASA Cluster** > **Cluster Configuration** > **Site Periodic GARP** field
Multiple context mode HTTPS resource management	You can now set the maximum number of non-ASDM HTTPS sessions in a resource class. By default, the limit is set to 6 per context, the maximum. You can use up to 100 HTTPS sesssions across all contexts. New/Modified commands: **limit-resource http** No ASDM support.
Routing Features	
OSPF Keychain support for authentication	OSPF authenticates the neighbor and route updates using MD5 keys. In ASA, the keys that are used to generate the MD5 digest had no lifetime associated with it. Thus, user intervention was required to change the keys periodically. To overcome this limitation, OSPFv2 supports MD5 authentication with rotating keys. Based on the accept and send lifetimes of Keys in KeyChain, OSPF authenticates, accepts or rejects keys and forms adjacency. New/Modified commands: **accept-lifetime**, **area virtual-link authentication**, **cryptographic-algorithm**, **key**, **key chain**, **key-string**, **ospf authentication**, **send-lifetime** New/Modified screens: • **Configuration** > **Device Setup** > **Key Chain** • **Configuration** > **Device Setup** > **Routing** > **OSPF** > **Setup** > **Authentication** • **Configuration** > **Device Setup** > **Routing** > **OSPF** > **Setup** > **Virtual Link**

Feature	Description
Certificate Features	
Local CA configurable FQDN for enrollment URL	To make the FQDN of the enrollment URL configurable instead of using the ASA's configured FQDN, a new CLI option is introduced. This new option is added to the **smpt** mode of **crypto ca server**. New/Modified commands: **fqdn**
Administrative, Monitoring, and Troubleshooting Features	
enable password change now required on a login	The default **enable** password is blank. When you try to access privileged EXEC mode on the ASA, you are now required to change the password to a value of 3 characters or longer. You cannot keep it blank. The **no enable password** command is no longer supported. At the CLI, you can access privileged EXEC mode using the **enable** command, the **login** command (with a user at privilege level 2+), or an SSH or Telnet session when you enable **aaa authorization exec auto-enable**. All of these methods require you to set the enable password. This password change requirement is not enforced for ASDM logins. In ASDM, by default you can log in without a username and with the **enable** password. New/Modified commands: **enable password** No modified screens.
Configurable limitation of admin sessions	You can configure the maximum number of aggregate, per user, and per-protocol administrative sessions. Formerly, you could configure only the aggregate number of sessions. This feature does not affect console sessions. Note that in multiple context mode, you cannot configure the number of HTTPS sessions, where the maximum is fixed at 5 sessions. The **quota management-session** command is also no longer accepted in the system configuration, and is instead available in the context configuration. The maximum aggregate sessions is now 15; if you configured 0 (unlimited) or 16+, then when you upgrade, the value is changed to 15. New/Modified commands: **quota management-session**, **show quota management-session** New/Modified screens: **Configuration** > **Device Management** > **Management Access** > **Management Session Quota**
Notifications for administrative privilege level changes	When you authenticate for enable access (**aaa authentication enable console**) or allow privileged EXEC access directly (**aaa authorization exec auto-enable**), then the ASA now notifies users if their assigned access level has changed since their last login. New/Modified commands: **show aaa login-history** New/Modified screens: **Status** bar **>** **Login History** icon
NTP support on IPv6	You can now specify an IPv6 address for the NTP server. New/Modified commands: **ntp server** New/Modified screens: **Configuration** > **Device Setup** > **System Time** > **NTP** > **Add** button **> Add NTP Server Configuration** dialog box

Feature	Description
SSH stronger security	See the following SSH security improvements: • Diffie-Hellman Group 14 SHA256 key exchange support. This setting is now the default. The former default was Group 1 SHA1. • HMAC-SHA256 integrity cipher support. The default is now the high security set of ciphers (hmac-sha2-256 only). The former default was the medium set. New/Modified commands: **ssh cipher integrity** , **ssh key-exchange group dh-group14-sha256** New/Modified screens: • **Configuration** > **Device Management** > **Management Access** > **ASDM/HTTPS/Telnet/SSH** • **Configuration** > **Device Management** > **Advanced** > **SSH Ciphers**
Allow non-browser-based HTTPS clients to access the ASA	You can allow non-browser-based HTTPS clients to access HTTPS services on the ASA. By default, ASDM, CSM, and REST API are allowed. New/Modified commands: **http server basic-auth-client** New/Modified screens. **Configuration** > **Device Management** > **Management Access** > **HTTP Non-Browser Client Support**
Capture control plane packets only on the cluster control link	You can now capture control plane packets only on the cluster control link (and no data plane packets). This option is useful in the system in multiple context mode where you cannot match traffic using an ACL. New/Modified commands: **capture interface cluster cp-cluster** New/Modified screens: **Wizards** > **Packet Capture Wizard** > **Cluster Option**
debug conn command	The **debug conn** command was added to provide two history mechanisms that record connection processing. The first history list is a per-thread list that records the operations of the thread. The second history list is a list that records the operations into the conn-group. When a connection is enabled, processing events such as a connection lock, unlock, and delete are recorded into the two history lists. When a problem occurs, these two lists can be used to look back at the processing to determine the incorrect logic. New/Modified commands: **debug conn**
show tech-support includes additional output	The output of the **show tech-support** is enhanced to display the output of the following: • **show ipv6 interface** • **show aaa-server** • **show fragment** New/Modified commands: **show tech-support**

Feature	Description
ASDM support to enable and disable the results for free memory and used memory statistics during SNMP walk operations	To avoid overutilization of CPU resources, you can enable and disable the query of free memory and used memory statistics collected through SNMP walk operations. New or modified screen: **Configuration** > **Device Management** > **Management Access** > **SNMP**
Configurable graph update interval for the ASDM Home pane for the System in multiple-context mode	For the System in multiple context mode, you can now set the amount of time between updates for the graphs on the Home pane. New/Modified screens: **Tools** > **Preferences** > **Graph User time interval in System Context**

New Features in Version 9.10

New Features in ASA 9.10(1)/ASDM 7.10(1)

Released: October 25, 2018

Feature	Description
Platform Features	
ASA Virtual VHD custom images for Azure	You can now create your own custom ASA virtual images on Azure using a compressed VHD image available from Cisco. To deploy using a VHD image, you upload the VHD image to your Azure storage account. Then, you can create a managed image using the uploaded disk image and an Azure Resource Manager template. Azure templates are JSON files that contain resource descriptions and parameter definitions.
ASA Virtual for Azure	The ASA virtual is available in the Azure China Marketplace.
ASA Virtual support for DPDK	DPDK (Dataplane Development Kit) is integrated into the dataplane of the ASA virtual using poll-mode drivers.
ISA 3000 support for FirePOWER module Version 6.3	The previous supported version was FirePOWER 5.4.
Firewall Features	

Feature	Description
Cisco Umbrella support	You can configure the device to redirect DNS requests to Cisco Umbrella, so that your Enterprise Security policy defined in Cisco Umbrella can be applied to user connections. You can allow or block connections based on FQDN, or for suspicious FQDNs, you can redirect the user to the Cisco Umbrella intelligent proxy, which can perform URL filtering. The Umbrella configuration is part of the DNS inspection policy. New/Modified commands: **umbrella**, **umbrella-global**, **token**, **public-key**, **timeout edns**, **dnscrypt**, **show service-policy inspect dns detail** New/Modified screens: **Configuration** > **Firewall** > **Objects** > **Umbrella**, **Configuration** > **Firewall** > **Objects** > **Inspect Maps** > **DNS**
GTP inspection enhancements for MSISDN and Selection Mode filtering, anti-replay, and user spoofing protection	You can now configure GTP inspection to drop Create PDP Context messages based on Mobile Station International Subscriber Directory Number (MSISDN) or Selection Mode. You can also implement anti-replay and user spoofing protection. New/Modified commands: **anti-replay**, **gtp-u-header-check**, **match msisdn**, **match selection-mode** New/Modified screens: **Configuration** > **Firewall** > **Objects** > **Inspection Maps** > **GTP** > **Add/Edit** dialog box
Default idle timeout for TCP state bypass	The default idle timeout for TCP state bypass connections is now 2 minutes instead of 1 hour.
Support for removing the logout button from the cut-through proxy login page	If you configure the cut-through proxy to obtain user identity information (the AAA authentication listener), you can now remove the logout button from the page. This is useful in case where users connect from behind a NAT device and cannot be distinguished by IP address. When one user logs out, it logs out all users of the IP address. New/Modified commands: **aaa authentication listener no-logout-button** No ASDM support. *Also in 9.8(3).*
Trustsec SXP connection configurable delete hold down timer	The default SXP connection hold down timer is 120 seconds. You can now configure this timer, between 120 to 64000 seconds. New/Modified commands: **cts sxp delete-hold-down period**, **show cts sxp connection brief**, **show cts sxp connections** No ASDM support. *Also in 9.8(3).*
Support for offloading NAT'ed flows in transparent mode.	If you are using flow offload (the **flow-offload enable** and **set connection advanced-options flow-offload** commands), offloaded flows can now include flows that require NAT in transparent mode.

Feature	Description
Support for transparent mode deployment for a Firepower Firepower 4100/9300 ASA logical device	You can now specify transparent or routed mode when you deploy the ASA on a Firepower 4100/9300. New/Modified FXOS commands: **enter bootstrap-key FIREWALL_MODE**, **set value routed**, **set value transparent** New/Modified Firepower Chassis Manager screens: **Logical Devices** > **Add Device** > **Settings** New/Modified options: **Firewall Mode** drop-down list
VPN Features	
Support for legacy SAML authentication	If you deploy an ASA with the fix for CSCvg65072, then the default SAML behavior is to use the embedded browser, which is not supported on AnyConnect 4.4 or 4.5. Therefore, to continue to use AnyConnect 4.4 or 4.5, you must enable the legacy external browser SAML authentication method. Because of security limitations, use this option only as part of a temporary plan to migrate to AnyConnect 4.6 (or later). This option will be deprecated in the near future. New/Modified commands: **saml external-browser** New/Modified screens: **Configuration** > **Remote Access VPN** > **Network (Client) Access> Secure Client Connection Profiles** page **> Connection Profiles** area **> Add** button **> Add Secure Client Connection Profile** dialog box **Configuration** > **Remote Access VPN** > **Clientless SSL VPN Access** > **Connection Profiles** > page **> Connection Profiles** area **> Add** button **> Add Clientless SSL VPN Connection Profile** dialog box New/Modified options: **SAML External Browser** check box *Also in 9.8(3).*
DTLS 1.2 support for Secure Client VPN remote access connections.	DTLS 1.2, as defined in RFC- 6347, is now supported for AnyConnect VPN module of Cisco Secure Client in addition to the currently supported DTLS 1.0 (1.1 version number is not used for DTLS.) This applies to all ASA models except the 5506-X, 5508-X, and 5516-X; and applies when the ASA is acting as a server only, not a client. DTLS 1.2 supports additional ciphers, as well as all current TLS/DTLS cyphers, and a larger cookie size. New/Modified commands: **show run ssl**, **show vpn-sessiondb detail anyconnectssl cipher**, **ssl server-version** New/Modified screens: **Configuration** > **Remote Access VPN** > **Advanced** > **SSL Settings**
High Availability and Scalability Features	

Feature	Description
Cluster control link customizable IP Address for the Firepower 4100/9300	By default, the cluster control link uses the 127.2.0.0/16 network. You can now set the network when you deploy the cluster in FXOS. The chassis auto-generates the cluster control link interface IP address for each unit based on the chassis ID and slot ID: 127.2.*chassis_id*.*slot_id*. However, some networking deployments do not allow 127.2.0.0/16 traffic to pass. Therefore, you can now set a custom /16 subnet for the cluster control link in FXOS except for loopback (127.0.0.0/8) and multicast (224.0.0.0/4) addresses. New/Modified FXOS commands: **set cluster-control-link network** New/Modified Firepower Chassis Manager screens: **Logical Devices** > **Add Device** > **Cluster Information** New/Modified options: **CCL Subnet IP** field
Parallel joining of cluster units per Firepower 9300 chassis	For the Firepower 9300, this feature ensures that the security modules in a chassis join the cluster simultaneously, so that traffic is evenly distributed between the modules. If a module joins very much in advance of other modules, it can receive more traffic than desired, because the other modules cannot yet share the load. New/Modified commands: **unit parallel-join** New/Modified screens: **Configuration** > **Device Management** > **High Availability and Scalability** > **ASA Cluster** New/Modified options: **Parallel Join of Units Per Chassis** area
Cluster interface debounce time now applies to interfaces changing from a down state to an up state	When an interface status update occurs, the ASA waits the number of milliseconds specified in the **health-check monitor-interface debounce-time** command or the ASDM **Configuration** > **Device Management** > **High Availability and Scalability** > **ASA Cluster** screen before marking the interface as failed and the unit is removed from the cluster. This feature now applies to interfaces changing from a down state to an up state. For example, in the case of an EtherChannel that transitions from a down state to an up state (for example, the switch reloaded, or the switch enabled an EtherChannel), a longer debounce time can prevent the interface from appearing to be failed on a cluster unit just because another cluster unit was faster at bundling the ports. We did not modify any commands. We did not modify any screens.
Active/Backup High Availability for ASA virtual on Microsoft Azure Government Cloud	The stateless Active/Backup solution that allows for a failure of the active ASA virtual to trigger an automatic failover of the system to the backup ASA virtual in the Microsoft Azure public cloud is now available in the Azure Government Cloud. New or modified command: **failover cloud** New or modified screens: **Configuration** > **Device Management** > **High Availability and Scalability** > **Failover** **Monitoring** > **Properties** > **Failover** > **Status** **Monitoring** > **Properties** > **Failover** > **History**
Interface Features	

Feature	Description
show interface ip brief and **show ipv6 interface** output enhancement to show the supervisor association for the Firepower 2100/4100/9300	For the Firepower 2100/4100/9300, the output of the command is enhanced to indicate the supervisor association status of the interfaces. New/Modified commands: **show interface ip brief**, **show ipv6 interface**
The **set lacp-mode** command was changed to **set port-channel-mode** on the Firepower 2100	The **set lacp-mode** command was changed to **set port-channel-mode** to match the command usage in the Firepower 4100/9300. New/Modified FXOS commands: **set port-channel-mode**
Administrative, Monitoring, and Troubleshooting Features	
Support for NTP Authentication on the Firepower 2100	You can now configure SHA1 NTP server authentication in FXOS. New/Modified FXOS commands: **enable ntp-authentication, set ntp-sha1-key-id, set ntp-sha1-key-string** New/Modified Firepower Chassis Manager screens: **Platform Settings** > **NTP** New/Modified options: **NTP Server Authentication: Enable** check box, **Authentication Key** field, **Authentication Value** field
Packet capture support for matching IPv6 traffic without using an ACL	If you use the **match** keyword for the **capture** command, the **any** keyword only matches IPv4 traffic. You can now specify **any4** and **any6** keywords to capture either IPv4 or IPv6 traffic. The **any** keyword continues to match only IPv4 traffic. New/Modified commands: **capture match** No ASDM support.
Support for public key authentication for SSH to FXOS on the Firepower 2100	You can set the SSH key so you can use public key authentication instead of/as well as password authentication. New/Modified FXOS commands: **set sshkey** No Firepower Chassis Manager support.
Support for GRE and IPinIP encapsulation	When you do a packet capture on interface inside, the output of the command is enhanced to display the GRE and IPinIP encapsulation on ICMP, UDP, TCP, and others. New/Modified commands: **show capture**
Support to enable memory threshold that restricts application cache allocations	You can restrict application cache allocations on reaching certain memory threshold so that there is a reservation of memory to maintain stability and manageability of the device. New/Modified commands: **memory threshold enable, show run memory threshold,clear conf memory threshold**
Support for RFC 5424 logging timestamp	You can enable the logging timestamp as per RFC 5424 format. New/Modified command: **logging timestamp**
Support to display memory usage of TCB-IPS	Shows application level memory cache for TCB-IPS New/Modified command: **show memory app-cache**

Feature	Description
Support to enable and disable the results for free memory and used memory statistics during SNMP walk operations	To avoid overutilization of CPU resources, you can enable and disable the query of free memory and used memory statistics collected through SNMP walk operations. New/Modified command: **snmp-server enable oid** No ASDM support.

New Features in Version 9.9

New Features in ASDM 7.9(2.152)

Released: May 9, 2018

Feature	Description
VPN Features	
Support for legacy SAML authentication	If you deploy an ASA with the fix for CSCvg65072, then the default SAML behavior is to use the embedded browser, which is not supported on AnyConnect 4.4 or 4.5. Therefore, to continue to use AnyConnect 4.4 or 4.5, you must enable the legacy external browser SAML authentication method. Because of security limitations, use this option only as part of a temporary plan to migrate to AnyConnect 4.6. This option will be deprecated in the near future. New/Modified screens: **Configuration** > **Remote Access VPN** > **Network (Client) Access**Secure Client **Connection Profiles** page **> Connection Profiles** area **> Add** button **> Add** Secure Client **Connection Profile** dialog box **Configuration** > **Remote Access VPN** > **Clientless SSL VPN Access** > **Connection Profiles** > page **> Connection Profiles** area **> Add** button **> Add Clientless SSL VPN Connection Profile** dialog box New/Modified options: **SAML External Browser** check box

New Features in ASA 9.9(2)/ASDM 7.9(2)

Released: March 26, 2018

Feature	Description
Platform Features	

Feature	Description
ASA virtual support for VMware ESXi 6.5	The ASA virtual platform supports hosts running on VMware ESXi 6.5. New VMware hardware versions have been added to the *vi.ovf* and *esxi.ovf* files to enable optimal performance and usability of the ASA virtual on ESXi 6.5. We did not modify any commands. We did not modify any screens.
ASA virtual support for VMXNET3 interfaces	The ASA virtual platform supports VMXNET3 interfaces on VMware hypervisors. We did not modify any commands. We did not modify any screens.
ASA virtual support for virtual serial console on first boot	You can now configure the ASA virtual to use the virtual serial console on first boot, instead of the virtual VGA console, to access and configure the ASA virtual. New or Modified commands: **console serial**
ASA Virtual support to update user-defined routes in more than one Azure subscription for High Availability on Microsoft Azure	You can now configure the ASA virtual in an Azure High Availability configuration to update user-defined routes in more than one Azure subscription. New or Modified commands: **failover cloud route-table** New or modified screens: **Configuration** > **Device Management** > **High Availability and Scalability** > **Failover** > **Route-Table**
VPN Features	
Remote Access VPN multi-context support extended to IKEv2 protocol	Support for configuring ASA to allow Secure Client and third party Standards-based IPSec IKEv2 VPN clients to establish Remote Access VPN sessions to ASA operating in multi-context mode.
IPv6 connectivity to Radius Servers	ASA 9.9.2 now supports IPv6 connectivity to external AAA Radius Servers.
Easy VPN Enhancements for BVI Support	Easy VPN has been enhanced to support a Bridged Virtual Interface (BVI) as its internal secure interface, and you can now directly configure which interface to use as the internal secure interface. Otherwise, the ASA chooses its internal secure interface using security levels. Also, management services, such as **telnet**, **http**, and **ssh**, can now be configured on a BVI if VPN **management-access** has been enabled on that BVI. For non-VPN management access, you should continue to configure these services on the bridge group member interfaces. New or Modified commands: **vpnclient secure interface** [*interface-name*], **https**, **telnet**, **ssh**, **management-access**
Distributed VPN Session Improvements	• The Active Session Redistribution logic, which balances Distributed S2S VPN active and backup sessions, has been improved. Also, the balancing process may be repeated up to eight times in the background for a single **cluster redistribute vpn-sessiondb** command entered by the administrator. • The handling of dynamic Reverse Route Injections (RRI) across the cluster has been improved.
High Availability and Scalability Features	

Feature	Description
Automatically rejoin the cluster after an internal failure	Formerly, many error conditions caused a cluster unit to be removed from the cluster, and you were required to manually rejoin the cluster after resolving the issue. Now, a unit will attempt to rejoin the cluster automatically at the following intervals by default: 5 minutes, 10 minutes, and then 20 minutes. These values are configurable. Internal failures include: application sync timeout; inconsistent application statuses; and so on. New or Modified commands: **health-check system auto-rejoin, show cluster info auto-join** New or modified screen: **Configuration** > **Device Management** > **High Availability and Scalability** > **ASA Cluster** > **Auto Rejoin**
Configurable debounce time to mark an interface as failed for the ASA 5000-X series	You can now configure the debounce time before the ASA considers an interface to be failed and the unit is removed from the cluster on the ASA 5500-X series. This feature allows for faster detection of interface failures. Note that configuring a lower debounce time increases the chances of false-positives. When an interface status update occurs, the ASA waits the number of milliseconds specified before marking the interface as failed and the unit is removed from the cluster. The default debounce time is 500 ms, with a range of 300 ms to 9 seconds. This feature was previously available for the Firepower 4100/9300. New or modified command: **health-check monitor-interface debounce-time** New or modified screen: **Configuration** > **Device Management** > **High Availability and Scalability** > **ASA Cluster**
Show transport related statistics for cluster reliable transport protocol messages	You can now view per-unit cluster reliable transport buffer usage so you can identify packet drop issues when the buffer is full in the control plane. New or modified command: **show cluster info transport cp detail**
Show failover history from peer unit	You can now view failover history from the peer unit, using the **details** keyword . This includes failover state changes and reason for the state change. New or modified command: **show failover**
Interface Features	
Unique MAC address generation for single context mode	You can now enable unique MAC address generation for VLAN subinterfaces in single context mode. Normally, subinterfaces share the same MAC address with the main interface. Because IPv6 link-local addresses are generated based on the MAC address, this feature allows for unique IPv6 link-local addresses. New or modified command: **mac-address auto** No ASDM support. *Also in 9.8(3) and 9.8(4).*
Administrative Features	
RSA key pair supports 3072-bit keys	You can now set the modulus size to 3072. New or modified command: **crypto key generate rsa modulus** New or modified screen: **Configuration** > **Device Management** > **Certificate Management** > **Identity Certificates**

Feature	Description
The FXOS bootstrap configuration now sets the enable password	When you deploy the ASA on the Firepower 4100/9300, the password setting in the bootstrap configuration now sets the enable password as well as the admin user password. Requires FXOS Version 2.3.1.
Monitoring and Troubleshooting Features	
SNMP IPv6 support	The ASA now supports SNMP over IPv6, including communicating with SNMP servers over IPv6, allowing the execution of queries and traps over IPv6, and supporting IPv6 addresses for existing MIBs. We added the following new SNMP IPv6 MIB objects as described in RFC 8096. • ipv6InterfaceTable (OID: 1.3.6.1.2.1.4.30)—Contains per-interface IPv6-specific information. • ipAddressPrefixTable (OID:1.3.6.1.2.1.4.32)—Includes all the prefixes learned by this entity. • ipAddressTable (OID: 1.3.6.1.2.1.4.34)—Contains addressing information relevant to the entity's interfaces. • ipNetToPhysicalTable (OID: 1.3.6.1.2.1.4.35)—Contains the mapping from IP addresses to physical addresses. New or modified command: **snmp-server host** **Note** The **snmp-server host-group** command does not support IPv6. New or modified screen: **Configuration** > **Device Management** > **Management Access** > **SNMP**
Conditional Debugging to troubleshoot a single user session	Conditional debugging feature now assists you to verify the logs of specific ASA VPN sessions based on the filter conditions that are set. Support for "any, any" for IPv4 and IPv6 subnets is provided.

New Features in ASDM 7.9(1.151)

Released: February 14, 2018

There are no new features in this release.

New Features in ASA 9.9(1)/ASDM 7.9(1)

Released: December 4, 2017

Feature	Description
Firewall Features	

Feature	Description
Ethertype access control list changes	EtherType access control lists now support Ethernet II IPX (EII IPX). In addition, new keywords are added to the DSAP keyword to support common DSAP values: BPDU (0x42), IPX (0xE0), Raw IPX (0xFF), and ISIS (0xFE). Consequently, existing EtherType access contol entries that use the BPDU or ISIS keywords will be converted automatically to use the DSAP specification, and rules for IPX will be converted to 3 rules (DSAP IPX, DSAP Raw IPX, and EII IPX). In addition, packet capture that uses IPX as an EtherType value has been deprecated, because IPX corresponds to 3 separate EtherTypes. New or modified command: **access-list ethertype** added the new keywords **eii-ipx** and **dsap** {**bpdu** | **ipx** | **isis** | **raw-ipx**}; **capture ethernet-type** no longer supports the **ipx** keyword. New or modified screen: **Configuration** > **Firewall** > **Ethertype Rules**.
VPN Features	
Distributed Site-to-Site VPN with clustering on the Firepower 9300	An ASA cluster on the Firepower 9300 supports Site-to-Site VPN in distributed mode. Distributed mode provides the ability to have many Site-to-Site IPsec IKEv2 VPN connections distributed across members of an ASA cluster, not just on the control unit (as in centralized mode). This significantly scales VPN support beyond Centralized VPN capabilities and provides high availability. Distributed S2S VPN runs on a cluster of up to two chassis, each containing up to three modules (six total cluster members), each module supporting up to 6K active sessions (12K total), for a maximum of approximately 36K active sessions (72K total). New or modified commands: **cluster redistribute vpn-sessiondb**, **show cluster vpn-sessiondb**, **vpn mode** , **show cluster resource usage**, **show vpn-sessiondb** , **show connection detail**, **show crypto ikev2** New or modified screens: **Monitoring > ASA Cluster > ASA Cluster > VPN Cluster Summary** **Monitoring > VPN > VPN Statistics > Sessions** **Configuration > Device Management > High Availablility and Scalability > ASA Cluster** **Wizards > Site-to-Site** **Monitoring > VPN > VPN Statistics > Sessions** **Monitoring > ASA Cluster > ASA Cluster > VPN Cluster Summary** **Monitoring > ASA Cluster > ASA Cluster > System Resource Graphs > CPU/Memory** **Monitoring > Logging > Real-Time Log Viewer**
High Availability and Scalability Features	

Feature	Description
Active/Backup High Availability for ASA virtual on Microsoft Azure	A stateless Active/Backup solution that allows for a failure of the active ASA virtual to trigger an automatic failover of the system to the backup ASA virtual in the Microsoft Azure public cloud. New or modified command: **failover cloud** New or modified screens: **Configuration** > **Device Management** > **High Availability and Scalability** > **Failover** **Monitoring** > **Properties** > **Failover** > **Status** **Monitoring** > **Properties** > **Failover** > **History** *Also in 9.8(1.200).*
Improved chassis health check failure detection for the Firepower chassis	You can now configure a lower holdtime for the chassis health check: 100 ms. The previous minimum was 300 ms. New or modified command: **app-agent heartbeat interval** No ASDM support.
Inter-site redundancy for clustering	Inter-site redundancy ensures that a backup owner for a traffic flow will always be at the other site from the owner. This feature guards against site failure. New or modified commands: **site-redundancy, show asp cluster counter change, show asp table cluster chash-table, show conn flag** New or modified screen: **Configuration** > **Device Management** > **High Availability and Scalability** > **ASA Cluster**
cluster remove unit command behavior matches **no enable** behavior	The **cluster remove unit** command now removes a unit from the cluster until you manually reenable clustering or reload, similar to the **no enable** command. Previously, if you redeployed the bootstrap configuration from FXOS, clustering would be reenabled. Now, the disabled status persists even in the case of a bootstrap configuration redeployment. Reloading the ASA, however, will reenable clustering. New/Modified command: **cluster remove unit** New/Modified screen: **Configuration** > **Device Management** > **High Availability and Scalability** > **ASA Cluster**
Administrative, Monitoring, and Troubleshooting Features	
SSH version 1 has been deprecated	SSH version 1 has been deprecated, and will be removed in a future release. The default setting has changed from both SSH v1 and v2 to just SSH v2. New/Modified commands: **ssh version** New/Modified screens: • **Configuration** > **Device Management** > **Management Access** > **ASDM/HTTPS/Telnet/SSH**

Feature	Description
Enhanced packet tracer and packet capture capabilities	The packet tracer has been enhanced with the following features: • Trace a packet when it passes between cluster units. • Allow simulated packets to egress the ASA. • Bypass security checks for a similated packet. • Treat a simulated packet as an IPsec/SSL decrypted packet. The packet capture has been enhanced with the following features: • Capture packets after they are decrypted. • Capture traces and retain them in the persistent list. New or modified commands: **cluster exec capture test trace include-decrypted, cluster exec capture test trace persist, cluster exec clear packet-tracer, cluster exec show packet-tracer id, cluster exec show packet-tracer origin, packet-tracer persist, packet-tracer transmit, packet-tracer decrypted, packet-tracer bypass-checks** New or modified screens: **Tools** > **Packet Tracer** We added **Cluster Capture** field to support these options: **decrypted**, **persist**, **bypass-checks**, **transmit** We added two new options in the **Filter By** view under the **All Sessions** drop-down list: **Origin** and **Origin-ID** **Monitoring** > **VPN** > **VPN Statistics** > **Packet Tracer and Capture** We added **ICMP Capture** field in the Packet Capture Wizard screen:**Wizards** > **Packet Capture Wizard** We added two options **include-decrypted** and **persist** to support ICMP Capture.

New Features in Version 9.8

New Features in ASA 9.8(4)

Released: April 24, 2019

Feature	Description
VPN Features	

Feature	Description
Add subdomains to webVPN HSTS	Allows domain owners to submit what domains should be included in the HSTS preload list for web browsers. New/Modified commands: **hostname(config-webvpn) includesubdomains** New/Modified screens: **Configuration** > **Remote Access VPN** > **Clientless SSL VPN Access** > **Advanced** > **Proxies** > **Enable HSTS Subdomains**field *Also in 9.12(1).*
Administrative Features	
Allow non-browser-based HTTPS clients to access the ASA	You can allow non-browser-based HTTPS clients to access HTTPS services on the ASA. By default, ASDM, CSM, and REST API are allowed. Many specialty clients (for example, python libraries, curl, and wget) do not support Cross-site request forgery (CSRF) token-based authentication, so you need to specifically allow these clients to use the ASA basic authentication method. For security purposes, you should only allow required clients. New/Modified commands: **http server basic-auth-client** New/Modified screens. **Configuration** > **Device Management** > **Management Access** > **HTTP Non-Browser Client Support** *Also in 9.12(1).*
show tech-support includes additional output	The output of the **show tech-support** is enhanced to display the output of the following: • **show ipv6 interface** • **show aaa-server** • **show fragment** New/Modified commands: **show tech-support** *Also in 9.12(1).*
Support to enable and disable the results for free memory and used memory statistics during SNMP walk operations	To avoid overutilization of CPU resources, you can enable and disable the query of free memory and used memory statistics collected through SNMP walk operations. New/Modified command: **snmp-server enable oid** New or modified screen: **Configuration** > **Device Management** > **Management Access** > **SNMP** *Also in 9.10(1).*

New Features in ASA 9.8(3)/ASDM 7.9(2.152)

Released: July 2, 2018

Feature	Description
Platform Features	
Firepower 2100 Active LED now lights amber when in standby mode	Formerly, the Active LED was unlit in standby mode.
Firewall Features	
Support for removing the logout button from the cut-through proxy login page.	If you configure the cut-through proxy to obtain user identity information (the AAA authentication listener), you can now remove the logout button from the page. This is useful in case where users connect from behind a NAT device and cannot be distinguished by IP address. When one user logs out, it logs out all users of the IP address. New/Modified commands: **aaa authentication listener no-logout-button**. No ASDM support.
Trustsec SXP connection configurable delete hold down timer	The default SXP connection hold down timer is 120 seconds. You can now configure this timer, between 120 to 64000 seconds. New/Modified commands: **cts sxp delete-hold-down period**, **show cts sxp connection brief**, **show cts sxp connections** No ASDM support.
VPN Features	
Support for legacy SAML authentication	If you deploy an ASA with the fix for CSCvg65072, then the default SAML behavior is to use the embedded browser, which is not supported on AnyConnect 4.4 or 4.5. Therefore, to continue to use AnyConnect 4.4 or 4.5, you must enable the legacy external browser SAML authentication method. Because of security limitations, use this option only as part of a temporary plan to migrate to AnyConnect 4.6. This option will be deprecated in the near future. New/Modified commands: **saml external-browser** New/Modified screens: **Configuration** > **Remote Access VPN** > **Network (Client) Access**Secure Client **Connection Profiles** page **>** **Connection Profiles** area **>** **Add** button **>** **Add** Secure Client **Connection Profile** dialog box **Configuration** > **Remote Access VPN** > **Clientless SSL VPN Access** > **Connection Profiles** > page **>** **Connection Profiles** area **>** **Add** button **>** **Add Clientless SSL VPN Connection Profile** dialog box New/Modified options: **SAML External Browser** check box
Interface Features	

Feature	Description
Unique MAC address generation for single context mode	You can now enable unique MAC address generation for VLAN subinterfaces in single context mode. Normally, subinterfaces share the same MAC address with the main interface. Because IPv6 link-local addresses are generated based on the MAC address, this feature allows for unique IPv6 link-local addresses. New or modified command: **mac-address auto** No ASDM support. *Also in 9.9(2) and later.*

New Features in ASDM 7.8(2.151)

Released: October 12, 2017

Feature	Description
Firewall Features	
Ethertype access control list changes	EtherType access control lists now support Ethernet II IPX (EII IPX). In addition, new keywords are added to the DSAP keyword to support common DSAP values: BPDU (0x42), IPX (0xE0), Raw IPX (0xFF), and ISIS (0xFE). Consequently, existing EtherType access contol entries that use the BPDU or ISIS keywords will be converted automatically to use the DSAP specification, and rules for IPX will be converted to 3 rules (DSAP IPX, DSAP Raw IPX, and EII IPX). In addition, packet capture that uses IPX as an EtherType value has been deprecated, because IPX corresponds to 3 separate EtherTypes. This feature is supported in 9.8(2.9) and other interim releases. For more information, see CSCvf57908. We modified the following commands: **access-list ethertype** added the new keywords **eii-ipx** and **dsap** {**bpdu** | **ipx** | **isis** | **raw-ipx**}; **capture ethernet-type** no longer supports the **ipx** keyword. We modified the following screens: **Configuration** > **Firewall** > **Ethertype Rules**.

New Features in ASA 9.8(2)/ASDM 7.8(2)

Released: August 28, 2017

Feature	Description
Platform Features	

Feature	Description
ASA for the Firepower 2100 series	We introduced the ASA for the Firepower 2110, 2120, 2130, and 2140. Similar to the Firepower 4100 and 9300, the Firepower 2100 runs the base FXOS operating system and then the ASA operating system as an application. The Firepower 2100 implementation couples FXOS more closely with the ASA than the Firepower 4100 and 9300 do (pared down FXOS functions, single device image bundle, easy management access for both ASA and FXOS). FXOS owns configuring hardware settings for interfaces, including creating EtherChannels, as well as NTP services, hardware monitoring, and other basic functions. You can use the Firepower Chassis Manager or the FXOS CLI for this configuration. The ASA owns all other functionality, including Smart Licensing (unlike the Firepower 4100 and 9300). The ASA and FXOS each have their own IP address on the Management 1/1 interface, and you can configure management of both the ASA and FXOS instances from any data interface. We introduced the following commands: **connect fxos, fxos https, fxos snmp, fxos ssh, ip-client** We introduced the following screens: **Configuration** > **Device Management** > **Management Access** > **FXOS Remote Management**
Department of Defense Unified Capabilities Approved Products List	The ASA was updated to comply with the Unified Capabilities Approved Products List (UC APL) requirements. In this release, when you enter the **fips enable** command, the ASA will reload. Both failover peers must be in the same FIPS mode before you enable failover. We modified the following command: **fips enable**
ASA virtual for Amazon Web Services M4 instance support	You can now deploy the ASA virtual as an M4 instance. We did not modify any commands. We did not modify any screens.
ASAv5 1.5 GB RAM capability	Starting in Version 9.7(1), the ASAv5 may experience memory exhaustion where certain functions such as enabling Secure Client or downloading files to the ASA virtual fail. You can now assign 1.5 GB (up from 1 GB) of RAM to the ASAv5. We did not modify any commands. We did not modify any screens.
VPN Features	
HTTP Strict Transport Security (HSTS) header support	HSTS protects websites against protocol downgrade attacks and cookie hijacking on clientless SSL VPN. It lets web servers declare that web browsers (or other complying user agents) should only interact with it using secure HTTPS connections, and never via the insecure HTTP protocol. HSTS is an IETF standards track protocol and is specified in RFC 6797. We introduced the following commands: **hsts enable, hsts max-age** *age_in_seconds* We modified the following screens: **Configuration > Remote Access VPN > Clientless SSL VPN Access > Advanced > Proxies**
Interface Features	

Feature	Description
VLAN support for the ASAv50	The ASAv50 now supports VLANs on the ixgbe-vf vNIC for SR-IOV interfaces. We did not modify any commands. We did not modify any screens.

New Features in ASA 9.8(1.200)

Released: July 30, 2017

Note This release is only supported on the ASA virtual for Microsoft Azure. These features are not supported in Version 9.8(2).

Feature	Description
High Availability and Scalability Features	
Active/Backup High Availability for ASA virtual on Microsoft Azure	A stateless Active/Backup solution that allows for a failure of the active ASA virtual to trigger an automatic failover of the system to the backup ASA virtual in the Microsoft Azure public cloud. We introduced the following commands: **failover cloud** No ASDM support.

New Features in ASDM 7.8(1.150)

Released: June 20, 2017

There are no new features in this release.

New Features in ASA 9.8(1)/ASDM 7.8(1)

Released: May 15, 2017

Feature	Description
Platform Features	
ASAv50 platform	The ASA virtual platform has added a high-end performance ASAv50 platform that provides 10 Gbps Firewall throughput levels. The ASAv50 requires ixgbe-vf vNICs, which are supported on VMware and KVM only.
SR-IOV on the ASA virtual platform	The ASA virtual platform supports Single Root I/O Virtualization (SR-IOV) interfaces, which allows multiple VMs to share a single PCIe network adapter inside a host. ASA virtual SR-IOV support is available on VMware, KVM, and AWS only.

Feature	Description
Automatic ASP load balancing now supported for the ASA virtual	Formerly, you could only manually enable and disable ASP load balancing. We modified the following command: **asp load-balance per-packet auto** We modified the following screen: **Configuration > Device Management > Advanced > ASP Load Balancing**
Firewall Features	
Support for setting the TLS proxy server SSL cipher suite	You can now set the SSL cipher suite when the ASA acts as a TLS proxy server. Formerly, you could only set global settings for the ASA using the **ssl cipher** command on the **Configuration** > **Device Management** > **Advanced** > **SSL Settings** > **Encryption** page. We introduced the following command: **server cipher-suite** We modified the following screen: **Configuration** > **Firewall** > **Unified Communications** > **TLS Proxy**, Add/Edit dialog boxes, **Server Configuration** page.
Global timeout for ICMP errors	You can now set the idle time before the ASA removes an ICMP connection after receiving an ICMP echo-reply packet. When this timeout is disabled (the default), and you enable ICMP inspection, then the ASA removes the ICMP connection as soon as an echo-reply is received; thus any ICMP errors that are generated for the (now closed) connection are dropped. This timeout delays the removal of ICMP connections so you can receive important ICMP errors. We added the following command: **timeout icmp-error** We modified the following screen: **Configuration** > **Firewall** > **Advanced** > **Global Timeouts**.
High Availability and Scalability Features	
Improved cluster unit health-check failure detection	You can now configure a lower holdtime for the unit health check: .3 seconds minimum. The previous minimum was .8 seconds. This feature changes the unit health check messaging scheme to *heartbeats* in the data plane from *keepalives* in the control plane. Using heartbeats improves the reliability and the responsiveness of clustering by not being susceptible to control plane CPU hogging and scheduling delays. Note that configuring a lower holdtime increases cluster control link messaging activity. We suggest that you analyze your network before you configure a low holdtime; for example, make sure a ping from one unit to another over the cluster control link returns within the *holdtime*/3, because there will be three heartbeat messages during one holdtime interval. If you downgrade your ASA software after setting the hold time to .3 - .7, this setting will revert to the default of 3 seconds because the new setting is unsupported. We modified the following commands: **health-check holdtime, show asp drop cluster counter, show cluster info health details** We modified the following screen: **Configuration** > **Device Management** > **High Availability and Scalability** > **ASA Cluster**

Feature	Description
Configurable debounce time to mark an interface as failed for the Firepower 4100/9300 chassis	You can now configure the debounce time before the ASA considers an interface to be failed, and the unit is removed from the cluster. This feature allows for faster detection of interface failures. Note that configuring a lower debounce time increases the chances of false-positives. When an interface status update occurs, the ASA waits the number of milliseconds specified before marking the interface as failed and the unit is removed from the cluster. The default debounce time is 500 ms, with a range of 300 ms to 9 seconds. New or modified command: **health-check monitor-interface debounce-time** New or modified screen: **Configuration** > **Device Management** > **High Availability and Scalability** > **ASA Cluster**
VPN Features	
Support for IKEv2, certificate based authentication, and ACL in VTI	Virtual Tunnel Interface (VTI) now supports BGP (static VTI). You can now use IKEv2 in standalone and high availability modes. You can use certificate based authentication by setting up a trustpoint in the IPsec profile. You can also apply access lists on VTI using access-group commands to filter ingress traffic. We introduced the following command in the IPsec profile configuration mode: **set trustpoint**. We introduced options to select the trustpoint for certificate based authentication in the following screen: **Configuration** > **Site-to-Site VPN** > **Advanced** > **IPsec Proposals (Transform Sets)** > **IPsec Profile** > **Add**
Mobile IKEv2 (MobIKE) is enabled by default	Mobile devices operating as remote access clients require transparent IP address changes while moving. Supporting MobIKE on ASA allows a current IKE security association (SA) to be updated without deleting the current SA. MobIKE is “always on.” We introduced the following command: **ikev2 mobike-rrc**. Used to enable/disable return routability checking.
SAML 2.0 SSO Updates	The default signing method for a signature in a SAML request changed from SHA1 to SHA2, and you can configure which signing method you prefer: rsa-sha1, rsa-sha256, rsa-sha384, or rsa-sha512. We changed the following command in webvpn mode: **saml idp signature** can be configured with a *value*. Disabled is still the default. We introduced changes to the following screen: **Configuration > Remote Access VPN > Clientless SSL VPN Access > Advanced > Single Sign On Servers > Add**.
Change for **tunnelgroup webvpn-attributes**	We changed the **pre-fill-username** and **secondary-pre-fill-username** value from **ssl-client** to **client**. We changed the following commands in webvpn mode: **pre-fill-username** and **secondary-pre-fill-username** can be configured with a **client** value.
AAA Features	

Feature	Description
Login history	By default, the login history is saved for 90 days. You can disable this feature or change the duration, up to 365 days. This feature only applies to usernames in the local database when you enable local AAA authentication for one or more of the management methods (SSH, ASDM, Telnet, and so on). We introduced the following commands: **aaa authentication login-history, show aaa login-history** We introduced the following screen: **Configuration** > **Device Management** > **Users/AAA** > **Login History**
Password policy enforcement to prohibit the reuse of passwords, and prohibit use of a password matching a username	You can now prohibit the reuse of previous passwords for up to 7 generations, and you can also prohibit the use of a password that matches a username. We introduced the following commands: **password-history, password-policy reuse-interval, password-policy username-check** We modified the following screen: **Configuration** > **Device Management** > **Users/AAA** > **Password Policy**
Separate authentication for users with SSH public key authentication and users with passwords	In releases prior to 9.6(2), you could enable SSH public key authentication (**ssh authentication**) without also explicitly enabling AAA SSH authentication with the Local user database (**aaa authentication ssh console LOCAL**). In 9.6(2), the ASA required you to explicitly enable AAA SSH authentication. In this release, you no longer have to explicitly enable AAA SSH authentication; when you configure the **ssh authentication** command for a user, local authentication is enabled by default for users with this type of authentication. Moreover, when you explicitly configure AAA SSH authentication, this configuration only applies for usernames with *passwords*, and you can use any AAA server type (**aaa authentication ssh console radius_1**, for example). For example, some users can use public key authentication using the local database, and other users can use passwords with RADIUS. We did not modify any commands. We did not modify any screens. *Also in Version 9.6(3).*
Monitoring and Troubleshooting Features	
Saving currently-running packet captures when the ASA crashes	Formerly, active packet captures were lost if the ASA crashed. Now, packet captures are saved to disk 0 at the time of the crash with the filename [*context_name*.]*capture_name*.**pcap**. We did not modify any commands. We did not modify any screens.

New Features in Version 9.7

New Features in ASDM 7.7(1.151)

Released: April 28, 2017

Note ASDM 7.7(1.150) was removed from Cisco.com due to bug CSCvd90344.

Feature	Description
Admin Features	
New background service for the ASDM upgrade tool	ASDM uses a new background service for **Tools > Check for ASA/ASDM Upgrades**. The older service used by earlier versions of ASDM will be discontinued by Cisco in the future.

New Features in ASA 9.7(1.4)/ASDM 7.7(1)

Released: April 4, 2017

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

Feature	Description
Platform Features	

Feature	Description
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**. We introduced the following screens: **Configuration** > **Device Management** > **Alarm Port** > **Alarm Contact** **Configuration** > **Device Management** > **Alarm Port** > **Redundant Power Supply** **Configuration** > **Device Management** > **Alarm Port** > **Temperature** **Monitoring** > **Properties** > **Alarm** > **Alarm Settings** **Monitoring** > **Properties** > **Alarm** > **Alarm Contact** **Monitoring** > **Properties** > **Alarm** > **Facility Alarm Status**
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 ASA virtual into Azure Security Center allows the ASA virtual 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** We introduced the following screens: **Configuration** > **Device Management** > **PTP** **Monitoring** > **Properties** > **PTP**

Feature	Description
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** We introduced the following screen: **Configuration** > **Device Management** > **Auto Backup & Restore Configuration**
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**. We did not modify any screens.
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**. We modified the following screens: **Configuration** > **Firewall** > **Objects** > **Inspection Maps** > **M3UA** Add/Edit dialog boxes.
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** We did not modify any screens.

Feature	Description
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** We modified the following screens: **Configuration** > **Device Setup** > **Interface Settings** > **Interfaces** **Configuration** > **Device Setup** > **Routing** > **Static Routes** **Configuration** > **Device Management** > **DHCP** > **DHCP Server** **Configuration** > **Firewall** > **Access Rules** **Configuration** > **Firewall** > **EtherType Rules**
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**. We added the following screen: **Configuration** > **Firewall** > **VM Atttribute Agent**
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**. We modified the following screen: **Configuration** > **Firewall** > **Advanced** > **Global Timeouts**.

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** We modified the following screens: **Configuration** > **Device Setup** > **Interface Settings** > **Interfaces** > **Add Interface** > **General**
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** We modified the following screen: **Configuration** > **Device Management** > **High Availability and Scalability** > **ASA Cluster** > **Cluster Configuration**

Feature	Description
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** We modified the following screen: **Configuration** > **Device Management** > **High Availability and Scalability** > **ASA Cluster** > **Cluster Configuration**
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** We modified the following screen: **Configuration** > **Device Management** > **High Availability and Scalability** > **Failover** > **Criteria**
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** We modified the following screen: **Configuration** > **Device Management** > **High Availability and Scalability** > **Failover** > **Setup**
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**. We modified the following screen: **Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPsec > Crypto Maps > Add/Edit > Tunnel Policy (Crypto Maps) - Advanced**

Feature	Description
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**. We introduced the following screens: **Configuration** > **Site-to-Site VPN** > **Advanced** > **IPsec Proposals (Transform Sets)** > **IPsec Profile** **Configuration** > **Site-to-Site VPN** > **Advanced** > **IPsec Proposals (Transform Sets)** > **IPsec Profile** > **Add** > **Add IPsec Profile** **Configuration** > **Device Setup** > **Interface Settings** > **Interfaces** > **Add** > **VTI Interface** **Configuration** > **Device Setup** > **Interface Settings** > **Interfaces** > **Add** > **VTI Interface** > **General** **Configuration** > **Device Setup** > **Interface Settings** > **Interfaces** > **Add** > **VTI Interface** > **Advanced**
SAML 2.0 based SSO for Secure Client	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** We modified the following screen: **Configuration > Remote Access VPN > Clientless SSL VPN Access > Advanced > Single Sign On Servers > Add SSO Server**.
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** We modified the following screens: **Configuration > Remote Access VPN > Certificate Management > Identity Certificates > Add an Identity Certificate**

Feature	Description
Multiple certificate authentication	You can now validate multiple certificates per session with Secure Client 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}** We modified the following screens: **Configuration > Remote Access VPN > Network (Client) Access > Dynamic Access Policies > Edit Secure Client Connection Profile** **Configuration > Remote Access VPN > Network Client Access > Secure Client Connection Profiles > Edit Secure Client Connection Profiles**
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.
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.
Secure Client: Maximum Connect Time Alert Interval is now supported in the Group Policy for AnyConnect VPN module of Cisco Secure 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 Secure Client connections: **vpn-session-timeout alert-interval** We modified the following screen: **Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Add/Edit > General > More Options**, adding a **Maximum Connect Time Alert Interval** field
AAA Features	

Feature	Description
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** We modified the following screen: **Configuration** > **Device Management** > **Users/AAA** > **AAA Server Groups** > **Add AAA Server Group**
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** We modified the following screens: **Configuration** > **Device Setup** > **Device Name/Password** > **Enable Password** **Configuration** > **Device Management** > **Users/AAA** > **User Accounts** > **Add/Edit User Account** > **Identity**
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	
IPv6 address support for traceroute	The **traceroute** command was modified to accept an IPv6 address. We modified the following command: **traceroute** We modified the following screen: **Tools** > **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** We added **VLAN ID** and **Destination MAC Address** fields in the packet-tracer screen:**Tools** > **Packet Tracer**
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** We modified the following screen: **Configuration** > **Device Management** > **Logging** > **Syslog Servers** > **Add Syslog Server**

Feature	Description
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** Added/Modified screens: **Wizards** > **Packet Capture Wizard** > **Run Captures** Added/Modified options: **Start** button, **Stop** button

New Features in Version 9.6

New Features in ASA 9.6(4)/ASDM 7.9(1)

Released: December 13, 2017

There are no new features in this release.

New Features in ASA 9.6(3.1)/ASDM 7.7(1)

Released: April 3, 2017

Note Version 9.6(3) was removed from Cisco.com due to bug CSCvd78303.

Feature	Description
AAA Features	

Feature	Description
Separate authentication for users with SSH public key authentication and users with passwords	In releases prior to 9.6(2), you could enable SSH public key authentication (**ssh authentication**) without also explicitly enabling AAA SSH authentication with the Local user database (**aaa authentication ssh console LOCAL**). In 9.6(2), the ASA required you to explicitly enable AAA SSH authentication. In this release, you no longer have to explicitly enable AAA SSH authentication; when you configure the **ssh authentication** command for a user, local authentication is enabled by default for users with this type of authentication. Moreover, when you explicitly configure AAA SSH authentication, this configuration only applies for for usernames with *passwords*, and you can use any AAA server type (**aaa authentication ssh console radius_1**, for example). For example, some users can use public key authentication using the local database, and other users can use passwords with RADIUS. We did not modify any commands. We did not modify any screens. *Also in Version 9.8(1).*

New Features in ASDM 7.6(2.150)

Released: October 12, 2016

There are no new features in this release.

New Features in ASA 9.6(2)/ASDM 7.6(2)

Released: August 24, 2016

Feature	Description
Platform Features	
ASA for the Firepower 4150	We introduced the ASA for the Firepower 4150. Requires FXOS 2.0.1. We did not add or modify any commands. We did not add or modify any screens.
Hot Plug Interfaces on the ASA virtual	You can add and remove Virtio virtual interfaces on the ASA virtual while the system is active. When you add a new interface to the ASA virtual, the virtual machine detects and provisions the interface. When you remove an existing interface, the virtual machine releases any resource associated with the interface. Hot plug interfaces are limited to Virtio virtual interfaces on the Kernel-based Virtual Machine (KVM) hypervisor.
Microsoft Azure support on the ASAv10	Microsoft Azure is a public cloud environment that uses a private Microsoft Hyper V Hypervisor. The ASA virtual runs as a guest in the Microsoft Azure environment of the Hyper V Hypervisor. The ASA virtual on Microsoft Azure supports one instance type, the Standard D3, which supports four vCPUs, 14 GB, and four interfaces. *Also in 9.5(2.200).*

Feature	Description
Through traffic support on the Management 0/0 interface for the ASA virtual	You can now allow through traffic on the Management 0/0 interface on the ASA virtual. Previously, only the ASA virtual on Microsoft Azure supported through traffic; now all ASA virtuals support through traffic. You can optionally configure this interface to be management-only, but it is not configured by default. We modified the following command: **management-only**
Common Criteria Certification	The ASA was updated to comply with the Common Criteria requirements. See the rows in this table for the following features that were added for this certification: • ASA SSL Server mode matching for ASDM • SSL client RFC 6125 support: • Reference Identities for Secure Syslog Server connections and Smart Licensing connections • ASA client checks Extended Key Usage in server certificates • Mutual authentication when ASA acts as a TLS client for TLS1.1 and 1.2 • PKI debug messages • Crypto Key Zeroization verification • IPsec/ESP Transport Mode Support for IKEv2 • New syslog messages
Firewall Features	
DNS over TCP inspection	You can now inspect DNS over TCP traffic (TCP/53). We added the following command: **tcp-inspection** We modified the following page: **Configuration** > **Firewall** > **Objects** > **Inspection Maps** > **DNS** Add/Edit dialog box
MTP3 User Adaptation (M3UA) inspection	You can now inspect M3UA traffic and also apply actions based on point code, service indicator, and message class and type. We added or modified the following commands: **clear service-policy inspect m3ua** {**drops** | **endpoint** [*IP_address*]}, **inspect m3ua**, **match dpc**, **match opc**, **match service-indicator**, **policy-map type inspect m3ua**, **show asp table classify domain inspect-m3ua**, **show conn detail**, **show service-policy inspect m3ua** {**drops** | **endpoint** *IP_address*}, **ss7 variant**, **timeout endpoint** We added or modified the following pages: **Configuration** > **Firewall** > **Objects** > **Inspection Maps** > **M3UA**; the **Rule Action** > **Protocol Inspection** tab for service policy rules

Feature	Description
Session Traversal Utilities for NAT (STUN) inspection	You can now inspect STUN traffic for WebRTC applications including Cisco Spark. Inspection opens pinholes required for return traffic. We added or modified the following commands: **inspect stun**, **show conn detail**, **show service-policy inspect stun** We added an option to the Rule Actions > Protocol Inspection tab of the Add/Edit Service Policy dialog box
Application layer health checking for Cisco Cloud Web Security	You can now configure Cisco Cloud Web Security to check the health of the Cloud Web Security application when determining if the server is healthy. By checking application health, the system can fail over to the backup server when the primary server responds to the TCP three-way handshake but cannot process requests. This ensures a more reliable system. We added the following commands: **health-check application url**, **health-check application timeout** We modified the following screen: **Configuration** > **Device Management** > **Cloud Web Security**
Connection holddown timeout for route convergence.	You can now configure how long the system should maintain a connection when the route used by the connection no longer exists or is inactive. If the route does not become active within this holddown period, the connection is freed. You can reduce the holddown timer to make route convergence happen more quickly. However, the 15 second default is appropriate for most networks to prevent route flapping. We added the following command: **timeout conn-holddown** We modified the following screen: **Configuration** > **Firewall** > **Advanced** > **Global Timeouts** *Also in 9.4(3).*
Changes in TCP option handling	You can now specify actions for the TCP MSS and MD5 options in a packet's TCP header when configuring a TCP map. In addition, the default handling of the MSS, timestamp, window-size, and selective-ack options has changed. Previously, these options were allowed, even if there were more than one option of a given type in the header. Now, packets are dropped by default if they contain more than one option of a given type. For example, previously a packet with 2 timestamp options would be allowed, now it will be dropped. You can configure a TCP map to allow multiple options of the same type for MD5, MSS, selective-ack, timestamp, and window-size. For the MD5 option, the previous default was to clear the option, whereas the default now is to allow it. You can also drop packets that contain the MD5 option. For the MSS option, you can set the maximum segment size in the TCP map (per traffic class). The default for all other TCP options remains the same: they are cleared. We modified the following command: **tcp-options** We modified the following screen: **Configuration** > **Firewall** > **Objects** > **TCP Maps** Add/Edit dialog box
Transparent mode maximum interfaces per bridge group increased to 64	The maximum interfaces per bridge group was increased from 4 to 64. We did not modify any commands. We did not modify any screens.

Feature	Description
Flow offload support for multicast connections in transparent mode.	You can now offload multicast connections to be switched directly in the NIC on transparent mode Firepower 4100 and 9300 series devices. Multicast offload is available for bridge groups that contain two and only two interfaces. There are no new commands or ASDM screens for this feature.
Customizable ARP rate limiting	You can set the maximum number of ARP packets allowed per second. The default value depends on your ASA model. You can customize this value to prevent an ARP storm attack. We added the following commands: **arp rate-limit, show arp rate-limit** We modified the following screen: **Configuration** > **Device Management** > **Advanced** > **ARP** > **ARP Static Table**
Ethertype rule support for the IEEE 802.2 Logical Link Control packet's Destination Service Access Point address.	You can now write Ethertype access control rules for the IEEE 802.2 Logical Link Control packet's Destination Service Access Point address. Because of this addition, the **bpdu** keyword no longer matches the intended traffic. Rewrite **bpdu** rules for **dsap 0x42**. We modified the following commands: **access-list ethertype** We modified the following screen: **Configuration** > **Firewall** > **EtherType Rules**.
Remote Access Features	
Pre-fill/Username-from-cert feature for multiple context mode	Secure Client SSL support is extended, allowing pre-fill/username-from-certificate feature CLIs, previously available only in single mode, to be enabled in multiple context mode as well. We did not modify any commands. We did not modify any screens.
Flash Virtualization for Remote Access VPN	Remote access VPN in multiple context mode now supports flash virtualization. Each context can have a private storage space and a shared storage place based on the total flash that is available: • Private storage—Store files associated only with that user and specific to the content that you want for that user. • Shared storage—Upload files to this space and have it accessible to any user context for read/write access once you enable it. We introduced the following commands: **limit-resource storage, storage-url** We modified the following screens: **Configuration** > **Context Management** > **Resource Class** > **Add Resource Class** **Configuration** > **Context Management** > **Security Contexts**
Secure Client profiles supported in multiple context mode	Secure Client profiles are supported in multiple context mode. To add a new profile using ASDM, you must have the Secure Client release 4.2.00748 or 4.3.03013 and later.
Stateful failover for Secure Client connections in multiple context mode	Stateful failover is now supported for Secure Client connections in multiple context mode. We did not modify any commands. We did not modify any screens.

Feature	Description
Remote Access VPN Dynamic Access Policy (DAP) is supported in multiple context mode	You can now configure DAP per context in multiple context mode. We did not modify any commands. We did not modify any screens.
Remote Access VPN CoA (Change of Authorization) is supported in multiple context mode	You can now configure CoA per context in multiple context mode. We did not modify any commands. We did not modify any screens.
Remote Access VPN localization is supported in multiple context mode	Localization is supported globally. There is only one set of localization files that are shared across different contexts. We did not modify any commands. We did not modify any screens.
Umbrella Roaming Security module support	You can choose to configure the Secure Client's Umbrella Roaming Security module for additional DNS-layer security when no VPN is active. We did not modify any commands. We modified the following screen: **Configuration > Remote Access VPN > Network (Client) Access >** Secure Client **Profile**.
IPsec/ESP Transport Mode Support for IKEv2	Transport mode is now supported for ASA IKEv2 negotiation. It can be used in place of tunnel (default) mode. Tunnel mode encapsulates the entire IP packet. Transport mode encapsulates only the upper-layer protocols of an IP packet. Transport mode requires that both the source and destination hosts support IPSec, and can only be used when the destination peer of the tunnel is the final destination of the IP packet. We modified the following command: **crypto map set ikev2 mode** We modified the following screen: **Configuration** > **Remote Access VPN > Network (Client) Access** > **Advanced** > **IPsec** > **IPsec Proposals (Transform Sets)** > **IKEv2 proposals** > **Add/Edit**
Per-packet routing lookups for IPsec inner packets	By default, per-packet adjacency lookups are done for outer ESP packets; lookups are not done for packets sent through the IPsec tunnel. In some network topologies, when a routing update has altered the inner packet's path, but the local IPsec tunnel is still up, packets through the tunnel may not be routed correctly and fail to reach their destination. To prevent this, use the new option to enable per-packet routing lookups for the IPsec inner packets. We added the following command: **crypto ipsec inner-routing-lookup** We modified the following screen: **Configuration** > **Remote Access VPN > Network (Client) Access** > **Advanced** > **IPsec** > **Crypto Maps** adding the **Enable IPsec Inner Routing Lookup** checkbox.
Certificate and Secure Connection Features	
ASA client checks Extended Key Usage in server certificates	Syslog and Smart licensing Server Certificates must contain "ServerAuth" in the Extended Key Usage field. If not, the connection fails.

Feature	Description
Mutual authentication when ASA acts as a TLS client for TLS1.1 and 1.2	If the server requests a client certificate from the ASA for authentication, the ASA will send the client identity certificate configured for that interface. The certificate is configured by the **ssl trust-point** command.
PKI debug messages	The ASA PKI module makes connections to CA servers such as SCEP enrollment, revocation checking using HTTP, etc. All of these ASA PKI exchanges will be logged as debug traces under debug crypto ca message 5.
ASA SSL Server mode matching for ASDM	For an ASDM user who authenticates with a certificate, you can now require the certificate to match a certificate map. We modified the following command: **http authentication-certificate match** We modified the following screen: **Configuration** > **Device Management** > **Management Access** > **ASDM/HTTPS/Telnet/SSH**
Reference Identities for Secure Syslog Server connections and Smart Licensing connections	TLS client processing now supports rules for verification of a server identity defined in RFC 6125, Section 6. Identity verification will be done during PKI validation for TLS connections to the Syslog Server and the Smart Licensing server only. If the presented identity cannot be matched against the configured reference identity, the connection is not established. We added or modified the following commands: **crypto ca reference-identity, logging host, call home profile destination address** We modifed the following screens: **Configuration** > **Remote Access VPN** > **Advanced** **Configuration** > **Device Management** > **Logging** > **Syslog Servers** > **Add/Edit** **Configuration** > **Device Management** > **Smart Call Home**
Crypto Key Zeroization verification	The ASA crypto system has been updated to comply with new key zeroization requirements. Keys must be overwritten with all zeros and then the data must be read to verify that the write was successful.
SSH public key authentication improvements	In earlier releases, you could enable SSH public key authentication (**ssh authentication**) without also enabling AAA SSH authentication with the Local user database (**aaa authentication ssh console LOCAL**). The configuration is now fixed so that you must explicitly enable AAA SSH authentication. To disallow users from using a password instead of the private key, you can now create a username without any password defined. We modified the following commands: **ssh authentication, username** We modifed the following screens: **Configuration** > **Device Management** > **Management Access** > **ASDM/HTTPS/Telnet/SSH** **Configuration** > **Device Management** > **Users/AAA** > **User Accounts** > **Add/Edit User Account**
Interface Features	

Feature	Description
Increased MTU size for the ASA on the Firepower 4100/9300 chassis	You can set the maximum MTU to 9188 bytes on the Firepower 4100 and 9300; formerly, the maximum was 9000 bytes. This MTU is supported with FXOS 2.0.1.68 and later. We modified the following command: **mtu** We modified the following screen: **Configuration** > **Device Setup** > **Interface Settings** > **Interfaces** > **Advanced**
Routing Features	
Bidirectional Forwarding Detection (BFD) Support	The ASA now supports the BFD routing protocol. Support was added for configuring BFD templates, interfaces, and maps. Support for BGP routing protocol to use BFD was also added. We added or modified the following commands: **authentication, bfd echo, bfd interval, bfd map, bfd slow-timers, bfd template, bfd-template, clear bfd counters, echo, debug bfd, neighbor fall-over bfd, show bfd drops, show bfd map, show bfd neighbors, show bfd summary** We added or modified the following screens: **Configuration** > **Device Setup** > **Routing** > **BFD** > **Template** **Configuration** > **Device Setup** > **Routing** > **BFD** > **Interface** **Configuration** > **Device Setup** > **Routing** > **BFD** > **Map** **Configuration** > **Device Setup** > **Routing** > **BGP** > **IPv6 Family** > **Neighbors**

Feature	Description
IPv6 DHCP	The ASA now supports the following features for IPv6 addressing: • DHCPv6 Address client—The ASA obtains an IPv6 global address and optional default route from the DHCPv6 server. • DHCPv6 Prefix Delegation client—The ASA obtains delegated prefix(es) from a DHCPv6 server. The ASA can then use these prefixes to configure other ASA interface addresess so that StateLess Address Auto Configuration (SLAAC) clients can autoconfigure IPv6 addresses on the same network. • BGP router advertisement for delegated prefixes • DHCPv6 stateless server—The ASA provides other information such as the domain name to SLAAC clients when they send Information Request (IR) packets to the ASA. The ASA only accepts IR packets, and does not assign addresses to the clients. We added or modified the following commands: **clear ipv6 dhcp statistics, domain-name, dns-server, import, ipv6 address autoconfig, ipv6 address dhcp, ipv6 dhcp client pd, ipv6 dhcp client pd hint, ipv6 dhcp pool, ipv6 dhcp server, network, nis address, nis domain-name, nisp address, nisp domain-name, show bgp ipv6 unicast, show ipv6 dhcp, show ipv6 general-prefix, sip address, sip domain-name, sntp address** We added or modified the following screens: **Configuration** > **Device Setup** > **Interface Settings** > **Interfaces** > **Add Interface** > **IPv6** **Configuration** > **Device Management** > **DHCP** > **DHCP Pool** **Configuration** > **Device Setup** > **Routing** > **BGP** > **IPv6 Family** > **Networks** **Monitoring** > **interfaces** > **DHCP**
High Availability and Scalability Features	
Improved sync time for dynamic ACLs from Secure Client when using Active/Standby failover	When you use Secure Client on a failover pair, then the sync time for the associated dynamic ACLs (dACLs) to the standby unit is now improved. Previously, with large dACLs, the sync time could take hours during which time the standby unit is busy syncing instead of providing high availability backup. We did not modify any commands. We did not modify any screens.
Licensing Features	

Feature	Description
Permanent License Reservation for the ASA virtual	For highly secure environments where communication with the Cisco Smart Software Manager is not allowed, you can request a permanent license for the ASA virtual. In 9.6(2), we also added support for this feature for the ASA virtual on Amazon Web Services. This feature is not supported for Microsoft Azure. **Note** Not all accounts are approved for permanent license reservation. Make sure you have approval from Cisco for this feature before you attempt to configure it. We introduced the following commands: **license smart reservation, license smart reservation cancel, license smart reservation install, license smart reservation request universal, license smart reservation return** No ASDM support. *Also in 9.5(2.200).*
Satellite Server support for the ASA virtual	If your devices cannot access the internet for security reasons, you can optionally install a local Smart Software Manager satellite server as a virtual machine (VM). We did not modify any commands. We did not modify any screens.
Permanent License Reservation for the ASA virtual Short String enhancement	Due to an update to the Smart Agent (to 1.6.4), the request and authorization codes now use shorter strings. We did not modify any commands. We did not modify any screens.
Permanent License Reservation for the ASA on the Firepower 4100/9300 chassis	For highly secure environments where communication with the Cisco Smart Software Manager is not allowed, you can request a permanent license for the ASA on the Firepower 9300 and Firepower 4100. All available license entitlements are included in the permanent license, including the Standard Tier, Strong Encryption (if qualified), Security Contexts, and Carrier licenses. Requires FXOS 2.0.1. All configuration is performed on the Firepower 4100/9300 chassis; no configuration is required on the ASA.

Feature	Description
Smart Agent Upgrade for ASA virtual to v1.6	The smart agent was upgraded from Version 1.1 to Version 1.6. This upgrade supports permanent license reservation and also supports setting the Strong Encryption (3DES/AES) license entitlement according to the permission set in your license account. **Note** If you downgrade from Version 9.5(2.200), the ASA virtual does not retain the licensing registration state. You need to re-register with the **license smart register idtoken** *id_token* **force** command**Configuration > Device Management > Licensing > Smart Licensing** page with the **Force registration** option; obtain the ID token from the Smart Software Manager. We introduced the following commands: **show license status, show license summary, show license udi, show license usage** We modified the following commands: **show license all, show tech-support license** We deprecated the following commands: **show license cert, show license entitlement, show license pool, show license registration** We did not change any screens. *Also in 9.5(2.200).*
Monitoring Features	
Packet capture of type asp-drop supports ACL and match filtering	When you create a packet capture of type asp-drop, you can now also specify an ACL or match option to limit the scope of the capture. We modified the following command: **capture type asp-drop** We did not modify any screens.
Forensic Analysis enhancements	You can create a core dump of any process running on the ASA. The ASA also extracts the text section of the main ASA process that you can copy from the ASA for examination. We modified the following commands: **copy system:text, verify system:text, crashinfo force dump process** We did not modify any screens.
Tracking Packet Count on a Per-Connection Basis through NetFlow	Two counters were added that allow Netflow users to see the number of Layer 4 packets being sent in both directions on a connection. You can use these counters to determine average packet rates and sizes and to better predict traffic types, anomalies, and events. We did not modify any commands. We did not modify any screens.

Feature	Description
SNMP engineID sync for Failover	In a failover pair, the SNMP engineIDs of the paired ASAs are synced on both units. Three sets of engineIDs are maintained per ASA—synced engineID, native engineID and remote engineID. An SNMPv3 user can also specify the engineID of the ASA when creating a profile to preserve localized **snmp-server user** authentication and privacy options. If a user does not specify the native engineID, the **show running config** output will show two engineIDs per user. We modified the following command: **snmp-server user** No ASDM support. *Also in 9.4(3).*

New Features in ASA 9.6(1)/ASDM 7.6(1)

Released: March 21, 2016

Note The ASAv 9.5.2(200) features, including Microsoft Azure support, are not available in 9.6(1). They are available in 9.6(2).

Feature	Description
Platform Features	
ASA for the Firepower 4100 series	We introduced the ASA for the Firepower 4110, 4120, and 4140. Requires FXOS 1.1.4. We did not add or modify any commands. We did not add or modify any screens.
SD card support for the ISA 3000	You can now use an SD card for external storage on the ISA 3000. The card appears as disk3 in the ASA file system. Note that plug and play support requires hardware version 2.1 and later. Use the **show module** command to check your hardware version. We did not add or modify any commands. We did not add or modify any screens.
Dual power supply support for the ISA 3000	For dual power supplies in the ISA 3000, you can establish dual power supplies as the expected configuration in the ASA OS. If one power supply fails, the ASA issues an alarm. By default, the ASA expects a single power supply and won't issue an alarm as long as it includes one working power supply. We introduced the following command: **power-supply dual**. No ASDM support.
Firewall Features	

Feature	Description
Diameter inspection improvements	You can now inspect Diameter over TCP/TLS traffic, apply strict protocol conformance checking, and inspect Diameter over SCTP in cluster mode. We introduced or modified the following commands: **client clear-text**, **inspect diameter**, **strict-diameter**. We added or modified the following screens: **Configuration** > **Firewall** > **Objects** > **Inspect Maps** > **Diameter** **Configuration** > **Firewall** > **Service Policy** add/edit wizard's **Rule Actions** > **Protocol Inspection** tab
SCTP stateful inspection in cluster mode	SCTP stateful inspection now works in cluster mode. You can also configure SCTP stateful inspection bypass in cluster mode. We did not add or modify any commands. We did not add or modify any screens.
H.323 inspection support for the H.255 FACILITY message coming before the H.225 SETUP message for H.460.18 compatibility.	You can now configure an H.323 inspection policy map to allow for H.225 FACILITY messages to come before the H.225 SETUP message, which can happen when endpoints comply with H.460.18. We introduced the following command: **early-message**. We added an option to the Call Attributes tab in the H.323 inspection policy map.
Cisco Trustsec support for Security Exchange Protocol (SXP) version 3.	Cisco Trustsec on ASA now implements SXPv3, which enables SGT-to-subnet bindings, which are more efficient than host bindings. We introduced or modified the following commands: **cts sxp mapping network-map** *maximum_hosts*, **cts role-based sgt-map**, **show cts sgt-map**, **show cts sxp sgt-map**, **show asp table cts sgt-map**. We modified the following screens: **Configuration** > **Firewall** > **Identity By TrustSec** and the **SGT Map Setup** dialog boxes.
Flow off-load support for the Firepower 4100 series.	You can identify flows that should be off-loaded from the ASA and switched directly in the NIC for the Firepower 4100 series. Requires FXOS 1.1.4. We did not add or modify any commands. We did not add or modify any screens.
Remote Access Features	
IKEv2 Fragmentation, RFC-7383 support	The ASA now supports this standard fragmentation of IKEv2 packets. This allows interoperability with other IKEv2 implementations such as Apple, Strongswan etc. ASA continues to support the current, proprietary IKEv2 fragmentation to maintain backward compatibility with Cisco products that do not support RFC-7383, such as the Secure Client. We introduced the following commands: **crypto ikev2 fragmentation**, **show running-config crypto ikev2**, **show crypto ikev2 sa detail**

Feature	Description
VPN Throughput Performance Enhancements on Firepower 9300 and Firepower 4100 series	The **crypto engine accelerator-bias** command is now supported on the ASA security module on the Firepower 9300 and Firepower 4100 series. This command lets you "bias" more crypto cores toward either IPSec or SSL. We modified the following command: **crypto engine accelerator-bias** We did not add or modify any screens.
Configurable SSH encryption and HMAC algorithm.	Users can select cipher modes when doing SSH encryption management and can configure HMAC and encryption for varying key exchange algorithms. You might want to change the ciphers to be more or less strict, depending on your application. Note that the performance of secure copy depends partly on the encryption cipher used. By default, the ASA negotiates one of the following algorithms in order: 3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr. If the first algorithm proposed (3des-cbc) is chosen, then the performance is much slower than a more efficient algorithm such as aes128-cbc. To change the proposed ciphers, use **ssh cipher encryption custom aes128-cbc**, for example. We introduced the following commands: **ssh cipher encryption, ssh cipher integrity**. We introduced the following screen: **Configuration** > **Device Management** > **Advanced** > **SSH Ciphers** *Also available in 9.1(7), 9.4(3), and 9.5(3).*
HTTP redirect support for IPv6	When you enable HTTP redirect to HTTPS for ASDM access or clientless SSL VPN, you can now redirect traffic sent an to IPv6 address. We added functionality to the following command: **http redirect** We added functionality to the following screen: **Configuration** > **Device Management** > **HTTP Redirect** *Also available in 9.1(7) and 9.4(3).*
Routing Features	

Feature	Description
IS-IS routing	The ASA now supports the Intermediate System to Intermediate System (IS-IS) routing protocol. Support was added for routing data, performing authentication, and redistributing and monitoring routing information using the IS-IS routing protocol. We introduced the following commands: **advertise passive-only, area-password, authentication key, authentication mode, authentication send-only, clear isis, debug isis, distance, domain-password, fast-flood, hello padding, hostname dynamic, ignore-lsp-errors, isis adjacency-filter, isis advertise prefix, isis authentication key, isis authentication mode, isis authentication send-only, isis circuit-type, isis csnp-interval, isis hello-interval, isis hello-multiplier, isis hello padding, isis lsp-interval, isis metric, isis password, isis priority, isis protocol shutdown, isis retransmit-interval, isis retransmit-throttle-interval, isis tag, is-type, log-adjacency-changes, lsp-full suppress, lsp-gen-interval, lsp-refresh-interval, max-area-addresses, max-lsp-lifetime, maximum-paths, metric, metric-style, net, passive-interface, prc-interval, protocol shutdown, redistribute isis, route priority high, route isis, set-attached-bit, set-overload-bit, show clns, show isis, show router isis, spf-interval, summary-address.** We introduced the following screens: **Configuration > Device Setup > Routing > ISIS** **Monitoring > Routing > ISIS**
High Availability and Scalability Features	
Support for site-specific IP addresses in Routed, Spanned EtherChannel mode	For inter-site clustering in routed mode with Spanned EtherChannels, you can now configure site-specific IP addresess in addition to site-specific MAC addresses. The addition of site IP addresses allows you to use ARP inspection on the Overlay Transport Virtualization (OTV) devices to prevent ARP responses from the global MAC address from traveling over the Data Center Interconnect (DCI), which can cause routing problems. ARP inspection is required for some switches that cannot use VACLs to filter MAC addresses. We modified the following commands: **mac-address, show interface** We modified the following screen: **Configuration** > **Device Setup** > **Interface Settings** > **Interfaces** > **Add/Edit EtherChannel Interface** > **Advanced**
Administrative Features	
Longer password support for local **username** and **enable** passwords (up to 127 characters)	You can now create local **username** and **enable** passwords up to 127 characters (the former limit was 32). When you create a password longer than 32 characters, it is stored in the configuration using a PBKDF2 (Password-Based Key Derivation Function 2) hash. Shorter passwords continue to use the MD5-based hashing method. We modified the following commands: **enable, username** We modified the following screens: **Configuration** > **Device Setup** > **Device Name/Password** > **Enable Password** **Configuration** > **Device Management** > **Users/AAA** > **User Accounts** > **Add/Edit User Account** > **Identity**

Feature	Description
Support for the cempMemPoolTable in the CISCO-ENHANCED-MEMPOOL-MIB	The cempMemPoolTable of the CISCO-ENHANCED-MEMPOOL-MIB is now supported. This is a table of memory pool monitoring entries for all physical entities on a managed system. **Note** The CISCO-ENHANCED-MEMPOOL-MIB uses 64-bit counters and supports reporting of memory on platforms with more than 4GB of RAM. We did not add or modify any commands. We did not add or modify any screens. *Also available in 9.1(7) and 9.4(3).*
REST API Version 1.3.1	We added support for the REST API Version 1.3.1.

New Features in Version 9.5

New Features in ASA 9.5(3.9)/ASDM 7.6(2)

Released: April 11, 2017

Note Verion 9.5(3) was removed from Cisco.com due to bug CSCvd78303.

Feature	Description
Remote Access Features	
Configurable SSH encryption and HMAC algorithm.	Users can select cipher modes when doing SSH encryption management and can configure HMAC and encryption for varying key exchange algorithms. You might want to change the ciphers to be more or less strict, depending on your application. Note that the performance of secure copy depends partly on the encryption cipher used. By default, the ASA negotiates one of the following algorithms in order: 3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr. If the first algorithm proposed (3des-cbc) is chosen, then the performance is much slower than a more efficient algorithm such as aes128-cbc. To change the proposed ciphers, use **ssh cipher encryption custom aes128-cbc**, for example. We introduced the following commands: **ssh cipher encryption, ssh cipher integrity**. We introduced the following screen: **Configuration** > **Device Management** > **Advanced** > **SSH Ciphers** *Also available in 9.1(7) and 9.4(3).*

New Features in ASA Virtual 9.5(2.200)/ASDM 7.5(2.153)

Released: January 28, 2016

Note This release supports only the ASA virtual.

Feature	Description
Platform Features	
Microsoft Azure support on the ASAv10	Microsoft Azure is a public cloud environment that uses a private Microsoft Hyper V Hypervisor. The ASA virtual runs as a guest in the Microsoft Azure environment of the Hyper V Hypervisor. The ASA virtual on Microsoft Azure supports one instance type, the Standard D3, which supports four vCPUs, 14 GB, and four interfaces.
Licensing Features	
Permanent License Reservation for the ASA virtual	For highly secure environments where communication with the Cisco Smart Software Manager is not allowed, you can request a permanent license for the ASA virtual. **Note** Not all accounts are approved for permanent license reservation. Make sure you have approval from Cisco for this feature before you attempt to configure it. We introduced the following commands: **license smart reservation, license smart reservation cancel, license smart reservation install, license smart reservation request universal, license smart reservation return** No ASDM support.
Smart Agent Upgrade to v1.6	The smart agent was upgraded from Version 1.1 to Version 1.6. This upgrade supports permanent license reservation and also supports setting the Strong Encryption (3DES/AES) license entitlement according to the permission set in your license account. **Note** If you downgrade from Version 9.5(2.200), the ASA virtual does not retain the licensing registration state. You need to re-register with the **license smart register idtoken** *id_token* **force** command**Configuration > Device Management > Licensing > Smart Licensing** page with the **Force registration** option; obtain the ID token from the Smart Software Manager. We introduced the following commands: **show license status, show license summary, show license udi, show license usage** We modified the following commands: **show license all, show tech-support license** We deprecated the following commands: **show license cert, show license entitlement, show license pool, show license registration** We did not change any screens.

New Features in ASA 9.5(2.1)/ASDM 7.5(2)

Released: December 14, 2015

Note This release supports only the ASA on the Firepower 9300.

Feature	Description
Platform Features	
VPN support for the ASA on the Firepower 9300	With FXOS 1.1.3, you can now configure VPN features.
Firewall Features	
Flow off-load for the ASA on the Firepower 9300	You can identify flows that should be off-loaded from the ASA and switched directly in the NIC (on the Firepower 9300). This provides improved performance for large data flows in data centers. Also requires FXOS 1.1.3. We added or modified the following commands: **clear flow-offload**, **flow-offload enable**, **set-connection advanced-options flow-offload**, **show conn detail**, **show flow-offload**. We added or modified the following screens: **Configuration** > **Firewall** > **Advanced** > **Offload Engine**, the **Rule Actions** > **Connection Settings** tab when adding or editing rules under **Configuration** > **Firewall** > **Service Policy Rules**.
High Availability Features	
Inter-chassis clustering for 6 modules, and inter-site clustering for the ASA on the Firepower 9300	With FXOS 1.1.3, you can now enable inter-chassis, and by extension inter-site clustering. You can include up to 6 modules in up to 6 chassis. We did not modify any commands. We did not modify any screens.
Licensing Features	
Strong Encryption (3DES) license automatically applied for the ASA on the Firepower 9300	For regular Cisco Smart Software Manager users, the Strong Encryption license is automatically enabled for qualified customers when you apply the registration token on the Firepower 9300. **Note** If you are using the Smart Software Manager satellite deployment, to use ASDM and other strong encryption features, after you deploy the ASA you must enable the Strong Encryption (3DES) license using the ASA CLI. This feature requires FXOS 1.1.3. We removed the following command for non-satellite configurations: **feature strong-encryption** We modified the following screen: **Configuration** > **Device Management** > **Licensing** > **Smart License**

New Features in ASA 9.5(2)/ASDM 7.5(2)

Released: November 30, 2015

Feature	Description
Platform Features	
Cisco ISA 3000 Support	The Cisco ISA 3000 is a DIN Rail mounted, ruggedized, industrial security appliance. It is low-power, fan-less, with Gigabit Ethernet and a dedicated management port. This model comes with the ASA Firepower module pre-installed. Special features for this model include a customized transparent mode default configuration, as well as a hardware bypass function to allow traffic to continue flowing through the appliance when there is a loss of power. We introduced the following command: **hardware-bypass, hardware-bypass manual, hardware-bypass boot-delay** We modified the following screen: **Configuration** > **Device Management** > **Hardware Bypass** *Also in Version 9.4(1.225).*
Firewall Features	
DCERPC inspection improvements and UUID filtering	DCERPC inspection now supports NAT for OxidResolver ServerAlive2 opnum5 messages. You can also now filter on DCERPC message universally unique identifiers (UUIDs) to reset or log particular message types. There is a new DCERPC inspection class map for UUID filtering. We introduced the following command: **match** [**not**] **uuid**. We modified the following command: **class-map type inspect**. We added the following screen: **Configuration** > **Firewall** > **Objects** > **Class Maps** > **DCERPC**. We modified the following screen: **Configuration** > **Firewall** > **Objects** > **Inspect Maps** > **DCERPC**.
Diameter inspection	You can now inspect Diameter traffic. Diameter inspection requires the Carrier license. We introduced or modified the following commands: **class-map type inspect diameter**, **diameter**, **inspect diameter**, **match application-id**, **match avp**, **match command-code**, **policy-map type inspect diameter**, **show conn detail**, **show diameter**, **show service-policy inspect diameter**, **unsupported** We added or modified the following screens: **Configuration** > **Firewall** > **Objects** > **Inspect Maps** > **Diameter** and **Diameter AVP** **Configuration** > **Firewall** > **Service Policy** add/edit wizard's **Rule Actions** > **Protocol Inspection** tab

Feature	Description
SCTP inspection and access control	You can now use the SCTP protocol and port specifications in service objects, access control lists (ACLs) and access rules, and inspect SCTP traffic. SCTP inspection requires the Carrier license. We introduced the following commands: **access-list extended** , **clear conn protocol sctp**, **inspect sctp**, **match ppid**, **nat static** (object), **policy-map type inspect sctp**, **service-object**, **service**, **set connection advanced-options sctp-state-bypass**, **show conn protocol sctp**, **show local-host connection sctp**, **show service-policy inspect sctp**, **timeout sctp** We added or modified the following screens: **Configuration** > **Firewall** > **Access Rules** add/edit dialogs **Configuration** > **Firewall** > **Advanced** > **ACL Manager** add/edit dialogs **Configuration** > **Firewall** > **Advanced** > **Global Timeouts** **Configuration** > **Firewall** > **NAT** add/edit static network object NAT rule, **Advanced NAT Settings** dialog box **Configuration** > **Firewall** > **Objects** > **Service Objects/Groups** add/edit dialogs **Configuration** > **Firewall** > **Objects** > **Inspect Maps** > **SCTP** **Configuration** > **Firewall** > **Service Policy** add/edit wizard' s **Rule Actions** > **Protocol Inspection** and **Connection Settings** tabs
Carrier Grade NAT enhancements now supported in failover and ASA clustering	For carrier-grade or large-scale PAT, you can allocate a block of ports for each host, rather than have NAT allocate one port translation at a time (see RFC 6888). This feature is now supported in failover and ASA cluster deployments. We modified the following command: **show local-host** We did not modify any screens.
Captive portal for active authentication on ASA FirePOWER 6.0.	The captive portal feature is required to enable active authentication using identity policies starting with ASA FirePOWER 6.0. We introduced or modified the following commands: **captive-portal**, **clear configure captive-portal**, **show running-config captive-portal**.
High Availability Features	

Feature	Description
LISP Inspection for Inter-Site Flow Mobility	Cisco Locator/ID Separation Protocol (LISP) architecture separates the device identity from its location into two different numbering spaces, making server migration transparent to clients. The ASA can inspect LISP traffic for location changes and then use this information for seamless clustering operation; the ASA cluster members inspect LISP traffic passing between the first hop router and the egress tunnel router (ETR) or ingress tunnel router (ITR), and then change the flow owner to be at the new site. We introduced or modified the following commands: **allowed-eid, clear cluster info flow-mobility counters, clear lisp eid, cluster flow-mobility lisp, debug cluster flow-mobility, debug lisp eid-notify-intercept, flow-mobility lisp, inspect lisp, policy-map type inspect lisp, site-id, show asp table classify domain inspect-lisp, show cluster info flow-mobility counters, show conn, show lisp eid, show service-policy, validate-key** We introduced or modified the following screens: **Configuration** > **Device Management** > **High Availability and Scalability** > **ASA Cluster** > **Cluster Configuration** **Configuration** > **Firewall** > **Objects** > **Inspect Maps** > **LISP** **Configuration** > **Firewall** > **Service Policy Rules** > **Protocol Inspection** **Configuration** > **Firewall** > **Service Policy Rules** > **Cluster** **Monitoring** > **Routing** > **LISP-EID Table**
ASA 5516-X support for clustering	The ASA 5516-X now supports 2-unit clusters. Clustering for 2 units is enabled by default in the base license. We did not modify any commands. We did not modify any screens.
Configurable level for clustering trace entries	By default, all levels of clustering events are included in the trace buffer, including many low level events. To limit the trace to higher level events, you can set the minimum trace level for the cluster. We introduced the following command: **trace-level** We did not modify any screens.
Interface Features	
Support to map Secondary VLANs to a Primary VLAN	You can now configure one or more secondary VLANs for a subinterface. When the ASA receives traffic on the secondary VLANs, it maps the traffic to the primary VLAN. We introduced or modified the following commands: **vlan secondary, show vlan mapping** We modified the following screens: **Configuration** > **Device Setup** > **Interface Settings** > **Interfaces** **Configuration** > **Device Setup** > **Interface Settings** > **Interfaces** > **Add Interface** > **General**
Routing Features	

Feature	Description
PIM Bootstrap Router (BSR) support for multicast routing	The ASA currently supports configuring static RPs to route multicast traffic for different groups. For large complex networks where multiple RPs could exist, the ASA now supports dynamic RP selection using PIM BSR to support mobility of RPs. We introduced the following commands: **clear pim group-map, debug pim bsr, pim bsr-border, pim bsr-candidate, show pim bsr-router, show pim group-map rp-timers** We introduced the following screen: **Configuration** > **Device Setup** > **Routing** > **Multicast** > **PIM** > **Bootstrap Router**
Remote Access Features	
Support for Remote Access VPN in multiple context mode	You can now use the following remote access features in multiple context mode: • AnyConnect 3.x and later (SSL VPN only; no IKEv2 support) • Centralized Secure Client image configuration • Secure Client image upgrade • Context Resource Management for Secure Client connections **Note** The Secure Client Premier license is required for multiple context mode; you cannot use the default or legacy license. We introduced the following commands: **limit-resource vpn anyconnect, limit-resource vpn burst anyconnect** We modified the following screen: **Configuration** > **Context Management** > **Resource Class** > **Add Resource Class**
Clientless SSL VPN offers SAML 2.0-based Single Sign-On (SSO) functionality	The ASA acts as a SAML Service Provider.
Clientless SSL VPN conditional debugging	You can debug logs by filtering, based on the filter condition sets, and can then better analyze them. We introduced the following additions to the debug command: • [no] debug webvpn condition user <user name> • [no] debug webvpn condition group <group name> • [no] debug webvpn condition p-ipaddress <ipv4> [subnet<mask>] • [no] debug webvpn condition p-ipaddress <ipv6> [prefix<prefix>] • debug webvpn condition reset • show debug webvpn condition • show webvpn debug-condition

Feature	Description
Clientless SSL VPN cache disabled by default	The clientless SSL VPN cache is now disabled by default. Disabling the clientless SSL VPN cache provides better stability. If you want to enable the cache, you must manually enable it. `webvpn` `  cache` `  no disable` We modified the following command: **cache** We modified the following screen: **Configuration** > **Remote Access VPN** > **Clientless SSL VPN Access** > **Advanced** > **Content Cache**
Licensing Features	
Validation of the Smart Call Home/Smart Licensing certificate if the issuing hierarchy of the server certificate changes	Smart licensing uses the Smart Call Home infrastructure. When the ASA first configures Smart Call Home anonymous reporting in the background, it automatically creates a trustpoint containing the certificate of the CA that issued the Smart Call Home server certificate. The ASA now supports validation of the certificate if the issuing hierarchy of the server certificate changes; you can enable the automatic update of the trustpool bundle at periodic intervals. We introduced the following command: **auto-import** We modified the following screen: **Configuration** > **Remote Access VPN** > **Certificate Management** > **Trusted Certificate Pool** > **Edit Policy**
New Carrier license	The new Carrier license replaces the existing GTP/GPRS license, and also includes support for SCTP and Diameter inspection. For the ASA on the Firepower 9300, the **feature mobile-sp** command will automatically migrate to the **feature carrier** command. We introduced or modified the following commands: **feature carrier, show activation-key, show license, show tech-support, show version** We modified the following screen: **Configuration** > **Device Management** > **Licensing** > **Smart License**
Monitoring Features	
SNMP engineID sync	In an HA pair, the SNMP engineIDs of the paired ASAs are synced on both units. Three sets of engineIDs are maintained per ASA—synced engineID, native engineID and remote engineID. An SNMPv3 user can also specify the engineID of the ASA when creating a profile to preserve localized **snmp-server user** authentication and privacy options. If a user does not specify the native engineID, the **show running config** output will show two engineIDs per user. We modified the following commands: **snmp-server user, no snmp-server user** We did not add or modify any screens. *Also available in 9.4(3).*

Feature	Description
show tech support enhancements	The **show tech support** command now: • Includes **dir all-filesystems** output—This output can be helpful in the following cases: • SSL VPN configuration: check if the required resources are on the ASA • Crash: check for the date timestamp and presence of a crash file • Removes the **show kernel cgroup-controller detail** output—This command output will remain in the output of **show tech-support detail**. We modified the following command: **show tech support** We did not add or modify any screens. *Also available in 9.1(7) and 9.4(3).*
logging debug-trace persistence	Formerly, when you enabled **logging debug-trace** to redirect debugs to a syslog server, if the SSH connection were disconnected (due to network connectivity or timeout), then the debugs were removed. Now, debugs persist for as long as the **logging** command is in effect. We modified the following command: **logging debug-trace** We did not modify any screens.

New Features in ASA 9.5(1.5)/ASDM 7.5(1.112)

Released: November 11, 2015

Feature	Description
Platform Features	
Support for ASA FirePOWER 6.0	The 6.0 software version for the ASA FirePOWER module is supported on all previously supported device models.
Support for managing the ASA FirePOWER module through ASDM for the 5512-X through 5585-X.	You can manage the ASA FirePOWER module using ASDM instead of using management center (formerly FireSIGHT Management Center) when running version 6.0 on the module. You can still use ASDM to manage the module on the 5506-X, 5506H-X, 5506W-X, 5508-X, and 5516-X when running 6.0. No new screens or commands were added.

New Features in ASDM 7.5(1.90)

Released: October 14, 2015

Feature	Description
Remote Access Features	

Feature	Description
AnyConnect Version 4.2 support	ASDM supports AnyConnect 4.2 and the Network Visibility Module (NVM). NVM enhances the enterprise administrator's ability to do capacity and service planning, auditing, compliance, and security analytics. The NVM collects the endpoint telemetry and logs both the flow data and the file reputation in the syslog and also exports the flow records to a collector (a third-party vendor), which performs the file analysis and provides a UI interface. We modified the following screen: **Configuration > Remote Access VPN > Network (Client) Access > Secure Client Profile** (a new profile called **Network Visibility Service Profile**)

New Features in ASA Virtual 9.5(1.200)/ASDM 7.5(1)

Released: August 31, 2015

Note This release supports only the ASA virtual.

Feature	Description
Platform Features	
Microsoft Hyper-V supervisor support	Extends the hypervisor portfolio for the ASA virtual.
ASAv5 low memory support	The ASAv5 now only requires 1 GB RAM to operate. Formerly, it required 2 GB. For already-deployed ASAv5s, you should reduce the allocated memory to 1 GB or you will see an error that you are using more memory than is licensed.

New Features in ASA 9.5(1)/ASDM 7.5(1)

Released: August 12, 2015

Note This version does not support the Firepower 9300 ASA security module or the ISA 3000.

Feature	Description
Firewall Features	

Feature	Description
GTPv2 inspection and improvements to GTPv0/1 inspection	GTP inspection can now handle GTPv2. In addition, GTP inspection for all versions now supports IPv6 addresses. We modified the following commands: **clear service-policy inspect gtp statistics, clear service-policy inspect gtp pdpmcb, clear service-policy inspect gtp request, match message id, show service-policy inspect gtp pdpmcb, show service-policy inspect gtp request, show service-policy inspect gtp statistics, timeout endpoint** We deprecated the following command: **timeout gsn** We modified the following screen: **Configuration > Firewall > Objects > Inspect Maps > GTP**
IP Options inspection improvements	IP Options inspection now supports all possible IP options. You can tune the inspection to allow, clear, or drop any standard or experimental options, including those not yet defined. You can also set a default behavior for options not explicitly defined in an IP options inspection map. We introduced the following commands: **basic-security, commercial-security, default, exp-flow-control, exp-measure, extended-security, imi-traffic-description, quick-start, record-route, timestamp** We modified the following screen: **Configuration > Firewall > Objects > Inspect Maps > IP Options**
Carrier Grade NAT enhancements	For carrier-grade or large-scale PAT, you can allocate a block of ports for each host, rather than have NAT allocate one port translation at a time (see RFC 6888). We introduced the following commands: **xlate block-allocation size, xlate block-allocation maximum-per-host**. We added the **block-allocation** keyword to the **nat** command. We introduced the following screen: **Configuration > Firewall > Advanced > PAT Port Block Allocation**. We added **Enable Block Allocation** the object NAT and twice NAT dialog boxes.
High Availability Features	
Inter-site clustering support for Spanned EtherChannel in Routed firewall mode	You can now use inter-site clustering for Spanned EtherChannels in routed mode. To avoid MAC address flapping, configure a site ID for each cluster member so that a site-specific MAC address for each interface can be shared among a site's units. We introduced or modified the following commands: **site-id, mac-address site-id, show cluster info, show interface** We modified the following screen: **Configuration > Device Management > High Availability and Scalability > ASA Cluster > Cluster Configuration**
ASA cluster customization of the auto-rejoin behavior when an interface or the cluster control link fails	You can now customize the auto-rejoin behavior when an interface or the cluster control link fails. We introduced the following command: **health-check auto-rejoin** We introduced the following screen: **Configuration > Device Management > High Availability and Scalability > ASA Cluster > Auto Rejoin**

Feature	Description
The ASA cluster supports GTPv1 and GTPv2	The ASA cluster now supports GTPv1 and GTPv2 inspection. We did not modify any commands. We did not modify any screens.
Cluster replication delay for TCP connections	This feature helps eliminate the "unnecessary work" related to short-lived flows by delaying the director/backup flow creation. We introduced the following command: **cluster replication delay** We introduced the following screen: **Configuration** > **Device Management** > **High Availability and Scalability** > **ASA Cluster Replication** *Also available for the Firepower 9300 ASA security module in Version 9.4(1.152).*
Disable health monitoring of a hardware module in ASA clustering	By default when using clustering, the ASA monitors the health of an installed hardware module such as the ASA FirePOWER module. If you do not want a hardware module failure to trigger failover, you can disable module monitoring. We modified the following command: **health-check monitor-interface service-module** We modified the following screen: **Configuration > Device Management > High Availability and Scalability > ASA Cluster > Cluster Interface Health Monitoring**
Enable use of the Management 1/1 interface as the failover link on the ASA 5506H	On the ASA 5506H only, you can now configure the Management 1/1 interface as the failover link. This feature lets you use all other interfaces on the device as data interfaces. Note that if you use this feature, you cannot use the ASA Firepower module, which requires the Management 1/1 interface to remain as a regular management interface. We modified the following commands: **failover lan interface, failover link** We modified the following screen: **Configuration > Device Management > High Availability and Scalability > Failover > Setup**
Routing Features	
Support for IPv6 in Policy Based Routing	IPv6 addresses are now supported for Policy Based Routing. We introduced the following commands: **set ipv6 next-hop, set default ipv6-next hop, set ipv6 dscp** We modified the following screens: **Configuration > Device Setup > Routing > Route Maps > Add Route Map > Policy Based Routing** **Configuration > Device Setup > Routing > Route Maps > Add Route Maps > Match Clause**
VXLAN support for Policy Based Routing	You can now enable Policy Based Routing on a VNI interface. We did not modify any commands. We modified the following screen: **Configuration > Device Setup > Interface Settings > Interfaces > Add/Edit Interface > General**

Feature	Description
Policy Based Routing support for Identity Firewall and Cisco Trustsec	You can configure Identity Firewall and Cisco TrustSec and then use Identity Firewall and Cisco TrustSec ACLs in Policy Based Routing route maps. We did not modify any commands. We modified the following screen: **Configuration > Device Setup > Routing > Route Maps > Add Route Maps > Match Clause**
Separate routing table for management-only interfaces	To segregate and isolate management traffic from data traffic, the ASA now supports a separate routing table for management-only interfaces. We introduced or modified the following commands: **backup, clear ipv6 route management-only, clear route management-only, configure http, configure net, copy, enrollment source, name-server, restore, show asp table route-management-only, show ipv6 route management-only show route management-only** We did not modify any screens.
Protocol Independent Multicast Source-Specific Multicast (PIM-SSM) pass-through support	The ASA now allows PIM-SSM packets to pass through when you enable multicast routing, unless the ASA is the Last-Hop Router. This feature allows greater flexibility in choosing a multicast group while also protecting against different attacks; hosts only receive traffic from explicitly-requested sources. We did not modify any commands. We did not modify any screens.
Remote Access Features	
IPv6 VLAN Mapping	ASA VPN code has been enhanced to support full IPv6 capabilities. No configuration change is necessary for the administrator.
Clientless SSL VPN SharePoint 2013 Support	Added support and a predefined application template for this new SharePoint version. We modified the following screen: **Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Bookmarks > Add Bookmark List > Select Bookmark Type > Predefined application templates**
Dynamic Bookmarks for Clientless VPN	Added CSCO_WEBVPN_DYNAMIC_URL and CSCO_WEBVPN_MACROLIST to the list of macros when using bookmarks. These macros allow the administrator to configure a single bookmark that can generate multiple bookmark links on the clientless user's portal and to statically configure bookmarks to take advantage of arbitrarily sized lists provided by LDAP attribute maps. We modified the following screen: **Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Bookmarks**
VPN Banner Length Increase	The overall banner length, which is displayed during post-login on the VPN remote client portal, has increased from 500 to 4000. We modified the following command: **banner** (group-policy). We modified the following screen: **Configuration > Remote Access VPN > .... Add/Edit Internal Group Policy > General Parameters > Banner**

Feature	Description
Cisco Easy VPN client on the ASA 5506-X, 5506W-X, 5506H-X, and 5508-X	This release supports Cisco Easy VPN on the ASA 5506-X series and for the ASA 5508-X. The ASA acts as a VPN hardware client when connecting to the VPN headend. Any devices (computers, printers, and so on) behind the ASA on the Easy VPN port can communicate over the VPN; they do not have to run VPN clients individually. Note that only one ASA interface can act as the Easy VPN port; to connect multiple devices to that port, you need to place a Layer 2 switch on the port, and then connect your devices to the switch. We introduced the following commands: **vpnclient enable, vpnclient server, vpnclient mode, vpnclient username, vpnclient ipsec-over-tcp, vpnclient management, vpnclient vpngroup, vpnclient trustpoint, vpnclient nem-st-autoconnect, vpnclient mac-exempt** We introduced the following screen: **Configuration > VPN > Easy VPN Remote**
Monitoring Features	
Show invalid usernames in syslog messages	You can now show invalid usernames in syslog messages for unsuccessful login attempts. The default setting is to hide usernames when the username is invalid or if the validity is unknown. If a user accidentally types a password instead of a username, for example, then it is more secure to hide the “username” in the resultant syslog message. You might want to show invalid usernames to help with troubleshooting login issues. We introduced the following command: **no logging hide username** We modified the following screen: **Configuration > Device Management > Logging > Syslog Setup** *This feature is also available in 9.2(4) and 9.3(3).*
REST API Features	
REST API Version 1.2.1	We added support for the REST API Version 1.2.1.

New Features in Version 9.4

New Features in ASA 9.4(4.5)/ASDM 7.6(2)

Released: April 3, 2017

Note Verion 9.4(4) was removed from Cisco.com due to bug CSCvd78303.

There are no new features in this release.

New Features in ASA 9.4(3)/ASDM 7.6(1)

Released: April 25, 2016

Feature	Description
Firewall Features	
Connection holddown timeout for route convergence	You can now configure how long the system should maintain a connection when the route used by the connection no longer exists or is inactive. If the route does not become active within this holddown period, the connection is freed. You can reduce the holddown timer to make route convergence happen more quickly. However, the 15 second default is appropriate for most networks to prevent route flapping. We added the following command: **timeout conn-holddown** We modified the following screen: **Configuration** > **Firewall** > **Advanced** > **Global Timeouts**
Remote Access Features	
Configurable SSH encryption and HMAC algorithm.	Users can select cipher modes when doing SSH encryption management and can configure HMAC and encryption for varying key exchange algorithms. We introduced the following commands: **ssh cipher encryption, ssh cipher integrity**. We introduced the following screen: **Configuration** > **Device Management** > **Advanced** > **SSH Ciphers** *Also available in 9.1(7).*
HTTP redirect support for IPv6	When you enable HTTP redirect to HTTPS for ASDM access or clientless SSL VPN, you can now redirect traffic sent an to IPv6 address. We added functionality to the following command: **http redirect** We added functionality to the following screen: **Configuration** > **Device Management** > **HTTP Redirect** *Also available in 9.1(7).*
Monitoring Features	
SNMP engineID sync for Failover	In a failover pair, the SNMP engineIDs of the paired ASAs are synced on both units. Three sets of engineIDs are maintained per ASA—synced engineID, native engineID and remote engineID. An SNMPv3 user can also specify the engineID of the ASA when creating a profile to preserve localized **snmp-server user** authentication and privacy options. If a user does not specify the native engineID, the **show running config** output will show two engineIDs per user. We modified the following command: **snmp-server user** No ASDM support.

Feature	Description
show tech support enhancements	The **show tech support** command now: • Includes **dir all-filesystems** output—This output can be helpful in the following cases: • SSL VPN configuration: check if the required resources are on the ASA • Crash: check for the date timestamp and presence of a crash file • Removes the **show kernel cgroup-controller detail** output—This command output will remain in the output of **show tech-support detail**. We modified the following command: **show tech support** We did not add or modify any screens. *Also available in 9.1(7).*
Support for the cempMemPoolTable in the CISCO-ENHANCED-MEMPOOL-MIB	The cempMemPoolTable of the CISCO-ENHANCED-MEMPOOL-MIB is now supported. This is a table of memory pool monitoring entries for all physical entities on a managed system. **Note** The CISCO-ENHANCED-MEMPOOL-MIB uses 64-bit counters and supports reporting of memory on platforms with more than 4GB of RAM. We did not add or modify any commands. We did not add or modify any screens. *Also available in 9.1(7).*

New Features in ASA 9.4(2.145)/ASDM 7.5(1)

Released: November 13, 2015

There are no new features in this release.

Note This release supports only the Firepower 9300 ASA security module.

New Features in ASA 9.4(2)/ASDM 7.5(1)

Released: September 24, 2015

There are no new features in this release.

Note ASAv 9.4(1.200) features are not included in this release.

Note This version does not support the ISA 3000.

New Features in ASA 9.4(1.225)/ASDM 7.5(1)

Released: September 17, 2015

Note This release supports only the Cisco ISA 3000.

Feature	Description
Platform Features	
Cisco ISA 3000 Support	The Cisco ISA 3000 is a DIN Rail mounted, ruggedized, industrial security appliance. It is low-power, fan-less, with Gigabit Ethernet and a dedicated management port. This model comes with the ASA Firepower module pre-installed. Special features for this model include a customized transparent mode default configuration, as well as a hardware bypass function to allow traffic to continue flowing through the appliance when there is a loss of power. We introduced the following commands: **hardware-bypass, hardware-bypass manual, hardware-bypass boot-delay, show hardware-bypass** We introduced the following screen: **Configuration** > **Device Management** > **Hardware Bypass** The **hardware-bypass boot-delay** command is not available in ASDM 7.5(1). *This feature is not available in Version 9.5(1).*

New Features in ASA 9.4(1.152)/ASDM 7.4(3)

Released: July 13, 2015

Note This release supports only the ASA on the Firepower 9300.

Feature	Description
Platform Features	
ASA security module on the Firepower 9300	We introduced the ASA security module on the Firepower 9300. **Note** Chassis Manager 1.1.1 does not support any VPN features (site-to-site or remote access) for the ASA security module on the Firepower 9300.
High Availability Features	

Feature	Description
Intra-chassis ASA Clustering for the Firepower 9300	You can cluster up to 3 security modules within the Firepower 9300 chassis. All modules in the chassis must belong to the cluster. We introduced the following commands: **cluster replication delay, debug service-module, management-only individual, show cluster chassis** We introduced the following screen: **Configuration** > **Device Management** > **High Availability and Scalability** > **ASA Cluster Replication**
Licensing Features	
Cisco Smart Software Licensing for the ASA on the Firepower 9300	We introduced Smart Software Licensing for the ASA on the Firepower 9300. We introduced the following commands: **feature strong-encryption, feature mobile-sp, feature context** We modified the following screen: **Configuration** > **Device Management** > **Licensing** > **Smart License**

New Features in ASA Virtual 9.4(1.200)/ASDM 7.4(2)

Released: May 12, 2015

Note This release supports only the ASA virtual.

Feature	Description
Platform Features	
ASA virtual on VMware no longer requires vCenter support	You can now install the ASA virtual on VMware without vCenter using the vSphere client or the OVFTool using a Day 0 configuration.
ASA virtual on Amazon Web Services (AWS)	You can now use the ASA virtual with Amazon Web Services (AWS) and the Day 0 configuration. **Note** Amazon Web Services only supports models ASAv10 and ASAv30.

New Features in ASDM 7.4(2)

Released: May 6, 2015

Feature	Description
Remote Access Features	

Feature	Description
AnyConnect Version 4.1 support	ASDM now supports AnyConnect Version 4.1. We modified the following screen: **Configuration > Remote Access VPN > Network (Client) Access > Secure Client Profile** (a new profile called **AMP Enabler Service Profile**)

New Features in ASA 9.4(1)/ASDM 7.4(1)

Released: March 30, 2015

Feature	Description
Platform Features	
ASA 5506W-X, ASA 5506H-X, ASA 5508-X, ASA 5516-X	We introduced the ASA 5506W-X with wireless access point, hardened ASA 5506H-X, ASA 5508-X, and ASA 5516-X models. We introduced the following command: **hw-module module wlan recover image**, **hw-module module wlan recover image**. We did not modify any ASDM screens.
Certification Features	
Department of Defense Unified Capabilities Requirements (UCR) 2013 Certification	The ASA was updated to comply with the DoD UCR 2013 requirements. See the rows in this table for the following features that were added for this certification: • Periodic certificate authentication • Certificate expiration alerts • Enforcement of the basic constraints CA flag • ASDM Username From Certificate Configuration • ASDM management authorization • IKEv2 invalid selectors notification configuration • IKEv2 pre-shared key in Hex

Feature	Description
FIPS 140-2 Certification compliance updates	When you enable FIPS mode on the ASA, additional restrictions are put in place for the ASA to be FIPS 140-2 compliant. Restrictions include: • RSA and DH Key Size Restrictions—Only RSA and DH keys 2K (2048 bits) or larger are allowed. For DH, this means groups 1 (768 bit), 2 (1024 bit), and 5 (1536 bit) are not allowed. **Note** The key size restrictions disable use of IKEv1 with FIPS. • Restrictions on the Hash Algorithm for Digital Signatures—Only SHA256 or better is allowed. • SSH Cipher Restrictions—Allowed ciphers: aes128-cbc or aes256-cbc. MACs: SHA1 To see the FIPS certification status for the ASA, see: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140InProcess.pdf This PDF is updated weekly. See the Computer Security Division Computer Security Resource Center site for more information: http://csrc.nist.gov/groups/STM/cmvp/inprocess.html We modified the following command: **fips enable**
Firewall Features	
Improved SIP inspection performance on multiple core ASAs.	If you have multiple SIP signaling flows going through an ASA with multiple cores, SIP inspection performance has been improved. However, you will not see improved performance if you are using a TLS, phone, or IME proxy. We did not modify any commands. We did not modify any screens.
SIP inspection support for Phone Proxy and UC-IME Proxy was removed.	You can no longer use Phone Proxy or UC-IME Proxy when configuring SIP inspection. Use TLS Proxy to inspect encrypted traffic. We removed the following commands: **phone-proxy**, **uc-ime**. We removed the **phone-proxy** and **uc-ime** keywords from the **inspect sip** command. We removed Phone Proxy and UC-IME Proxy from the **Select SIP Inspect Map** service policy dialog box.
DCERPC inspection support for ISystemMapper UUID message RemoteGetClassObject opnum3.	The ASA started supporting non-EPM DCERPC messages in release 8.3, supporting the ISystemMapper UUID message RemoteCreateInstance opnum4. This change extends support to the RemoteGetClassObject opnum3 message. We did not modify any commands. We did not modify any screens.

Feature	Description
Unlimited SNMP server trap hosts per context	The ASA supports an unlimited number of SNMP server trap hosts per context. The **show snmp-server host** command output displays only the active hosts that are polling the ASA, as well as the statically configured hosts. We modified the following command: **show snmp-server host**. We did not modify any screens.
VXLAN packet inspection	The ASA can inspect the VXLAN header to enforce compliance with the standard format. We introduced the following command: **inspect vxlan**. We modified the following screen: **Configuration > Firewall > Service Policy Rules > Add Service Policy Rule > Rule Actions > Protocol Inspection**
DHCP monitoring for IPv6	You can now monitor DHCP statistics and DHCP bindings for IPv6. We introduced the following screens: **Monitoring > Interfaces > DHCP > IPV6 DHCP Statistics Monitoring > Interfaces > DHCP > IPV6 DHCP Binding**.
ESMTP inspection change in default behavior for TLS sessions.	The default for ESMTP inspection was changed to allow TLS sessions, which are not inspected. However, this default applies to new or reimaged systems. If you upgrade a system that includes **no allow-tls**, the command is not changed. The change in default behavior was also made in these older versions: 8.4(7.25), 8.5(1.23), 8.6(1.16), 8.7(1.15), 9.0(4.28), 9.1(6.1), 9.2(3.2) 9.3(1.2), 9.3(2.2).
High Availability Features	
Blocking syslog generation on a standby ASA	You can now block specific syslogs from being generated on a standby unit. We introduced the following command: **no logging message** *syslog-id* **standby**. We did not modify any screens.
Enable and disable ASA cluster health monitoring per interface	You can now enable or disable health monitoring per interface. Health monitoring is enabled by default on all port-channel, redundant, and single physical interfaces. Health monitoring is not performed on VLAN subinterfaces or virtual interfaces such as VNIs or BVIs. You cannot configure monitoring for the cluster control link; it is always monitored. You might want to disable health monitoring of non-essential interfaces, for example, the management interface. We introduced the following command: **health-check monitor-interface.** We introduced the following screen: **Configuration > Device Management > High Availability and Scalability > ASA Cluster > Cluster Interface Health Monitoring**
ASA clustering support for DHCP relay	You can now configure DHCP relay on the ASA cluster. Client DHCP requests are load-balanced to the cluster members using a hash of the client MAC address. DHCP client and server functions are still not supported. We introduced the following command: **debug cluster dhcp-relay** We did not modify any screens.

Feature	Description
SIP inspection support in ASA clustering	You can now configure SIP inspection on the ASA cluster. A control flow can be created on any unit (due to load balancing), but its child data flows must reside on the same unit. TLS Proxy configuration is not supported. We introduced the following command: **show cluster service-policy** We did not modify any screens.
Routing Features	
Policy Based Routing	Policy Based Routing (PBR) is a mechanism by which traffic is routed through specific paths with a specified QoS using ACLs. ACLs let traffic be classified based on the content of the packet's Layer 3 and Layer 4 headers. This solution lets administrators provide QoS to differentiated traffic, distribute interactive and batch traffic among low-bandwidth, low-cost permanent paths and high-bandwidth, high-cost switched paths, and allows Internet service providers and other organizations to route traffic originating from various sets of users through well-defined Internet connections. We introduced the following commands: **set ip next-hop verify-availability, set ip next-hop, set ip next-hop recursive, set interface, set ip default next-hop, set default interface, set ip df, set ip dscp, policy-route route-map, show policy-route, debug policy-route** We introduced or modified the following screens: **Configuration > Device Setup > Routing > Route Maps > Policy Based Routing** **Configuration > Device Setup > Routing > Interface Settings > Interfaces.**
Interface Features	
VXLAN support	VXLAN support was added, including VXLAN tunnel endpoint (VTEP) support. You can define one VTEP source interface per ASA or security context. We introduced the following commands: **debug vxlan, default-mcast-group, encapsulation vxlan, inspect vxlan, interface vni, mcast-group, nve, nve-only, peer ip, segment-id, show arp vtep-mapping, show interface vni, show mac-address-table vtep-mapping, show nve, show vni vlan-mapping, source-interface, vtep-nve, vxlan port** We introduced the following screens: **Configuration > Device Setup > Interface Settings > Interfaces > Add > VNI Interface** **Configuration > Device Setup > Interface Settings > VXLAN**
Monitoring Features	
Memory tracking for the EEM	We have added a new debugging feature to log memory allocations and memory usage, and to respond to memory logging wrap events. We introduced or modified the following commands: **memory logging, show memory logging, show memory logging include, event memory-logging-wrap** We modified the following screen: **Configuration > Device Management > Advanced > Embedded Event Manager > Add Event Manager Applet > Add Event Manager Applet Event**

Feature	Description
Troubleshooting crashes	The **show tech-support** command output and **show crashinfo** command output includes the most recent 50 lines of generated syslogs. Note that you must enable the **logging buffer** command to enable these results to appear.
Remote Access Features	
Support for ECDHE-ECDSA ciphers	TLSv1.2 added support for the following ciphers: • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • DHE-RSA-AES256-GCM-SHA384 • AES256-GCM-SHA384 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA384 • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • DHE-RSA-AES128-GCM-SHA256 • RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-RSA-AES128-SHA256 **Note** ECDSA and DHE ciphers are the highest priority. We introduced the following command: **ssl ecdh-group**. We modified the following screen: **Configuration > Remote Access VPN > Advanced > SSL Settings.**

Feature	Description
Clientless SSL VPN session cookie access restriction	You can now prevent a Clientless SSL VPN session cookie from being accessed by a third party through a client-side script such as Javascript. **Note** Use this feature only if Cisco TAC advises you to do so. Enabling this command presents a security risk because the following Clientless SSL VPN features will not work without any warning. • Java plug-ins • Java rewriter • Port forwarding • File browser • Sharepoint features that require desktop applications (for example, MS Office applications) • Secure Client Web launch • Citrix Receiver, XenDesktop, and Xenon • Other non-browser-based and browser plugin-based applications We introduced the following command: **http-only-cookie**. We introduced the following screen: **Configuration > Remote Access VPN > Clientless SSL VPN Access > Advanced > HTTP Cookie**. *This feature is also in 9.2(3).*
Virtual desktop access control using security group tagging	The ASA now supports security group tagging-based policy control for Clientless SSL remote access to internal applications and websites. This feature uses Citrix's virtual desktop infrastructure (VDI) with XenDesktop as the delivery controller and the ASA's content transformation engine. See the following Citrix product documentation for more information: • Policies for XenDesktop and XenApp: http://support.citrix.com/proddocs/topic/infocenter/ic-how-to-use.html • Managing policies in XenDesktop 7: http://support.citrix.com/proddocs/topic/xendesktop-7/cds-policies-wrapper-rho.html • Using group policy editor for XenDesktop 7 policies: http://support.citrix.com/proddocs/topic/xendesktop-7/cds-policies-use-gpmc.html

Feature	Description
OWA 2013 feature support has been added for Clientless SSL VPN	Clientless SSL VPN supports the new features in OWA 2013 except for the following: • Support for tablets and smartphones • Offline mode • Active Directory Federation Services (AD FS) 2.0. The ASA and AD FS 2.0 can't negotiate encryption protocols. We did not modify any commands. We did not modify any screens.
Citrix XenDesktop 7.5 and StoreFront 2.5 support has been added for Clientless SSL VPN	Clientless SSL VPN supports the access of XenDesktop 7.5 and StoreFront 2.5. See http://support.citrix.com/proddocs/topic/xenapp-xendesktop-75/cds-75-about-whats-new.html for the full list of XenDesktop 7.5 features, and for more details. See http://support.citrix.com/proddocs/topic/dws-storefront-25/dws-about.html for the full list of StoreFront 2.5 features, and for more details. We did not modify any commands. We did not modify any screens.
Periodic certificate authentication	When you enable periodic certificate authentication, the ASA stores certificate chains received from VPN clients and re-authenticates them periodically. We introduced or modified the following commands: **periodic-authentication certificate, revocation-check, show vpn-sessiondb** We modified the following screens: **Configuration > Device Management > Certificate Management > Identity Certificates** **Configuration > Device Management > Certificate Management > CA Certificates**
Certificate expiration alerts	The ASA checks all CA and ID certificates in the trust points for expiration once every 24 hours. If a certificate is nearing expiration, a syslog will be issued as an alert. You can configure the reminder and recurrence intervals. By default, reminders will start at 60 days prior to expiration and recur every 7 days. We introduced or modified the following commands: **crypto ca alerts expiration** We modified the following screens: **Configuration > Device Management > Certificate Management > Identity Certificates** **Configuration > Device Management > Certificate Management > CA Certificates**
Enforcement of the basic constraints CA flag	Certificates without the CA flag now cannot be installed on the ASA as CA certificates by default. The basic constraints extension identifies whether the subject of the certificate is a CA and the maximum depth of valid certification paths that include this certificate. You can configure the ASA to allow installation of these certificates if desired. We introduced the following command: **ca-check** We modified the following screens: **Configuration > Device Management > Certificate Management > CA Certificates**

Feature	Description
IKEv2 invalid selectors notification configuration	Currently, if the ASA receives an inbound packet on an SA, and the packet's header fields are not consistent with the selectors for the SA, then the ASA discards the packet. You can now enable or disable sending an IKEv2 notification to the peer. Sending this notification is disabled by default. **Note** This feature is supported with Secure Client 3.1.06060 and later. We introduced the following command: **crypto ikev2 notify invalid-selectors**
IKEv2 pre-shared key in Hex	You can now configure the IKEv2 pre-shared keys in hex. We introduced the following command: **ikev2 local-authentication pre-shared-key hex**, **ikev2 remote-authentication pre-shared-key hex**
Administrative Features	
ASDM management authorization	You can now configure management authorization separately for HTTP access vs. Telnet and SSH access. We introduced the following command: **aaa authorization http console** We modified the following screen: **Configuration > Device Management > Users/AAA > AAA Access > Authorization**
ASDM Username From Certificate Configuration	When you enable ASDM certificate authentication (**http authentication-certificate**), you can configure how ASDM extracts the username from the certificate; you can also enable pre-filling the username at the login prompt. We introduced the following command: **http username-from-certificate** We introduced the following screen: **Configuration > Device Management > Management Access > HTTP Certificate Rule.**
terminal interactive command to enable or disable help when you enter **?** at the CLI	Normally, when you enter **?** at the ASA CLI, you see command help. To be able to enter **?** as text within a command (for example, to include a ? as part of a URL), you can disable interactive help using the **no terminal interactive** command. We introduced the following command: terminal interactive
REST API Features	
REST API Version 1.1	We added support for the REST API Version 1.1.
Support for token-based authentication (in addition to existing basic authentication)	Client can send log-in request to a specific URL; if successful, a token is returned (in response header). Client then uses this token (in a special request header) for sending additional API calls. The token is valid until explicitly invalidated, or the idle/session timeout is reached.

Feature	Description
Limited multiple-context support	The REST API agent can now be enabled in multi-context mode; the CLI commands can be issued only in system-context mode (same commands as single-context mode). Pass-through CLI API commands can be used to configure any context, as follows. `https://<asa_admin_context_ip>/api/cli?context=<context_name>` If the **context** parameter is not present, it is assumed that the request is directed to the **admin** context.
Advanced (granular) inspection	Granular inspection of these protocols is supported: • DNS over UDP • HTTP • ICMP • ICMP ERROR • RTSP • SIP • FTP • DCERPC • IP Options • NetBIOS Name Server over IP • SQL*Net

New Features in Version 9.3

New Features in ASA 9.3(3)/ASDM 7.4(1)

Released: April 22, 2015

Feature	Description
Platform Features	

Feature	Description
Show invalid usernames in syslog messages	You can now show invalid usernames in syslog messages for unsuccessful login attempts. The default setting is to hide usernames when the username is invalid or if the validity is unknown. If a user accidentally types a password instead of a username, for example, then it is more secure to hide the "username" in the resultant syslog message. You might want to show invalid usernames to help with troubleshooting login issues. We introduced the following command: **no logging hide username** This feature is not supported in ASDM. *This feature is not available in 9.4(1).*

New Features in ASA 9.3(2)/ASDM 7.3(3)

Released: February 2, 2015

Feature	Description
Platform Features	
ASA FirePOWER software module for the ASA 5506-X	You can configure ASA FirePOWER on the ASA 5506-X using ASDM; a separate FireSIGHT Management Center is not required, although you can use one instead of ASDM. We introduced the following screens: **Home > ASA FirePOWER Dashboard** **Home > ASA FirePOWER Reporting** **Configuration > ASA FirePOWER Configuration** **Monitoring > ASA FirePOWER Monitoring**

New Features in ASA 9.3(2.200)/ASDM 7.3(2)

Released: December 18, 2014

Note This release supports only the ASAv.

Feature	Description
Platform Features	
ASAv with KVM and Virtio	You can deploy the ASAv using the Kernel-based Virtual Machine (KVM) and the Virtio virtual interface driver.

New Features in ASA 9.3(2)/ASDM 7.3(2)

Released: December 18, 2014

Feature	Description
Platform Features	
ASA 5506-X	We introduced the ASA 5506-X. We introduced or modified the following commands: **service sw-reset-button**, **upgrade rommon**, **show environment temperature accelerator**
ASA FirePOWER software module for the ASA 5506-X	You can configure ASA FirePOWER on the ASA 5506-X using ASDM; a separate FireSIGHT Management Center is not required, although you can use one instead of ASDM. **Note:** This feature requires ASA 7.3(3). We introduced the following screens: **Home > ASA FirePOWER Dashboard** **Home > ASA FirePOWER Reporting** **Configuration > ASA FirePOWER Configuration** **Monitoring > ASA FirePOWER Monitoring**
ASA FirePOWER passive monitor-only mode using traffic redirection interfaces	You can now configure a traffic forwarding interface to send traffic to the module instead of using a service policy. In this mode, neither the module nor the ASA affects the traffic. We fully supported the following command: **traffic-forward sfr monitor-only**. You can configure this in CLI only.
Mixed level SSPs in the ASA 5585-X	You can now use the following mixed level SSPs in the ASA 5585-X: • ASA SSP-10/ASA FirePOWER SSP-40 • ASA SSP-20/ASA FirePOWER SSP-60 Requirements: ASA SSP in slot 0, ASA FirePOWER SSP in slot 1
ASA REST API 1.0.1	A REST API was added to support configuring and managing major functions of the ASA. We introduced or modified the following commands: **rest-api image**, **rest-api agent**, **show rest-api agent**, **debug rest-api**, **show version**
Support for ASA image signing and verification	ASA images are now signed using a digital signature. The digital signature is verified after the ASA is booted. We introduced the following commands: **copy /noverify**, **verify /image-signature**, **show software authenticity keys**, **show software authenticity file**, **show software authenticity running**, **show software authenticity development, software authenticity development**, **software authenticity key add special**, **software authenticity key revoke special** This feature is not supported in ASDM.

Feature	Description
Accelerated security path load balancing	The accelerated security path (ASP) load balancing mechanism reduces packet drop and improves throughput by allowing multiple cores of the CPU to receive packets from an interface receive ring and work on them independently. We introduced the following command: **asp load-balance per-packet-auto** We introduced the following screen: **Configuration > Device Management > Advanced > ASP Load Balancing**
Firewall Features	
Configuration session for editing ACLs and objects. Forward referencing of objects and ACLs in access rules.	You can now edit ACLs and objects in an isolated configuration session. You can also forward reference objects and ACLs, that is, configure rules and access groups for objects or ACLs that do not yet exist. We introduced the following commands: **clear configuration session**, **clear session**, **configure session**, **forward-reference**, **show configuration session** This feature is not supported in ASDM.
SIP support for Trust Verification Services, NAT66, CUCM 10.5(1), and model 8831 phones.	You can now configure Trust Verification Services servers in SIP inspection. You can also use NAT66. SIP inspection has been tested with CUCM 10.5(1). We introduced the following command: **trust-verification-server**. We introduced the following screen: **Configuration > Firewall > Objects > Inspection Maps > SIP > Add/Edit SIP Inspect Map > Details > TVS Server**
Unified Communications support for CUCM 10.5(1)	SIP and SCCP inspections were tested and verified with Cisco Unified Communications Manager 10.5(1).
Remote Access Features	
Browser support for Citrix VDI	We now support an HTML 5-based browser solution for accessing the Citrix VDI without requiring the Citrix Receiver client on the desktop.
Clientless SSL VPN for Mac OSX 10.9	We now support Clientless SSL VPN features such as the rewriter, smart tunnels, and plugins on all browsers that are supported on Mac OSX 10.9.

Feature	Description
Interoperability with standards-based, third-party, IKEv2 remote access clients	We now support VPN connectivity via standards-based, third-party, IKEv2 remote-access clients (in addition to AnyConnect). Authentication support includes preshared keys, certificates, and user authentication via the Extensible Authentication Protocol (EAP). We introduced or modified the following commands: **ikev2 remote-authentication, ikev2 local-authentication**, **clear vpn-sessiondb**, **show vpn-sessiondb**, **vpn-sessiondb logoff** We introduced or modified the following screens: **Wizards > IPsec IKEv2 Remote Access Wizard**. **Configuration > Remote Access VPN > Network (Client) Access > IPsec (IKEv2) Connection Profiles** **Configuration > Remote Access VPN > Network (Client) Access > IPsec (IKEv2) Connection Profiles > Add/Edit > Advanced > IPsec** **Monitoring > VPN > VPN Statistics > Sessions**
Transport Layer Security (TLS) version 1.2 support	We now support TLS version 1.2 for secure message transmission for ASDM, Clientless SSVPN, and AnyConnect VPN. We introduced or modified the following commands: **ssl client-version**, **ssl server-version**, **ssl cipher**, **ssl trust-point**, **ssl dh-group**, **show ssl**, **show ssl cipher**, **show vpn-sessiondb** We deprecated the following command: **ssl encryption** We modified the following screens: **Configuration > Device Management > Advanced > SSL Settings** **Configuration > Remote Access VPN > Advanced > SSL Settings**
AnyConnect 4.0 support for TLS version 1.2	AnyConnect 4.0 now supports TLS version 1.2 with the following four additional cipher suites: DHE-RSA-AES256-SHA256, DHE-RSA-AES128-SHA256, AES256-SHA256, and AES128-SHA256.
Licensing Features	

Feature	Description
Cisco Smart Software Licensing for the ASAv	Smart Software Licensing lets you purchase and manage a pool of licenses. Unlike PAK licenses, smart licenses are not tied to a specific serial number. You can easily deploy or retire ASAvs without having to manage each unit's license key. Smart Software Licensing also lets you see your license usage and needs at a glance. We introduced the following commands: **clear configure license, debug license agent, feature tier, http-proxy, license smart, license smart deregister, license smart register, license smart renew, show license, show running-config license, throughput level** We introduced or modified the following screens: **Configuration > Device Management > Licensing > Smart License** **Configuration > Device Management > Smart Call-Home** **Monitoring > Properties > Smart License**
High Availability Features	
Lock configuration changes on the standby unit or standby context in a failover pair	You can now lock configuration changes on the standby unit (Active/Standby failover) or the standby context (Active/Active failover) so you cannot make changes on the standby unit outside normal configuration syncing. We introduced the following command: **failover standby config-lock** We modified the following screen: **Configuration > Device Management > High Availability and Scalability > Failover > Setup**
ASA clustering inter-site deployment in transparent mode with the ASA cluster firewalling between inside networks	You can now deploy a cluster in transparent mode between inside networks and the gateway router at each site (AKA East-West insertion), and extend the inside VLANs between sites. We recommend using Overlay Transport Virtualization (OTV), but you can use any method that ensures that the overlapping MAC Addresses and IP addresses of the gateway router do not leak between sites. Use a First Hop Redundancy Protocol (FHRP) such as HSRP to provide the same virtual MAC and IP addresses to the gateway routers.
Interface Features	

Feature	Description
Traffic Zones	You can group interfaces together into a traffic zone to accomplish traffic load balancing (using Equal Cost Multi-Path (ECMP) routing), route redundancy, and asymmetric routing across multiple interfaces. **Note** You cannot apply a security policy to a named zone; the security policy is interface-based. When interfaces in a zone are configured with the same access rule, NAT, and service policy, then load-balancing and asymmetric routing operate correctly. We introduced or modified the following commands: **zone, zone-member, show running-config zone, clear configure zone, show zone, show asp table zone, show nameif zone, show conn long, show local-host zone, show route zone, show asp table routing, clear conn zone, clear local-host zone** We introduced or modified the following screens: **Configuration > Device Setup > Interface Parameters > Zones** **Configuration > Device Setup > Interface Parameters > Interfaces**
Routing Features	
BGP support for IPv6	We added support for IPv6. We introduced or modified the following commands: **address-family ipv6, bgp router-id, ipv6 prefix-list, ipv6 prefix-list description, ipv6 prefix-list sequence-number, match ipv6 next-hop, match ipv6 route-source, match ipv6-address prefix-list, set ipv6-address prefix -list, set ipv6 next-hop, set ipv6 next-hop peer-address** We introduced the following screen: **Configuration > Device Setup > Routing > BGP > IPv6 Family**
Monitoring Features	

Feature	Description
SNMP MIBs and traps	The CISCO-PRODUCTS-MIB and CISCO-ENTITY-VENDORTYPE-OID-MIB have been updated to support the new ASA 5506-X. The ASA 5506-X have been added as new products to the SNMP sysObjectID OID and entPhysicalVendorType OID. The ASA now supports the CISCO-CONFIG-MAN-MIB, which enables you to do the following: • Know which commands have been entered for a specific configuration. • Notify the NMS when a change has occurred in the running configuration. • Track the time stamps associated with the last time that the running configuration was changed or saved. • Track other changes to commands, such as terminal details and command sources. We modified the following command: **snmp-server enable traps** We modified the following screen: **Configuration > Device Management > Management Access > SNMP > Configure Traps > SNMP Trap Configuration**
Showing route summary information for troubleshooting	The **show route-summary** command output has been added to the **show tech-support detail** command.
Management Features	
System backup and restore	We now support complete system backup and restoration using the CLI. We introduced the following commands: **backup**, **restore** We did not modify any screens. This functionality is already available in ASDM.

New Features in ASA 9.3(1)/ASDM 7.3(1)

Released: July 24, 2014

Note The ASA 5505 is not supported in this release or later. ASA Version 9.2 was the final release for the ASA 5505.

Feature	Description
Firewall Features	
SIP, SCCP, and TLS Proxy support for IPv6	You can now inspect IPv6 traffic when using SIP, SCCP, and TLS P SIP or SCCP). We did not modify any commands. We did not modify any ASDM screens.

Feature	Description
Support for Cisco Unified Communications Manager 8.6	The ASA now interoperates with Cisco Unified Communications Manag 8.6 (including SCCPv21 support). We did not modify any commands. We did not modify any ASDM screens.
Transactional Commit Model on rule engine for access groups and NAT	When enabled, a rule update is applied after the rule compilation is com without affecting the rule matching performance. We introduced the following commands: **asp rule-engine transactiona show running-config asp rule-engine transactional-commit**, **clear co asp rule-engine transactional-commit** We introduced the following screen: **Configuration > Device Manage Advanced > Rule Engine**
Remote Access Features	
XenDesktop 7 Support for clientless SSL VPN	We added support for XenDesktop 7 to clientless SSL VPN. When crea bookmark with auto sign-on, you can now specify a landing page URL o ID. We did not modify any commands. We modified the following screen: **Configuration > Remote Access V Clientless SSL VPN Access > Portal > Bookmarks**
AnyConnect Custom Attribute Enhancements	Custom attributes define and configure AnyConnect features that have r incorporated into the ASA, such as Deferred Upgrade. Custom attribute co has been enhanced to allow multiple values and longer values, and now specification of their type, name and value. They can now be added to D Access Policies as well as Group Policies. Previously defined custom at will be updated to this enhanced configuration format upon upgrade to 9 We introduced or modified the following commands: **anyconnect-custo anyconnect-custom-data**, and **anyconnect-custom** We introduced or modified the following screens: **Configuration > Remote Access VPN > Network (Client) Access > A > AnyConnect Custom Attributes** **Configuration > Remote Access VPN > Network (Client) Access > A > AnyConnect Custom Attribute Names** **Configuration > Remote Access VPN > Network (Client) Access > G Policies > Add/Edit > Advanced > AnyConnect Client > Custom Att** **Configuration > Remote Access VPN > Network (Client) Access > D Access Policies > Add/Edit > AnyConnect Custom Attributes**

Feature	Description
AnyConnect Identity Extensions (ACIDex) for Desktop Platforms	ACIDex, also known as AnyConnect Endpoint Attributes or Mobile method used by the AnyConnect VPN client to communicate postur to the ASA. Dynamic Access Polices use these endpoint attributes to users. The AnyConnect VPN client now provides Platform identification fo operating systems (Windows, Mac OS X, and Linux) and a pool of MA which can be used by DAPs. We did not modify any commands. We modified the following screen: Configuration > Remote Access VP Access Policies > Add/Edit > Add/Edit (endpoint attribute), select **A** for the **Endpoint Attribute Type**. Additional operating systems are in drop-down list and MAC Address has changed to **Mac Address Poo**
TrustSec SGT Assignment for VPN	TrustSec Security Group Tags (SGT) can now be added to the SGT-I ASA when a remote user connects. We introduced the following new command: **security-group-tag va** We introduced or modified the following screens: **Configuration > Remote Access VPN > AAA/Local Users > Local User > VPN Policy** **Configuration > Remote Access VPN > Network (Client) Access Policies > Add a Policy**
High Availability Features	
Improved support for monitoring module health in clustering	We added improved support for monitoring module health in cluster We modified the following command: **show cluster info health** We did not modify any ASDM screens.
Disable health monitoring of a hardware module	By default, the ASA monitors the health of an installed hardware mo the ASA FirePOWER module. If you do not want a hardware modul trigger failover, you can disable module monitoring. We modified the following command: **monitor-interface service-m** We modified the following screen: **Configuration > Device Manage Availability and Scalability > Failover > Interfaces**
Platform Features	

Feature	Description
ASP Load Balancing	The new **auto** option in the **asp load-balance per-packet** command ena ASA to adaptively switch ASP load balancing per-packet on and off on interface receive ring. This automatic mechanism detects whether or not as traffic has been introduced and helps avoid the following issues: • Overruns caused by sporadic traffic spikes on flows • Overruns caused by bulk flows oversubscribing specific interface rec • Overruns caused by relatively heavily overloaded interface receive which a single core cannot sustain the load We introduced or modified the following commands: **asp load-balance p auto**, **show asp load-balance per-packet**, **show asp load-balance per- history**, and **clear asp load-balance history** We did not modify any ASDM screens.
SNMP MIBs	The CISCO-REMOTE-ACCESS-MONITOR-MIB now supports the AS
Interface Features	
Transparent mode bridge group maximum increased to 250	The bridge group maximum was increased from 8 to 250 bridge groups. configure up to 250 bridge groups in single mode or per context in multi with 4 interfaces maximum per bridge group. We modified the following commands: **interface bvi**, **bridge-group** We modified the following screens: **Configuration > Device Setup > Interfaces** **Configuration > Device Setup > Interfaces > Add/Edit Bridge Group** **Configuration > Device Setup > Interfaces > Add/Edit Interface**
Routing Features	
BGP support for ASA clustering	We added support for BGP with ASA clustering. We introduced the following new command: bgp router-id clusterpool We modified the following screen: **Configuration > Device Setup > Ro BGP > IPv4 Family > General**
BGP support for nonstop forwarding	We added support for BGP Nonstop Forwarding. We introduced the following new commands: bgp graceful-restart, neighbo graceful-restart We modified the following screens: **Configuration > Device Setup > Routing > BGP > General** **Configuration > Device Setup > Routing > BGP > IPv4 Family > Ne** **Monitoring > Routing > BGP Neighbors**

Feature	Description
BGP support for advertised maps	We added support for BGPv4 advertised map. We introduced the following new command: neighbor advertise-map We modified the following screen: **Configuration > Device Setup > BGP > IPv4 Family > Neighbor > Add BGP Neighbor > Routes**
OSPF Support for Non-Stop Forwarding (NSF)	OSPFv2 and OSPFv3 support for NSF was added. We added the following commands: capability, nsf cisco, nsf cisco h nsf ietf helper, nsf ietf helper strict-lsa-checking, graceful-restart, gra helper, graceful-restart helper strict-lsa-checking We added the following screens: **Configuration > Device Setup > Routing > OSPF > Setup > NSF** **Configuration > Device Setup > Routing > OSPFv3 > Setup > NS**
AAA Features	
Layer 2 Security Group Tag Imposition	You can now use security group tagging combined with Ethernet tagg policies. SGT plus Ethernet Tagging, also called Layer 2 SGT Impos the ASA to send and receive security group tags on Gigabit Ethernet using Cisco proprietary Ethernet framing (Ether Type 0x8909), whic insertion of source security group tags into plain-text Ethernet frame We introduced or modified the following commands: **cts manual**, **p sgt**, **propagate sgt**, **cts role-based sgt-map**, **show cts sgt-map**, **pac capture**, **show capture**, **show asp drop**, **show asp table classify**, **sh running-config all**, **clear configure all**, and **write memory** We modified the following screens: **Configuration > Device Setup > Interfaces > Add Interface > Ad** **Configuration > Device Setup > Interfaces > Add Redundant Int Advanced** **Configuration > Device Setup > Add Ethernet Interface > Advan** **Wizards > Packet Capture Wizard** **Tools > Packet Tracer**
Removal of AAA Windows NT domain authentication	We removed NTLM support for remote access VPN users. We deprecated the following command: aaa-server protocol nt We modified the following screen: **Configuration > Remote Access AAA/Local Users > AAA Server Groups > Add AAA Server Gro**

Feature	Description
ASDM Identity Certificate Wizard	When using the current Java version, the ASDM Launcher requires a tru certificate. An easy approach to fulfill the certificate requirements is to i self-signed identity certificate. The ASDM Identity Certificate Wizard r creating a self-signed identity certificate easy. When you first launch AS do not have a trusted certificate, you are prompted to launch ASDM with Start; this new wizard starts automatically. After creating the identity ce you need to register it with the Java Control Panel. See https://www.cisco.com/go/asdm-certificate for instructions. We added the following screen: **Wizards > ASDM Identity Certificate**
Monitoring Features	
Monitoring Aggregated Traffic for Physical Interfaces	The **show traffic** command output has been updated to include aggregat for physical interfaces information. To enable this feature, you must firs **sysopt traffic detailed-statistics** command.
show tech support enhancements	The **show tech support** command now includes **show resource usage d 1** output, including information about xlates, conns, inspects, syslogs, ar This information is helpful for diagnosing performance issues. We modified the following command: **show tech support** We did not add or modify any screens.
ASDM can save Botnet Traffic Filter reports as HTML instead of PDF	ASDM can no longer save Botnet Traffic Filter reports as PDF files; it c save them as HTML. The following screen was modified: **Monitoring > Botnet Traffic Filte**

New Features in Version 9.2

New Features in ASA 9.2(4)/ ASDM 7.4(3)

Released: July 16, 2015

Feature	Description
Platform Features	
Show invalid usernames in syslog messages	You can now show invalid usernames in syslog messages for unsuccessf attempts. The default setting is to hide usernames when the username is if the validity is unknown. If a user accidentally types a password instea username, for example, then it is more secure to hide the "username" in th syslog message. You might want to show invalid usernames to help with troubleshooting login issues. We introduced the following command: **no logging hide username** We modified the following screen: **Configuration > Device Manageme Logging > Syslog Setup**

Feature	Description
DHCP features	
DHCP Relay server validates the DHCP Server Identifier for replies	If the ASA DHCP relay server receives a reply from an incorrect DH now verifies that the reply is from the correct server before acting on
Monitoring Features	
NAT-MIB cnatAddrBindNumberOfEntries and cnatAddrBindSessionCount OIDs to allow polling for Xlate count.	Support was added for the NAT-MIB cnatAddrBindNumberOfEntrie cnatAddrBindSessionCount OIDs to support xlate_count and max_x SNMP. This data is equivalent to the **show xlate count** command. We did not modify any ASDM screens. *Also available in 8.4(5) and 9.1(5).*

New Features in ASA 9.2(3)/ ASDM 7.3(1.101)

Released: December 15, 2014

Feature	Description
Remote Access Features	
Clientless SSL VPN session cookie access restriction	You can now prevent a Clientless SSL VPN session cookie from bei by a third party through a client-side script such as Javascript. **Note** Use this feature only if Cisco TAC advises you to do so. I command presents a security risk because the following SSL VPN features will not work without any warning. • Java plug-ins • Java rewriter • Port forwarding • File browser • Sharepoint features that require desktop applications MS Office applications) • AnyConnect Web launch • Citrix Receiver, XenDesktop, and Xenon • Other non-browser-based and browser plugin-based We introduced the following command: **http-only-cookie** We introduced the following screen: **Configuration > Remote Acce Clientless SSL VPN Access > Advanced > HTTP Cookie**

New Features in ASA 9.2(2.4)/ASDM 7.2(2)

Released: August 12, 2014

Note Version 9.2(2) was removed from Cisco.com due to build issues; please upgrade to Version 9.2(2.4) or later.

Feature	Description
Platform Features	
ASA 5585-X (all models) support for the matching ASA FirePOWER SSP hardware module. ASA 5512-X through ASA 5555-X support for the ASA FirePOWER software module.	The ASA FirePOWER module supplies next-generation firewall services, Next-Generation IPS (NGIPS), Application Visibility and Control (AVC filtering, and Advanced Malware Protection (AMP).You can use the mo single or multiple context mode, and in routed or transparent mode. We introduced or modified the following commands: **capture interface asa_dataplane**, **debug sfr**, **hw-module module 1 reload**, **hw-module reset**, **hw-module module 1 shutdown**, **session do setup host ip, sessi get-config, session do password-reset, session sfr, sfr, show asp table domain sfr**, **show capture**, **show conn**, **show module sfr**, **show servic sw-module sfr**. We introduced the following screens: **Home > ASA FirePOWER Status** **Wizards > Startup Wizard > ASA FirePOWER Basic Configuratio** **Configuration > Firewall > Service Policy Rules > Add Service Polic Rule Actions > ASA FirePOWER Inspection**
Remote Access Features	
Internet Explorer 11 browser support on Windows 8.1 and Windows 7 for clientless SSL VPN	We added support for Internet Explorer 11 with Windows 7 and Windov clientless SSL VPN.. We did not modify any commands. We did not modify any screens.

New Features in ASA 9.2(1)/ASDM 7.2(1)

Released: April 24, 2014

Note The ASA 5510, ASA 5520, ASA 5540, ASA 5550, and ASA 5580 are not supported in this release or later. ASA Version 9.1 was the final release for these models.

Feature	Description
Platform Features	

Feature	Description
The Cisco Adaptive Security Virtual Appliance (ASAv) has been added as a new platform to the ASA series.	The ASAv brings full firewall functionality to virtualized environme data center traffic and multi-tenant environments. The ASAv runs or vSphere. You can manage and monitor the ASAv using ASDM or th
Routing Features	
BGP Support	We now support the Border Gateway Protocol (BGP). BGP is an inte system routing protocol. BGP is used to exchange routing informatic Internet and is the protocol used between Internet service providers We introduced the following commands**: router bgp, bgp maxas-li log-neighbor-changes, bgp transport path-mtu-discovery, bgp fast-external-fallover, bgp enforce-first-as, bgp asnotation dot, tin default local-preference, bgp always-compare-med, bgp bestpath compare-routerid, bgp deterministic-med, bgp bestpath med miss policy-list, match as-path, match community, match metric, matcl access-list, community-list, address-family ipv4, bgp router-id, d table-map, bgp suppress-inactive, bgp redistribute-internal, bgp bgp nexthop, aggregate-address, neighbor, bgp inject-map, show bgp cidr-only, show bgp all community, show bgp all neighbors, community, show bgp community-list, show bgp filter-list, show injected-paths, show bgp ipv4 unicast, show bgp neighbors, show show bgp pending-prefixes, show bgp prefix-list, show bgp regex replication, show bgp rib-failure, show bgp route-map, show bgp show bgp system-config, show bgp update-group, clear route net maximum-path, network.** We modified the following commands: **show route**, **show route sur running-config router**, **clear config router**, **clear route all**, **timers timers pacing**, **timers throttle**, **redistribute bgp**. We introduced the following screens: **Configuration > Device Setup > Routing > BGP** **Monitoring > Routing > BGP Neighbors, Monitoring > Routing >** We modified the following screens: **Configuration > Device Setup > Routing > Static Routes> Add > Route** **Configuration > Device Setup > Routing > Route Maps> Add > Map**
Static route for Null0 interface	Sending traffic to a Null0 interface results in dropping the packets de specified network. This feature is useful in configuring Remotely Tri Hole (RTBH) for BGP. We modified the following command: **route**. We modified the following screen: Configuration > Device Setup > Ro Routes> Add > Add Static Route

Feature	Description
OSPF support for Fast Hellos	OSPF supports the Fast Hello Packets feature, resulting in a configuratio results in faster convergence in an OSPF network. We modified the following command: **ospf dead-interval** We modified the following screen: Configuration > Device Setup > Rou OSPF > Interface > Edit OSPF Interface Advanced properties
New OSPF Timers	New OSPF timers were added; old ones were deprecated. We introduced the following commands: **timers lsa arrival, timers pacin throttle**. We removed the following commands: **timers spf, timers lsa-grouping** We modified the following screen: **Configuration > Device Setup > Ro OSPF > Setup > Edit OSPF Process Advanced Properties**
OSPF Route filtering using ACL	Route filtering using ACL is now supported. We introduced the following command: **distribute-list** We introduced the following screen: Configuration > Device Setup > Ro OSPF > Filtering Rules > Add Filter Rules
OSPF Monitoring enhancements	Additional OSPF monitoring information was added. We modified the following commands: **show ospf events, show ospf ri ospf statistics, show ospf border-routers [detail], show ospf interfac**
OSPF redistribute BGP	OSPF redistribution feature was added. We added the following command: **redistribute bgp** We added the following screen: Configuration > Device Setup > Routin > Redistribution
EIGRP Auto- Summary	For EIGRP, the Auto-Summary field is now disabled by default. We modified the following screen: Configuration > Device Setup > Rou EIGRP > Setup > Edit EIGRP Process Advanced Properties
High Availability Features	
Support for cluster members at different geographical locations (inter-site) for transparent mode	You can now place cluster members at different geographical locations w Spanned EtherChannel mode in transparent firewall mode. Inter-site clust spanned EtherChannels in routed firewall mode is not supported. We did not modify any commands. We did not modify any ASDM screens.

Feature	Description
Static LACP port priority support for clustering	Some switches do not support dynamic port priority with LACP (activ links). You can now disable dynamic port priority to provide better c with spanned EtherChannels. You should also follow these guideline • Network elements on the cluster control link path should not ve checksum. Redirected traffic over the cluster control link does n correct L4 checksum. Switches that verify the L4 checksum coul to be dropped. • Port-channel bundling downtime should not exceed the configu interval. We introduced the following command: **clacp static-port-priority**. We modified the following screen: Configuration > Device Manager Availability and Scalability > ASA Cluster
Support for 32 active links in a spanned EtherChannel for clustering	ASA EtherChannels now support up to 16 active links. With *spanned* E that functionality is extended to support up to 32 active links across when used with two switches in a vPC and when you disable dynamic The switches must support EtherChannels with 16 active links, for e Cisco Nexus 7000 with with F2-Series 10 Gigabit Ethernet Module. For switches in a VSS or vPC that support 8 active links, you can no 16 active links in the spanned EtherChannel (8 connected to each switch the spanned EtherChannel only supported 8 active links and 8 standb for use with a VSS/vPC. **Note** If you want to use more than 8 active links in a spanned E you cannot also have standby links; the support for 9 to 3 requires you to disable cLACP dynamic port priority tha use of standby links. We introduced the following command: **clacp static-port-priority**. We modified the following screen: Configuration > Device Manager Availability and Scalability > ASA Cluster
Support for 16 cluster members for the ASA 5585-X	The ASA 5585-X now supports 16-unit clusters. We did not modify any commands. We did not modify any ASDM screens.
Support for clustering with the Cisco Nexus 9300	The ASA supports clustering when connected to the Cisco Nexus 93
Remote Access Features	

Feature	Description
ISE Change of Authorization	The ISE Change of Authorization (CoA) feature provides a mechanism the attributes of an authentication, authorization, and accounting (AAA) after it is established. When a policy changes for a user or user group in A packets can be sent directly to the ASA from the ISE to reinitialize auth and apply the new policy. An Inline Posture Enforcement Point (IPEP) is required to apply access control lists (ACLs) for each VPN session establ the ASA. When an end user requests a VPN connection the ASA authenticates the the ISE and receives a user ACL that provides limited access to the netw accounting start message is sent to the ISE to register the session. Posture a occurs directly between the NAC agent and the ISE. This process is tran the ASA. The ISE sends a policy update to the ASA via a CoA "policy p identifies a new user ACL that provides increased network access privil Additional policy evaluations may occur during the lifetime of the conn transparent to the ASA, via subsequent CoA updates. We introduced the following commands: **dynamic-authorization, autho debug radius dynamic-authorization**. We modified the following commands: **without-csd** [**anyconnect**], **interim-accounting-update** [**periodic** [*interval*]]. We removed the following commands: **nac-policy**, **eou**, **nac-settings**. We modified the following screen: Configuration > Remote Access VPN AAA/Local Users > AAA Server Groups > Add/Edit AAA Server Grou
Improved clientless rewriter HTTP 1.1 compression handling	The rewriter has been changed so that if the client supports compressed and the content will not be rewritten, then it will accept compressed con the server. If the content must be rewritten and it is identified as being co it will be decompressed, rewritten, and if the client supports it, recompr We did not introduce or modify any commands. We did not introduce or modify any ASDM screens.
OpenSSL upgrade	The version of OpenSSL on the ASA will be updated to version 1.0.1e. **Note** We disabled the heartbeat option, so the ASA is not vulnera Heartbleed Bug. We did not introduce or modify any commands. We did not introduce or modify any ASDM screens.
Interface Features	

Feature	Description
Support for 16 active links in an EtherChannel	You can now configure up to 16 active links in an EtherChannel. Pre could have 8 active links and 8 standby links. Be sure your switch ca active links (for example the Cisco Nexus 7000 with with F2-Series Ethernet Module). **Note** If you upgrade from an earlier ASA version, the maxim interfaces is set to 8 for compatibility purposes (the **lacp** command). We modified the following commands: **lacp max-bundle** and **port-c min-bundle**. We modified the following screen: Configuration > Device Setup > Add/Edit EtherChannel Interface > Advanced.
Maximum MTU is now 9198 bytes	The maximum MTU that the ASA can use is 9198 bytes (check for y exact limit at the CLI help). This value does not include the Layer 2 Formerly, the ASA let you specify the maximum MTU as 65535 byt inaccurate and could cause problems. If your MTU was set to a valu 9198, then the MTU is automatically lowered when you upgrade. In this MTU change can cause an MTU mismatch; be sure to set any co equipment to use the new MTU value. We modified the following command: **mtu** We modified the following screen: **Configuration > Device Setup > Settings > Interfaces > Edit Interface > Advanced** *Also in Version 9.1(6).*
Monitoring Features	
Embedded Event Manager (EEM)	The EEM feature enables you to debug problems and provides gener logging for troubleshooting. The EEM responds to events in the EEM performing actions. There are two components: events that the EEM event manager applets that define actions. You may add multiple eve event manager applet, which triggers it to invoke the actions that hav configured on it. We introduced or modified the following commands: **event manage description**, **event syslog id**, **event none**, **event timer**, **event crashi cli command**, **output**, **show running-config event manager**, **event m show event manager**, **show counters protocol eem**, **clear configur manager**, **debug event manager**, **debug menu eem**. We introduced the following screens: Configuration > Device Manag Advanced > Embedded Event Manager, Monitoring > Properties > E

Feature	Description
SNMP hosts, host groups, and user lists	You can now add up to 4000 hosts. The number of supported active poll destinations is 128. You can specify a network object to indicate the ind hosts that you want to add as a host group. You can associate more than with one host. We introduced or modified the following commands: **snmp-server host snmp-server user-list**, **show running-config snmp-server**, **clear confi snmp-server**. We modified the following screen: Configuration > Device Managemen Management Access > SNMP.
SNMP message size	The limit on the message size that SNMP sends has been increased to 1
SNMP OIDs and MIBs	The ASA now supports the cpmCPUTotal5minRev OID. The ASAv has been added as a new product to the SNMP sysObjectID entPhysicalVendorType OID. The CISCO-PRODUCTS-MIB and CISCO-ENTITY-VENDORTYPE- have been updated to support the new ASAv platform.
Administrative Features	
Improved one-time password authentication	Administrators who have sufficient authorization privileges may enter p EXEC mode by entering their authentication credentials once. The **auto** option was added to the **aaa authorization exec** command. We modified the following command: **aaa authorization exec**. We modified the following screen: Configuration > Device Managemen Users/AAA > AAA Access > Authorization.
Auto Update Server certificate verification enabled by default	The Auto Update Server certificate verification is now enabled by defau configurations, you must explicitly disable certificate verification. If yo upgrading from an earlier release, and you did not enable certificate ver then certificate verification is not enabled, and you see the following wa `WARNING: The certificate provided by the auto-update servers be verified.` `In order to verify this certificate please use the verify-ce option.` The configuration will be migrated to explicitly configure no verificatio **auto-update server no-verification** We modified the following command: **auto-update server** [**verify-cert no-verification**]. We modified the following screen: Configuration > Device Managemen System/Image Configuration > Auto Update > Add Auto Update Server

New Features in Version 9.1

New Features in ASA 9.1(7.4)/ASDM 7.5(2.153)

Released: February 19, 2016

Note Version 9.1(7) was removed from Cisco.com due to build issues; please upgrade to Version 9.1(7.4) or later.

Feature	Description
Remote Access Features	
Clientless SSL VPN session cookie access restriction	You can now prevent a Clientless SSL VPN session cookie from being accesse party through a client-side script such as Javascript. **Note** Use this feature only if Cisco TAC advises you to do so. Enabling th presents a security risk because the following Clientless SSL VPN not work without any warning. • Java plug-ins • Java rewriter • Port forwarding • File browser • Sharepoint features that require desktop applications (for example, MS Office • AnyConnect Web launch • Citrix Receiver, XenDesktop, and Xenon • Other non-browser-based and browser plugin-based applications We introduced the following command: **http-only-cookie**. We introduced the following screen: **Configuration > Remote Access VPN > SSL VPN Access > Advanced > HTTP Cookie**. *This feature is also in 9.2(3) and 9.4(1).*
Configurable SSH encryption and HMAC algorithm	Users can select cipher modes when doing SSH encryption management and ca HMAC and encryption for varying key exchange algorithms. We introduced the following commands: **ssh cipher encryption** and **ssh ciphe** No ASDM support.

Feature	Description
Clientless SSL VPN cache disabled by default	The clientless SSL VPN cache is now disabled by default. Disabling the clientless cache provides better stability. If you want to enable the cache, you must manually `webvpn` `cache` `no disable` We modified the following command: **cache** We modified the following screen: **Configuration > Remote Access VPN > Clien VPN Access > Advanced > Content Cache** *Also available in 9.5(2).*
HTTP redirect support for IPv6	When you enable HTTP redirect to HTTPS for ASDM access or clientless SSL VPN now redirect traffic sent an to IPv6 address. We added functionality to the following command: **http redirect** We added functionality to the following screen: **Configuration > Device Manage HTTP Redirect**
Administrative Features	
show tech support enhancements	The **show tech support** command now: • Includes **dir all-filesystems** output—This output can be helpful in the followi • SSL VPN configuration: check if the required resources are on the ASA • Crash: check for the date timestamp and presence of a crash file • Includes **show resource usage count all 1** output—Includes information abou conns, inspects, syslogs, and so on. This information is helpful for diagnosing pe issues. • Removes the **show kernel cgroup-controller detail** output—This command c remain in the output of **show tech-support detail**. We modified the following command: **show tech support** We did not add or modify any screens.
Support for the cempMemPoolTable in the CISCO-ENHANCED-MEMPOOL-MIB	The cempMemPoolTable of the CISCO-ENHANCED-MEMPOOL-MIB is now su This is a table of memory pool monitoring entries for all physical entities on a manage **Note** The CISCO-ENHANCED-MEMPOOL-MIB uses 64-bit counters and reporting of memory on platforms with more than 4GB of RAM. We did not add or modify any commands. We did not add or modify any screens.

New Features in ASA 9.1(6)/ASDM 7.1(7)

Released: March 2, 2015

Feature	Description
Interface Features	
Maximum MTU is now 9198 bytes	The maximum MTU that the ASA can use is 9198 bytes (check for your model at the CLI help). This value does not include the Layer 2 header. Formerly, the specify the maximum MTU as 65535 bytes, which was inaccurate and could ca If your MTU was set to a value higher than 9198, then the MTU is automatical when you upgrade. In some cases, this MTU change can cause an MTU mismat set any connecting equipment to use the new MTU value. We modified the following command: **mtu** We modified the following screen: **Configuration > Device Setup > Interface Interfaces > Edit Interface > Advanced**

New Features in ASA 9.1(5)/ASDM 7.1(6)

Released: March 31, 2014

Feature	Description
Administrative Features	
Secure Copy client	The ASA now supports the Secure Copy (SCP) client to transfer files to and from a S We introduced the following commands: **ssh pubkey-chain**, **server (ssh pubkey-chain key-hash**, **ssh stricthostkeycheck**. We modified the following command: **copy scp**. We modified the following screens: Tools > File Management > File Transfer > Between Remote Server and Flash Confi Device Management > Management Access > File Access > Secure Copy (SCP) Ser
Improved one-time password authentication	Administrators who have sufficient authorization privileges may enter privileged EX entering their authentication credentials once. The **auto-enable** option was added to **authorization exec** command. We modified the following command: **aaa authorization exec**. We modified the following screen: Configuration > Device Management > Users/AA Access > Authorization.
Firewall Features	

Feature	Description
Transactional Commit Model on rule engine for access groups	When enabled, a rule update is applied after the rule compilation is completed; without a the rule matching performance. We introduced the following comands: **asp rule-engine transactional-commit**, **show runn asp rule-engine transactional-commit**, **clear configure asp rule-engine transactiona** We introduced the following screen: Configuration > Device Management > Advanced > Engine.
Monitoring Features	
SNMP hosts, host groups, and user lists	You can now add up to 4000 hosts. The number of supported active polling destinations i can specify a network object to indicate the individual hosts that you want to add as a ho You can associate more than one user with one host. We introduced or modified the following commands: **snmp-server host-group**, **snmp-s user-list**, **show running-config snmp-server**, **clear configure snmp-server**. We modified the following screen: **Configuration > Device Management > Manageme > SNMP**.
NAT-MIB cnatAddrBindNumberOfEntries and cnatAddrBindSessionCount OIDs to allow polling for Xlate count.	Support was added for the NAT-MIB cnatAddrBindNumberOfEntries and cnatAddrBindSes OIDs to support xlate_count and max_xlate_count for SNMP. This data is equivalent to the **show xlate count** command. We did not modify any ASDM screens. *Also available in 8.4(5).*
Remote Access Features	
AnyConnect DTLS Single session Performance Improvement	UDP traffic, such as streaming media, was being affected by a high number of dropped p when sent over an AnyConnect DTLS connection. For example, this could result in strean playing poorly or cease streaming completely. The reason for this was the relatively sma the flow control queue. We increased the DTLS flow-control queue size and offset this by reducing the admin cry size. For TLS sessions, the priority of the crypto command was increased to high to com for this change. For both DTLS and TLS sessions, the session will now persist even if pa dropped. This will prevent media streams from closing and ensure that the number of dr packets is comparable with other connection methods. We did not modify any commands. We did not modify any ASDM screens.

Feature	Description
Webtype ACL enhancements	We introduced URL normalization. URL normalization is an additional security featur path normalization, case normalization and scheme normalization. URLs specified i portal address bar are normalized before comparison; for making decisions on webvpn t For example, if you have an https://calo.cisco.com/checkout/Devices bookmark, an https://calo.cisco.com/checkout/Devices/* under web type acl seems to match. Howev normalization has been introduced, both bookmark URL and web type ACL are norm comparison. In this example, https://calo.cisco.com/checkout/Devices is normalized https://calo.cisco.com/checkout/Devices and https://calo.cisco.com/checkout/Device same, so the two do not match. You must configure the following to meet the requirement: • to permit the bookmark URL (https://calo.cisco.com/checkout/Devices), configu permit that URL • to permit the URLs within the Devices folder, configure the ACL to permit https://calo.cisco.com/checkout/Devices/* We did not modify any commands. We did not modify any ASDM screens.

New Features in ASA 9.1(4)/ASDM 7.1(5)

Released: December 9, 2013

Feature	Description
Remote Access Features	
HTML5 WebSocket proxying	HTML5 WebSockets provide persistent connections between clients and servers. Du establishment of the clientless SSL VPN connection, the handshake appears to the serv Upgrade request. The ASA will now proxy this request to the backend and provide a handshake is complete. Gateway mode is not currently supported. We did not modify any commands. We did not modify any ASDM screens.

Feature	Description
Inner IPv6 for IKEv2	IPv6 traffic can now be tunneled through IPsec/IKEv2 tunnels. This makes the ASA to An VPN connections fully IPv6 compliant. GRE is used when both IPv4 and IPv6 traffic ar tunneled, and when both the client and headend support GRE. For a single traffic type, c GRE is not supported by the client or the headend, we use straight IPsec. **Note** This feature requires AnyConnect Client Version 3.1.05 or later. Output of the **show ipsec sa** and **show vpn-sessiondb detail anyconnect** commands has updated to reflect the assigned IPv6 address, and to indicate the GRE Transport Mode se association when doing IKEv2 dual traffic. The **vpn-filter** command must now be used for both IPv4 and IPv6 ACLs. If the depraca **ipv6-vpn-filter** command is used to configure IPv6 ACLs the connection will be termin We did not modify any ASDM screens.
Mobile Devices running Citrix Server Mobile have additional connection options	Support for mobile devices connecting to Citrix server through the ASA now includes se a tunnel-group, and RSA Securid for authorization. Allowing mobile users to select diffe tunnel-groups allows the administrator to use different authentication methods. We introduced the **application-type** command to configure the default tunnel group for connections when a Citrix Receiver user does not choose a tunnel-group. A **none** action to the **vdi** command to disable VDI configuration for a particular group policy or user. We modified the following screen: **Configuration > Remote Access VPN > Clientless Access > VDI Access**.
Split-tunneling supports exclude ACLs	Split-tunneling of VPN traffic has been enhanced to support both exclude and include ACL ACLs were previously ignored. **Note** This feature requires AnyConnect Client Version 3.1.03103 or later. We did not modify any commands. We did not modify any ASDM screens.
High Availability and Scalability Features	
ASA 5500-X support for clustering	The ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, and ASA 5555-X now sup clusters. Clustering for 2 units is enabled by default in the base license; for the ASA 551 need the Security Plus license. We did not modify any commands. We did not modify any ASDM screens.

Feature	Description
Improved VSS and vPC support for health check monitoring	If you configure the cluster control link as an EtherChannel (recommended), and it is a VSS or vPC pair, you can now increase stability with health check monitoring. For s such as the Nexus 5000, when one unit in the VSS/vPC is shutting down or booting up, member interfaces connected to that switch may appear to be Up to the ASA, but they a traffic on the switch side. The ASA can be erroneously removed from the cluster if yo holdtime timeout to a low value (such as .8 seconds), and the ASA sends keepalive m one of these EtherChannel interfaces. When you enable the VSS/vPC health check fea floods the keepalive messages on all EtherChannel interfaces in the cluster control li that at least one of the switches can receive them. We modified the following command: **health-check** [**vss-enabled**] We modified the following screen: Configuration > Device Management > High Ava Scalability > ASA Cluster
Support for cluster members at different geographical locations (inter-site); Individual Interface mode only	You can now place cluster members at different geographical locations when using in interface mode. See the configuration guide for inter-site guidelines. We did not modify any commands. We did not modify any ASDM screens.
Support for clustering with the Cisco Nexus 5000 and Cisco Catalyst 3750-X	The ASA supports clustering when connected to the Cisco Nexus 5000 and Cisco Cat We modified the following command: **health-check** [**vss-enabled**] We modified the following screen: Configuration > Device Management > High Ava Scalability > ASA Cluster
Basic Operation Features	
DHCP rebind function	During the DHCP rebind phase, the client now attempts to rebind to other DHCP ser tunnel group list. Prior to this release, the client did not rebind to an alternate server, wh lease fails to renew. We introduced the following commands: **show ip address dhcp lease proxy, show i dhcp lease summary**, and **show ip address dhcp lease server**. We introduced the following screen: **Monitoring > Interfaces > DHCP> DHCP Lease**
Troubleshooting Features	

Feature	Description
Crashinfo dumps include AK47 framework information	Application Kernel Layer 4 to 7 (AK47) framework-related information is now available in dumps. A new option, **ak47**, has been added to the **debug menu** command to help in de AK47 framework issues. The framework-related information in the crashinfo dump incl following: • Creating an AK47 instance. • Destroying an AK47 instance. • Generating an crashinfo with a memory manager frame. • Generating a crashinfo after fiber stack overflow. • Generating a crashinfo after a local variable overflow. • Generating a crashinfo after an exception has occurred.

New Features in ASA 9.1(3)/ASDM 7.1(4)

Released: September 18, 2013

Feature	Description
Module Features	
Support for the ASA CX module in multiple context mode	You can now configure ASA CX service policies per context on the ASA. **Note** Although you can configure per context ASA service policies, the ASA CX itself (configured in PRSM) is a single context mode device; the context-spec coming from the ASA is checked against the common ASA CX policy. Requires ASA CX 9.2(1) or later. We did not modify any commands. We did not modify any ASDM screens.
ASA 5585-X with SSP-40 and -60 support for the ASA CX SSP-40 and -60	ASA CX SSP-40 and -60 modules can be used with the matching level ASA 5585-X wi and -60. Requires ASA CX 9.2(1) or later. We did not modify any commands. We did not modify any screens.

Feature	Description
Filtering packets captured on the ASA CX backplane	You can now filter packets that have been captured on the ASA CX backplane using **access-list** keyword with the **capture interface asa_dataplane** command. Control t to the ASA CX module is not affected by the access-list or match filtering; the ASA control traffic. In multiple context mode, configure the packet capture per context. N control traffic in multiple context mode goes only to the system execution space. Be control traffic cannot be filtered using an access list or match, these options are not a system execution space. Requires ASA CX 9.2(1) or later. We modified the following command: **capture interface asa_dataplane**. A new option, Use backplane channel, was added to the Ingress Traffic Selector scre Egress Selector screen, in the Packet Capture Wizard to enable filtering of packets th captured on the ASA CX backplane.
Monitoring Features	
Ability to view top 10 memory users	You can now view the top bin sizes allocated and the top 10 PCs for each allocated b Previously, you had to enter multiple commands to see this information (the **show m** command and the **show memory binsize** command); the new command provides for qu of memory issues. We introduced the following command: **show memory top-usage**. We did not modify any ASDM screens. *Also available in 8.4(6).*
Smart Call Home	We added a new type of Smart Call Home message to support ASA clustering. A Smart Call Home clustering message is sent for only the following three events: • When a unit joins the cluster • When a unit leaves the cluster • When a cluster unit becomes the cluster master Each message that is sent includes the following information: • The active cluster member count • The output of the **show cluster info** command and the **show cluster history** co cluster master We modified the following commands: **show call-home, show running-config call-** We did not modify any ASDM screens. *Also available in 9.0(3).*
Remote Access Features	

Feature	Description
user-storage value command password is now encrypted in **show** commands	The password in the **user-storage value** command is now encrypted when you enter **sho running-config**. We modified the following command: **user-storage value**. We modified the following screen: **Configuration > Remote Access VPN > Clientless Access > Group Policies > More Options > Session Settings**. *Also available in 8.4(6).*

New Features in ASA 9.1(2)/ASDM 7.1(3)

Released: May 14, 2013

Note Features added in 8.4(6) are not included in 9.1(2) unless they are explicitly listed in this table.

Feature	Description
Certification Features	
FIPS and Common Criteria certifications	The FIPS 140-2 Non-Proprietary Security Policy was updated as part of the Level 2 FIP validation for the Cisco ASA series, which includes the Cisco ASA 5505, ASA 5510, A ASA 5540, ASA 5550, ASA 5580, ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 554 5555-X, ASA 5585-X, and the ASA Services Module. The Common Criteria Evaluation Assurance Level 4 (EAL4) was updated, which provide for a specific Target of Evaluation (TOE) of the Cisco ASA and VPN platform solutions
Encryption Features	
Support for IPsec LAN-to-LAN tunnels to encrypt failover and state link communications	Instead of using the proprietary encryption for the failover key (the **failover key** comma can now use an IPsec LAN-to-LAN tunnel for failover and state link encryption. **Note** Failover LAN-to-LAN tunnels do not count against the IPsec (Other VPN) We introduced or modified the following commands: **failover ipsec pre-shared-key**, **sh vpn-sessiondb**. We modified the following screen: **Configuration > Device Management > High Avai Failover > Setup**.

Feature	Description
Additional ephemeral Diffie-Hellman ciphers for SSL encryption	The ASA now supports the following ephemeral Diffie-Hellman (DHE) SSL cipher • DHE-AES128-SHA1 • DHE-AES256-SHA1 These cipher suites are specified in RFC 3268, *Advanced Encryption Standard (AES) for Transport Layer Security (TLS*). When supported by the client, DHE is the preferred cipher because it provides Perfe Secrecy. See the following limitations: • DHE is not supported on SSL 3.0 connections, so make sure to also enable TLS SSL server. `!! set server version` `ciscoasa(config)# ssl server-version tlsv1 sslv3` `!! set client version` `ciscoasa(config) # ssl client-version any` • Some popular applications do not support DHE, so include at least one other SS method to ensure that a cipher suite common to both the SSL client and server c • Some clients may not support DHE, including AnyConnect 2.5 and 3.0, Cisco Se and Internet Explorer 9.0. We modified the following command: **ssl encryption**. We modified the following screen: **Configuration > Device Management > Advan Settings**. *Also available in 8.4(4.1).*
Management Features	
Support for administrator password policy when using the local database	When you configure authentication for CLI or ASDM access using the local databas configure a password policy that requires a user to change their password after a spe of time and also requires password standards such as a minimum length and the mini of changed characters. We introduced the following commands: **change-password, password-policy lifeti password-policy minimum changes**, **password-policy minimum-length**, **passwor minimum-lowercase**, **password-policy minimum-uppercase**, **password-policy minim password-policy minimum-special**, **password-policy authenticate enable**, **clear c password-policy**, **show running-config password-policy**. We introduced the following screen: **Configuration > Device Management > Users Password Policy**. *Also available in 8.4(4.1).*

Feature	Description
Support for SSH public key authentication	You can now enable public key authentication for SSH connections to the ASA on a per- You can specify a public key file (PKF) formatted key or a Base64 key. The PKF key ca 4096 bits. Use PKF format for keys that are too large to for the ASA support of the Base (up to 2048 bits). We introduced the following commands: **ssh authentication**. We introduced the following screens: **Configuration > Device Management > Users/AAA > User Accounts > Edit User Ac Public Key Authentication** and **Configuration > Device Management > Users/AAA Accounts > Edit User Account > Public Key Using PKF**. *Also available in 8.4(4.1); PKF key format support is only in 9.1(2).*
AES-CTR encryption for SSH	The SSH server implementation in the ASA now supports AES-CTR mode encryption.
Improved SSH rekey interval	An SSH connection is rekeyed after 60 minutes of connection time or 1 GB of data traff We introduced the following command: **show ssh sessions detail**.
Support for Diffie-Hellman Group 14 for the SSH Key Exchange	Support for Diffie-Hellman Group 14 for SSH Key Exchange was added. Formerly, only was supported. We introduced the following command: **ssh key-exchange**. We modified the following screen: **Configuration > Device Management > Manageme > ASDM/HTTPS/Telnet/SSH**. *Also available in 8.4(4.1).*
Support for a maximum number of management sessions	You can set the maximum number of simultaneous ASDM, SSH, and Telnet sessions. We introduced the following commands: **quota management-session**, **show running-co management-session**, **show quota management-session**. We introduced the following screen: **Configuration > Device Management > Manageme > Management Session Quota**. *Also available in 8.4(4.1).*
Support for a pre-login banner in ASDM	Administrator can define a message that appears before a user logs into ASDM for mana access. This customizable content is called a pre-login banner, and can notify users of sp requirements or important information.

Feature	Description
The default Telnet password was removed	To improve security for management access to the ASA, the default login password f removed; you must manually set the password before you can log in using Telnet. **No** password is only used for Telnet if you do not configure Telnet user authentication (t **authentication telnet console** command). Formerly, when you cleared the password, the ASA restored the default of "cisco." N clear the password, the password is removed. The login password is also used for Telnet sessions from the switch to the ASASM (s command). For initial ASASM access, you must use the **service-module session** con you set a login password. We modified the following command: **passwd**. We did not modify any ASDM screens. *Also available in 9.0(2).*
Platform Features	
Support for Power-On Self-Test (POST)	The ASA runs its power-on self-test at boot time even if it is not running in FIPS 140 mode. Additional tests have been added to the POST to address the changes in the AES-GC algorithms, ECDSA algorithms, PRNG, and Deterministic Random Bit Generator Vali (DRBGVS).
Improved pseudo-random number generation (PRNG)	The X9.31 implementation has been upgraded to use AES-256 encryption instead of 3D to comply with the Network Device Protection Profile (NDPP) in single-core ASAs.
Support for image verification	Support for SHA-512 image integrity checking was added. We modified the following command: **verify**. We did not modify any ASDM screens. *Also available in 8.4(4.1).*
Support for private VLANs on the ASA Services Module	You can use private VLANs with the ASASM. Assign the primary VLAN to the ASA ASASM automatically handles secondary VLAN traffic. There is no configuration re ASASM for this feature; see the switch configuration guide for more information.
CPU profile enhancements	The **cpu profile activate** command now supports the following: • Delayed start of the profiler until triggered (global or specific thread CPU%) • Sampling of a single thread We modified the following command: **cpu profile activate** [*n-samples*] [**sample-pro** *process-name*] [**trigger cpu-usage** *cpu%* [*process-name*]. We did not modify any ASDM screens. *Also available in 8.4(6).*
DHCP Features	

Feature	Description
DHCP relay servers per interface (IPv4 only)	You can now configure DHCP relay servers per-interface, so requests that enter a given are relayed only to servers specified for that interface. IPv6 is not supported for per-interf relay. We introduced or modified the following commands: **dhcprelay server** (interface config **clear configure dhcprelay**, **show running-config dhcprelay**. We modified the following screen: **Configuration > Device Management > DHCP > D Relay**.
DHCP trusted interfaces	You can now configure interfaces as trusted interfaces to preserve DHCP Option 82. DH 82 is used by downstream switches and routers for DHCP snooping and IP Source Guard. if the ASA DHCP relay agent receives a DHCP packet with Option 82 already set, but th field (which specifies the DHCP relay agent address that is set by the relay agent before i the packet to the server) is set to 0, then the ASA will drop that packet by default. You c preserve Option 82 and forward the packet by identifying an interface as a trusted interfa We introduced or modified the following commands: **dhcprelay information trusted**, d **informarion trust-all**, **show running-config dhcprelay**. We modified the following screen: **Configuration > Device Management > DHCP > D Relay**.
Module Features	
ASA 5585-X support for network modules	The ASA 5585-X now supports additional interfaces on network modules in slot 1. You one or two of the following optional network modules: • ASA 4-port 10G Network Module • ASA 8-port 10G Network Module • ASA 20-port 1G Network Module *Also available in 8.4(4.1).*
ASA 5585-X DC power supply support	Support was added for the ASA 5585-X DC power supply. *Also available in 8.4(5).*
Support for ASA CX monitor-only mode for demonstration purposes	For demonstration purposes only, you can enable monitor-only mode for the service poli forwards a copy of traffic to the ASA CX module, while the original traffic remains una Another option for demonstration purposes is to configure a traffic-forwarding interface a service policy in monitor-only mode. The traffic-forwarding interface sends all traffic the ASA CX module, bypassing the ASA. We modified or introduced the following commands: **cxsc** {**fail-close** | **fail-open**} **moni traffic-forward cxsc monitor-only**. We modified the following screen: **Configuration > Firewall > Service Policy Rules > Ac Policy Rule > Rule Actions > ASA CX Inspection**. The traffic-forwarding feature is supported by CLI only.

Feature	Description
Support for the ASA CX module and NAT 64	You can now use NAT 64 in conjunction with the ASA CX module. We did not modify any commands. We did not modify any ASDM screens.
NetFlow Features	
Support for NetFlow flow-update events and an expanded set of NetFlow templates	In addition to adding the flow-update events, there are now NetFlow templates that a track flows that experience a change to their IP version with NAT, as well as IPv6 flo IPv6 after NAT. Two new fields were added for IPv6 translation support. Several NetFlow field IDs were changed to their IPFIX equivalents. For more information, see the *Cisco ASA Implementation Note for NetFlow Collecto*
Firewall Features	
EtherType ACL support for IS-IS traffic (transparent firewall mode)	In transparent firewall mode, the ASA can now pass IS-IS traffic using an EtherType We modified the following command: **access-list ethertype** {**permit** | **deny**} **is-is**. We modified the following screen: **Configuration > Device Management > Manag > EtherType Rules**. *Also available in 8.4(5).*
Decreased the half-closed timeout minimum value to 30 seconds	The half-closed timeout minimum value for both the global timeout and connection t lowered from 5 minutes to 30 seconds to provide better DoS protection. We modified the following commands: **set connection timeout half-closed**, **timeou** We modified the following screens: **Configuration > Firewall > Service Policy Rules > Connection Settings** **Configuration > Firewall > Advanced > Global Timeouts.**
Remote Access Features	

Feature	Description
IKE security and performance improvements	The number of IPsec-IKE security associations (SAs) can be limited for IKE v1 now, as IKE v2. We modified the following command: **crypto ikev1 limit**. We modified the following screen: **Configuration > Site-to-Site VPN > Advanced > I Parameters**.
	The IKE v2 Nonce size has been increased to 64 bytes. There are no ASDM screen or CLI changes.
	For IKE v2 on Site-to-Site, a new algorithm ensures that the encryption algorithm used l IPsec SAs is not higher strength than the parent IKE. Higher strength algorithms will be do to the IKE level. This new algorithm is enabled by default. We recommend that you do not disable this fe We introduced the following command: **crypto ipsec ikev2 sa-strength-enforcement**. We did not modify any ASDM screens.
	For Site-to-Site, IPsec data-based rekeying can be disabled. We modified the following command: **crypto ipsec security-association**. We modified the following screen: **Configuration > Site-to-Site > IKE Parameters**.
Improved Host Scan and ASA Interoperability	Host Scan and the ASA use an improved process to transfer posture attributes from the cl ASA. This gives the ASA more time to establish a VPN connection with the client and a dynamic access policy. *Also available in 8.4(5).*

Feature	Description
Clientless SSL VPN: Windows 8 Support	This release adds support for Windows 8 x86 (32-bit) and Windows 8 x64 (64-bit) oper We support the following browsers on Windows 8: • Internet Explorer 10 (desktop only) • Firefox (all supported Windows 8 versions) • Chrome (all supported Windows 8 versions) See the following limitations: • Internet Explorer 10: • The Modern (AKA Metro) browser is not supported. • If you enable Enhanced Protected Mode, we recommend that you add the A trusted zone. • If you enable Enhanced Protected Mode, Smart Tunnel and Port Forwarder supported. • A Java Remote Desktop Protocol (RDP) plugin connection to a Windows 8 PC is *Also available in 9.0(2).*
Cisco Secure Desktop: Windows 8 Support	CSD 3.6.6215 was updated to enable selection of Windows 8 in the Prelogin Policy ope check. See the following limitations: • Secure Desktop (Vault) is not supported with Windows 8. *Also available in 9.0(2).*
Dynamic Access Policies: Windows 8 Support	ASDM was updated to enable selection of Windows 8 in the DAP Operating System *Also available in 9.0(2).*
Monitoring Features	
NSEL	Flow-update events have been introduced to provide periodic byte counters for flow can change the time interval at which flow-update events are sent to the NetFlow coll filter to which collectors flow-update records will be sent. We introduced or modified the following commands: **flow-export active refresh-int** **flow-export event-type**. We modified the following screens: **Configuration > Device Management > Logging > NetFlow**. **Configuration > Firewall > Service Policy Rules > Add Service Policy Rule Wiza Actions > NetFlow > Add Flow Event** *Also available in 8.4(5).*

New Features in ASA 9.1(1)/ASDM 7.1(1)

Released: December 3, 2012

Note Features added in 8.4(4.x), 8.4(5), 8.4(6), and 9.0(2) are not included in 9.1(1) unless they were listed in the 9.0(1) feature table.

Feature	Description
Module Features	
Support for the ASA CX SSP for the ASA 5512-X through ASA 5555-X	We introduced support for the ASA CX SSP software module for the ASA ASA 5515-X, ASA 5525-X, ASA 5545-X, and ASA 5555-X. The ASA CX module requires a Cisco solid state drive (SSD) on the ASA. For more in about the SSD, see the ASA 5500-X hardware guide. We modified the following commands: **session cxsc**, **show module cxsc**, **s cxsc**. We did not modify any screens.

New Features in Version 9.0

New Features in ASA 9.0(4)/ASDM 7.1(4)

There were no new features in ASA 9.0(4)/ASDM 7.1(4).

New Features in ASA 9.0(3)/ASDM 7.1(3)

Released: July 22, 2013

Note Features added in 8.4(4.x), 8.4(5), and 8.4(6) are not included in 9.0(3) unless they were listed in the 9.0(1) feature table.

Feature	Description
Monitoring Features	

Feature	Description
Smart Call Home	We added a new type of Smart Call Home message to support ASA A Smart Call Home clustering message is sent for only the following • When a unit joins the cluster • When a unit leaves the cluster • When a cluster unit becomes the cluster master Each message that is sent includes the following information: • The active cluster member count • The output of the **show cluster info** command and the **show cl** command on the cluster master

New Features in ASA 9.0(2)/ASDM 7.1(2)

Released: February 25, 2013

Note Features added in 8.4(4.x), 8.4(5), and 8.4(6) are not included in 9.0(2) unless they were listed in the 9.0(1) feature table.

Feature	Description
Remote Access Features	

Feature	Description
Clientless SSL VPN: Windows 8 Support	This release adds support for Windows 8 x86 (32-bit) and Windows 8 x6 operating systems. We support the following browsers on Windows 8: • Internet Explorer 10 (desktop only) • Firefox (all supported Windows 8 versions) • Chrome (all supported Windows 8 versions) See the following limitations: • Internet Explorer 10: • The Modern (AKA Metro) browser is not supported. • If you enable Enhanced Protected Mode, we recommend that the ASA to the trusted zone. • If you enable Enhanced Protected Mode, Smart Tunnel and Port are not supported. • A Java Remote Desktop Protocol (RDP) plugin connection to a Wi PC is not supported.
Management Features	
The default Telnet password was removed	To improve security for management access to the ASA, the default login for Telnet was removed; you must manually set the password before you in using Telnet. **Note**: The login password is only used for Telnet if you configure Telnet user authentication (the **aaa authentication telnet con** command). Formerly, when you cleared the password, the ASA restored the default Now when you clear the password, the password is removed. The login password is also used for Telnet sessions from the switch to the (see the **session** command). For initial ASASM access, you must use the **service-module session** command, until you set a login password. We modified the following command: **passwd**. We did not modify any ASDM screens.

New Features in ASA 9.0(1)/ASDM 7.0(1)

Released: October 29, 2012

Note Features added in 8.4(4.x), 8.4(5), and 8.4(6) are not included in 9.0(1) unless they are explicitly listed in this table.

Feature	Description
Firewall Features	
Cisco TrustSec integration	Cisco TrustSec provides an access-control solution that builds upon identity-aware infrastructure to ensure data confidentiality between ne and integrate security access services on one platform. In the Cisco T solution, enforcement devices utilize a combination of user attributes attributes to make role-based and identity-based access control decis In this release, the ASA integrates with Cisco TrustSec to provide se based policy enforcement. Access policies within the Cisco TrustSec topology-independent, based on the roles of source and destination d than on network IP addresses. The ASA can utilize the Cisco TrustSec solution for other types of s based policies, such as application inspection; for example, you can class map containing an access policy based on a security group. We introduced or modified the following commands: **access-list exte enable**, **cts server-group**, **cts sxp default**, **cts sxp retry period**, **cts period**, **cts sxp connection peer**, **cts import-pac**, **cts refresh enviro object-group security**, **security-group**, **show running-config cts**, s **running-config object-group**, **clear configure cts**, **clear configure o show cts**, **show object-group**, **show conn security-group**, **clear cts** We introduced the following MIB: CISCO-TRUSTSEC-SXP-MIB. We introduced or modified the following screens: **Configuration > Firewall > Identity by TrustSec** **Configuration > Firewall > Objects > Security Groups Object G** **Configuration > Firewall > Access Rules > Add Access Rules** **Monitoring > Properties > Identity by TrustSec > PAC** **Monitoring > Properties > Identity by TrustSec > Environment D** **Monitoring > Properties > Identity by TrustSec > SXP Connecti** **Monitoring > Properties > Identity by TrustSec > IP Mappings** **Monitoring > Properties > Connections** **Tools > Packet Tracer**

Feature	Description
Cisco Cloud Web Security (ScanSafe)	Cisco Cloud Web Security provides content scanning and other malware service for web traffic. It can also redirect and report about web traffic b user identity. **Note** Clientless SSL VPN is not supported with Cloud Web Secu sure to exempt any clientless SSL VPN traffic from the AS policy for Cloud Web Security. We introduced or modified the following commands: **class-map type in scansafe**, **default user group**, **http**[**s**] (parameters), **inspect scansafe**, **l match user group**, **policy-map type inspect scansafe**, **retry-count**, **sc scansafe general-options**, **server** {**primary** | **backup**}, **show conn scans scansafe server**, **show scansafe statistics**, **user-identity monitor**, **whit** We introduced or modified the following screens: **Configuration > Device Management > Cloud Web Security** **Configuration > Firewall > Objects > Class Maps > Cloud Web Secu** **Configuration > Firewall > Objects > Class Maps > Cloud Web Secu Add/Edit** **Configuration > Firewall > Objects > Inspect Maps > Cloud Web Se** **Configuration > Firewall > Objects > Inspect Maps > Cloud Web Se Add/Edit** **Configuration > Firewall > Objects > Inspect Maps > Cloud Web Se Add/Edit > Manage Cloud Web Security Class Maps** **Configuration > Firewall > Identity Options Configuration > Firewall Policy Rules** **Monitoring > Properties > Cloud Web Security**
Extended ACL and object enhancement to filter ICMP traffic by ICMP code	ICMP traffic can now be permitted/denied based on ICMP code. We introduced or modified the following commands: **access-list extend service-object**, **service**. We introduced or modified the following screens: **Configuration > Firewall > Objects > Service Objects/Groups Confi > Firewall > Access Rule**
Unified communications support on the ASASM	The ASASM now supports all Unified Communications features.
NAT support for reverse DNS lookups	NAT now supports translation of the DNS PTR record for reverse DNS when using IPv4 NAT, IPv6 NAT, and NAT64 with DNS inspection ena the NAT rule.

Feature	Description
Per-session PAT	The per-session PAT feature improves the scalability of PAT and, fo clustering, allows each member unit to own PAT connections; multi- connections have to be forwarded to and owned by the master unit. a per-session PAT session, the ASA sends a reset and immediately re xlate. This reset causes the end node to immediately release the connec the TIME_WAIT state. Multi-session PAT, on the other hand, uses the by default 30 seconds. For "hit-and-run" traffic, such as HTTP or H per-session feature can dramatically increase the connection rate sup address. Without the per-session feature, the maximum connection r address for an IP protocol is approximately 2000 per second. With th feature, the connection rate for one address for an IP protocol is 65535/*average-lifetime*. By default, all TCP traffic and UDP DNS traffic use a per-session PA traffic that can benefit from multi-session PAT, such as H.323, SIP, o can disable per-session PAT by creating a per-session deny rule. We introduced the following commands: **xlate per-session**, **clear co show running-config xlate**. We introduced the following screen: **Configuration > Firewall > A Per-Session NAT Rules**.
ARP cache additions for non-connected subnets	The ASA ARP cache only contains entries from directly-connected default. You can now enable the ARP cache to also include non-direc subnets. We do not recommend enabling this feature unless you kno risks. This feature could facilitate denial of service (DoS) attack aga a user on any interface could send out many ARP replies and overlo ARP table with false entries. You may want to use this feature if you use: • Secondary subnets. • Proxy ARP on adjacent routes for traffic forwarding. We introduced the following command: **arp permit-nonconnected**. We modified the following screen: Configuration > Device Manageme > ARP > ARP Static Table. *Also available in 8.4(5).*
SunRPC change from dynamic ACL to pin-hole mechanism	Previously, Sun RPC inspection does not support outbound access lis inspection engine uses dynamic access lists instead of secondary co In this release, when you configure dynamic access lists on the ASA supported on the ingress direction only and the ASA drops egress tra to dynamic ports. Therefore, Sun RPC inspection implements a pinho to support egress traffic. Sun RPC inspection uses this pinhole mechan outbound dynamic access lists. *Also available in 8.4(4.1).*

Feature	Description
Inspection reset action change	Previously, when the ASA dropped a packet due to an inspection engine ASA sent only one RST to the source device of the dropped packet. This could cause resource issues. In this release, when you configure an inspection engine to use a reset a a packet triggers a reset, the ASA sends a TCP reset under the following c • The ASA sends a TCP reset to the inside host when the **service reset** command is enabled. (The **service resetoutbound** command is ena default.) • The ASA sends a TCP reset to the outside host when the **service rese** command is enabled. (The **service resetinbound** command is disal default.) For more information, see the **service** command in the ASA command r This behavior ensures that a reset action will reset the connections on the on inside servers; therefore countering denial of service attacks. For outs the ASA does not send a reset by default and information is not revealed a TCP reset. *Also available in 8.4(4.1).*
Increased maximum connection limits for service policy rules	The maximum number of connections for service policy rules was incre 65535 to 2000000. We modified the following commands: **set connection conn-max**, **set co embryonic-conn-max**, **set connection per-client-embryonic-max**, **set co per-client-max**. We modified the following screen: **Configuration > Firewall > Service Rules > Connection Settings**. *Also available in 8.4(5)*
High Availability and Scalability Features	

Feature	Description
ASA Clustering for the ASA 5580 and 5585-X	ASA Clustering lets you group multiple ASAs together as a single lo A cluster provides all the convenience of a single device (manageme into a network) while achieving the increased throughput and redundan devices. ASA clustering is supported for the ASA 5580 and the ASA units in a cluster must be the same model with the same hardware sp See the configuration guide for a list of unsupported features when c enabled. We introduced or modified the following commands: **channel-group** **system-mac**, **clear cluster info**, **clear configure cluster**, **cluster ex** **group**, **cluster interface-mode**, **cluster-interface**, **conn-rebalance**, **console-replicate**, **cluster master unit**, **cluster remove unit**, **debug c** **lacp cluster**, **enable** (cluster group), **health-check**, **ip address**, **ipv6** (cluster group), **local-unit, mac-address** (interface), **mac-address p** **cluster, port-channel span-cluster, priority** (cluster group), **prompt** **show asp cluster counter**, **show asp table cluster chash-table**, **sho** **show cluster info**, **show cluster user-identity**, **show lacp cluster**, **s** **running-config cluster**. We introduced or modified the following screens: Home > Device Dashboard Home > Cluster Dashboard Home > Cluster Firewall Dashboard **Configuration > Device Management > Advanced > Address Poo** **Address Pools** **Configuration > Device Management > High Availability and Sc** **ASA Cluster** **Configuration > Device Management > Logging > Syslog Setup >** **Configuration > Device Setup > Interfaces > Add/Edit Interface** **Configuration > Device Setup > Interfaces > Add/Edit Interface** **Configuration > Device Setup > Interfaces > Add/Edit EtherChan** **> Advanced** **Configuration > Firewall > Advanced > Per-Session NAT Rules** **Monitoring > ASA Cluster Monitoring > Properties > System Reso** **> Cluster Control Link** **Tools > Preferences > General** **Tools > System Reload** **Tools > Upgrade Software from Local Computer** **Wizards > High Availability and Scalability Wizard** **Wizards > Packet Capture Wizard** **Wizards > Startup Wizard**

Feature	Description
OSPF, EIGRP, and Multicast for clustering	For OSPFv2 and OSPFv3, bulk synchronization, route synchronization, an EtherChannels are supported in the clustering environment. For EIGRP, bulk synchronization, route synchronization, and spanned Ethe are supported in the clustering environment. Multicast routing supports clustering. We introduced or modified the following commands: **show route cluste route cluster**, **show mfib cluster**, **debug mfib cluster**.
Packet capture for clustering	To support cluster-wide troubleshooting, you can enable capture of cluste traffic on the master unit using the **cluster exec capture** command, whi automatically enabled on all of the slave units in the cluster. The **cluster** keywords are the new keywords that you place in front of the **capture** c to enable cluster-wide capture. We modified the following commands: **capture**, **show capture**. We modified the following screen: Wizards > **Packet Capture Wizard**
Logging for clustering	Each unit in the cluster generates syslog messages independently. You c **logging device-id** command to generate syslog messages with identical o device IDs to make messages appear to come from the same or different the cluster. We modified the following command: **logging device-id**. We modified the following screen: **Configuration > Logging > Syslog Advanced > Advanced Syslog Configuration**.
Support for clustering with the Cisco Nexus 7000 and Cisco Catalyst 6500	The ASA supports clustering when connected to the Cisco Nexus 7000 Catalyst 6500 with Supervisor 32, 720, and 720-10GE.
Configure the connection replication rate during a bulk sync	You can now configure the rate at which the ASA replicates connection standby unit when using Stateful Failover. By default, connections are r to the standby unit during a 15 second period. However, when a bulk sy (for example, when you first enable failover), 15 seconds may not be lon to sync large numbers of connections due to a limit on the maximum co per second. For example, the maximum connections on the ASA is 8 mi replicating 8 million connections in 15 seconds means creating 533 K co per second. However, the maximum connections allowed per second is 3 can now specify the rate of replication to be less than or equal to the ma connections per second, and the sync period will be adjusted until all the co are synchronized. We introduced the following command: **failover replication rate** *rate*. *Also available in 8.4(4.1) and 8.5(1.7).*
IPv6 Features	

Feature	Description
IPv6 Support on the ASA's outside interface for VPN Features.	This release of the ASA adds support for IPv6 VPN connections to i interface using SSL and IKEv2/IPsec protocols. This release of the ASA continues to support IPv6 VPN traffic on its in using the SSL protocol as it has in the past. This release does not pro IKEv2/IPsec protocol on the inside interface.
Remote Access VPN support for IPv6: IPv6 Address Assignment Policy	You can configure the ASA to assign an IPv4 address, an IPv6 addre IPv4 and an IPv6 address to an AnyConnect client by creating intern addresses on the ASA or by assigning a dedicated address to a local ASA. The endpoint must have the dual-stack protocol implemented in its ope to be assigned both types of addresses. Assigning an IPv6 address to the client is supported for the SSL prot feature is not supported for the IKEv2/IPsec protocol. We introduced the following commands: **ipv6-vpn-addr-assign**, **vpn-framed-ipv6-address**. We modified the following screens: **Configuration > Remote Access VPN > Network (Client) Access Assignment > Assignment Policy** **Configuration > Remote Access VPN > AAA/Local Users > Local local user account) > VPN Policy**
Remote Access VPN support for IPv6: Assigning DNS Servers with IPv6 Addresses to group policies	DNS servers can be defined in a Network (Client) Access internal gr the ASA. You can specify up to four DNS server addresses including IPv4 addresses and up to two IPv6 addresses. DNS servers with IPv6 addresses can be reached by VPN clients wh configured to use the SSL protocol. This feature is not supported for configured to use the IKEv2/IPsec protocol. We modified the following command: **dns-server value**. We modified the following screen: Configuration > Remote Access VI (Client) Access > Group Policies > (Edit group policy) > Servers.

Feature	Description
Remote Access VPN support for IPv6: Split tunneling	Split tunneling enables you to route some network traffic through the V (encrypted) and to route other network traffic outside the VPN tunnel (un or "in the clear"). You can now perform split tunneling on IPv6 network defining an IPv6 policy which specifies a unified access control rule. IPv6 split tunneling is reported with the telemetric data sent by the Smart C feature. If either IPv4 or IPv6 split tunneling is enabled, Smart Call Hor split tunneling as "enabled." For telemetric data, the VPN session databas the IPv6 data typically reported with session management. You can include or exclude IPv6 traffic from the VPN "tunnel" for VPN configured to use the SSL protocol. This feature is not supported for the IK protocol. We introduced the following command: **ipv6-split-tunnel-policy**. We modified the following screen: **Configuration > Remote Access VI Network (Client) Access > Group Policies > (Edit group policy) > A > Split Tunneling**.
Remote Access VPN support for IPv6: AnyConnect Client Firewall Rules	Access control rules for client firewalls support access list entries for bo and IPv6 addresses. ACLs containing IPv6 addresses can be applied to clients configured to SSL protocol. This feature is not supported for the IKEv2/IPsec protoco We modified the following command: **anyconnect firewall-rule**. We modified the following screen: **Configuration > Remote Access VI Network (Client) Access > Group Policies > (Edit group policy) > A > AnyConnect Client > Client Firewall.**

Feature	Description
Remote Access VPN support for IPv6: Client Protocol Bypass	The Client Protocol Bypass feature allows you to configure how the A IPv4 traffic when it is expecting only IPv6 traffic or how it manages when it is expecting only IPv4 traffic. When the AnyConnect client makes a VPN connection to the ASA, th assign it an IPv4, IPv6, or both an IPv4 and IPv6 address. If the ASA AnyConnect connection only an IPv4 address or only an IPv6 addre now configure the Client Bypass Protocol to drop network traffic for ASA did not assign an IP address, or allow that traffic to bypass the sent from the client unencrypted or "in the clear." For example, assume that the ASA assigns only an IPv4 address to an connection and the endpoint is dual stacked. When the endpoint atte an IPv6 address, if Client Bypass Protocol is disabled, the IPv6 traff however, if Client Bypass Protocol is enabled, the IPv6 traffic is sent f in the clear. This feature can be used by clients configured to use the SSL or IKE protocol. We introduced the following command: **client-bypass-protocol**. We modified the following screen: **Configuration > Remote Acces Network (Client) Access > Group Policies > (Group Policy) Adva AnyConnect Client > Client Bypass Protocol**.
Remote Access VPN support for IPv6: IPv6 Interface ID and prefix	You can now specify a dedicated IPv6 address for local VPN users. This feature benefits users configured to use the SSL protocol. This supported for the IKEv2/IPsec protocol. We introduced the following command: **vpn-framed-ipv6-address**. We modified the following screen: **Configuration > Remote Acces AAA/Local Users > Local Users > (Edit User) > VPN Policy**.
Remote Access VPN support for IPv6: Sending ASA FQDN to AnyConnect client	You can return the FQDN of the ASA to the AnyConnect client to fa balancing and session roaming. This feature can be used by clients configured to use the SSL or IKE protocol. We introduced the following command: **gateway-fqdn**. We modified the following screen: **Configuration > Remote Acces Network (Client) Access > Group Policies > (Edit group policy) > > AnyConnect.**

Feature	Description
Remote Access VPN support for IPv6: ASA VPN Load Balancing	Clients with IPv6 addresses can make AnyConnect connections through public-facing IPv6 address of the ASA cluster or through a GSS server. clients with IPv6 addresses can make AnyConnect VPN connections thr public-facing IPv4 address of the ASA cluster or through a GSS server. E of connection can be load-balanced within the ASA cluster. For clients with IPv6 addresses to successfully connect to the ASAs pub IPv4 address, a device that can perform network address translation fron IPv4 needs to be in the network. This feature can be used by clients configured to use the SSL or IKEv2/ protocol. We modified the following commands: **show run vpn load-balancing**. We modified the following screen: **Configuration > Remote Access VP Balancing**.
Remote Access VPN support for IPv6: Dynamic Access Policies support IPv6 attributes	When using ASA 9.0 or later with ASDM 6.8 or later, you can now spe attributes as part of a dynamic access policy (DAP): • IPv6 addresses as a Cisco AAA attribute • IPv6 TCP and UDP ports as part of a Device endpoint attribute • Network ACL Filters (client) This feature can be used by clients configured to use the SSL or IKEv2/ protocol. We modified the following screens: **Configuration > Remote Access VPN > Network (Client) Access > D Access Policies > Add > Cisco AAA attribute** **Configuration > Remote Access VPN > Network (Client) Access > D Access Policies > Add > Device > Add Endpoint Attribute** **Configuration > Remote Access VPN > Network (Client) Access > D Access Policies > Network ACL Filters (client)** **Configuration > Remote Access VPN > Network (Client) Access > D Access Policies > Webtype ACL Filters (clientless)**
Remote Access VPN support for IPv6: Session Management	Session management output displays the IPv6 addresses in Public/Assign fields for AnyConnect connections, site-to-site VPN connections, and C SSL VPN connections. You can add new filter keywords to support filte output to show only IPv6 (outside or inside) connections. No changes to Filters exist. This feature can be used by clients configured to use the SSL protocol. Th does not support IKEv2/IPsec protocol. We modified the following command: **show vpn-sessiondb**. We modified these screen: **Monitoring > VPN > VPN Statistics > Sess**

Feature	Description
NAT support for IPv6	NAT now supports IPv6 traffic, as well as translating between IPv4 a (NAT64). Translating between IPv4 and IPv6 is not supported in trans We modified the following commands: **nat** (in global and object net configuration mode), **show conn**, **show nat**, **show nat pool**, **show x** We modified the following screens: **Configuration > Firewall > Objects > Network Objects/Group** **Configuration > Firewall > NAT Rules**
DHCPv6 relay	DHCP relay is supported for IPv6. We introduced the following commands: **ipv6 dhcprelay server**, **ipv enable**, **ipv6 dhcprelay timeout**, **clear config ipv6 dhcprelay**, **ipv6 managed-config-flag**, **ipv6 nd other-config-flag**, **debug ipv6 dhcp dhcprelay**, **show ipv6 dhcprelay binding**, **clear ipv6 dhcprelay bi ipv6 dhcprelay statistics**, and **clear ipv6 dhcprelay statistics**. We modified the following screen: **Configuration > Device Manager > DHCP Relay**.

Feature	Description
OSPFv3	

Feature	Description
	OSPFv3 routing is supported for IPv6. Note the following additiona and limitations for OSPFv2 and OSPFv3: Clustering • OSPFv2 and OSPFv3 support clustering. • When clustering is configured, OSPFv3 encryption is not suppo message appears if you try to configure OSPFv3 encryption in environment. • When using individual interfaces, make sure that you establish t slave units as either OSPFv2 or OSPFv3 neighbors. • When using individual interfaces, OSPFv2 adjacencies can only between two contexts on a shared interface on the master unit. static neighbors is supported only on point-to-point links; there neighbor statement is allowed on an interface. Other • OSPFv2 and OSPFv3 support multiple instances on an interfac • The ESP and AH protocol is supported for OSPFv3 authenticat • OSPFv3 supports Non-Payload Encryption. We introduced or modified the following commands: **ipv6 ospf cost** **database-filter all out**, **ipv6 ospf dead-interval**, **ipv6 ospf hello-in** **ospf mtu-ignore**, **ipv6 ospf neighbor**, **ipv6 ospf network**, **ipv6 osp** **ipv6 ospf retransmit-interval**, **ipv6 ospf transmit-delay**, **ipv6 rou** **router ospf area**, **ipv6 router ospf default**, **ipv6 router ospf default-** **ipv6 router ospf distance**, **ipv6 router ospf exit**, **ipv6 router ospf** **router ospf log-adjacency-changes**, **ipv6 router ospf no**, **ipv6 rou** **redistribute**, **ipv6 router ospf router-id**, **ipv6 router ospf summary** **router ospf timers**, **area range**, **area virtual-link**, **default**, **default** **originate**, **distance**, **ignore lsa mospf**, **log-adjacency-changes**, **red** **router-id**, **summary-prefix**, **timers lsa arrival**, **timers pacing floo** **pacing lsa-group**, **timers pacing retransmission**, **show ipv6 ospf**, **sh** **border-routers**, **show ipv6 ospf database-filter**, **show ipv6 ospf flo** **ipv6 ospf interface**, **show ipv6 ospf neighbor**, **show ipv6 ospf requ** **ipv6 ospf retransmission-list**, **show ipv6 ospf summary-prefix**, **sh** **virtual-links**, **show ospf**, **show run ipv6 router**, **clear ipv6 ospf**, **cl** **ipv6 router**, **debug ospfv3**. We introduced the following screens: **Configuration > Device Setup > Routing > OSPFv3 > Setup** **Configuration > Device Setup > Routing > OSPFv3 > Interface** **Configuration > Device Setup > Routing > OSPFv3 > Redistribu** **Configuration > Device Setup > Routing > OSPFv3 > Summary** **Configuration > Device Setup > Routing > OSPFv3 > Virtual Li**

Feature	Description
	Monitoring > Routing > OSPFv3 LSAs **Monitoring > Routing > OSPFv3 Neighbors**
Unified ACL for IPv4 and IPv6	ACLs now support IPv4 and IPv6 addresses. You can also specify a mix and IPv6 addresses for the source and destination. The IPv6-specific AC deprecated. Existing IPv6 ACLs are migrated to extended ACLs. ACLs containing IPv6 addresses can be applied to clients configured to SSL protocol. This feature is not supported for the IKEv2/IPsec protoco We modified the following commands: **access-list extended**, **access-list** We removed the following commands: **ipv6 access-list**, **ipv6 access-list ipv6-vpn-filter**. We modified the following screens: **Configuration > Firewall > Access Rules** **Configuration > Remote Access VPN > Network (Client) Access > G Policies > General > More Options**
Mixed IPv4 and IPv6 object groups	Previously, network object groups could only contain all IPv4 addresses addresses. Now network object groups can support a mix of both IPv4 a addresses. **Note** You cannot use a mixed object group for NAT. We modified the following command: **object-group network**. We modified the following screen: **Configuration > Firewall > Objects > Objects/Groups**.
Range of IPv6 addresses for a Network object	You can now configure a range of IPv6 addresses for a network object. We modified the following command: **range**. We modified the following screen: **Configuration > Firewall > Objects > Objects/Groups**.

Feature	Description
Inspection support for IPv6 and NAT64	We now support DNS inspection for IPv6 traffic. We also support translating between IPv4 and IPv6 for the following • DNS • FTP • HTTP • ICMP You can now also configure the service policy to generate a syslog mes when unsupported inspections receive and drop IPv6 traffic. We modified the following command: **service-policy fail-close**. We modified the following screen: **Configuration > Firewall > Ser Rules > Add Service Policy Rule Wizard - Service Policy**.
Remote Access Features	
Clientless SSL VPN: Additional Support	We have added additional support for these browsers, operating syst technologies and applications: **Internet browser support**: Microsoft Internet Explorer 9, Firefox 4 8 **Operating system support**: Mac OS X 10.7 **Web technology support**: HTML 5 **Application Support**: Sharepoint 2010
Clientless SSL VPN: Enhanced quality for rewriter engines	The clientless SSL VPN rewriter engines were significantly improve better quality and efficacy. As a result, you can expect a better end-us for clientless SSL VPN users. We did not add or modify any commands for this feature. We did not add or modify any ASDM screens for this feature. *Also available in 8.4(4.1).*
Clientless SSL VPN: Citrix Mobile Receiver	This feature provides secure remote access for Citrix Receiver applica on mobile devices to XenApp and XenDesktop VDI servers through For the ASA to proxy Citrix Receiver to a Citrix Server, when users to Citrix virtualized resource, instead of providing the Citrix Server' credentials, users enter the ASA's SSL VPN IP address and credenti We modified the following command: **vdi**. We modified the following screen: **Configuration > Remote Acces Clientless SSL VPN Access > Group Policy > Edit > More Optio Access > Add VDI Server**.

Feature	Description
Clientless SSL VPN: Enhanced Auto-sign-on	This feature improves support for web applications that require dynamic p for authentication. We modified the following screen: **Configuration > Remote Access VI Clientless SSL VPN Access > Portal > Bookmarks**.
Clientless SSL VPN: Clientless Java Rewriter Proxy Support	This feature provides proxy support for clientless Java plug-ins when a configured in client machines' browsers. We did not add or modify any commands for this feature. We did not add or modify any ASDM screens for this feature.
Clientless SSL VPN: Remote File Explorer	The Remote File Explorer provides users with a way to browse the corpora from their web browser. When users click the Remote File System icon or SSL VPN portal page, an applet is launched on the user's system displa remote file system in a tree and folder view. We did not add or modify any commands for this feature. We did not add or modify any ASDM screens for this feature.
Clientless SSL VPN: Server Certificate Validation	This feature enhances clientless SSL VPN support to enable SSL server verification for remote HTTPS sites against a list of trusted CA certifica We modified the following commands: ssl-server-check, crypto, crypto ca crl, certificate, revocation-check. We modified the following screen: **Configuration > Remote Access VI Certificate Management > Trusted Certificate Pool**.
AnyConnect Performance Improvements	This feature improves throughput performance for AnyConnect TLS/DT in multi-core platforms. It accelerates the SSL VPN datapath and provid customer-visible performance gains in AnyConnect, smart tunnels, and forwarding. We modified the following commands: **crypto engine accelerator-bias crypto accelerator**. We modified the following screen: **Configuration > Remote Access VI Advanced > Crypto Engine**.
Custom Attributes	Custom attributes define and configure AnyConnect features that have no added to ASDM. You add custom attributes to a group policy, and defin for those attributes. For AnyConnect 3.1, custom attributes are available to support AnyConnec Upgrade. Custom attributes can benefit AnyConnect clients configured for either IK or SSL protocols. We added the following command: **anyconnect-custom-attr**. A new screen was added: **Configuration > Remote Access VPN > Net (Client) Access > Advanced > AnyConnect Custom Attributes**.

Feature	Description
Next Generation Encryption	

Feature	Description
	The National Standards Association (NSA) specified a set of cryptograp algorithms that devices must support to meet U.S. federal standards for cry strength. RFC 6379 defines the Suite B cryptographic suites. Because the set of algorithms defined as NSA Suite B are becoming a standard, the Ar IPsec VPN (IKEv2 only) and public key infrastructure (PKI) subsystem support them. The next generation encryption (NGE) includes a larger s this set adding cryptographic algorithms for IPsec V3 VPN, Diffie-Hellm 14 and 24 for IKEv2, and RSA certificates with 4096 bit keys for DTLS a The following functionality is added to ASA to support the Suite B algo • AES-GCM/GMAC support (128-, 192-, and 256-bit keys) • IKEv2 payload encryption and authentication • ESP packet encryption and authentication • Hardware supported only on multi-core platforms • SHA-2 support (256-, 384-, and 512-bit hashes) • ESP packet authentication • Hardware and software supported only on multi-core platform • ECDH support (groups 19, 20, and 21) • IKEv2 key exchange • IKEv2 PFS • Software only supported on single- or multi-core platforms • ECDSA support (256-, 384-, and 521-bit elliptic curves) • IKEv2 user authentication • PKI certificate enrollment • PKI certificate generation and verification • Software only supported on single- or multi-core platforms New cryptographic algorithms are added for IPsecV3. **Note** Suite B algorithm support requires an AnyConnect Premiu for IKEv2 remote access connections, but Suite B usage fo connections or purposes (such as PKI) has no limitations. I has no licensing restrictions. We introduced or modified the following commands: **crypto ikev2 poli ipsec ikev2 ipsec-proposal**, **crypto key generate**, **crypto key zeroize**, **sh key mypubkey**, **show vpn-sessiondb**. We introduced or modified the following screens:

Feature	Description
	Monitor > VPN > Sessions **Monitor > VPN > Encryption Statistics** **Configuration > Site-to-Site VPN > Certificate Management > Ic Certificates** **Configuration > Site-to-Site VPN > Advanced > System Options** **Configuration > Remote Access VPN > Network (Client) Access > IPsec > Crypto Maps**
Support for VPN on the ASASM	The ASASM now supports all VPN features.
Multiple Context Mode Features	
Site-to-Site VPN in multiple context mode	Site-to-site VPN tunnels are now supported in multiple context mod
New resource type for site-to-site VPN tunnels	New resource types, vpn other and vpn burst other, were created to set number of site-to-site VPN tunnels in each context. We modified the following commands: **limit-resource**, **show resourc resource usage**, **show resource allocation**. We modified the following screen: **Configuration > Context Mana Resource Class > Add Resource Class**.
Dynamic routing in Security Contexts	EIGRP and OSPFv2 dynamic routing protocols are now supported i context mode. OSPFv3, RIP, and multicast routing are not supported
New resource type for routing table entries	A new resource class, routes, was created to set the maximum numb table entries in each context. We modified the following commands: **limit-resource**, **show resourc resource usage**, **show resource allocation**. We modified the following screen: **Configuration > Context Mana Resource Class > Add Resource Class**.
Mixed firewall mode support in multiple context mode	You can set the firewall mode independently for each security conte context mode, so some can run in transparent mode while others run in We modified the following command: **firewall transparent**. You cannot set the firewall mode in ASDM; you must use the comm interface. *Also available in Version 8.5(1).*
Module Features	
ASA Services Module support on the Cisco 7600 switch	The Cisco 7600 series now supports the ASASM. For specific hardwar requirements, see: http://www.cisco.com/en/US/docs/security/asa/compatibility/asamat

Feature	Description
ASA 5585-X support for the ASA CX SSP-10 and -20	The ASA CX module lets you enforce security based on the complete co situation. This context includes the identity of the user (who), the applic website that the user is trying to access (what), the origin of the access a (where), the time of the attempted access (when), and the properties of t used for the access (how). With the ASA CX module, you can extract the fi of a flow and enforce granular policies such as permitting access to Face denying access to games on Facebook or permitting finance employees a sensitive enterprise database but denying the same to other employees We introduced or modified the following commands: **capture**, **cxsc**, **cxs auth-proxy**, **debug cxsc**, **hw-module module password-reset**, **hw-modu reload**, **hw-module module reset**, **hw-module module shutdown**, **sess setup host ip**, **session do get-config**, **session do password-reset**, **show classify domain cxsc**, **show asp table classify domain cxsc-auth-prox capture**, **show conn**, **show module**, **show service-policy**. We introduced the following screens: **Home > ASA CX Status** **Wizards > Startup Wizard > ASA CX Basic Configuration** **Configuration > Firewall > Service Policy Rules > Add Service Polic Rule Actions > ASA CX Inspection** *Also available in 8.4(4.1).*
ASA 5585-X Dual SSP support for the SSP-10 and SSP-20 (in addition to the SSP-40 and SSP-60); VPN support for Dual SSPs	The ASA 5585-X now supports dual SSPs using all SSP models (you ca SSPs of the same level in the same chassis). VPN is now supported whe dual SSPs. We did not modify any commands. We did not modify any screens.

New Features in Version 8.7

New Features in ASA 8.7(1.1)/ASDM 6.7(1)

Released: October 16, 2012

Note Version 8.7(1) was removed from Cisco.com due to build issues; please upgrade to Version 8.7(1.1) or later.

Feature	Description
Platform Features	
Support for the ASA 1000V	We introduced support for the ASA 1000V for the Nexus 1000V switch.

Feature	Description
Cloning the ASA 1000V	You can add one or multiple instances of the ASA 1000V to your deployment using cloning VMs.
Management Features	
ASDM mode	You can configure, manage, and monitor the ASA 1000V using the Adaptive Securit Manager (ASDM), which is the single GUI-based device manager for the ASA.
VNMC mode	You can configure and manage the ASA 1000V using the Cisco Virtual Network Ma Center (VNMC), which is a GUI-based multi-device manager for multiple tenants.
XML APIs	You can configure and manage the ASA 1000V using XML APIs, which are application interfaces provided through the Cisco VNMC. This feature is only available in VNM
Firewall Features	
Cisco VNMC access and configuration	Cisco VNMC access and configuration are required to create security profiles. You c access to the Cisco VNMC through the Configuration > Device Setup > Interfaces pa Enter the login username and password, hostname, and shared secret to access the Ci Then you can configure security profiles and security profile interfaces. In VNMC m CLI to configure security profiles.
Security profiles and security profile interfaces	Security profiles are interfaces that correspond to an edge security profile that has be in the Cisco VNMC and assigned in the Cisco Nexus 1000V VSM. Policies for throu assigned to these interfaces and the outside interface. You can add security profiles th Configuration > Device Setup > Interfaces pane. You create the security profile by ad and selecting the service interface. ASDM then generates the security profile through VNMC, assigns the security profile ID, and automatically generates a unique interfac interface name is used in the security policy configuration. We introduced or modified the following commands: **interface security-profile**, **sec mtu**, **vpath path-mtu, clear interface security-profile**, **clear configure interface sec show interface security-profile**, **show running-config interface security-profile**, **sh ip brief**, **show running-config mtu**, **show vsn ip binding**, **show vsn security-profi** We introduced or modified the following screens: **Configuration > Device Setup > Interfaces Configuration > Device Setup > Inter Security Profile Monitoring > Interfaces > Security Profiles**
Service interface	The service interface is the Ethernet interface associated with security profile interfac only configure one service interface, which must be the inside interface. We introduced the following command: **service-interface security-profile all**. We modified the following screen: **Configuration > Device Setup > Interfaces**.

Feature	Description
VNMC policy agent	The VNMC policy agent enables policy configuration through both the ASDM and VNM It includes a web server that receives XML-based requests from Cisco VNMC over HTT converts it to the ASA 1000V configuration. We introduced the following commands: **vnmc policy-agent**, **login**, **shared-secret**, **regi** **host**, **vnmc org**, **show vnmc policy-agent**, **show running-config vnmc policy-agent**, **clear** **vnmc policy-agent**. We modified the following screen: **Configuration > Device Setup > Interfaces**.

New Features in Version 8.6

New Features in ASA 8.6(1)/ASDM 6.6(1)

Released: February 28, 2012

Note This ASA software version is only supported on the ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, and ASA 5555-X.

Version 8.6(1) includes all features in 8.4(2), plus the features listed in this table.

Features added in 8.4(3) are not included in 8.6(1) unless they are explicitly listed in this table.

Feature	Description
Hardware Features	
Support for the ASA 5512-X through ASA 5555-X	We introduced support for the ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, 5555-X.
IPS Features	
Support for the IPS SSP for the ASA 5512-X through ASA 5555-X	We introduced support for the IPS SSP software module for the ASA 5512-X, ASA 551 5525-X, ASA 5545-X, and ASA 5555-X. We introduced or modified the following commands: **session**, **show module**, **sw-modul** We did not modify any screens.
Remote Access Features	
Clientless SSL VPN browser support	The ASA now supports clientless SSL VPN with Microsoft Internet Explorer 9 and Fire *Also available in Version 8.4(3).*

Feature	Description
Compression for DTLS and TLS	To improve throughput, Cisco now supports compression for DTLS and TLS on Any or later. Each tunneling method configures compression separately, and the preferred is to have both SSL and DTLS compression as LZS. This feature enhances migration VPN clients. **Note** Using data compression on high speed remote access connections passin compressible data requires significant processing power on the ASA. With and traffic on the ASA, the number of sessions that can be supported on is reduced. We introduced or modified the following commands: **anyconnect dtls compression** and **anyconnect ssl compression** [**deflate** | **lzs** | **none**]. We modified the following screen: **Configuration > Remote Access VPN > Clientl Access > Group Policies > Edit > Edit Internal Group Policy > Advanced > AnyC > SSL Compression**. *Also available in Version 8.4(3).*
Clientless SSL VPN Session Timeout Alerts	Allows you to create custom messages to alert users that their VPN session is about t of inactivity or a session timeout. We introduced the following commands: **vpn-session-timeout alert-interval**, **vpn-i alert-interval**. We introduced the following screens: Remote Access VPN > Configuration > Clientless SSL VPN Access > Portal > Cust Add/Edit > Timeout Alerts Remote Access VPN > Configuration > Clientless SSL V Group Policies > Add/Edit General *Also available in Version 8.4(3).*
Multiple Context Mode Features	
Automatic generation of a MAC address prefix	In multiple context mode, the ASA now converts the automatic MAC address generation to use a default prefix. The ASA auto-generates the prefix based on the last two bytes o MAC address. This conversion happens automatically when you reload, or if you ree address generation. The prefix method of generation provides many benefits, includi guarantee of unique MAC addresses on a segment. You can view the auto-generated entering the **show running-config mac-address** command. If you want to change th can reconfigure the feature with a custom prefix. The legacy method of MAC address no longer available. **Note** To maintain hitless upgrade for failover pairs, the ASA does *not* convert address method in an existing configuration upon a reload if failover is e However, we strongly recommend that you manually change to the prefi generation. After upgrading, to use the prefix method of MAC address g reenable MAC address generation to use the default prefix. We modified the following command: **mac-address auto**. We modified the following screen: **Configuration > Context Management > Secur**

Feature	Description
AAA Features	
Increased maximum LDAP values per attribute	The maximum number of values that the ASA can receive for a single attribute was incre 1000 (the default) to 5000, with an allowed range of 500 to 5000. If a response message i that exceeds the configured limit, the ASA rejects the authentication. If the ASA detects th attribute has more than 1000 values, then the ASA generates informational syslog 109036 than 5000 attributes, the ASA generates error level syslog 109037. We introduced the following command: **ldap-max-value-range** *number* (Enter this com aaa-server host configuration mode). ASDM does not support this command; enter the command using the Command Line To *Also available in Version 8.4(3).*
Support for sub-range of LDAP search results	When an LDAP search results in an attribute with a large number of values, depending on configuration, it might return a sub-range of the values and expect the ASA to initiate ad queries for the remaining value ranges. The ASA now makes multiple queries for the rer ranges, and combines the responses into a complete array of attribute values. *Also available in Version 8.4(3).*
Troubleshooting Features	
Regular expression matching for the **show asp table classifier** and **show asp table filter** commands	You can now enter the **show asp table classifier** and **show asp table filter** commands wit expression to filter output. We modified the following commands: **show asp table classifier match** *regex*, **show as filter match** *regex*. ASDM does not support this command; enter the command using the Command Line To *Also available in Version 8.4(3).*

New Features in Version 8.5

New Features in ASA 8.5(1.7)/ASDM 6.5(1.101)

Released: March 5, 2012

Note We recommend that you upgrade to a Cisco.com-posted ASA interim release only if you have a specific problem that it resolves. If you decide to run an interim release in a production environment, keep in mind that only targeted testing is performed on interim releases. Interim releases are fully supported by Cisco TAC and will usually remain on the download site only until the next maintenance release is available. If you choose to run an interim release, we strongly encourage you to upgrade to a fully-tested maintenance or feature release when it becomes available.

We will document interim release features at the time of the next maintenance or feature release. For a list of resolved caveats for each ASA interim release, see the interim release notes available on the Cisco.com software download site.

Table 1: New Features for ASA Interim Version 8.5(1.7)/ASDM Version 6.5(1.101)

Feature	Description
Hardware Features	
Support for the Catalyst 6500 Supervisor 2T	The ASA now interoperates with the Catalyst 6500 Supervisor 2T. For hardware and compatibility, see: http://www.cisco.com/en/US/docs/security/asa/compatibility/asan **Note** You may have to upgrade the FPD image on the ASA. See the Upgradin the in the release notes.
Multiple Context Features	
ASDM support for Automatic generation of a MAC address prefix	ASDM now shows that an autogenerated prefix will be used if you do not specify on We modified the following screen: **Configuration > Context Management > Secur**
Failover Features	

Feature	Description
Configure the connection replication rate during a bulk sync	You can now configure the rate at which the ASA replicates connections to the standby u using stateful failover. By default, connections are replicated to the standby unit during a period. However, when a bulk sync occurs (for example, when you first enable failover), t may not be long enough to sync large numbers of connections due to a limit on the maxi connections per second. For example, the maximum connections on the ASA is 8 million; r 8 million connections in 15 seconds means creating 533K connections per second. Howe maximum connections allowed per second is 300K. You can now specify the rate of repl be less than or equal to the maximum connections per second, and the sync period will b until all the connections are synced. We introduced the following command: **failover replication rate** *rate*. We modified the following screen: **Configuration > Device Management > High Avai Failover**.

New Features in ASA 8.5(1.6)/ASDM 6.5(1)

Released: January 27, 2012

Note We recommend that you upgrade to a Cisco.com-posted ASA interim release only if you have a specific problem that it resolves. If you decide to run an interim release in a production environment, keep in mind that only targeted testing is performed on interim releases. Interim releases are fully supported by Cisco TAC and will usually remain on the download site only until the next maintenance release is available. If you choose to run an interim release, we strongly encourage you to upgrade to a fully-tested maintenance or feature release when it becomes available.

We will document interim release features at the time of the next maintenance or feature release. For a list of resolved caveats for each ASA interim release, see the interim release notes available on the Cisco.com software download site.

Table 2: New Features for ASA Interim Version 8.5(1.6)/ASDM Version 6.5(1)

Feature	Description
Multiple Context Features	

Feature	Description
Automatic generation of a MAC address prefix	In multiple context mode, the ASA now converts the automatic MAC address generation to use a default prefix. The ASA auto-generates the prefix based on the last two bytes of MAC address. This conversion happens automatically when you reload, or if you ree address generation. The prefix method of generation provides many benefits, includi guarantee of unique MAC addresses on a segment. You can view the auto-generated entering the **show running-config mac-address** command. If you want to change th can reconfigure the feature with a custom prefix. The legacy method of MAC address no longer available. **Note** To maintain hitless upgrade for failover pairs, the ASA does *not* convert address method in an existing configuration upon a reload if failover is e However, we strongly recommend that you manually change to the prefi generation when using failover. Without the prefix method, ASASMs in different slot numbers experience a MAC address change upon failover, experience traffic interruption. After upgrading, to use the prefix method address generation, reenable MAC address generation to use the default We modified the following command: **mac-address auto**. ASDM was not changed.

New Features in ASA 8.5(1)/ASDM 6.5(1)

Released: July 8, 2011

This ASA and ASDM software version is only supported on the ASASM.

Version 8.5(1) includes all features in 8.4(1), plus the features listed in this table. The following features, however, are not supported in No Payload Encryption software, and this release is only available as a No Payload Encryption release:

- VPN
- Unified Communications

Features added in 8.4(2) are not included in 8.5(1) unless they are explicitly listed in this table.

Table 3: New Features for ASA Version 8.5(1)/ASDM Version 6.5(1)

Feature	Description
Hardware Features	
Support for the ASA Services Module	We introduced support for the ASASM for the Cisco Catalyst 6500 E switch.
Firewall Features	

Feature	Description
Mixed firewall mode support in multiple context mode	You can set the firewall mode independently for each security context in multiple contex some can run in transparent mode while others run in routed mode. We modified the following command: **firewall transparent**. You cannot set the firewall mode in ASDM; you must use the command line interface.
Interface Features	
Automatic MAC address generation is now enabled by default in multiple context mode	Automatic generation of MAC addresses is now enabled by default in multiple context r We modified the following command: **mac address auto**. We modified the following screen: System > Configuration > Context Management > Se Contexts.
NAT Features	
Identity NAT configurable proxy ARP and route lookup	In earlier releases for identity NAT, proxy ARP was disabled, and a route lookup was alv to determine the egress interface. You could not configure these settings. In 8.4(2) and la default behavior for identity NAT was changed to match the behavior of other static NA configurations: proxy ARP is enabled, and the NAT configuration determines the egress (if specified) by default. You can leave these settings as is, or you can enable or disable t discretely. Note that you can now also disable proxy ARP for regular static NAT. For pre-8.3 configurations, the migration of NAT exempt rules (the **nat 0 access-list** con 8.4(2) and later now includes the following keywords to disable proxy ARP and to use a lookup: **no-proxy-arp** and **route-lookup**. The **unidirectional** keyword that was used for to 8.3(2) and 8.4(1) is no longer used for migration. When upgrading to 8.4(2) from 8.3(and 8.4(1), all identity NAT configurations will now include the **no-proxy-arp** and **rout** keywords, to maintain existing functionality. The **unidirectional** keyword is removed. We modified the following commands: **nat static** [**no-proxy-arp**] [**route-lookup**] (objec and **nat source static** [**no-proxy-arp**] [**route-lookup**] (global). We modified the following screens: Configuration > Firewall > NAT Rules > Add/Edit Network Object > Advanced NAT Se Configuration > Firewall > NAT Rules > Add/Edit NAT Rule *Also available in Version 8.4(2).*

Feature	Description
PAT pool and round robin address assignment	You can now specify a pool of PAT addresses instead of a single address. You can als enable round-robin assignment of PAT addresses instead of first using all ports on a before using the next address in the pool. These features help prevent a large number from a single PAT address from appearing to be part of a DoS attack and makes conf large numbers of PAT addresses easy. **Note** Currently in 8.5(1), the PAT pool feature is not available as a fallback m dynamic NAT or PAT. You can only configure the PAT pool as the prima for dynamic PAT (CSCtq20634). We modifed the following commands: **nat dynamic** [**pat-pool** *mapped_object* [**rou** (object network) and **nat source dynamic** [**pat-pool** *mapped_object* [**round-robin**]] We modified the following screens: Configuration > Firewall > NAT Rules > Add/Edit Network Object Configuration > NAT Rules > Add/Edit NAT Rule *Also available in Version 8.4(2).*
Switch Integration Features	
Autostate	The switch supervisor engine can send autostate messages to the ASASM about the sta interfaces associated with ASA VLANs. For example, when all physical interfaces a a VLAN go down, the autostate message tells the ASA that the VLAN is down. This lets the ASA declare the VLAN as down, bypassing the interface monitoring tests nor for determining which side suffered a link failure. Autostate messaging provides a d improvement in the time the ASA takes to detect a link failure (a few milliseconds a up to 45 seconds without autostate support). **Note** The switch supports autostate messaging only if you install a single ASA See the following Cisco IOS command: **firewall autostate**.
Virtual Switching System	The ASASM supports VSS when configured on the switches. No ASA configuration

New Features in Version 8.4

New Features in ASA 8.4(7)/ASDM 7.1(3)

Released: September 3, 2013

There were no new features in ASA 8.4(7)/ASDM 7.1(3).

New Features in ASA 8.4(6)/ASDM 7.1(2.102)

Released: April 29, 2013

Feature	Description
Monitoring Features	
Ability to view top 10 memory users	You can now view the top bin sizes allocated and the top 10 PCs for each allocated bin s Previously, you had to enter multiple commands to see this information (the **show mem** command and the **show memory binsize** command); the new command provides for quick of memory issues. We introduced the following command: **show memory top-usage**. No ASDM changes were made. *This feature is not available in 8.5(1), 8.6(1), 8.7(1), 9.0(1), or 9.1(1).*
CPU profile enhancements	The **cpu profile activate** command now supports the following: • Delayed start of the profiler until triggered (global or specific thread CPU %) • Sampling of a single thread We modified the following command: **cpu profile activate** [*n-samples*] [**sample-proces** *process-name*] [**trigger cpu-usage** *cpu%* [*process-name*]. No ASDM changes were made. *This feature is not available in 8.5(1), 8.6(1), 8.7(1), 9.0(1), or 9.1(1).*
Remote Access Features	
user-storage value command password is now encrypted in **show** commands	The password in the **user-storage value** command is now encrypted when you enter **sho running-config**. We modified the following command: **user-storage value**. We modified the following screen: **Configuration > Remote Access VPN > Clientless Access > Group Policies > More Options > Session Settings**. *This feature is not available in 8.5(1), 8.6(1), 8.7(1), 9.0(1), or 9.1(1).*

New Features in ASA 8.4(5)/ASDM 7.0(2)

Released: October 31, 2012

Feature	Description
Firewall Features	

Feature	Description
EtherType ACL support for IS-IS traffic (transparent firewall mode)	In transparent firewall mode, the ASA can now pass IS-IS traffic using an EtherType We modified the following command: **access-list ethertype** {**permit** | **deny**} **is-is**. We modified the following screen: **Configuration > Device Management > Manag > EtherType Rules**. *This feature is not available in 8.5(1), 8.6(1), 8.7(1), 9.0(1), or 9.1(1).*
ARP cache additions for non-connected subnets	The ASA ARP cache only contains entries from directly-connected subnets by defau now enable the ARP cache to also include non-directly-connected subnets. We do no enabling this feature unless you know the security risks. This feature could facilitate de (DoS) attack against the ASA; a user on any interface could send out many ARP replies the ASA ARP table with false entries. You may want to use this feature if you use: • Secondary subnets. • Proxy ARP on adjacent routes for traffic forwarding. We introduced the following command: **arp permit-nonconnected**. We modified the following screen: **Configuration > Device Management > Advan ARP Static Table**. *This feature is not available in 8.5(1), 8.6(1), or 8.7(1).*
Increased maximum connection limits for service policy rules	The maximum number of connections for service policy rules was increased from 6553 We modified the following commands: **set connection conn-max**, **set connection embryonic-conn-max**, **set connection per-client-embryonic-max**, **set connection pe** We modified the following screen: **Configuration > Firewall > Service Policy Rules Settings**. *This feature is not available in 8.5(1), 8.6(1), or 8.7(1).*
Remote Access Features	
Improved Host Scan and ASA Interoperability	Host Scan and the ASA use an improved process to transfer posture attributes from th ASA. This gives the ASA more time to establish a VPN connection with the client a dynamic access policy. *This feature is not available in 8.5(1), 8.6(1), 8.7(1), 9.0(1), or 9.1(1).*
Cisco Secure Desktop: Windows 8 Support	CSD 3.6.6215 was updated to enable selection of Windows 8 in the Prelogin Policy op check. See the following limitations: • Secure Desktop (Vault) is not supported with Windows 8.
Dynamic Access Policies: Windows 8 Support	ASDM was updated to enable selection of Windows 8 in the DAP Operating System
Monitoring Features	

Feature	Description
NAT-MIB cnatAddrBindNumberOfEntries and cnatAddrBindSessionCount OIDs to allow polling for Xlate count.	Support was added for the NAT-MIB cnatAddrBindNumberOfEntries and cnatAddrBindSes OIDs to support xlate_count and max_xlate_count for SNMP. This data is equivalent to the **show xlate count** command. *This feature is not available in 8.5(1), 8.6(1), 8.7(1), 9.0(1), or 9.1(1).*
NSEL	Flow-update events have been introduced to provide periodic byte counters for flow traf can change the time interval at which flow-update events are sent to the NetFlow collecto filter to which collectors flow-update records will be sent. We introduced the following command: **flow-export active refresh-interval**. We modified the following command: **flow-export event-type**. We modified the following screens: **Configuration > Device Management > Logging > NetFlow**. **Configuration > Firewall > Service Policy Rules > Add Service Policy Rule Wizard Actions > NetFlow > Add Flow Event** *This feature is not available in 8.5(1), 8.6(1), 8.7(1), 9.0(1), or 9.1(1).*
Hardware Features	
ASA 5585-X DC power supply support	Support was added for the ASA 5585-X DC power supply. *This feature is not available in 8.5(1), 8.6(1), 8.7(1), 9.0(1), or 9.1(1).*

New Features in ASA 8.4(4.5)/ASDM 6.4(9.103)

Released: August 13, 2012

Note Version 8.4(4.3) was removed from Cisco.com due to build issues; please upgrade to Version 8.4(4.5) or later.

We recommend that you upgrade to a Cisco.com-posted interim release only if you have a specific problem that it resolves. If you decide to run an interim release in a production environment, keep in mind that only targeted testing is performed on interim releases. Interim releases are fully supported by Cisco TAC and will remain on the download site only until the next maintenance release is available. If you choose to run an interim release, we strongly encourage you to upgrade to a fully-tested maintenance or feature release when it becomes available. We will document interim release features at the time of the next maintenance or feature release. For a list of resolved caveats for each interim release, see the interim release notes available on the Cisco.com software download site.

Feature	Description
Firewall Features	

Feature	Description
ARP cache additions for non-connected subnets	The ASA ARP cache only contains entries from directly-connected subnets by defau now enable the ARP cache to also include non-directly-connected subnets. We do no enabling this feature unless you know the security risks. This feature could facilitate de (DoS) attack against the ASA; a user on any interface could send out many ARP replies the ASA ARP table with false entries. You may want to use this feature if you use: • Secondary subnets. • Proxy ARP on adjacent routes for traffic forwarding. We introduced the following command: **arp permit-nonconnected**. We modified the following screen: **Configuration > Device Management > Advan ARP Static Table**. *This feature is not available in 8.5(1), 8.6(1), or 8.7(1).*
Monitoring Features	
NAT-MIB cnatAddrBindNumberOfEntries and cnatAddrBindSessionCount OIDs to allow polling for Xlate count.	Support was added for the NAT-MIB cnatAddrBindNumberOfEntries and cnatAddrBind OIDs to support xlate_count and max_xlate_count for SNMP. This data is equivalent to the **show xlate count** command. *This feature is not available in 8.5(1), 8.6(1), 8.7(1), 9.0(1), or 9.1(1).*

New Features in ASA 8.4(4.1)/ASDM 6.4(9)

Released: June 18, 2012

Note Version 8.4(4) was removed from Cisco.com due to build issues; please upgrade to Version 8.4(4.1) or later.

Feature	Description
Certification Features	
FIPS and Common Criteria certifications	The FIPS 140-2 Non-Proprietary Security Policy was updated as part of the Level 2 validation for the Cisco ASA 5500 series, which includes the Cisco ASA 5505, ASA 5520, ASA 5540, ASA 5550, ASA 5580, and ASA 5585-X. The Common Criteria Evaluation Assurance Level 4 (EAL4) was updated, which prov for a specific Target of Evaluation (TOE) of the Cisco ASA and VPN platform soluti *This feature is not available in 8.5(1), 8.6(1), 8.7(1), 9.0(1), 9.0(2), or 9.1(1).*

Feature	Description
Support for administrator password policy when using the local database	When you configure authentication for CLI or ASDM access using the local database, y configure a password policy that requires a user to change their password after a specifie of time and also requires password standards such as a minimum length and the minimu of changed characters. We introduced or modified the following commands: **change-password**, **password-polic password-policy minimum changes**, **password-policy minimum-length**, **password-p minimum-lowercase**, **password-policy minimum-uppercase**, **password-policy minimum password-policy minimum-special**, **password-policy authenticate enable**, **clear conf password-policy**, **show running-config password-policy**. We introduced the following screen: **Configuration > Device Management > Users/A Password Policy** *This feature is not available in 8.5(1), 8.6(1), 8.7(1), 9.0(1), 9.0(2), or 9.1(1).*
Support for SSH public key authentication	You can now enable public key authentication for SSH connections to the ASA on a per- using Base64 key up to 2048 bits. We introduced the following commands: **ssh authentication**. We introduced the following screen: **Configuration > Device Management > Users/A Accounts > Edit User Account > Public Key Authentication** *This feature is not available in 8.5(1), 8.6(1), 8.7(1), 9.0(1), 9.0(2), or 9.1(1).*
Support for Diffie-Hellman Group 14 for the SSH Key Exchange	Support for Diffie-Hellman Group 14 for SSH Key Exchange was added. Formerly, onl was supported. We introduced the following command: **ssh key-exchange**. We modified the following screen: **Configuration > Device Management > Manageme > ASDM/HTTPS/Telnet/SSH**. *This feature is not available in 8.5(1), 8.6(1), 8.7(1), 9.0(1), 9.0(2), or 9.1(1).*
Support for a maximum number of management sessions	You can set the maximum number of simultaneous ASDM, SSH, and Telnet sessions. We introduced the following commands: **quota management-session**, **show running-co management-session**, **show quota management-session**. We introduced the following screen: **Configuration > Device Management > Manageme > Management Session Quota**. *This feature is not available in 8.5(1), 8.6(1), 8.7(1), 9.0(1), 9.0(2), or 9.1(1).*

Feature	Description
Additional ephemeral Diffie-Hellman ciphers for SSL encryption	The ASA now supports the following ephemeral Diffie-Hellman (DHE) SSL cipher • DHE-AES128-SHA1 • DHE-AES256-SHA1 These cipher suites are specified in RFC 3268, *Advanced Encryption Standard (AES) for Transport Layer Security (TLS*). When supported by the client, DHE is the preferred cipher because it provides Perfe Secrecy. See the following limitations: • DHE is not supported on SSL 3.0 connections, so make sure to also enable TLS SSL server. `!! set server version` `ciscoasa(config)# ssl server-version tlsv1 sslv3` `!! set client version` `ciscoasa(config) # ssl client-version any` • Some popular applications do not support DHE, so include at least one other SS method to ensure that a cipher suite common to both the SSL client and server c • Some clients may not support DHE, including AnyConnect 2.5 and 3.0, Cisco Se and Internet Explorer 9.0. We modified the following command: **ssl encryption**. We modified the following screen: **Configuration > Device Management > Advan Settings**. *This feature is not available in 8.5(1), 8.6(1), 8.7(1), 9.0(1), 9.0(2), or 9.1(1).*
Image verification	Support for SHA-512 image integrity checking was added. We modified the following command: **verify**. *This feature is not available in 8.5(1), 8.6(1), 8.7(1), 9.0(1), 9.0(2), or 9.1(1).*

Feature	Description
Improved pseudo-random number generation	Hardware-based noise for additional entropy was added to the software-based random n generation process. This change makes pseudo-random number generation (PRNG) mor and more difficult for attackers to get a repeatable pattern or guess the next random num used for encryption and decryption operations. Two changes were made to improve PRN • Use the current hardware-based RNG for random data to use as one of the paramete software-based RNG. • If the hardware-based RNG is not available, use additional hardware noise sources software-based RNG. Depending on your model, the following hardware sensors ar • ASA 5505—Voltage sensors. • ASA 5510 and 5550—Fan speed sensors. • ASA 5520, 5540, and 5580—Temperature sensors. • ASA 5585-X—Fan speed sensors. We introduced the following commands: **show debug menu cts** [**128** | **129**] *This feature is not available in 8.5(1), 8.6(1), 8.7(1), 9.0(1), 9.0(2), or 9.1(1).*
Remote Access Features	
Clientless SSL VPN: Enhanced quality for rewriter engines	The clientless SSL VPN rewriter engines were significantly improved to provide better q efficacy. As a result, you can expect a better end-user experience for clientless SSL VPN We did not add or modify any commands for this feature. We did not add or modify any ASDM screens for this feature. *This feature is not available in 8.5(1), 8.6(1), or 8.7(1).*
Failover Features	
Configure the connection replication rate during a bulk sync	You can now configure the rate at which the ASA replicates connections to the standby u using Stateful Failover. By default, connections are replicated to the standby unit during a period. However, when a bulk sync occurs (for example, when you first enable failover), may not be long enough to sync large numbers of connections due to a limit on the maxi connections per second. For example, the maximum connections on the ASA is 8 million; 8 million connections in 15 seconds means creating 533 K connections per second. How maximum connections allowed per second is 300 K. You can now specify the rate of rep be less than or equal to the maximum connections per second, and the sync period will b until all the connections are synced. We introduced the following command: **failover replication rate** *rate*. *This feature is not available in 8.6(1) or 8.7(1). This feature is also in 8.5(1.7).*
Application Inspection Features	

Feature	Description
SunRPC change from dynamic ACL to pin-hole mechanism	Previously, Sun RPC inspection does not support outbound access lists because the insp uses dynamic access lists instead of secondary connections. In this release, when you configure dynamic access lists on the ASA, they are suppor ingress direction only and the ASA drops egress traffic destined to dynamic ports. Th RPC inspection implements a pinhole mechanism to support egress traffic. Sun RPC in this pinhole mechanism to support outbound dynamic access lists. *This feature is not available in 8.5(1), 8.6(1), or 8.7(1).*
Inspection reset action change	Previously, when the ASA dropped a packet due to an inspection engine rule, the AS one RST to the source device of the dropped packet. This behavior could cause resou In this release, when you configure an inspection engine to use a reset action and a p a reset, the ASA sends a TCP reset under the following conditions: • The ASA sends a TCP reset to the inside host when the **service resetoutbound** enabled. (The **service resetoutbound** command is disabled by default.) • The ASA sends a TCP reset to the outside host when the **service resetinbound** enabled. (The **service resetinbound** command is disabled by default.) For more information, see the **service** command in the ASA command reference. This behavior ensures that a reset action will reset the connections on the ASA and on i therefore countering denial of service attacks. For outside hosts, the ASA does not se default and information is not revealed through a TCP reset. *This feature is not available in 8.5(1), 8.6(1), or 8.7(1).*
Module Features	
ASA 5585-X support for the ASA CX SSP-10 and -20	The ASA CX module lets you enforce security based on the complete context of a si context includes the identity of the user (who), the application or website that the use access (what), the origin of the access attempt (where), the time of the attempted acces the properties of the device used for the access (how). With the ASA CX module, yo the full context of a flow and enforce granular policies such as permitting access to F denying access to games on Facebook or permitting finance employees access to a sensi database but denying the same to other employees. We introduced or modified the following commands: **capture**, **cxsc**, **cxsc auth-proxy hw-module module password-reset**, **hw-module module reload**, **hw-module mod hw-module module shutdown**, **session do setup host ip, session do get-config, ses password-reset, show asp table classify domain cxsc**, **show asp table classify dom cxsc-auth-proxy**, **show capture**, **show conn**, **show module**, **show service-policy**. We introduced the following screens: **Home > ASA CX Status Wizards > Startup Wizard > ASA CX Basic Configura** **Configuration > Firewall > Service Policy Rules > Add Service Policy Rule > Ru ASA CX Inspection**

Feature	Description
ASA 5585-X support for network modules	The ASA 5585-X now supports additional interfaces on network modules in slot 1. You one or two of the following optional network modules: • ASA 4-port 10G Network Module • ASA 8-port 10G Network Module • ASA 20-port 1G Network Module *This feature is not available in 9.0(1), 9.0(2), or 9.1(1).*

New Features in ASA 8.4(3)/ASDM 6.4(7)

Released: January 9, 2012

Feature	Description
NAT Features	
Round robin PAT pool allocation uses the same IP address for existing hosts	When using a PAT pool with round robin allocation, if a host has an existing connection subsequent connections from that host will use the same PAT IP address if ports are avai We did not modify any commands. We did not modify any screens. *This feature is not available in 8.5(1) or 8.6(1).*
Flat range of PAT ports for a PAT pool	If available, the real source port number is used for the mapped port. However, if the real available, by default the mapped ports are chosen from the same range of ports as the rea number: 0 to 511, 512 to 1023, and 1024 to 65535. Therefore, ports below 1024 have on PAT pool. If you have a lot of traffic that uses the lower port ranges, when using a PAT pool, you c specify a flat range of ports to be used instead of the three unequal-sized tiers: either 1024 or 1 to 65535. We modified the following commands: **nat dynamic** [**pat-pool** *mapped_object* [**flat** [**include-reserve**]]] (object network configuration mode) and **nat source dynamic** [**pat-** *mapped_object* [**flat** [**include-reserve**]]] (global configuration mode). We modified the following screens: **Configuration > Firewall > NAT Rules > Add/Edit Network Object** **Configuration > Firewall > NAT Rules > Add/Edit NAT Rule** *This feature is not available in 8.5(1) or 8.6(1).*

Feature	Description
Extended PAT for a PAT pool	Each PAT IP address allows up to 65535 ports. If 65535 ports do not provide enough you can now enable extended PAT for a PAT pool. Extended PAT uses 65535 ports p opposed to per IP address, by including the destination address and port in the translatio We modified the following commands: **nat dynamic** [**pat-pool** *mapped_object* [**exte** network configuration mode) and **nat source dynamic** [**pat-pool** *mapped_object* [**exte** configuration mode). We modified the following screens: **Configuration > Firewall > NAT Rules > Add/Edit Network Object** **Configuration > Firewall > NAT Rules > Add/Edit NAT Rule** *This feature is not available in 8.5(1) or 8.6(1).*
Configurable timeout for PAT xlate	When a PAT xlate times out (by default after 30 seconds), and the ASA reuses the po translation, some upstream routers might reject the new connection because the previo might still be open on the upstream device. The PAT xlate timeout is now configurab between 30 seconds and 5 minutes. We introduced the following command: **timeout pat-xlate**. We modified the following screen: **Configuration > Firewall > Advanced > Globa** *This feature is not available in 8.5(1) or 8.6(1).*
Automatic NAT rules to translate a VPN peer's local IP address back to the peer's real IP address	In rare situations, you might want to use a VPN peer's real IP address on the inside ne of an assigned local IP address. Normally with VPN, the peer is given an assigned lo to access the inside network. However, you might want to translate the local IP addre peer's real public IP address if, for example, your inside servers and network security the peer's real IP address. You can enable this feature on one interface per tunnel group. Object NAT rules are added and deleted when the VPN session is established or disconnected. You can vie using the **show nat** command. **Note** Because of routing issues, we do not recommend using this feature unle you need this feature; contact Cisco TAC to confirm feature compatibili network. See the following limitations: • Only supports Cisco IPsec and AnyConnect Client. • Return traffic to the public IP addresses must be routed back to the NAT policy and VPN policy can be applied. • Does not support load-balancing (because of routing issues). • Does not support roaming (public IP changing). We introduced the following command: **nat-assigned-to-public-ip** *interface* (tunnel general-attributes configuration mode). ASDM does not support this command; enter the command using the Command Lin
Remote Access Features	

Feature	Description
Clientless SSL VPN browser support	The ASA now supports clientless SSL VPN with Microsoft Internet Explorer 9 and Fire
Compression for DTLS and TLS	To improve throughput, Cisco now supports compression for DTLS and TLS on AnyCo or later. Each tunneling method configures compression separately, and the preferred cor is to have both SSL and DTLS compression as LZS. This feature enhances migration fr VPN clients. **Note** Using data compression on high speed remote access connections passing h compressible data requires significant processing power on the ASA. With oth and traffic on the ASA, the number of sessions that can be supported on the is reduced. We introduced or modified the following commands: **anyconnect dtls compression** [**lzs** and **anyconnect ssl compression** [**deflate** | **lzs** | **none**]. We modified the following screen: **Configuration > Remote Access VPN > Clientless Access > Group Policies > Edit > Edit Internal Group Policy > Advanced > AnyConn > SSL Compression**.
Clientless SSL VPN Session Timeout Alerts	Allows you to create custom messages to alert users that their VPN session is about to en of inactivity or a session timeout. We introduced the following commands: **vpn-session-timeout alert-interval**, **vpn-idle- alert-interval**. We introduced the following screens: **Remote Access VPN > Configuration > Clientless SSL VPN Access > Portal > Custo > Add/Edit > Timeout Alerts** **Remote Access VPN > Configuration > Clientless SSL VPN Access > Group Policies > General**
AAA Features	
Increased maximum LDAP values per attribute	The maximum number of values that the ASA can receive for a single attribute was incre 1000 (the default) to 5000, with an allowed range of 500 to 5000. If a response message i that exceeds the configured limit, the ASA rejects the authentication. If the ASA detects th attribute has more than 1000 values, then the ASA generates informational syslog 109036 than 5000 attributes, the ASA generates error level syslog 109037. We introduced the following command: **ldap-max-value-range** *number* (Enter this com aaa-server host configuration mode). ASDM does not support this command; enter the command using the Command Line To
Support for sub-range of LDAP search results	When an LDAP search results in an attribute with a large number of values, depending on configuration, it might return a sub-range of the values and expect the ASA to initiate ad queries for the remaining value ranges. The ASA now makes multiple queries for the rem ranges, and combines the responses into a complete array of attribute values.

Feature	Description
Key vendor-specific attributes (VSAs) sent in RADIUS access request and accounting request packets from the ASA	Four New VSAs—Tunnel Group Name (146) and Client Type (150) are sent in RAD request packets from the ASA. Session Type (151) and Session Subtype (152) are ser accounting request packets from the ASA. All four attributes are sent for all accounti packet types: Start, Interim-Update, and Stop. The RADIUS server (for example, ACS then enforce authorization and policy attributes or use them for accounting and billin
Troubleshooting Features	
Regular expression matching for the **show asp table classifier** and **show asp table filter** commands	You can now enter the **show asp table classifier** and **show asp table filter** commands expression to filter output. We modified the following commands: **show asp table classifier match** *regex*, **show filter match** *regex*. ASDM does not support this command; enter the command using the Command Lin

New Features in ASA 8.4(2.8)/ASDM 6.4(5.106)

Released: August 31, 2011

Note We recommend that you upgrade to a Cisco.com-posted ASA interim release only if you have a specific problem that it resolves. If you decide to run an interim release in a production environment, keep in mind that only targeted testing is performed on interim releases. Interim releases are fully supported by Cisco TAC and will usually remain on the download site only until the next maintenance release is available. If you choose to run an interim release, we strongly encourage you to upgrade to a fully-tested maintenance or feature release when it becomes available.

We will document interim release features at the time of the next maintenance or feature release. For a list of resolved caveats for each ASA interim release, see the interim release notes available on the Cisco.com software download site.

Feature	Description
Remote Access Features	
Clientless SSL VPN browser support	The ASA now supports clientless SSL VPN with Microsoft Internet Explorer 9 and I *Also available in Version 8.2(5.13) and 8.3.2(25).*

Feature	Description
Compression for DTLS and TLS	To improve throughput, Cisco now supports compression for DTLS and TLS on AnyCo or later. Each tunneling method configures compression separately, and the preferred cor is to have both SSL and DTLS compression as LZS. This feature enhances migration fro VPN clients. **Note** Using data compression on high speed remote access connections passing h compressible data requires significant processing power on the ASA. With oth and traffic on the ASA, the number of sessions that can be supported on the is reduced. We introduced or modified the following commands: **anyconnect dtls compression** [**lzs** and **anyconnect ssl compression** [**deflate** | **lzs** | **none**]. We modified the following screen: **Configuration > Remote Access VPN > Clientless Access > Group Policies > Edit > Edit Internal Group Policy > Advanced > AnyConn > SSL Compression**. *Also available in Version 8.2(5.13) and 8.3.2(25).*
Clientless SSL VPN Session Timeout Alerts	Allows you to create custom messages to alert users that their VPN session is about to en of inactivity or a session timeout. We introduced the following commands: **vpn-session-timeout alert-interval**, **vpn-idle- alert-interval**. We introduced the following screens: **Remote Access VPN > Configuration > Clientless SSL VPN Access > Portal > Custo > Add/Edit > Timeout Alerts** **Remote Access VPN > Configuration > Clientless SSL VPN Access > Group Policies > General**
AAA Features	
Increased maximum LDAP values per attribute	The maximum number of values that the ASA can receive for a single attribute was incre 1000 (the default) to 5000, with an allowed range of 500 to 5000. If a response message i that exceeds the configured limit, the ASA rejects the authentication. If the ASA detects th attribute has more than 1000 values, then the ASA generates informational syslog 109036 than 5000 attributes, the ASA generates error level syslog 109037. We introduced the following command: **ldap-max-value-range** *number* (Enter this com aaa-server host configuration mode). ASDM does not support this command; enter the command using the Command Line To
Support for sub-range of LDAP search results	When an LDAP search results in an attribute with a large number of values, depending on configuration, it might return a sub-range of the values and expect the ASA to initiate ad queries for the remaining value ranges. The ASA now makes multiple queries for the rer ranges, and combines the responses into a complete array of attribute values.
Troubleshooting Features	

Feature	Description
Regular expression matching for the **show asp table classifier** and **show asp table filter** commands	You can now enter the **show asp table classifier** and **show asp table filter** commands expression to filter output. We modified the following commands: **show asp table classifier match** *regex*, **show filter match** *regex*. ASDM does not support this command; enter the command using the Command Lin *Also available in Version 8.2(5.13) and 8.3.2(25).*

New Features in ASA 8.4(2)/ASDM 6.4(5)

Released: June 20, 2011

Feature	Description
Firewall Features	

Feature	Description
Identity Firewall	Typically, a firewall is not aware of the user identities and, therefore, cannot apply securi based on identity. The Identity Firewall in the ASA provides more granular access control based on users' You can configure access rules and security policies based on usernames and user group rather than through source IP addresses. The ASA applies the security policies based on an a of IP addresses to Windows Active Directory login information and reports events based mapped usernames instead of network IP addresses. The Identity Firewall integrates with Window Active Directory in conjunction with an e Active Directory (AD) Agent that provides the actual identity mapping. The ASA uses W Active Directory as the source to retrieve the current user identity information for specif addresses. In an enterprise, some users log onto the network by using other authentication mechani as authenticating with a web portal (cut-through proxy) or by using a VPN. You can con Identity Firewall to allow these types of authentication in connection with identity-based policies. We introduced or modified the following commands: **user-identity enable**, **user-identit default-domain**, **user-identity domain**, **user-identity logout-probe**, **user-identity inactive-user-timer**, **user-identity poll-import-user-group-timer**, **user-identity actio netbios-response-fail**, **user-identity user-not-found**, **user-identity action ad-agent-do user-identity action mac-address-mismatch**, **user-identity action domain-controller user-identity ad-agent active-user-database**, **user-identity ad-agent hello-timer**, **use ad-agent aaa-server**, **user-identity update import-user**, **user-identity static user**, **ad-ag dns domain-lookup**, **dns poll-timer**, **dns expire-entry-timer**, **object-group user, show user-identity, show dns**, **clear configure user-identity**, **clear dns, debug user-identity aaa-server ad-agent**. We introduced the following screens: **Configuration > Firewall > Identity Options. Configuration > Firewall > Objects > L Groups** **Monitoring > Properties > Identity** We modified the following screen: **Configuration > Device Management > Users/AAA > AAA Server Groups > Add/E Group.**

Feature	Description
Identity NAT configurable proxy ARP and route lookup	In earlier releases for identity NAT, proxy ARP was disabled, and a route lookup was to determine the egress interface. You could not configure these settings. In 8.4(2) and default behavior for identity NAT was changed to match the behavior of other static configurations: proxy ARP is enabled, and the NAT configuration determines the egr (if specified) by default. You can leave these settings as is, or you can enable or disab discretely. Note that you can now also disable proxy ARP for regular static NAT. For pre-8.3 configurations, the migration of NAT exempt rules (the **nat 0 access-list** 8.4(2) and later now includes the following keywords to disable proxy ARP and to u lookup: **no-proxy-arp** and **route-lookup**. The **unidirectional** keyword that was used to 8.3(2) and 8.4(1) is no longer used for migration. When upgrading to 8.4(2) from and 8.4(1), all identity NAT configurations will now include the **no-proxy-arp** and **r** keywords, to maintain existing functionality. The **unidirectional** keyword is remove We modified the following commands: **nat static** [**no-proxy-arp**] [**route-lookup**] (ob and **nat source static** [**no-proxy-arp**] [**route-lookup**] (global). We modified the following screens: **Configuration > Firewall > NAT Rules > Add/Edit Network Object > Advanced** **Configuration > Firewall > NAT Rules > Add/Edit NAT Rule**
PAT pool and round robin address assignment	You can now specify a pool of PAT addresses instead of a single address. You can als enable round-robin assignment of PAT addresses instead of first using all ports on a before using the next address in the pool. These features help prevent a large number o from a single PAT address from appearing to be part of a DoS attack and makes conf large numbers of PAT addresses easy. **Note** Currently in 8.4(2), the PAT pool feature is not available as a fallback m dynamic NAT or PAT. You can only configure the PAT pool as the prima for dynamic PAT (CSCtq20634). We modifed the following commands: **nat dynamic** [**pat-pool** *mapped_object* [**roun** (object network) and **nat source dynamic** [**pat-pool** *mapped_object* [**round-robin**]] We modified the following screens: **Configuration > Firewall > NAT Rules > Add/Edit Network Object** **Configuration > Firewall > NAT Rules > Add/Edit NAT Rul**

Feature	Description
IPv6 Inspection	You can configure IPv6 inspection by configuring a service policy to selectively block I based on the extension header. IPv6 packets are subjected to an early security check. Th always passes hop-by-hop and destination option types of extension headers while block header and no next header. You can enable default IPv6 inspection or customize IPv6 inspection. By defining a polic IPv6 inspection you can configure the ASA to selectively drop IPv6 packets based on fo types of extension headers found anywhere in the IPv6 packet: • Hop-by-Hop Options • Routing (Type 0) • Fragment • Destination Options • Authentication • Encapsulating Security Payload We modified the following commands: **policy-map type inspect ipv6, verify-header, m header, match header routing-type**, **match header routing-address count gt, match count gt**. We introduced the following screen: **Configuration > Firewall > Objects > Inspect Ma**
Remote Access Features	
Portal Access Rules	This enhancement allows customers to configure a global clientless SSL VPN access policy or deny clientless SSL VPN sessions based on the data present in the HTTP header. If de error code is returned to the clients. This denial is performed before user authentication a minimizes the use of processing resources. We modified the following command: **webvpn portal-access-rule**. We modified the following screen: **Configuration > Remote Access VPN > Clientless Access > Portal > Portal Access Rules**. *Also available in Version 8.2(5).*
Clientless support for Microsoft Outlook Web App 2010	The ASA 8.4(2) clientless SSL VPN core rewriter now supports Microsoft Outlook Web
Secure Hash Algorithm SHA-2 Support for IPsec IKEv2 Integrity and PRF	This release supports the Secure Hash Algorithm SHA-2 for increased cryptographic hashi for IPsec/IKEv2 AnyConnect Secure Mobility Client connections to the ASA. SHA-2 inc functions with digests of 256, 384, or 512 bits, to meet U.S. government requirements. We modified the following commands: **integrity**, **prf, show crypto ikev2 sa detail**, **sho vpn-sessiondb detail remote**. We modified the following screen: **Configuration > Remote Access VPN > Network (Access > Advanced > IPsec > IKE Policies > Add/Edit IKEv2 Policy (Proposal)**.

Feature	Description
Secure Hash Algorithm SHA-2 Support for Digital Signature over IPsec IKEv2	This release supports the use of SHA-2 compliant signature algorithms to authenticate VPN connections that use digital certificates, with the hash sizes SHA-256, SHA-384, a SHA-2 digital signature for IPsec IKEv2 connections is supported with the AnyConn Mobility Client, Version 3.0.1 or later.
Split Tunnel DNS policy for AnyConnect	This release includes a new policy pushed down to the AnyConnect Secure Mobility resolving DNS addresses over split tunnels. This policy applies to VPN connections or IPsec/IKEv2 protocol and instructs the AnyConnect client to resolve all DNS addr the VPN tunnel. If DNS resolution fails, the address remains unresolved and the AnyC does not try to resolve the address through public DNS servers. By default, this feature is disabled. The client sends DNS queries over the tunnel acc split tunnel policy: tunnel all networks, tunnel networks specified in a network list, o networks specified in a network list. We introduced the following command: split-tunnel-all-dns. We modified the following screen: **Configuration > Remote Access VPN > Networ Access > Group Policies > Add/Edit Group Policy > Advanced > Split Tunneling** All DNS Lookups Through Tunnel check box). *Also available in Version 8.2(5).*

Feature	Description
Mobile Posture (formerly referred to as AnyConnect Identification Extensions for Mobile Device Detection)	You can now configure the ASA to permit or deny VPN connections to mobile devices, disable mobile device access on a per group bases, and gather information about connect devices based on a mobile device's posture data. The following mobile platforms suppor capability: AnyConnect for iPhone/iPad/iPod Versions 2.5.x and AnyConnect for Andro 2.4.x. Licensing Requirements Enforcing remote access controls and gathering posture data from mobile devices requir AnyConnect Mobile license and either an AnyConnect Essentials or AnyConnect Premiu to be installed on the ASA. You receive the following functionality based on the license y • **AnyConnect Premium License Functionality** Enterprises that install the AnyConnect Premium license will be able to enforce DAP po supported mobile devices, based on these DAP attributes and any other existing endpoint This includes allowing or denying remote access from a mobile device. • **AnyConnect Essentials License Functionality** Enterprises that install the AnyConnect Essentials license will be able to do the followin • Enable or disable mobile device access on a per group basis and to configure that fea ASDM. • Display information about connected mobile devices via CLI or ASDM without ha ability to enforce DAP policies or deny or allow remote access to those mobile dev We modified the following screen: **Configuration > Remote Access VPN > Network (Access > Dynamic Access Policies > Add/Edit Endpoint Attributes > Endpoint Attr Type:AnyConnect**. *Also available in Version 8.2(5).*
SSL SHA-2 digital signature	You can now use of SHA-2 compliant signature algorithms to authenticate SSL VPN co that use digital certificates. Our support for SHA-2 includes all three hash sizes: SHA-256, and SHA-512. SHA-2 requires AnyConnect 2.5(1) or later (2.5(2) or later recommended release does not support SHA-2 for other uses or products. Caution: To support failover of SHA-2 connections, the standby ASA must be running th image. We modified the following command: **show crypto ca certificate** (the Signature Algorit identifies the digest algorithm used when generating the signature). We did not modify any screens. *Also available in Version 8.2(5).*

Feature	Description
SHA2 certificate signature support for Microsoft Windows 7 and Android-native VPN clients	ASA supports SHA2 certificate signature support for Microsoft Windows 7 and And VPN clients when using the L2TP/IPsec protocol. We did not modify any commands. We did not modify any screens. *Also available in Version 8.2(5).*
Enable/disable certificate mapping to override the group-url attribute	This feature changes the preference of a connection profile during the connection pro process. By default, if the ASA matches a certificate field value specified in a connec the field value of the certificate used by the endpoint, the ASA assigns that profile to connection. This optional feature changes the preference to a connection profile that group URL requested by the endpoint. The new option lets administrators rely on the preference used by many older ASA software releases. We introduced the following command: **tunnel-group-preference**. We modified the following screens: **Configuration > Remote Access VPN > Clientless SSL VPN > Connection Profil** **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Profiles** *Also available in Version 8.2(5).*
ASA 5585-X Features	
Support for Dual SSPs for SSP-40 and SSP-60	For SSP-40 and SSP-60, you can use two SSPs of the same level in the same chassis SSPs are not supported (for example, an SSP-40 with an SSP-60 is not supported). E as an independent device, with separate configurations and management. You can use as a failover pair if desired. **Note** When using two SSPs in the chassis, VPN is not supported; note, howev has not been disabled. We modified the following commands: **show module**, **show inventory**, **show enviro** We did not modify any screens.
Support for the IPS SSP-10, -20, -40, and -60	We introduced support for the IPS SSP-10, -20, -40, and -60 for the ASA 5585-X. Y install the IPS SSP with a matching-level SSP; for example, SSP-10 and IPS SSP-10 *Also available in Version 8.2(5).*
CSC SSM Features	

Feature	Description
CSC SSM Support	For the CSC SSM, support for the following features has been added: • HTTPS traffic redirection: URL filtering and WRS queries for incoming HTTPS co • Configuring global approved whitelists for incoming and outgoing SMTP and POP • E-mail notification for product license renewals. We did not modify any commands. We modified the following screens: **Configuration > Trend Micro Content Security > Mail > SMTP** **Configuration > Trend Micro Content Security > Mail > POP3** **Configuration > Trend Micro Content Security > Host/Notification Settings** **Configuration > Trend Micro Content Security > CSC Setup > Host Configuration**
Monitoring Features	
Smart Call-Home Anonymous Reporting	Customers can now help to improve the ASA platform by enabling Anonymous Reporti allows Cisco to securely receive minimal error and health information from the device. We introduced the following commands: **call-home reporting anonymous, call-home test anonymous**. We modified the following screen: **Configuration > Device Monitoring > Smart Call-** *Also available in Version 8.2(5).*
IF-MIB ifAlias OID support	The ASA now supports the ifAlias OID. When you browse the IF-MIB, the ifAlias OID to the value that has been set for the interface description. *Also available in Version 8.2(5).*
Interface Features	
Support for Pause Frames for Flow Control on 1-Gigabit Ethernet Interface	You can now enable pause (XOFF) frames for flow control on 1-Gigabit Ethernet interface was previously added for 10-Gigabit Ethernet interfaces in 8.2(2). We modified the following command: **flowcontrol**. We modified the following screens: (Single Mode) **Configuration > Device Setup > Interfaces > Add/Edit Interface > Ge** (Multiple Mode, System) **Configuration > Interfaces > Add/Edit Interface** *Also available in Version 8.2(5).*
Management Features	

Feature	Description
Increased SSH security; the SSH default username is no longer supported	Starting in 8.4(2), you can no longer connect to the ASA using SSH with the **pix** or **a** and the login password. To use SSH, you must configure AAA authentication using t **authentication ssh console LOCAL** command (CLI) or Configuration > Device Ma Users/AAA > AAA Access > Authentication (ASDM); then define a local user by en **username** command (CLI) or choosing Configuration > Device Management > Users Accounts (ASDM). If you want to use a AAA server for authentication instead of the l we recommend also configuring local authentication as a backup method.
Unified Communications Features	
ASA-Tandberg Interoperability with H.323 Inspection	H.323 Inspection now supports uni-directional signaling for two-way video sessions enhancement allows H.323 Inspection of one-way video conferences supported by Ta phones. Supporting uni-directional signaling allows Tandberg phones to switch video their side of an H.263 video session and reopen the session using H.264, the compres for high-definition video). We did not modify any commands. We did not modify any screens. *Also available in Version 8.2(5).*
Routing Features	
Timeout for connections using a backup static route	When multiple static routes exist to a network with different metrics, the ASA uses th best metric at the time of connection creation. If a better route becomes available, the lets connections be closed so a connection can be reestablished to use the better route is 0 (the connection never times out). To take advantage of this feature, change the tim value. We modified the following command: **timeout floating-conn**. We modified the following screen: **Configuration > Firewall > Advanced > Globa** *Also available in Version 8.2(5).*
ASDM Features	
Migrate Network Object Group Members	If you migrate to 8.3 or later, the ASA creates named network objects to replace inlin in some features. In addition to named objects, ASDM automatically creates non-nam any IP addresses used in the configuration. These auto-created objects are identified by only, do not have a name, and are not present as named objects in the platform confi When the ASA creates named objects as part of the migration, the matching non-name objects are replaced with the named objects. The only exception are non-named object object group. When the ASA creates named objects for IP addresses that are inside a n group, ASDM retains the non-named objects as well, creating duplicate objects in ASI these objects, choose **Tools > Migrate Network Object Group Members**. We introduced the following screen: **Tools > Migrate Network Object Group Men** See *Cisco ASA 5500 Migration to Version 8.3 and Later* for more information.

New Features in ASA 8.4(1.11)/ASDM 6.4(2)

Released: May 20, 2011

Note We recommend that you upgrade to a Cisco.com-posted interim release only if you have a specific problem that it resolves. If you decide to run an interim release in a production environment, keep in mind that only targeted testing is performed on interim releases. Interim releases are fully supported by Cisco TAC and will remain on the download site only until the next maintenance release is available. If you choose to run an interim release, we strongly encourage you to upgrade to a fully-tested maintenance or feature release when it becomes available. We will document interim release features at the time of the next maintenance or feature release. For a list of resolved caveats for each interim release, see the interim release notes available on the Cisco.com software download site.

Feature	Description
Firewall Features	
PAT pool and round robin address assignment	You can now specify a pool of PAT addresses instead of a single address. You can also o enable round-robin assignment of PAT addresses instead of first using all ports on a PAT before using the next address in the pool. These features help prevent a large number of co from a single PAT address from appearing to be part of a DoS attack and makes configur large numbers of PAT addresses easy. **Note** Currently in 8.4(1.11), the PAT pool feature is not available as a fallback me dynamic NAT or PAT. You can only configure the PAT pool as the primary r for dynamic PAT (CSCtq20634). We modifed the following commands: **nat dynamic** [**pat-pool** *mapped_object* [**round-r** (object network) and **nat source dynamic** [**pat-pool** *mapped_object* [**round-robin**]] (gl We modified the following screens: **Configuration > Firewall > NAT Rules > Add/Edit Network Object Configuration >** **> NAT Rules > Add/Edit NAT Rule**

New Features in ASA 8.4(1)/ASDM 6.4(1)

Released: January 31, 2011

Feature	Description
Hardware Features	
Support for the ASA 5585-X	We introduced support for the ASA 5585-X with Security Services Processor (SSP)-10, and -60. **Note** Support was previously added in 8.2(3) and 8.2(4); the ASA 5585-X is not s in 8.3(x).

Feature	Description
No Payload Encryption hardware for export	You can purchase the ASA 5585-X with No Payload Encryption. For export to some payload encryption cannot be enabled on the Cisco ASA 5500 series. The ASA softw No Payload Encryption model, and disables the following features: • Unified Communications • VPN You can still install the Strong Encryption (3DES/AES) license for use with managemen For example, you can use ASDM HTTPS/SSL, SSHv2, Telnet and SNMPv3. You can a the dynamic database for the Botnet Traffic Filer (which uses SSL).
Remote Access Features	
L2TP/IPsec Support on Android Platforms	We now support VPN connections between Android mobile devices and ASA 5500 s when using the L2TP/IPsec protocol and the native Android VPN client. Mobile dev using the Android 2.1, or later, operating system. *Also available in Version 8.2(5).*
UTF-8 Character Support for AnyConnect Passwords	AnyConnect 3.0 used with ASA 8.4(1), supports UTF-8 characters in passwords sen RADIUS/MSCHAP and LDAP protocols.
IPsec VPN Connections with IKEv2	Internet Key Exchange Version 2 (IKEv2) is the latest key exchange protocol used to control Internet Protocol Security (IPsec) tunnels. The ASA now supports IPsec with AnyConnect Secure Mobility Client, Version 3.0(1), for all client operating systems. On the ASA, you enable IPsec connections for users in the group policy. For the AnyC you specify the primary protocol (IPsec or SSL) for each ASA in the server list of the IPsec remote access VPN using IKEv2 was added to the AnyConnect Essentials and Premium licenses. Site-to-site sessions were added to the Other VPN license (formerly IPsec VPN). Th license is included in the Base license. We modified the following commands: **vpn-tunnel-protocol**, **crypto ikev2 policy**, **c enable**, **crypto ipsec ikev2**, **crypto dynamic-map**, **crypto map**. We modified the following screens: **Configure > Site-to-Site VPN > Connection Profiles** **Configure > Remote Access > Network (Client) Access > AnyConnect Connecti** **Network (Client) Access > Advanced > IPsec > IKE Parameters > IKE Policies** **Network (Client) Access > Advanced > IPsec > IKE Parameters > IKE Paramet** **Network (Client) Access > Advanced > IPsec > IKE Parameters > IKE Proposa**

Feature	Description
SSL SHA-2 digital signature	This release supports the use of SHA-2 compliant signature algorithms to authenticate S connections that use digital certificates. Our support for SHA-2 includes all three hash sizes: SHA-384, and SHA-512. SHA-2 requires AnyConnect 2.5.1 or later (2.5.2 or later recon This release does not support SHA-2 for other uses or products. This feature does not in configuration changes. **Caution**: To support failover of SHA-2 connections, the standby ASA must be running image. To support this feature, we added the Signature Algorithm field to the **show cryp certificate command** to identify the digest algorithm used when generating the signatur
SCEP Proxy	SCEP Proxy provides the AnyConnect Secure Mobility Client with support for automated certificate enrollment. Use this feature to support AnyConnect with zero-touch, secure d of device certificates to authorize endpoint connections, enforce policies that prevent ac non-corporate assets, and track corporate assets. This feature requires an AnyConnect Pr license and will not work with an Essentials license. We introduced or modified the following commands: **crypto ikev2 enable**, **scep-enrollme scep-forwarding-url**, **debug crypto ca scep-proxy**, **secondary-username-from-certifi secondary-pre-fill-username**.
Host Scan Package Support	This feature provides the necessary support for the ASA to install or upgrade a Host Sca and enable or disable Host Scan. This package may either be a standalone Host Scan pac one that ASA extracts from an AnyConnect Next Generation package. In previous releases of AnyConnect, an endpoint's posture was determined by Cisco Secur (CSD). Host Scan was one of many features bundled in CSD. Unbundling Host Scan fro gives AnyConnect administrators greater freedom to update and install Host Scan separa the other features of CSD. We introduced the following command: **csd hostscan image path**.
Kerberos Constrained Delegation (KCD)	This release implements the KCD protocol transition and constrained delegation extensi ASA. KCD provides Clientless SSL VPN (also known as WebVPN) users with SSO acc web services protected by Kerberos. Examples of such services or applications include C Web Access (OWA), Sharepoint, and Internet Information Server (IIS). Implementing protocol transition allows the ASA to obtain Kerberos service tickets on b remote access users without requiring them to authenticate to the KDC (through Kerberos a user authenticates to ASA using any of the supported authentication mechanisms, includ certificates and Smartcards, for Clientless SSL VPN (also known as WebVPN). When u authentication is complete, the ASA requests and obtains an impersonate ticket, which is ticket for ASA on behalf of the user. The ASA may then use the impersonate ticket to ob service tickets for the remote access user. Constrained delegation provides a way for domain administrators to limit the network reso a service trusted for delegation (for example, the ASA) can access. This task is accompli configuring the account under which the service is running to be trusted for delegation to instance of a service running on a specific computer. We modified the following commands: **kcd-server**, **clear aaa**, **show aaa**, **test aaa-serve authentication**. We modified the following screen: **Configuration > Remote Access VPN > Clientless Access > Advanced > Microsoft KCD Server**.

Feature	Description
Clientless SSL VPN browser support	The ASA now supports clientless SSL VPN with Apple Safari 5.
Clientless VPN Auto Sign-on Enhancement	Smart tunnel now supports HTTP-based auto sign-on on Firefox as well as Internet Exp to when Internet Explorer is used, the administrator decides to which hosts a Firefox automatically send credentials. For some authentication methods, if may be necessar administrator to specify a realm string on the ASA to match that on the web applicatio Smart Tunnel Auto Sign-on Server window). You can now use bookmarks with macro for auto sign-on with Smart tunnel as well. The POST plug-in is now obsolete. The former POST plug-in was created so that ad could specify a bookmark with sign-on macros and receive a kick-off page to load pr the the POST request. The POST plug-in approach allows requests that required the cookies, and other header items, fetched ahead of time to go through. The administra specify pre-load pages when creating bookmarks to achieve the same functionality. S POST plug-in, the administrator specifies the pre-load page URL and the URL to ser request to. You can now replace the default preconfigured SSL VPN portal with your own porta administrators do this by specifying a URL as an External Portal. Unlike the group-p page, the External Portal supports POST requests with macro substitution (for auto si as pre-load pages. We introduced or modified the following command: **smart-tunnel auto-signon**. We introduced or modified the following screens: **Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Cu** **Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > B** **Edit > Edit Bookmark**
Expanded Smart Tunnel application support	Smart Tunnel adds support for the following applications: • Microsoft Outlook Exchange Server 2010 (native support). Users can now use Smart Tunnel to connect Microsoft Office Outlook to a Microsoft Server. • Microsoft Sharepoint/Office 2010. Users can now perform remote file editing using Microsoft Office 2010 Applications Sharepoint by using Smart Tunnel.
Interface Features	

Feature	Description
EtherChannel support (ASA 5510 and higher)	You can configure up to 48 802.3ad EtherChannels of eight active interfaces each. **Note** You cannot use interfaces on the 4GE SSM, including the integrated 4GE S slot 1 on the ASA 5550, as part of an EtherChannel. We introduced the following commands: **channel-group**, **lacp port-priority**, **interface por lacp max-bundle**, **port-channel min-bundle**, **port-channel load-balance**, **lacp system clear lacp counters**, **show lacp**, **show port-channel**. We introduced or modified the following screens: **Configuration > Device Setup > Interfaces** **Configuration > Device Setup > Interfaces > Add/Edit EtherChannel Interface** **Configuration > Device Setup > Interfaces > Add/Edit Interface** **Configuration > Device Setup > EtherChannel**
Bridge groups for transparent mode	If you do not want the overhead of security contexts, or want to maximize your use of se contexts, you can group interfaces together in a bridge group, and then configure multip groups, one for each network. Bridge group traffic is isolated from other bridge groups. configure up to 8 bridge groups in single mode or per context in multiple mode, with 4 i maximum per bridge group. **Note** Although you can configure multiple bridge groups on the ASA 5505, the r of 2 data interfaces in transparent mode on the ASA 5505 means you can or effectively use 1 bridge group. **We introduced the following commands: interface bvi, bridge-group, show bridge-g** **We modified or introduced the following screens:** **Configuration > Device Setup > Interfaces** **Configuration > Device Setup > Interfaces > Add/Edit Bridge Group Interface Conf > Device Setup > Interfaces > Add/Edit Interface**
Scalability Features	
Increased contexts for the ASA 5550, 5580, and 5585-X	For the ASA 5550 and ASA 5585-X with SSP-10, the maximum contexts was increased to 100. For the ASA 5580 and 5585-X with SSP-20 and higher, the maximum was incre 50 to 250.
Increased VLANs for the ASA 5580 and 5585-X	For the ASA 5580 and 5585-X, the maximum VLANs was increased from 250 to 1024.
Additional platform support	Google Chrome has been added as a supported platform for ASA Version 8.4. Both 32-bit platforms are supported on Windows XP, Vista, and 7 and Mac OS X Version 6.0.

Feature	Description
Increased connections for the ASA 5580 and 5585-X	We increased the firewall connection limits: • ASA 5580-20—1,000,000 to 2,000,000. • ASA 5580-40—2,000,000 to 4,000,000. • ASA 5585-X with SSP-10: 750,000 to 1,000,000. • ASA 5585-X with SSP-20: 1,000,000 to 2,000,000. • ASA 5585-X with SSP-40: 2,000,000 to 4,000,000. • ASA 5585-X with SSP-60: 2,000,000 to 10,000,000.
Increased AnyConnect VPN sessions for the ASA 5580	The AnyConnect VPN session limit was increased from 5,000 to 10,000.
Increased Other VPN sessions for the ASA 5580	The other VPN session limit was increased from 5,000 to 10,000.
High Availability Features	
Stateful Failover with Dynamic Routing Protocols	Routes that are learned through dynamic routing protocols (such as OSPF and EIGRP unit are now maintained in a Routing Information Base (RIB) table on the standby u failover event, traffic on the secondary active unit now passes with minimal disrupti routes are known. Routes are synchronized only for link-up or link-down events on a If the link goes up or down on the standby unit, dynamic routes sent from the active lost. This is normal, expected behavior. We modified the following commands: **show failover**, **show route**, **show route failo** We did not modify any screens.
Unified Communication Features	
Phone Proxy addition to Unified Communication Wizard	The Unified Communications wizard guides you through the complete configuration and configures required aspects for the Phone Proxy. The wizard automatically creates th TLS proxy, then guides you through creating the Phone Proxy instance, importing an the required certificates, and finally enables the SIP and SCCP inspection for the Phon automatically. We modified the following screens: **Wizards > Unified Communications Wizard.** **Configuration > Firewall > Unified Communications.**
UC Protocol Inspection Enhancements	SIP Inspection and SCCP Inspection are enhanced to support new features in the Un Communications Solutions; such as, SCCP v2.0 support, support for GETPORT mess Inspection, SDP field support in INVITE messages with SIP Inspection, and QSIG t SIP. Additionally, the Cisco Intercompany Media Engine supports Cisco RT Lite pho third-party video endpoints (such as, Tandberg). We did not modify any commands. We did not modify any screens.

Feature	Description
Inspection Features	
DCERPC Enhancement	DCERPC Inspection was enhanced to support inspection of RemoteCreateInstance RPC We did not modify an commands. We did not modify any screens.
Troubleshooting and Monitoring Features	
SNMP traps and MIBs	Supports the following additional keywords: **connection-limit-reached**, **entity cpu-tem cpu threshold rising**, **entity fan-failure**, **entity power-supply**, **ikev2 stop | start**, **interface-threshold**, **memory-threshold**, **nat packet-discard**, **warmstart**. The entPhysicalTable reports entries for sensors, fans, power supplies, and related comp Supports the following additional MIBs: ENTITY-SENSOR-MIB, CISCO-ENTITY-SENSOR-EXT-MIB, CISCO-ENTITY-FRU-CONTROL-MIB, CISCO-PROCESS-MIB, CISCO-ENHANCED-MEMPOOL-MIB, CISCO-L4L7MODULE-RESOURCE-LIMIT-MIB, NAT-MIB, EVENT-MIB, EXPRESS Supports the following additional traps: warmstart, cpmCPURisingThreshold, mteTrigg cirResourceLimitReached, natPacketDiscard, ciscoEntSensorExtThresholdNotification. We introduced or modified the following commands: **snmp cpu threshold rising**, **snmp threshold**, **snmp-server enable traps**. We modified the following screen: **Configuration > Device Management > Manageme > SNMP**.
TCP Ping Enhancement	TCP ping allows users whose ICMP echo requests are blocked to check connectivity ov With the TCP ping enhancement you can specify a source IP address and a port and sourc to send pings to a hostname or an IPv4 address. We modified the following command: **ping tcp**. We modified the following screen: **Tools > Ping**.
Show Top CPU Processes	You can now monitor the processes that run on the CPU to obtain information related to percentage of the CPU used by any given process. You can also see information about th the CPU, broken down per process, at 5 minutes, 1 minute, and 5 seconds prior to the lo Information is updated automatically every 5 seconds to provide real-time statistics, and button in the pane allows a manual data refresh at any time. We introduced the following command: **show process cpu-usage sorted**. We introduced the following screen: **Monitoring > Properties > CPU - Per Process**.
General Features	
Password Encryption Visibility	You can show password encryption in a security context. We modified the following command: **show password encryption**. We did not modify any screens.
ASDM Features	

Feature	Description
ASDM Upgrade Enhancement	When ASDM loads on a device that has an incompatible ASA software version, a dialo users that they can select from the following options: • Upgrade the image version from Cisco.com. • Upgrade the image version from their local drive. • Continue with the incompatible ASDM/ASA pair (new choice). We did not modify any screens. This feature interoperates with all ASA versions.
Implementing IKEv2 in Wizards	IKEv2 support has been implemented into the AnyConnect VPN Wizard (formerly SSL the Clientless SSL VPN Wizard, and the Site-to-Site IPsec VPN Wizard (formerly IP Wizard) to comply with IPsec remote access requirements defined in federal and pub mandates. Along with the enhanced security, the new support offers the same end us independent of the tunneling protocol used by the AnyConnect client session. IKEv2 other vendors' VPN clients to connect to the ASAs. We modified the following wizards: Site-to-Site IPsec VPN Wizard, AnyConnect VP and Clientless SSL VPN Wizard.
IPS Startup Wizard enhancements	For the IPS SSP in the ASA 5585-X, the IPS Basic Configuration screen was added wizard. Signature updates for the IPS SSP were also added to the Auto Update scree Zone and Clock Configuration screen was added to ensure the clock is set on the ASA gets its clock from the ASA. We introduced or modified the following screens: Wizards > Startup Wizard > IPS B Configuration Wizards > Startup Wizard > Auto Update Wizards > Startup Wizard > and Clock Configuration

New Features in Version 8.3

New Features in ASA 8.3(2.25)/ASDM 6.4(5.106)

Released: August 31, 2011

Note We recommend that you upgrade to a Cisco.com-posted ASA interim release only if you have a specific problem that it resolves. If you decide to run an interim release in a production environment, keep in mind that only targeted testing is performed on interim releases. Interim releases are fully supported by Cisco TAC and will usually remain on the download site only until the next maintenance release is available. If you choose to run an interim release, we strongly encourage you to upgrade to a fully-tested maintenance or feature release when it becomes available.

We will document interim release features at the time of the next maintenance or feature release. For a list of resolved caveats for each ASA interim release, see the interim release notes available on the Cisco.com software download site.

Feature	Description
Remote Access Features	
Clientless SSL VPN browser support	The ASA now supports clientless SSL VPN with Microsoft Internet Explorer 9 and Fire *Also available in Version 8.2(5.13) and 8.4.2(8).*
Compression for DTLS and TLS	To improve throughput, Cisco now supports compression for DTLS and TLS on AnyCo or later. Each tunneling method configures compression separately, and the preferred cor is to have both SSL and DTLS compression as LZS. This feature enhances migration fr VPN clients. **Note** Using data compression on high speed remote access connections passing h compressible data requires significant processing power on the ASA. With oth and traffic on the ASA, the number of sessions that can be supported on the is reduced. We introduced or modified the following commands: **anyconnect dtls compression** [**lzs** and **anyconnect ssl compression** [**deflate** | **lzs** | **none**]. We modified the following screen: **Configuration > Remote Access VPN > Clientless Access > Group Policies > Edit > Edit Internal Group Policy > Advanced > AnyConn > SSL Compression**. *Also available in Version 8.2(5.13) and 8.4.2(8).*
Troubleshooting Features	
Regular expression matching for the **show asp table classifier** and **show asp table filter** commands	You can now enter the **show asp table classifier** and **show asp table filter** commands wit expression to filter output. We modified the following commands: **show asp table classifier match** *regex*, **show as filter match** *regex*. ASDM does not support this command; enter the command using the Command Line To *Also available in Version 8.2(5.13) and 8.4.2(8).*

New Features in ASA 8.3(2)/ASDM 6.3(2)

Released: August 2, 2010

Feature	Description
Monitoring Features	

Feature	Description
Enhanced logging and connection blocking	When you configure a syslog server to use TCP, and the syslog server is unavailable, th new connections that generate syslog messages until the server becomes available again VPN, firewall, and cut-through-proxy connections). This feature has been enhanced new connections when the logging queue on the ASA is full; connections resume wh queue is cleared. This feature was added for compliance with Common Criteria EAL4+. Unless requir recommend allowing new connections when syslog messages cannot be sent. To allo connections, configure the syslog server to use UDP or use the **logging permit-hostdo** check the **Allow user traffic to pass when TCP syslog server is down** check box o Configuration > Device Management > Logging > Syslog Servers pane. The following commands were modified: **show logging**. The following syslog messages were introduced: 414005, 414006, 414007, and 414 No ASDM screens were modified.
Syslog message filtering and sorting	Support has been added for the following: • Syslog message filtering based on multiple text strings that correspond to variou • Creation of custom filters • Column sorting of messages. For detailed information, see the ASDM configura The following screens were modified: **Monitoring > Logging > Real-Time Log Viewer > View** **Monitoring > Logging > Log Buffer Viewer > View** *This feature interoperates with all ASA versions.*
Clearing syslog messages for the CSC SSM	Support for clearing syslog messages has been added in the Latest CSC Security Eve The following screen was modified: **Home > Content Security**. *This feature interoperates with all ASA versions.*
Remote Access Features	

Feature	Description
2048-bit RSA certificate and Diffie-Hellman Group 5 (DH5) performance improvement	(ASA 5510, ASA 5520, ASA 5540, and ASA 5550 only) We strongly recommend that y hardware processing instead of software for large modulus operations such as 2048-bit c and DH5 keys. If you continue to use software processing for large keys, you could expe significant performance degradation due to slow session establishment for IPsec and SS connections. We recommend that you initially enable hardware processing during a low- maintenance period to minimize a temporary packet loss that can occur during the transi processing from software to hardware. **Note** For the ASA 5540 and ASA 5550 using SSL VPN, in specific load conditio may want to continue to use software processing for large keys. If VPN sess added very slowly and the ASA runs at capacity, then the negative impact t throughput is larger than the positive impact for session establishment. The following commands were introduced or modified: **crypto engine large-mod-accel configure crypto engine**, **show running-config crypto engine**, and **show running-conf** In ASDM, use the Command Line Interface tool to enter the **crypto engine large-mod-** command. *Also available in Version 8.2(3).*
Microsoft Internet Explorer proxy lockdown control	Enabling this feature hides the Connections tab in Microsoft Internet Explorer for the du an AnyConnect VPN session. Disabling the feature leaves the display of the Connection unchanged; the default setting for the tab can be shown or hidden, depending on the user settings. The following command was introduced: **msie-proxy lockdown**. In ASDM, use the Command Line Interface tool to enter this command. *Also available in Version 8.2(3).*
Secondary password enhancement	You can now configure SSL VPN support for a common secondary password for all authe or use the primary password as the secondary password. The following command was modified: **secondary-pre-fill-username** [**use-primary-pa use-common-password**]] The following screen was modified: **Configuration > Remote Access VPN > Clientless S > Connection Profiles > Add/Edit Clientless SSL VPN Connection Profile > Advanc Secondary Authentication**.
General Features	

Feature	Description
No Payload Encryption image for export	For export to some countries, payload encryption cannot be enabled on the Cisco ASA For version 8.3(2), you can now install a No Payload Encryption image (asa832-npe- following models: • ASA 5505 • ASA 5510 • ASA 5520 • ASA 5540 • ASA 5550 Features that are disabled in the No Payload Encryption image include: • Unified Communications. • Strong encryption for VPN (DES encryption is still available for VPN). • VPN load balancing (note that the CLI GUI is still present; the feature will not f however). • Downloading of the dynamic database for the Botnet Traffic Filer (Static black are still supported. Note that the CLI GUI is still present; the feature will not functi • Management protocols requiring strong encryption, including SSL, SSHv2, and S can, however, use SSL or SNMPv3 using base encryption (DES). Also, SSHv1 and v2 are still available. If you attempt to install a Strong Encryption (3DES/AES) license, you see the follow `WARNING: Strong encryption types have been disabled in this image; the VPN-3DES-AES license option has been ignored.`

New Features in ASA 8.3(1)/ASDM 6.3(1)

Released: March 8, 2010

Feature	Description
Remote Access Features	

Feature	Description
Smart Tunnel Enhancements	Logoff enhancement—Smart tunnel can now be logged off when all browser windows h closed (parent affinity), or you can right click the notification icon in the system tray and log out. Tunnel Policy—An administrator can dictate which connections go through the VPN ga which do not. An end user can browse the Internet directly while accessing company interna with smart tunnel if the administrator chooses. Simplified configuration of which applications to tunnel—When a smart tunnel is requir no longer needs to configure a list of processes that can access smart tunnel and in turn acc web pages. An "enable smart tunnel" check box for either a bookmark or standalone app allows for an easier configuration process. Group policy home page—Using a check box in ASDM, administrators can now specify t page in group policy in order to connect via smart tunnel. The following commands were introduced: **smart-tunnel network**, **smart-tunnel tunn** The following screen was modified: **Configuration > Remote Access VPN > AAA/Lo > Local Users > Edit > VPN Policy > Clientless SSL VPN**.
Newly Supported Platforms for Browser-based VPN	Release 8.3(1) provides browser-based (clientless) VPN access from the following newly platforms: • Windows 7 x86 (32-bit) and x64 (64-bit) via Internet Explorer 8.x and Firefox 3.x • Windows Vista x64 via Internet Explorer 7.x/8.x, or Firefox 3.x. • Windows XP x64 via Internet Explorer 6.x/7.x/8.x and Firefox 3.x • Mac OS 10.6.x 32- and 64-bit via Safari 4.x and Firefox 3.x. Firefox 2.x is likely to work, although we no longer test it. Release 8.3(1) introduces browser-based support for 64-bit applications on Mac OS 10.5 Release 8.3(1) now supports smart tunnel access on all 32-bit and 64-bit Windows OSs s for browser-based VPN access, Mac OS 10.5 running on an Intel processor only, and Mac The ASA does not support port forwarding on 64-bit OSs. Browser-based VPN access does not support Web Folders on Windows 7, Vista, and Interne 8. An ActiveX version of the RDP plug-in is not available for 64-bit browsers. **Note** Windows 2000 and Mac OS X 10.4 are no longer supported for browser-base

Feature	Description
IPv6 support for IKEv1 LAN-to-LAN VPN connections	For LAN-to-LAN connections using mixed IPv4 and IPv6 addressing, or all IPv6 ad ASA supports VPN tunnels if both peers are Cisco ASA 5500 series ASAs, and if bo networks have matching addressing schemes (both IPv4 or both IPv6). Specifically, the following topologies are supported when both peers are Cisco ASA ASAs: • The ASAs have IPv4 inside networks and the outside network is IPv6 (IPv4 add inside interfaces and IPv6 addresses on the outside interfaces). • The ASAs have IPv6 inside networks and the outside network is IPv4 (IPv6 add inside interface and IPv4 addresses on the outside interfaces). • The ASAs have IPv6 inside networks and the outside network is IPv6 (IPv6 add inside and outside interfaces). **Note** The defect CSCtd38078 currently prevents the Cisco ASA 5500 se connecting to a Cisco IOS device as the peer device of a LAN-to-LAN The following commands were modified or introduced: **isakmp enable**, **crypto map dynamic-map**, **tunnel-group**, **ipv6-vpn-filter**, **vpn-sessiondb**, **show crypto isakm crypto ipsec sa**, **show crypto debug-condition**, **show debug crypto**, **show vpn-sess crypto condition**, **debug menu ike**. The following screens were modified or introduced: **Wizards > IPsec VPN Wizard,** **Configuration > Site-to-Site VPN > Connection Profiles Configuration > Site-to Connection Profiles > Basic > Add IPsec Site-to-Site Connection Profile** **Configuration > Site-to-Site VPN > Group Policies** **Configuration > Site-to-Site VPN > Group Policies > Edit Internal Group Policy** **Configuration > Site-to-Site VPN > Advanced > Crypto Maps** **Configuration > Site-to-Site VPN > Advanced > Crypto Maps > Add > Create I** **Configuration > Site-to-Site VPN > Advanced > ACL Manager**
Plug-in for AnyConnect Profile Editor	The AnyConnect Profile Editor is a convenient GUI-based configuration tool you can us the AnyConnect 2.5 or later client profile, an XML file containing settings that control Previously, you could only change profile settings manually by editing the XML tags file. The AnyConnect Profile Editor is a plug-in binary file named anyconnectprof.sg with the ASDM image and installed in the root directory of disk0:/ in the flash memor This design allows you to update the editor to be compatible with new AnyConnect feat in new client releases.

Feature	Description
SSL VPN Portal Customization Editor	You can rebrand and customize the screens presented to clientless SSL VPN users using Edit Customization Object window in ASDM. You can customize the logon, portal and screens, including corporate logos, text messages, and the general layout. Previously, the customization feature was embedded in the ASA software image. Moving it to ASDM p greater usability for this feature and future enhancements. The following screen was modified: Configuration > Remote Access VPN > Clientless S Access > Portal > Customization.
Usability Improvements for Remote Access VPN	ASDM provides a step-by-step guide to configuring Clientless SSL VPN, AnyConnect S Remote Access, or IPsec Remote Access using the ASDM Assistant. The ASDM Assista comprehensive than the VPN wizards, which are designed only to get you up and runnin The following screen was modified: **Configuration > Remote Access VPN > Introduc ASDM Assistant**.
Firewall Features	
Interface-Independent Access Policies	You can now configure access rules that are applied globally, as well as access rules that a to an interface. If the configuration specifies both a global access policy and interface-spec policies, the interface-specific policies are evaluated before the global policy. The following command was modified: **access-group global**. The following screen was modified: **Configuration > Firewall > Access Rules**.
Network and Service Objects	You can now create named network objects that you can use in place of a host, a subnet, of IP addresses in your configuration and named service objects that you can use in plac protocol and port in your configuration. You can then change the object definition in one without having to change any other part of your configuration. This release introduces su network and service objects in the following features: • NAT • Access lists rules • Network object groups **Note** ASDM used network objects internally in previous releases; this feature i platform support for network objects. The following commands were introduced or modified: **object network**, **object service**, **running-config object**, **clear configure object**, **access-list extended**, **object-group net** The following screens were modified or introduced: **Configuration > Firewall > Objects > Network Objects/Groups,** **Configuration > Firewall > Objects > Service Objects/Groups** **Configuration > Firewall > NAT Rules, Configuration > Firewall > Access Rules**

Feature	Description
Object-group Expansion Rule Reduction	Significantly reduces the network object-group expansion while maintaining a satisfa packet classification performance. The following commands were modified: **show object-group**, **clear object-group**, **sho** The following screen was modified: C**onfiguration > Firewall > Access Rules > Ac**
NAT Simplification	The NAT configuration was completely redesigned to allow greater flexibility and ea can now configure NAT using auto NAT, where you configure NAT as part of the att network object, and manual NAT, where you can configure more advanced NAT opti The following commands were introduced or modified: **nat** (in global and object net configuration mode), **show nat**, **show nat pool**, **show xlate**, **show running-config n** The following commands were removed: **global**, **static**, **nat-control**, **alias**. The following screens were modified or introduced: **Configuration > Firewall > Objects > Network Objects/Group Configuration > NAT Rules**
Use of Real IP addresses in access lists instead of translated addresses	When using NAT, mapped addresses are no longer required in an access list for many should always use the real, untranslated addresses when configuring these features. U address means that if the NAT configuration changes, you do not need to change the The following commands and features that use access lists now use real IP addresses. T are automatically migrated to use real IP addresses when you upgrade to 8.3, unless oth • **access-group command** Access rules • Modular Policy Framework **match access-list** command Service policy rules • Botnet Traffic Filter **dynamic-filter enable classify-list** command • AAA **aaa ... match** commands rules • WCCP **wccp redirect-list group-list** command redirect. **Note** WCCP is not automatically migrated when you upgrade to 8.3.
Threat Detection Enhancements	You can now customize the number of rate intervals for which advanced statistics are default number of rates was changed from 3 to 1. For basic statistics, advanced statistics threat detection, the memory usage was improved. The following commands were modified: **threat-detection statistics port number-o threat-detection statistics protocol number-of-rates**, **show threat-detection mem** The following screen was modified: **Configuration > Firewall > Threat Detection**
Unified Communication Features	
SCCP v19 support	The IP phone support in the Cisco Phone Proxy feature was enhanced to include suppo 19 of the SCCP protocol on the list of supported IP phones.

Feature	Description
Cisco Intercompany Media Engine Proxy	Cisco Intercompany Media Engine (UC-IME) enables companies to interconnect on-den the Internet with advanced features made available by VoIP technologies. Cisco Intercomp Engine allows for business-to-business federation between Cisco Unified Communication clusters in different enterprises by utilizing peer-to-peer, security, and SIP protocols to creat SIP trunks between businesses. A collection of enterprises work together to end up lookir large business with inter-cluster trunks between them. The following commands were modified or introduced: **uc-ime**, **fallback hold-down**, **fa monitoring**, **fallback sensitivity-file**, **mapping-service listening-interface**, **media-ter ticket epoch**, **ucm address**, **clear configure uc-ime**, **debug uc-ime**, **show running-conf inspect sip**. The following screens were modified or introduced: **Wizards > Unified Communications Wizard > Cisco Intercompany Media Engine P Configuration > Firewall > Unified Communications**, and then click **UC-IME Proxy Configuration > Firewall > Service Policy Rules > Add/Edit Service Policy Rule > Ru > Select SIP Inspection Map**
SIP Inspection Support for IME	SIP inspection has been enhance to support the new Cisco Intercompany Media Engine Proxy. The following command was modified: **inspect sip**. The following screen was modified: **Configuration > Firewall > Service Policy Rules > Service Policy Rule > Rule Actions > Select SIP Inspection Map**.
Unified Communication Wizard	The Unified Communications wizard guides you through the complete configuration and aut configures required aspects for the following proxies: Cisco Mobility Advantage Proxy, Presence Federation Proxy, Cisco Intercompany Media Engine proxy. Additionally, the U Communications wizard automatically configures other required aspects of the proxies. The following screens were modified: **Wizards > Unified Communications Wizard** **Configuration > Firewall > Unified Communications**
Enhanced Navigation for Unified Communication Features	The Unified Communications proxy features, such as the Phone Proxy, TLS Proxy, CTL CTL Provider pages, are moved from under the Objects category in the left Navigation pa new Unified Communications category. In addition, this new category contains pages fo Unified Communications wizard and the UC-IME Proxy page. *This feature interoperates with all ASA versions.*
Routing Features	
Route map support	ASDM has added enhanced support for static and dynamic routes. The following screen was modified: **Configuration > Device Setup > Routing > Route** *This feature interoperates with all ASA versions.*
Monitoring Features	

Feature	Description
Time Stamps for Access List Hit Counts	Displays the timestamp, along with the hash value and hit count, for a specified acce The following command was modified: **show access-list**. The following screen was modified: **Configuration > Firewall > Access Rules**. (Th appears when you hover the mouse over a cell in the Hits column.)
High Performance Monitoring for ASDM	You can now enable high performance monitoring for ASDM to show the top 200 ho through the ASA. Each entry of a host contains the IP address of the host and the nu connections initiated by the host, and is updated every 120 seconds. The following commands were introduced: **hpm topn enable**, **clear configure hpm** **running-config hpm**. The following screen was introduced: **Home > Firewall Dashboard > Top 200 Hos**
Licensing Features	
Non-identical failover licenses	Failover licenses no longer need to be identical on each unit. The license used for bo combined license from the primary and secondary units. **Note** For the ASA 5505 and 5510 ASAs, both units require the Security Plus Base license does not support failover, so you cannot enable failover on a that only has the Base license. The following commands were modified: **show activation-key** and **show version**. The following screen was modified: **Configuration > Device Management > Licensing Key**.
Stackable time-based licenses	Time-based licenses are now stackable. In many cases, you might need to renew you license and have a seamless transition from the old license to the new one. For feature available with a time-based license, it is especially important that the license not exp can apply the new license. The ASA allows you to *stack* time-based licenses so you worry about the license expiring or about losing time on your licenses because you ins one early. For licenses with numerical tiers, stacking is only supported for licenses w capacity, for example, two 1000-session SSL VPN licenses. You can view the state o using the show activation-key command at **Configuration > Device Management > Activation Key**.
Intercompany Media Engine License	The IME license was introduced.
Time-based licenses based on Uptime	Time-based licenses now count down according to the total uptime of the ASA; the s does not affect the license.
Multiple time-based licenses active at the same time	You can now install multiple time-based licenses, and have one license per feature ac The following commands were modified: **show activation-key** and **show version**. The following screen was modified: **Configuration > Device Management > Licensing Key**.

Feature	Description
Discrete activation and deactivation of time-based licenses.	You can now activate or deactivate time-based licenses using a command. The following command was modified: **activation-key** [**activate** | **deactivate**]. The following screen was modified: **Configuration > Device Management > Licensing > A Key**.
General Features	
Master Passphrase	The master passphrase feature allows you to securely store plain text passwords in encrypt It provides a master key that is used to universally encrypt or mask all passwords, withou any functionality. The Backup/Restore feature supports the master passphrase. The following commands were introduced: **key config-key password-encryption**, **pass encryption aes**. The following screens were introduced: **Configuration > Device Management > Advanced > Master Passphrase Configuratio Management > Device Administration > Master Passphrase**
ASDM Features	
Upgrade Software from Cisco.com Wizard	The Upgrade Software from Cisco.com wizard has changed to allow you to automaticall ASDM and the ASA to more current versions. Note that this feature is only available in si and, in multiple context mode, in the System execution space. It is not available in a con The following screen was modified: **Tools > Check for ASA/ASDM Updates**. *This feature interoperates with all ASA versions.*
Backup/Restore Enhancements	The Backup Configurations pane was re-ordered and re-grouped so you can choose the f want to backup more easily. A Backup Progress pane was added allowing you to visuall the progress of the backup. And you will see significant performance improvement whe backup or restore. The following screen was modified: **Tools > Backup Configurations or Tools > Resto Configurations**. *This feature interoperates with all ASA versions.*

New Features in Version 8.2

New Features in ASA 8.2(5.13)/ASDM 6.4(4.106)

Released: September 18, 2011

Note We recommend that you upgrade to a Cisco.com-posted ASA interim release only if you have a specific problem that it resolves. If you decide to run an interim release in a production environment, keep in mind that only targeted testing is performed on interim releases. Interim releases are fully supported by Cisco TAC and will usually remain on the download site only until the next maintenance release is available. If you choose to run an interim release, we strongly encourage you to upgrade to a fully-tested maintenance or feature release when it becomes available.

We will document interim release features at the time of the next maintenance or feature release. For a list of resolved caveats for each ASA interim release, see the interim release notes available on the Cisco.com software download site.

Feature	Description
Remote Access Features	
Clientless SSL VPN browser support	The ASA now supports clientless SSL VPN with Microsoft Internet Explorer 9 and *Also available in Version 8.3(2.25) and 8.4.2(8).*
Compression for DTLS and TLS	To improve throughput, Cisco now supports compression for DTLS and TLS on Any or later. Each tunneling method configures compression separately, and the preferred is to have both SSL and DTLS compression as LZS. This feature enhances migration VPN clients. **Note** Using data compression on high speed remote access connections passin compressible data requires significant processing power on the ASA. With and traffic on the ASA, the number of sessions that can be supported on is reduced. We introduced or modified the following commands: **anyconnect dtls compression** and **anyconnect ssl compression** [**deflate** | **lzs** | **none**]. We modified the following screen: **Configuration > Remote Access VPN > Clientl Access > Group Policies > Edit > Edit Internal Group Policy > Advanced > AnyC > SSL Compression**. *Also available in Version 8.3(2.25) and Version 8.4.2(8).*
Troubleshooting Features	

Feature	Description
Regular expression matching for the **show asp table classifier** and **show asp table filter** commands	You can now enter the **show asp table classifier** and **show asp table filter** commands wit expression to filter output. We modified the following commands: **show asp table classifier match** *regex*, **show as filter match** *regex*. ASDM does not support this command; enter the command using the Command Line To *Also available in Version 8.3(2.25) and Version 8.4.2(8).*

New Features in ASA 8.2(5)/ASDM 6.4(3)

Released: May 23, 2011

Feature	Description
Monitoring Features	
Smart Call-Home Anonymous Reporting	Customers can now help to improve the ASA platform by enabling Anonymous Reporting, wh Cisco to securely receive minimal error and health information from the device. We introduced the following commands: **call-home reporting anonymous, call-home test anonymous**. We modified the following screen: **Configuration > Device Monitoring > Smart Call-Hom** *Also available in Version 8.4(2).*
IF-MIB ifAlias OID support	The ASA now supports the ifAlias OID. When you browse the IF-MIB, the ifAlias OID will the value that has been set for the interface description. *Also available in Version 8.4(2).*
Remote Access Features	
Portal Access Rules	This enhancement allows customers to configure a global clientless SSL VPN access policy or deny clientless SSL VPN sessions based on the data present in the HTTP header. If denied code is returned to the clients. This denial is performed before user authentication and thus m the use of processing resources. We modified the following command: **portal-access-rule**. We modified the following screen: **Configuration > Remote Access VPN > Clientless SSL Access > Portal > Portal Access Rules**. *Also available in Version 8.4(2).*

Feature	Description
Mobile Posture (formerly referred to as AnyConnect Identification Extensions for Mobile Device Detection)	You can now configure the ASA to permit or deny VPN connections to mobile devices, ena mobile device access on a per-group basis, and gather information about connected mobile on the mobile device posture data. The following mobile platforms support this capability for iPhone/iPad/iPod Versions 2.5.x and AnyConnect for Android Version 2.4.x. You do enable CSD to configure these attributes in ASDM. Licensing Requirements Enforcing remote access controls and gathering posture data from mobile devices requires a Mobile license and either an AnyConnect Essentials or AnyConnect Premium license to b the ASA. You receive the following functionality based on the license you install: • **AnyConnect Premium License Functionality** Enterprises that install the AnyConnect Premium license will be able to enforce DAP pol supported mobile devices, based on these DAP attributes and any other existing endpoint a includes allowing or denying remote access from a mobile device. • **AnyConnect Essentials License Functionality** Enterprises that install the AnyConnect Essentials license will be able to do the followin • Enable or disable mobile device access on a per-group basis and to configure that fe ASDM. • Display information about connected mobile devices via CLI or ASDM without hav to enforce DAP policies or deny or allow remote access to those mobile devices. We modified the following screen: **Configuration > Remote Access VPN > Network (C > Dynamic Access Policies > Add/Edit Endpoint Attributes > Endpoint Attribute Type:** *Also available in Version 8.4(2).*
Split Tunnel DNS policy for AnyConnect	This release includes a new policy pushed down to the AnyConnect Secure Mobility Clien DNS addresses over split tunnels. This policy applies to VPN connections using the SSL o protocol and instructs the AnyConnect client to resolve all DNS addresses through the V DNS resolution fails, the address remains unresolved and the AnyConnect client does not the address through public DNS servers. By default, this feature is disabled. The client sends DNS queries over the tunnel accordi tunnel policy—tunnel all networks, tunnel networks specified in a network list, or exclud specified in a network list. We introduced the following command: **split-tunnel-all-dns**. We modified the following screen: **Configuration > Remote Access VPN > Network (C > Group Policies > Add/Edit Group Policy > Advanced > Split Tunneling** (see the Se Lookups Through Tunnel check box). *Also available in Version 8.4(2).*

Feature	Description
SSL SHA-2 digital signature	You can now use of SHA-2 compliant signature algorithms to authenticate SSL VPN connec use digital certificates. Our support for SHA-2 includes all three hash sizes: SHA-256, SHA- SHA-512. SHA-2 requires AnyConnect 2.5(1) or later (2.5(2) or later recommended). This re not support SHA-2 for other uses or products. Caution: To support failover of SHA-2 connections, the standby ASA must be running the sa We modified the following command: **show crypto ca certificate** (the Signature Algorithm fiel the digest algorithm used when generating the signature). We did not modify any screens. *Also available in Version 8.4(2).*
L2TP/IPsec support for Android	We now support VPN connections between Android mobile devices and ASA 5500 series dev using the L2TP/IPsec protocol and the native Android VPN client. Mobile devices must be u Android 2.1 or later operating system. We did not modify any commands. We did not modify any screens. *Also available in Version 8.4(1).*
SHA2 certificate signature support for Microsoft Windows 7 and Android-native VPN clients	ASA supports SHA2 certificate signature support for Microsoft Windows 7 and Android-nat clients when using the L2TP/IPsec protocol. We did not modify any commands. We did not modify any screens. *Also available in Version 8.4(2).*
Enable/disable certificate mapping to override the group-url attribute	This feature changes the preference of a connection profile during the connection profile sele process. By default, if the ASA matches a certificate field value specified in a connection pro field value of the certificate used by the endpoint, the ASA assigns that profile to the VPN co This optional feature changes the preference to a connection profile that specifies the group URL by the endpoint. The new option lets administrators rely on the group URL preference used b older ASA software releases. We introduced the following command: **tunnel-group-preference**. We modified the following screens: **Configuration > Remote Access VPN > Clientless SSL VPN > Connection Profiles** **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connectio** *Also available in Version 8.4(2).*
Interface Features	

Feature	Description
Support for Pause Frames for Flow Control on 1-Gigabit Ethernet Interface	You can now enable pause (XOFF) frames for flow control on 1-Gigabit Ethernet interfa was previously added for 10-Gigabit Ethernet interfaces in 8.2(2). We modified the following command: **flowcontrol**. We modified the following screens: (Single Mode) Configuration > Device Setup > Interfaces > Add/Edit Interface > Genera Mode, System) Configuration > Interfaces > Add/Edit Interface *Also available in Version 8.4(2).*
Unified Communications Features	
ASA-Tandberg Interoperability with H.323 Inspection	H.323 Inspection now supports uni-directional signaling for two-way video sessions. This allows H.323 Inspection of one-way video conferences supported by Tandberg video phon uni-directional signaling allows Tandberg phones to switch video modes (close their side video session and reopen the session using H.264, the compression standard for high-def We did not modify any commands. We did not modify any screens. *Also available in Version 8.4(2).*
Routing Features	
Timeout for connections using a backup static route	When multiple static routes exist to a network with different metrics, the ASA uses the on metric at the time of connection creation. If a better route becomes available, then this ti connections be closed so a connection can be reestablished to use the better route. The de connection never times out). To take advantage of this feature, change the timeout to a ne We modified the following command: **timeout floating-conn**. We modified the following screen: **Configuration > Firewall > Advanced > Global Ti** *Also available in Version 8.4(2).*

New Features in ASA 8.2(4.4)/ASDM 6.3(5)

Released: March 4, 2011

Note We recommend that you upgrade to a Cisco.com-posted interim release only if you have a specific problem that it resolves. If you decide to run an interim release in a production environment, keep in mind that only targeted testing is performed on interim releases. Interim releases are fully supported by Cisco TAC and will remain on the download site only until the next maintenance release is available. If you choose to run an interim release, we strongly encourage you to upgrade to a fully-tested maintenance or feature release when it becomes available. We will document interim release features at the time of the next maintenance or feature release. For a list of resolved caveats for each interim release, see the *Cisco ASA Interim Release Notes* available on the Cisco.com software download site.

Feature	Description
Hardware Features	
Support for the IPS SSP-10, -20, -40, and -60 for the ASA 5585-X	We introduced support for the IPS SSP-10, -20, -40, and -60 for the ASA 5585-X. You can o the IPS SSP with a matching-level SSP; for example, SSP-10 and IPS SSP-10.
Remote Access Features	
Clientless SSL VPN support for Outlook Web Access 2010	By default, Clientless SSL VPN now provides content transformation (rewriting) support for Web Access (OWA) 2010 traffic. We did not modify any commands. We did not modify any screens.

New Features in ASA 8.2(4.1)/ASDM 6.3(5)

Released: January 18, 2011

Note We recommend that you upgrade to a Cisco.com-posted interim release only if you have a specific problem that it resolves. If you decide to run an interim release in a production environment, keep in mind that only targeted testing is performed on interim releases. Interim releases are fully supported by Cisco TAC and will remain on the download site only until the next maintenance release is available. If you choose to run an interim release, we strongly encourage you to upgrade to a fully-tested maintenance or feature release when it becomes available. We will document interim release features at the time of the next maintenance or feature release. For a list of resolved caveats for each interim release, see the *Cisco ASA Interim Release Notes* available on the Cisco.com software download site.

Feature	Description
Remote Access Features	
SSL SHA-2 digital signature	This release supports the use of SHA-2 compliant signature algorithms to authenticate SSL V connections that use digital certificates. Our support for SHA-2 includes all three hash sizes: SHA-384, and SHA-512. SHA-2 requires AnyConnect 2.5.1 or later (2.5.2 or later recommen release does not support SHA-2 for other uses or products. This feature does not involve con changes. Caution: To support failover of SHA-2 connections, the standby ASA must be runn same image. To support this feature, we added the Signature Algorithm field to the **show cry certificate** command to identify the digest algorithm used when generating the signature.

New Features in ASA 8.2(4)/ASDM 6.3(5)

Released: December 15, 2010

Feature	Description
Hardware Features	

Feature	Description
Support for the Cisco ASA 5585-X with SSP-10 and SSP-40	We introduced support for the ASA 5585-X with Security Services Processor (SSP)-10 a **Note** The ASA 5585-X is not supported in Version 8.3(x).

New Features in ASA 8.2(3.9)/ASDM 6.3(4)

Released: November 2, 2010

Note We recommend that you upgrade to a Cisco.com-posted interim release only if you have a specific problem that it resolves. If you decide to run an interim release in a production environment, keep in mind that only targeted testing is performed on interim releases. Interim releases are fully supported by Cisco TAC and will remain on the download site only until the next maintenance release is available. If you choose to run an interim release, we strongly encourage you to upgrade to a fully-tested maintenance or feature release when it becomes available. We will document interim release features at the time of the next maintenance or feature release. For a list of resolved caveats for each interim release, see the *Cisco ASA Interim Release Notes* available on the Cisco.com software download site.

Feature	Description
Remote Access Features	
SSL SHA-2 digital signature	This release supports the use of SHA-2 compliant signature algorithms to authenticate SS connections that use digital certificates. Our support for SHA-2 includes all three hash siz SHA-384, and SHA-512. SHA-2 requires AnyConnect 2.5.1 or later (2.5.2 or later recomm release does not support SHA-2 for other uses or products. This feature does not involve changes. Caution: To support failover of SHA-2 connections, the standby ASA must be r same image. To support this feature, we added the Signature Algorithm field to the **show certificate** command to identify the digest algorithm used when generating the signature.

New Features in ASA 8.2(3)/ASDM 6.3(3) and 6.3(4)

Released: August 9, 2010

Note ASDM 6.3(4) does not include any new features; it includes a caveat fix required for support of the ASA 5585-X.

Feature	Description
Hardware Features	

Feature	Description
Support for the Cisco ASA 5585-X with SSP-20 and SSP-60	Support for the ASA 5585-X with Security Services Processor (SSP)-20 and -60 was introdu **Note** The ASA 5585-X is not supported in Version 8.3(x). The ASA 5585-X requires ASDM 6.3(4).
Remote Access Features	
2048-bit RSA certificate and Diffie-Hellman Group 5 (DH5) performance improvement	(ASA 5510, ASA 5520, ASA 5540, and ASA 5550 only) We strongly recommend that you e hardware processing instead of software for large modulus operations such as 2048-bit certif DH5 keys. If you continue to use software processing for large keys, you could experience s performance degradation due to slow session establishment for IPsec and SSL VPN connect recommend that you initially enable hardware processing during a low-use or maintenance p minimize a temporary packet loss that can occur during the transition of processing from sof hardware. **Note** For the ASA 5540 and ASA 5550 using SSL VPN, in specific load conditions, y want to continue to use software processing for large keys. If VPN sessions are a slowly and the ASA runs at capacity, then the negative impact to data throughpu than the positive impact for session establishment. The ASA 5580/5585-X platforms already integrate this capability; therefore, cryp commands are not applicable on these platforms. The following commands were introduced or modified: **crypto engine large-mod-accel**, **clear crypto engine**, **show running-config crypto engine**, and **show running-config crypto**. In ASDM, use the Command Line Interface tool to enter the **crypto engine large-mod-accel** *Also available in Version 8.3(2).*
Microsoft Internet Explorer proxy lockdown control	Enabling this feature hides the Connections tab in Microsoft Internet Explorer for the duratio AnyConnect VPN session. Disabling the feature leaves the display of the Connections tab un the default setting for the tab can be shown or hidden, depending on the user registry settings The following command was introduced: **msie-proxy lockdown**. In ASDM, use the Command Line Interface tool to enter this command.
Trusted Network Detection Pause and Resume	This feature enables the AnyConnect client to retain its session information and cookie so th seamlessly restore connectivity after the user leaves the office, as long as the session does no the idle timer setting. This feature requires an AnyConnect release that supports TND pause an

New Features in ASA 8.2(2)/ASDM 6.2(5)

Released: January 11, 2010

Feature	Description
Remote Access Features	

Feature	Description
Scalable Solutions for Waiting-to-Resume VPN Sessions	An administrator can now keep track of the number of users in the active state and can lo statistics. The sessions that have been inactive for the longest time are marked as idle (an automatically logged off) so that license capacity is not reached and new users can log in The following screen was modified: **Monitoring > VPN > VPN Statistics > Sessions**. *Also available in Version 8.0(5).*
Application Inspection Features	
Inspection for IP Options	You can now control which IP packets with specific IP options should be allowed throug You can also clear IP options from an IP packet, and then allow it through the ASA. Prev options were denied by default, except for some special cases. **Note** This inspection is enabled by default. The following command is added to the service policy: **inspect ip-options**. Therefore, the ASA allows RSVP traffic packets with the Router Alert option (option 20) when the ASA is in routed The following commands were introduced: **policy-map type inspect ip-options**, **inspect eool**, **nop**. The following screens were introduced: **Configuration > Firewall > Objects > Inspect Maps > IP-Options** **Configuration > Firewall > Service Policy > Add/Edit Service Policy Rule > Rule Actio Inspection**
Enabling Call Set up Between H.323 Endpoints	You can enable call setup between H.323 endpoints when the Gatekeeper is inside the ne ASA includes options to open pinholes for calls based on the RegistrationRequest/Registr (RRQ/RCF) messages. Because these RRQ/RCF messages are sent to and from the Gatekeeper, the calling endpo is unknown and the ASA opens a pinhole through source IP address/port 0/0. By default, disabled. The following command was introduced: **ras-rcf-pinholes enable** (under the **policy-map h323 > parameters** commands). The following screen was modified: **Configuration > Firewall > Objects > Inspect Ma Details > State Checking**. *Also available in Version 8.0(5).*
Unified Communication Features	
Mobility Proxy application no longer requires Unified Communications Proxy license	The Mobility Proxy no longer requires the UC Proxy license.
Interface Features	

Feature	Description
In multiple context mode, auto-generated MAC addresses now use a user-configurable prefix, and other enhancements	The MAC address format was changed to allow use of a prefix, to use a fixed starting value (to use a different scheme for the primary and secondary unit MAC addresses in a failover pa The MAC addresess are also now persistent accross reloads. The command parser now checks if auto-generation is enabled; if you want to also manually MAC address, you cannot start the manual MAC address with A2. The following command was modified: **mac-address auto prefix** *prefix.* The following screen was modified: **Configuration > Context Management > Security Co** *Also available in Version 8.0(5).*
Support for Pause Frames for Flow Control on the ASA 5580 10 Gigabit Ethernet Interfaces	You can now enable pause (XOFF) frames for flow control. The following command was introduced: **flowcontrol**. The following screens were modified: (Single Mode) **Configuration > Device Setup > Interfaces > Add/Edit Interface > Gener** (Multiple Mode, System) **Configuration > Interfaces > Add/Edit Interface**
Firewall Features	
Botnet Traffic Filter Enhancements	The Botnet Traffic Filter now supports automatic blocking of blacklisted traffic based on the th You can also view the category and threat level of malware sites in statistics and reports. Rep enhanced to show infected hosts. The 1 hour timeout for reports for top hosts was removed; th no timeout. The following commands were introduced or modified: **dynamic-filter ambiguous-is-black dynamic-filter drop blacklist**, **show dynamic-filter statistics**, **show dynamic-filter report infected-hosts**, and **show dynamic-filter reports top**. The following screens were introduced or modified: **Configuration > Firewall > Botnet Traffic Filter > Traffic Settings Monitoring > Botnet Filter > Infected Hosts**
Connection timeouts for all protocols	The idle timeout was changed to apply to all protocols, not just TCP. The following command was modified: **set connection timeout**. The following screen was modified: **Configuration > Firewall > Service Policies > Rule A Connection Settings**.
Routing Features	

Feature	Description
DHCP RFC compatibility (rfc3011, rfc3527) to resolve routing issues	This enhancement introduces ASA support for DHCP RFCs 3011 (The IPv4 Subnet Sele and 3527 (Link Selection Sub-option for the Relay Agent Information Option). For each configured for VPN clients, you can now configure the ASA to send the Subnet Selection Link Selection option. The following command was modified: **dhcp-server** [**subnet-selection** | **link-selection]**. The following screen was modified: **Remote Access VPN > Network Access > IPsec co profiles > Add/Edit**. *Also available in Version 8.0(5).*
High Availablility Features	
IPv6 Support in Failover Configurations	IPv6 is now supported in failover configurations. You can assign active and standby IPv6 interfaces and use IPv6 addresses for the failover and Stateful Failover interfaces. The following commands were modified: **failover interface ip**, **ipv6 address**. The following screens were modified: **Configuration > Device Management > High Availability > Failover > Setup** **Configuration > Device Management > High Availability > Failover > Interfaces** **Configuration > Device Management > High Availability > HA/Scalability Wizard**
No notifications when interfaces are brought up or brought down during a switchover event	To distinguish between link up/down transitions during normal operation from link up/do during failover, no link up/link down traps are sent during a failover. Also, no syslog mes link up/down transitions during failover are sent. *Also available in Version 8.0(5).*
AAA Features	
100 AAA Server Groups	You can now configure up to 100 AAA server groups; the previous limit was 15 server g The following command was modified: **aaa-server**. The following screen was modified: **Configuration > Device Management > Users/AA Server Groups**.
Monitoring Features	
Smart Call Home	Smart Call Home offers proactive diagnostics and real-time alerts on the ASA and provid network availability and increased operational efficiency. Customers and TAC engineers need to resolve problems quickly when an issue is detected. **Note** Smart Call Home server Version 3.0(1) has limited support for the ASA. See th Notes" for more information. The following commands were introduced: **call-home**, **call-home send alert-group**, **call call-home send**, **service call-home**, **show call-home**, **show call-home registered-modu** The following screen was introduced: **Configuration> Device Management> Smart Ca**

New Features in ASA 8.2(1)/ASDM 6.2(1)

Released: May 6, 2009

Hi

Feature	Description
Remote Access Features	
One Time Password Support for ASDM Authentication	ASDM now supports administrator authentication using one time passwords (OTPs) supporte SecurID (SDI). This feature addresses security concerns about administrators authenticating passwords. New session controls for ASDM users include the ability to limit the session time and the idl When the password used by the ASDM administrator times out, ASDM prompts the adminis re-authenticate. The following commands were introduced: **http server idle-timeout** and **http server session** The **http server idle-timeout** default is 20 minutes, and can be increased up to a maximum minutes. In ASDM, see **Configuration > Device Management > Management Access > ASDM/HTTPD/Telnet/SSH**.
Customizing Secure Desktop	You can use ASDM to customize the Secure Desktop windows displayed to remote users, inc Secure Desktop background (the lock icon) and its text color, and the dialog banners for the Cache Cleaner, Keystroke Logger, and Close Secure Desktop windows. In ASDM, see **Configuration > CSD Manager > Secure Desktop Manager**.
Pre-fill Username from Certificate	The pre-fill username feature enables the use of a username extracted from a certificate for username/password authentication. With this feature enabled, the username is “pre-filled” or screen, with the user being prompted only for the password. To use this feature, you must conf the **pre-fill username** and the **username-from-certificate** commands in tunnel-group config mode. The double-authentication feature is compatible with the pre-fill username feature, as the pre-fil feature can support extracting a primary username and a secondary username from the certif serve as the usernames for double authentication when two usernames are required. When co the pre-fill username feature for double authentication, the administrator uses the following tunnel-group general-attributes configuration mode commands: • **secondary-pre-fill-username**—Enables username extraction for Clientless or AnyCon connection. • **secondary-username-from-certificate**—Allows for extraction of a few standard DN fi a certificate for use as a username. In ASDM, see **Configuration> Remote Access VPN > Network (Client) Access > AnyCo Clienltess SSL VPN Connection Profiles > Advanced**. Settings are in the Authentication, Authentication, and Authorization panes.

Feature	Description
Double Authentication	The double authentication feature implements two-factor authentication for remote access t in accordance with the Payment Card Industry Standards Council Data Security Standard requires that the user enter two separate sets of login credentials at the login page. For ex primary authentication might be a one-time password, and the secondary authentication r domain (Active Directory) credential. If either authentication fails, the connection is deni Both the AnyConnect VPN client and Clientless SSL VPN support double authentication. Th client supports double authentication on Windows computers (including supported Wind devices and Start Before Logon), Mac computers, and Linux computers. The IPsec VPN client, cut-through-proxy authentication, hardware client authentication, and management do not support double authentication. Double authentication requires the following new tunnel-group general-attributes configu commands: • **secondary-authentication-server-group**—Specifies the secondary AAA server gro cannot be an SDI server group. • **secondary-username-from-certificate**—Allows for extraction of a few standard D a certificate for use as a username. • **secondary-pre-fill-username**—Enables username extraction for Clientless or AnyC connection. • **authentication-attr-from-server**—Specifies which authentication server authorizat are applied to the connection. • **authenticated-session-username**—Specifies which authentication username is asso the session. **Note** The RSA/SDI authentication server type cannot be used as the secondar username/password credential. It can only be used for primary authenti In ASDM, see **Configuration > Remote Access VPN > Network (Client) Access or Cl VPN > AnyConnect Connection Profiles > Add/Edit > Advanced > Secondary Autho**

Feature	Description
AnyConnect Essentials	AnyConnect Essentials is a separately licensed SSL VPN client, entirely configured on the A provides the full AnyConnect capability, with the following exceptions: • No CSD (including HostScan/Vault/Cache Cleaner) • No clientless SSL VPN • Optional Windows Mobile Support The AnyConnect Essentials client provides remote end users running Microsoft Windows Vista Mobile, Windows XP or Windows 2000, Linux, or Macintosh OS X, with the benefits of a C VPN client. To configure AnyConnect Essentials, the administrator uses the following command: **anyconnect-essentials**—Enables the AnyConnect Essentials feature. If this feature is disabl the **no** form of this command), the SSL Premium license is used. This feature is enabled by d **Note** This license cannot be used at the same time as the shared SSL VPN premium li In ASDM, see **Configuration > Remote Access VPN > Network (Client) Access > Advan AnyConnect Essentials License**. The AnyConnect Essentials license must be installed for A show this pane.
Disabling Cisco Secure Desktop per Connection Profile	When enabled, Cisco Secure Desktop automatically runs on all computers that make SSL VPN c to the ASA. This new feature lets you exempt certain users from running Cisco Secure Deskto connection profile basis. It prevents the detection of endpoint attributes for these sessions, so need to adjust the Dynamic Access Policy (DAP) configuration. CLI: [**no**] **without-csd** command **Note** "Connect Profile" in ASDM is also known as "Tunnel Group" in the CLI. Addit the **group-url** command is required for this feature. If the SSL VPN session use connection-alias, this feature will not take effect. In ASDM, see **Configuration > Remote Access VPN > Clientless SSL VPN Access > Con Profiles > Add or Edit > Advanced, Clientless SSL VPN Configuration**. or **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connectio > Add or Edit > Advanced > SSL VPN**.
Certificate Authentication Per Connection Profile	Previous versions supported certificate authentication for each ASA interface, so users received prompts even if they did not need a certificate. With this new feature, users receive a certifica only if the connection profile configuration requires a certificate. This feature is automatic; t **certificate authentication** command is no longer needed, but the ASA retains it for backwa compatibility. In ASDM, see **Configuration > Remote Access VPN > Network (Client) Access > AnyCo Connection Profiles > Add/Edit > Basic**. or **Configuraiton > Remote Access VPN > Clientless SSL VPN > Connection Profiles > Add/E**

Feature	Description
EKU Extensions for Certificate Mapping	This feature adds the ability to create certificate maps that look at the Extended Key Usag a client certificate and use these values in determining what connection profile the client the client does not match that profile, it uses the default group. The outcome of the conne depends on whether or not the certificate is valid and the authentication settings of the conn The following command was introduced: **extended-key-usage**. In ASDM, use the **IPSec Certificate to Connection Maps > Rules** pane, or **Certificate Connections Profile Maps** pane.
SSL VPN SharePoint Support for Win 2007 Server	Clientless SSL VPN sessions now support Microsoft Office SharePoint Server 2007.
Shared license for SSL VPN sessions	You can purchase a shared license with a large number of SSL VPN sessions and share th needed among a group of ASAs by configuring one of the ASAs as a shared license serve as clients. The following commands were introduced: **license-server** commands (various), **license**. **Note** This license cannot be used at the same time as the AnyConnect Essentials li In ASDM, see **Configuration > Device Management > Licensing > Shared SSL VPN L** see, **Monitoring > VPN > Clientless SSL VPN > Shared Licenses**.
Updated VPN Wizard	The VPN Wizard (accessible by choosing Wizards > IPSec VPN Wizard) was updated. The IPsec Encryption and Authentication (formerly Step 9 of 11) was removed because the W generates default values for these settings. In addition, the step to select IPsec Settings (C includes new fields to enable perfect forwarding secrecy (PFS) and set the Diffie-Hellma
Firewall Features	
TCP state bypass	If you have asymmetric routing configured on upstream routers, and traffic alternates betwe then you can configure TCP state bypass for specific traffic. The following command wa **set connection advanced tcp-state-bypass**. In ASDM, see **Configuration > Firewall > Service Policy Rules > Rule Actions > Connec**
Per-Interface IP Addresses for the Media-Termination Instance Used by the Phone Proxy	In Version 8.0(4), you configured a global media-termination address (MTA) on the ASA 8.2, you can now configure MTAs for individual interfaces (with a minimum of two MTA of this enhancement, the old CLI has been deprecated. You can continue to use the old co desired. However, if you need to change the configuration at all, only the new configurat accepted; you cannot later restore the old configuration. In ASDM, see **Configuration > Firewall > Advanced > Encrypted Traffic Inspection Termination Address**.
Displaying the CTL File for the Phone Proxy	The Cisco Phone Proxy feature includes the **show ctl-file** command, which shows the co CTL file used by the phone proxy. Using the **show ctl-file** command is useful for debugg configuring the phone proxy instance. This command is not supported in ASDM.

Feature	Description
Clearing Secure-phone Entries from the Phone Proxy Database	The Cisco Phone Proxy feature includes the **clear phone-proxy secure-phones** command, wh the secure-phone entries in the phone proxy database. Because secure IP phones always requ file upon bootup, the phone proxy creates a database that marks the IP phones as secure. The the secure phone database are removed after a specified configured timeout (via the **timeout secure-phones** command). Alternatively, you can use the **clear phone-proxy secure-phones** to clear the phone proxy database without waiting for the configured timeout. This command is not supported in ASDM.
H.239 Message Support in H.323 Application Inspection	In this release, the ASA supports the H.239 standard as part of H.323 application inspection. a standard that provides the ability for H.300 series endpoints to open an additional video ch single call. In a call, an endpoint (such as a video phone), sends a channel for video and a ch data presentation. The H.239 negotiation occurs on the H.245 channel. The ASA opens a pin the additional media channel. The endpoints use open logical channel message (OLC) to sig channel creation. The message extension is part of H.245 version 13. The decoding and encod telepresentation session is enabled by default. H.239 encoding and decoding is preformed by coder. In ASDM, see **Configuration > Firewall > Service Policy Rules > Add Service Policy Ru > Rule Actions > Protocol Inspection > H.323 H.225**. Click **Configure** and then choose th **Inspect Map**.
Processing H.323 Endpoints When the Endpoints Do Not Send OLCAck	H.323 application inspection has been enhanced to process common H.323 endpoints. The enh affects endpoints using the extendedVideoCapability OLC with the H.239 protocol identifier. I an H.323 endpoint does not send OLCAck after receiving an OLC message from a peer, the propagates OLC media proposal information into the media array and opens a pinhole for th channel (extendedVideoCapability). In ASDM, see **Configuration > Firewall > Service Policy Rules > Add Service Policy Ru > Rule Actions > Protocol Inspection > H.323 H.225**.
IPv6 in transparent firewall mode	Transparent firewall mode now participates in IPv6 routing. Prior to this release, the ASA cou IPv6 traffic in transparent mode. You can now configure an IPv6 management address in tra mode, create IPv6 access lists, and configure other IPv6 features; the ASA recognizes and pa packets. All IPv6 functionality is supported unless specifically noted. In ASDM, see **Configuration > Device Management > Management Access > Managem Address**.

Feature	Description
Botnet Traffic Filter	Malware is malicious software that is installed on an unknowing host. Malware that atter activity such as sending private data (passwords, credit card numbers, key strokes, or pro can be detected by the Botnet Traffic Filter when the malware starts a connection to a kn address. The Botnet Traffic Filter checks incoming and outgoing connections against a dyn of known bad domain names and IP addresses, and then logs any suspicious activity. You supplement the dynamic database with a static database by entering IP addresses or doma local "blacklist" or "whitelist." **Note** This feature requires the Botnet Traffic Filter license. See the following licensi for more information: http://www.cisco.com/en/US/docs/security/asa/asa82/license/license82.html The following commands were introduced: **dynamic-filter** commands (various), and the **dynamic-filter-snoop** keyword. In ASDM, see **Configuration > Firewall > Botnet Traffic Filter**.
AIP SSC card for the ASA 5505	The AIP SSC offers IPS for the ASA 5505 ASA. Note that the AIP SSM does not support v The following commands were introduced: **allow-ssc-mgmt**, **hw-module module ip**, an **module allow-ip**. In ASDM, see **Configuration > Device Setup > SSC Setup and Configuration > IPS**.
IPv6 support for IPS	You can now send IPv6 traffic to the AIP SSM or SSC when your traffic class uses the **m** command, and the policy map specifies the **ips** command. In ASDM, see **Configuration > Firewall > Service Policy Rules**.
Management Features	
SNMP version 3 and encryption	This release provides DES, 3DES, or AES encryption and support for SNMP Version 3, th form of the supported security models. This version allows you to configure authentication by using the User-based Security Model (USM). The following commands were introduced: • **show snmp engineid** • **show snmp group** • **show snmp-server group** • **show snmp-server user** • **snmp-server group** • **snmp-server user** The following command was modified: • **snmp-server host** In ASDM, see **Configuration > Device Management > Management Access > SNMP**

Feature	Description
NetFlow	This feature was introduced in Version 8.1(1) for the ASA 5580; this version introduces the f the other platforms. The new NetFlow feature enhances the ASA logging capabilities by log flow-based events through the NetFlow protocol. In ASDM, see **Configuration > Device Management > Logging > Netflow**.
Routing Features	
Multicast NAT	The ASA now offers Multicast NAT support for group addresses.
Troubleshooting Features	
Coredump functionality	A coredump is a snapshot of the running program when the program has terminated abnorma Coredumps are used to diagnose or debug errors and save a crash for later or off-site analysis TAC may request that users enable the coredump feature to troubleshoot application or syste on the ASA. To enable coredump, use the **coredump enable** command.
ASDM Features	
ASDM Support for IPv6	All IPv6 functionality is supported unless specifically noted.
Support for Public Server configuration	You can use ASDM to configure a public server. This allows to you define servers and service want to expose to an outside interface. In ASDM, see **Configuration > Firewall > Public Servers**.

New Features in Version 8.1

New Features in ASA 8.1(2)/ASDM 6.1(5)

Released: October 10, 2008

Feature	Description
Remote Access Features	

Feature	Description
Auto Sign-On with Smart Tunnels for IE	This feature lets you enable the replacement of logon credentials for WININET connecti Microsoft applications use WININET, including Internet Explorer. Mozilla Firefox does r supported by this feature. It also supports HTTP-based authentication, therefore form-based does not work with this feature. Credentials are statically associated to destination hosts, not services, so if initial credenti they cannot be dynamically corrected during runtime. Also, because of the association wit hosts, providing support for an auto sign-on enabled host may not be desirable if you want to some of the services on that host. To configure a group auto sign-on for smart tunnels, you create a global list of auto sign- assign the list to group policies or user names. This feature is not supported with Dynamic A In ASDM, see **Configuration > Firewall > Advanced > ACL Manager**.
Entrust Certificate Provisioning	ASDM 6.1.3 (which lets you manage security appliances running Versions 8.0x and 8.1x link to the Entrust website to apply for temporary (test) or discounted permanent SSL ident for your ASA. In ASDM, see **Configuration > Remote Access VPN > Certificate Management > Identit > Enroll ASA SSL VPN head-end with Entrust**.
Extended Time for User Reauthentication on IKE Rekey	You can configure the security appliance to give remote users more time to enter their cre Phase 1 SA rekey. Previously, when reauthenticate-on-rekey was configured for IKE tunne 1 rekey occurred, the security appliance prompted the user to authenticate and only gave approximately 2 minutes to enter their credentia minute window, the tunnel would be terminated. With this new feature enabled, users no time to enter credentials before the tunnel drops. The total amount of time is the differenc new Phase 1 SA being established, when the rekey actually takes place, and the old Phase With default Phase 1 rekey times set, the difference is roughly 3 hours, or about 15% of the In ASDM, see **Configuration > Device Management > Certificate Management > Ide Certificates**.
Persistent IPsec Tunneled Flows	With the persistent IPsec tunneled flows feature enabled, the security appliance preserves stateful (TCP) tunneled flows after the tunnel drops, then recovers. All other flows are dr the tunnel drops and must reestablish when a new tunnel comes up. Preserving the TCP f some older or sensitive applications to keep working through a short-lived tunnel drop. T supports IPsec LAN-to-LAN tunnels and Network Extension Mode tunnels from a hardw does not support IPsec or AnyConnect/SSL VPN remote access tunnels. See the **sysopt c preserve-vpn-flows** command. This option is disabled by default. In ASDM, see **Configuration > Remote Access VPN > Network (Client) Access > Adva > System Options**. Check the **Preserve stateful VPN flows when the tunnel drops for Extension Mode (NEM)** checkbox to enable persistent IPsec tunneled flows.
Show Active Directory Groups	The CLI command **show ad-groups** was added to list the active directory groups. ASDM Access Policy uses this command to present the administrator with a list of MS AD grou used to define the VPN policy. In ASDM, see **Configuration > Remote Access VPN > Clientless SSL VPN Access > Dy Policies > Add/Edit DAP > Add/Edit AAA Attribute**.

Feature	Description
Smart Tunnel over Mac OS	Smart tunnels now support Mac OS. In ASDM, see **Configuration > Remote Access VPN > Clientless SSL VPN Access > Porta Tunnels**.
Firewall Features	
NetFlow Filtering	You can filter NetFlow events based on traffic and event-type, and then send records to different For example, you can log all flow-create events to one collector, but log flow-denied events to collector. See the **flow-export event-type** command. In ASDM, see **Configuration > Firewall > Security Policy > Service Policy Rules > Add/Ed Policy Rule > Rule Actions > NetFlow**.
NetFlow Delay Flow Creation Event	For short-lived flows, NetFlow collecting devices benefit from processing a single event as o seeing two events: flow creation and teardown. You can now configure a delay before sendin creation event. If the flow is torn down before the timer expires, only the flow teardown ever sent. See the **flow-export delay flow-create** command. **Note** The teardown event includes all information regarding the flow; there is no loss information. In ASDM, see **Configuration > Device Management > Logging > NetFlow**.
QoS Traffic Shaping	If you have a device that transmits packets at a high speed, such as the ASA with Fast Ether is connected to a low speed device such as a cable modem, then the cable modem is a bottlenec packets are frequently dropped. To manage networks with differing line speeds, you can con security appliance to transmit packets at a fixed slower rate. See the **shape** command. See also the **crypto ipsec security-association replay** command, which lets you configure t anti-replay window size. One side-effect of priority queueing is packet re-ordering. For IPSe out-of-order packets that are not within the anti-replay window generate warning syslog messa warnings become false alarms in the case of priority queueing. This new command avoids pos alarms. In ASDM, see **Configuration > Firewall > Security Policy > Service Policy Rules > Add/Ed Policy Rule > Rule Actions > QoS**. Note that the only traffic class supported for traffic shap class-default, which matches all traffic.

Feature	Description
TCP Normalization Enhancements	You can now configure TCP normalization actions for certain packet types. Previously, t actions for these kinds of packets was to drop the packet. Now you can set the TCP norma the packets. • TCP invalid ACK check (the **invalid-ack** command) • TCP packet sequence past window check (the **seq-past-window** command) • TCP SYN-ACK with data check (the **synack-data** command) You can also set the TCP out-of-order packet buffer timeout (the **queue** command **timeo** Previously, the timeout was 4 seconds. You can now set the timeout to another value. The default action for packets that exceed MSS has changed from drop to allow (the **exc** command). The following non-configurable actions have changed from drop to clear for these packe • Bad option length in TCP • TCP Window scale on non-SYN • Bad TCP window scale value • Bad TCP SACK ALLOW option In ASDM, see **Configuration > Firewall > Objects > TCP Maps.**
TCP Intercept statistics	You can enable collection for TCP Intercept statistics using the **threat-detection statistics** command, and view them using the **show threat-detection statistics** command. In ASDM, see **Configuration > Firewall > Threat Detection.**
Threat detection shun timeout	You can now configure the shun timeout for threat detection using the **threat-detection sca shun duration** command. In ASDM, see **Configuration > Firewall > Threat Detection**.
Threat detection host statistics fine tuning	You can now reduce the amount of host statistics collected, thus reducing the system imp feature, by using the **threat-detection statistics host number-of-rate** command. In ASDM, see **Configuration > Firewall > Threat Detection**.
Platform Features	
Increased VLANs	The number of VLANs supported on the ASA 5580 are increased from 100 to 250.
SNMP support for unnamed interfaces	Formerly, SNMP only provided information about interfaces that were configured using command. For example, SNMP only sent traps and performed walks on the IF MIB and interfaces that were named. SNMP was enhanced to show information about all physical logical interfaces; a **nameif** command is no longer required to display the interfaces usin

New Features in ASA 8.1(1)/ASDM 6.1(1)

Released: March 1, 2008

Feature	Description
Introduction of the Cisco ASA 5580	The Cisco ASA 5580 comes in two models: • The ASA 5580-20 delivers 5 Gigabits per second of TCP traffic and UDP per is even greater. Many features in the system have been made multi-core capable this high throughput. In addition the system delivers greater than 60,000 TCP co per second and supports up to 1 million connections. • The ASA 5580-40 will deliver 10 Gigabits per second of TCP traffic and simil 5580-20 the UDP performance will be even greater. The ASA 5580-40 delive than 120,000 TCP connections per second and up to 2 million connections in In ASDM, see **Home > System Resource Status and Home > Device Informatio Environment Status**.
NetFlow	The new NetFlow feature enhances the ASA logging capabilities by logging flow-ba through the NetFlow protocol. For detailed information about this feature and the n commands, see the *Cisco ASA 5580 Adaptive Security Appliance Command Line Con Guide*. In ASDM, see **Configuration > Device Management > Logging > Netflow**.
Jumbo frame support	The Cisco ASA 5580 supports jumbo frames when you enter the **jumbo-frame re** command. A jumbo frame is an Ethernet packet larger than the standard maximun bytes (including Layer 2 header and FCS), up to 9216 bytes. You can enable support frames for all interfaces by increasing the amount of memory to process Ethernet f Assigning more memory for jumbo frames might limit the the maximum use of othe such as access lists. In ASDM, see **Configuration > Device Setup > Interfaces > Add/Edit Interface >** A
Per-packet load balancing for multi-core ASAs	For multi-core ASAs, the default behavior is to allow only one core to receive pac an interface receive ring at a time. The **asp load-balance per-packet** command ch behavior to allow multiple cores to receive packets from an interface receive ring a on them independently. The default behavior is optimized for scenarios where pac received uniformly on all interface rings. We introduced the following commands: **asp load-balance per-packet**, **show asp load-balance**.
Timeout for SIP Provisional Media	You can now configure the timeout for SIP provisional media using the timeout sip-provisional-media command. In ASDM, see **Configuration > Firewall > Advanced > Global Timeouts**.

Feature	Description
Details about the activation key	You can now view the permanent and temporary activation keys with their ena including all previously installed temporary keys and their expiration dates usi **activation key detail** command. In ASDM in single context mode, see **Configuration > Device Management > Image/Configuration > Activation Key**. In ASDM in multiple context mode, **Configuration > Device Management > Activation Key**.
New ASDM online help engine	ASDM now supports a new look for the online help. The online help now mai topic-based selection of the user from the left bookmark pane while browsing thr pane subject matter.
ASDM CPU Core Usage Graph	In single or multiple mode, the CPU core usage graph allows you to display th utilization status from the ASDM Home page.
Intelligent platform management interface (IPMI) for ASDM	Added support for intelligent platform management interface (IPMI), which pro with information on the status of the power supply, cooling fans, and temperatu processors and chassis from the ASDM Home page.
ASDM Assistant	The ASDM Assistant is now available from **View** Menu, instead of the **Tools** M has been changed to simplify the **Search** mechanism.
ASDM Backup and Restore Enhancement	The backup and restore enhancement allows you to back up configurations to the and then restore them back on the server as necessary. Additionally, this feature VPN-related files. This feature is found in **Tools > Backup Configuration**, an **Restore Configuration**. *Also supported for Version 8.0.*
ASDM Log Viewer	The Log viewer enhancement displays the source and destination port informatio the syslog messages. This information is displayed on the **Monitoring > Logging Log Viewer,** and **Log Buffer** page. *Also supported for Version 8.0.*
Enhanced VPN Search in ASDM	Added a CLI command-based Search facility that offers intelligent hints while y in keywords or a command. This search enhancement only exists on User Accoun Profiles, and Group Policies pages. *Also supported for Version 8.0.*

New Features in Version 8.0

New Features in ASA 8.0(5)/ASDM 6.2(3)

Released: November 3, 2009

Note Version 8.0(5) is not supported on the PIX security appliance.

Feature	Description
Remote Access Features	
Scalable Solutions for Waiting-to-Resume VPN Sessions	An administrator can now keep track of the number of users in the active state and can look a statistics. The sessions that have been inactive for the longest time are marked as idle (and ar automatically logged off) so that license capacity is not reached and new users can log in The following ASDM screen was modified: **Monitoring > VPN > VPN Statistics > Session** *Also available in Version 8.2(2).*
Application Inspection Features	
Enabling Call Set up Between H.323 Endpoints	You can enable call setup between H.323 endpoints when the Gatekeeper is inside the netwo ASA includes options to open pinholes for calls based on the RegistrationRequest/Registratio (RRQ/RCF) messages. Because these RRQ/RCF messages are sent to and from the Gatekeeper, the calling endpoint's is unknown and the security appliance opens a pinhole through source IP address/port 0/0. B this option is disabled. The following command was introduced:**ras-rcf-pinholes enable**. Use this command during configuration mode while creating an H.323 Inspection policy map. The following ASDM screen was modified: **Configuration > Firewall > Objects > Inspect H.323 > Details > State Checking**. *Also available in Version 8.2(2).*
Interface Features	

Feature	Description
In multiple context mode, auto-generated MAC addresses now use a user-configurable prefix, and other enhancements	The MAC address format was changed to allow use of a prefix, to use a fixed starting va to use a different scheme for the primary and secondary unit MAC addresses in a failove The MAC addresess are also now persistent accross reloads. The command parser now checks if auto-generation is enabled; if you want to also manu MAC address, you cannot start the manual MAC address with A2. The following command was modified: **mac-address auto prefix** *prefix.* The following ASDM screen was modified: **Configuration > Context Management > S Contexts**. *Also available in Version 8.2(2).*
High Availablility Features	
No notifications when interfaces are brought up or brought down during a switchover event	To distinguish between link up/down transitions during normal operation from link up/do during failover, no link up/link down traps are sent during a failover. Also, no syslog mes link up/down transitions during failover are sent. *Also available in Version 8.2(2).*
Routing Features	
DHCP RFC compatibility (rfc3011, rfc3527) to resolve routing issues	This enhancement introduces ASA support for DHCP RFCs 3011 (The IPv4 Subnet Sele and 3527 (Link Selection Sub-option for the Relay Agent Information Option). For each that is configured using the **dhcp-server** command, you can now configure the ASA to s **subnet-selection** option, and the **link-selection** option or neither. The following ASDM screen was modified: **Remote Access VPN > Network Access > IPs profiles > Add/Edit**. *Also available in Version 8.2(2).*
SSM Features	
CSC 6.3 Support in ASDM	ASDM displays Web Reputation, User Group Policies, and User ID Settings in the Plus I on the main home page. CSC 6.3 security event enhancements are included, such as the r Reputation events and user and group identifications.

New Features in ASA 8.0(4)/ASDM 6.1(3)

Released: August 11, 2008

Feature	Description
Unified Communications Features[1]	

Feature	Description
Phone Proxy	Phone Proxy functionality is supported. ASA Phone Proxy provides similar features to those Metreos Cisco Unified Phone Proxy with additional support for SIP inspection and enhanced The ASA Phone Proxy has the following key features: • Secures remote IP phones by forcing the phones to encrypt signaling and media • Performs certificate-based authentication with remote IP phones • Terminates TLS signaling from IP phones and initiates TCP and TLS to Cisco Unified I Advantage servers • Terminates SRTP and initiates RTP/SRTP to the called party In ASDM, see **Configuration > Firewall > Advanced > Encrypted Traffic Inspection > Pho**
Mobility Proxy	Secure connectivity (mobility proxy) between Cisco Unified Mobility Advantage clients and supported. Cisco Unified Mobility Advantage solutions include the Cisco Unified Mobile Communicato easy-to-use software application for mobile handsets that extends enterprise communications ap and services to mobile phones and smart phones and the Cisco Unified Mobility Advantage s mobility solution streamlines the communication experience, enabling real-time collaboratio the enterprise. The ASA in this solution delivers inspection for the MMP (formerly called OLWP) protocol, proprietary protocol between Cisco Unified Mobile Communicator and Cisco Unified Mobility A The ASA also acts as a TLS proxy, terminating and reoriginating the TLS signaling between Unified Mobile Communicator and Cisco Unified Mobility Advantage. In ASDM, see **Configuration > Firewall > Advanced > Encrypted Traffic Inspection > TI**
Presence Federation Proxy	Secure connectivity (presence federation proxy) between Cisco Unified Presence servers and Cisco/Microsoft Presence servers is supported. With the Presence solution, businesses can se connect their Cisco Unified Presence clients back to their enterprise networks, or share Prese information between Presence servers in different enterprises. The ASA delivers functionality to enable Presence for Internet and intra-enterprise communic SSL-enabled Cisco Unified Presence client can establish an SSL connection to the Presence S ASA enables SSL connectivity between server to server communication including third-party servers communicating with Cisco Unified Presence servers. Enterprises share Presence info and can use IM applications. The ASA inspects SIP messages between the servers. In ASDM, see **Configuration > Firewall > Service Policy Rules > Add/Edit Service Polic Rule Actions > Protocol Inspection or Configuration > Firewall > Advanced > Encrypte Inspection > TLS Proxy > Add > Client Configuration**.
Remote Access Features	

Feature	Description
Auto Sign-On with Smart Tunnels for IE1[1]	This feature lets you enable the replacement of logon credentials for WININET connecti Microsoft applications use WININET, including Internet Explorer. Mozilla Firefox does n supported by this feature. It also supports HTTP-based authentication, therefore form-based does not work with this feature. Credentials are statically associated to destination hosts, not services, so if initial credenti they cannot be dynamically corrected during runtime. Also, because of the association wit hosts, providing support for an auto sign-on enabled host may not be desirable if you want to some of the services on that host. To configure a group auto sign-on for smart tunnels, you create a global list of auto sign- assign the list to group policies or user names. This feature is not supported with Dynamic A In ASDM, see **Firewall > Advanced > ACL Manager**.
Entrust Certificate Provisioning[1]	ASDM includes a link to the Entrust website to apply for temporary (test) or discounted p identity certificates for your ASA. In ASDM, see **Configuration > Remote Access VPN > Certificate Management > Ide Certificates**. Click **Enroll ASA SSL VPN head-end with Entrust**.
Extended Time for User Reauthentication on IKE Rekey	You can configure the security appliance to give remote users more time to enter their cre Phase 1 SA rekey. Previously, when reauthenticate-on-rekey was configured for IKE tunne 1 rekey occurred, the security appliance prompted the user to authenticate and only gave approximately 2 minutes to enter their credentia minute window, the tunnel would be terminated. With this new feature enabled, users no time to enter credentials before the tunnel drops. The total amount of time is the differenc new Phase 1 SA being established, when the rekey actually takes place, and the old Phase With default Phase 1 rekey times set, the difference is roughly 3 hours, or about 15% of the In ASDM, see **Configuration > Device Management > Certificate Management > Ide Certificates**.
Persistent IPsec Tunneled Flows	With the persistent IPsec tunneled flows feature enabled, the security appliance preserves stateful (TCP) tunneled flows after the tunnel drops, then recovers. All other flows are dr the tunnel drops and must reestablish when a new tunnel comes up. Preserving the TCP f some older or sensitive applications to keep working through a short-lived tunnel drop. T supports IPsec LAN-to-LAN tunnels and Network Extension Mode tunnels from a Hardw does not support IPsec or AnyConnect/SSL VPN remote access tunnels. See the **[no] syso preserve-vpn-flows** command. This option is disabled by default. In ASDM, see **Configuration > Remote Access VPN > Network (Client) Access > Adva > System Options**. Check the **Preserve stateful VPN flows when the tunnel drops for Extension Mode (NEM)** checkbox to enable persistent IPsec tunneled flows.
Show Active Directory Groups	The CLI command **show ad-groups** was added to list the active directory groups. ASDM Access Policy uses this command to present the administrator with a list of MS AD grou used to define the VPN policy. In ASDM, see **Configuration > Remote Access VPN > Clientless SSL VPN Access > Dy Policies > Add/Edit DAP > Add/Edit AAA Attribute**.

Feature	Description
Smart Tunnel over Mac OS1 [1]	Smart tunnels now support Mac OS. In ASDM, see **Configuration > Remote Access VPN > Clientless SSL VPN Access > Porta Tunnels**.
Local Address Pool Edit	Address pools can be edited without affecting the desired connection. If an address in use is eliminated from the pool, the connection is not affected. However, if the address in use is being from the pool, the connection is brought down. *Also available in Version 7.0(8) and 7.2(4).*
Firewall Features	
QoS Traffic Shaping	If you have a device that transmits packets at a high speed, such as the ASA with Fast Ether is connected to a low speed device such as a cable modem, then the cable modem is a bottlenec packets are frequently dropped. To manage networks with differing line speeds, you can con security appliance to transmit packets at a fixed slower rate. See the **shape** command. See also **ipsec security-association replay** command, which lets you configure the IPSec anti-replay size. One side-effect of priority queueing is packet re-ordering. For IPSec packets, out-of-ord that are not within the anti-replay window generate warning syslog messages. These warning false alarms in the case of priority queueing. This new command avoids possible false alarm In ASDM, see **Configuration > Firewall > Security Policy > Service Policy Rules > Add/Ed Policy Rule > Rule Actions > QoS**. Note that the only traffic class supported for traffic shap class-default, which matches all traffic. *Also available in Version 7.2(4).*

Feature	Description
TCP Normalization Enhancements	You can now configure TCP normalization actions for certain packet types. Previously, th actions for these kinds of packets was to drop the packet. Now you can set the TCP norma the packets. • TCP invalid ACK check (the **invalid-ack** command) • TCP packet sequence past window check (the **seq-past-window** command) • TCP SYN-ACK with data check (the **synack-data** command) You can also set the TCP out-of-order packet buffer timeout (the **queue** command **timeo** Previously, the timeout was 4 seconds. You can now set the timeout to another value. The default action for packets that exceed MSS has changed from drop to allow (the **exc** command). The following non-configurable actions have changed from drop to clear for these packet • Bad option length in TCP • TCP Window scale on non-SYN • Bad TCP window scale value • Bad TCP SACK ALLOW option In ASDM, see **Configuration** > **Firewall** > **Objects** > **TCP Maps**. *Also available in Version 7.2(4).*
TCP Intercept statistics	You can enable collection for TCP Intercept statistics using the **threat-detection statistics** command, and view them using the **show threat-detection statistics** command. In ASDM 6.1(5) and later, see **Configuration** > **Firewall** > **Threat Detection**. This com supported in ASDM 6.1(3).
Threat detection shun timeout	You can now configure the shun timeout for threat detection using the **threat-detection sca shun duration** command. In ASDM 6.1(5) and later, see **Configuration** > **Firewall** > **Threat Detection**. This com supported in ASDM 6.1(3).
Timeout for SIP Provisional Media	You can now configure the timeout for SIP provisional media using the **timeout sip-provi** command. In ASDM, see **Configuration** > **Firewall** > **Advanced** > **Global Timeouts**. *Also available in Version 7.2(4).*
clear conn Command	The **clear conn** command was added to remove connections. *Also available in Version 7.0(8) and 7.2(4).*
Fragment full reassembly	The **fragment** command was enhanced with the **reassembly full** keywords to enable full for fragments that are routed through the device. Fragments that terminate at the device ar reassembled. *Also available in Version 7.0(8) and 7.2(4).*

Feature	Description
Ethertype ACL MAC Enhancement	EtherType ACLs have been enhanced to allow non-standard MACs. Existing default rules ar but no new ones need to be added. *Also available in Version 7.0(8) and 7.2(4).*
Troubleshooting and Monitoring Features	
capture command Enhancement	The **capture type asp-drop** *drop_code* command now accepts **all** as the *drop_code*, so you c capture all packets that the ASA drops, including those dropped due to security checks. *Also available in Version 7.0(8) and 7.2(4).*
show asp drop Command Enhancement	Output now includes a timestamp indicating when the counters were last cleared (see the **clear** command). It also displays the drop reason keywords next to the description, so you can easi **capture asp-drop** command using the keyword. *Also available in Version 7.0(8) and 8.0(4).*
clear asp table Command	Added the **clear asp table** command to clear the hits output by the show asp table command *Also available in Version 7.0(8) and 7.2(4).*
show asp table classify hits Command Enhancement	The **hits** option was added to the **show asp table classify** command, showing the timestamp the last time the asp table counters were cleared. It also shows rules with hits values not equa This permits users to quickly see what rules are being hit, especially since a simple configura end up with hundreds of entries in the **show asp table classify** command. *Also available in Version 7.0(8) and 8.0(4).*
MIB Enhancement	The CISCO-REMOTE-ACCESS-MONITOR-MIB is implemented more completely. *Also available in 8.0(4).*
show perfmon Command	Added the following rate outputs: TCP Intercept Connections Established, TCP Intercept Atte Embryonic Connections Timeout, and Valid Connections Rate in TCP Intercept. *Also available in Version 7.0(8) and 7.2(4).*

Feature	Description
memory tracking Commands	The following new commands are introduced in this release: • **memory tracking enable**–This command enables the tracking of heap memory req • **no memory tracking enable**–This command disables tracking of heap memory req up all currently gathered information, and returns all heap memory used by the tool system. • **clear memory tracking**–This command clears out all currently gathered information to track further memory requests. • **show memory tracking**–This command shows currently allocated memory tracked broken down by the topmost caller function address. • **show memory tracking address**–This command shows currently allocated memory by each individual piece of memory. The output lists the size, location, and topmost of each currently allocated piece memory tracked by the tool. • **show memory tracking dump**–This command shows the size, location, partial call memory dump of the given memory address. • **show memory tracking detail**–This command shows various internal details to be u insight into the internal behavior of the tool. *Also available in Version 7.0(8) and 7.2(4).*
Routing Features	
IPv6 Multicast Listener Discovery Protocol v2 Support	The ASA now supports the Multicast Listener Discovery Protocol (MLD) Version 2, to d presence of multicast address listeners on their directly attached links, and to discover spec multicast addresses are of interest to those neighboring nodes. The ASA becomes a multi listener, or a host, but not a a multicast router, and responds to Multicast Listener Queries Multicast Listener Reports only. The following commands support this feature: • **clear ipv6 mld traffic**—The clear ipv6 mld traffic command allows you to reset all Listener Discovery traffic counters. • **show ipv6 mld traffic**—The show ipv6 mld command allows you to display all the Listener Discovery traffic counters. • **debug ipv6 mld**—The enhancement to the debug ipv6 command allows the user to debug messages for MLD, to see whether the MLD protocol activities are working p • **show debug ipv6 mld** —The enhancement to the show debug ipv6 command allow display whether debug ipv6 mld is enabled or disabled. *Also available in Version 7.2(4).*
Platform Features	

Feature	Description
Native VLAN support for the ASA 5505	You can now include the native VLAN in an ASA 5505 trunk port using the **switchport trun vlan** command. In ASDM, see **Configuration > Device Setup > Interfaces > Switch Ports > Edit** dialog. *Also available in Version 7.2(4).*
SNMP support for unnamed interfaces	Previously, SNMP only provided information about interfaces that were configured using the command. For example, SNMP only sent traps and performed walks on the IF MIB and IP M interfaces that were named. Because the ASA 5505 has both unnamed switch ports and name interfaces, SNMP was enhanced to show information about all physical interfaces and logical a **nameif** command is no longer required to display the interfaces using SNMP. These chang all models, and not just the ASA 5505.
Failover Features	
failover timeout Command	The **failover timeout** command no longer requires a failover license for use with the static nail *Also available in Version 7.0(8) and 7.2(4).*
ASDM Features	
Simplify DNS Panel	The DNS Panel on the ASDM GUI has been modified for ease of use. See **Configuration > Management > DNS**.
Redesign the File Transfer Dialog box	You can drag-and-drop files in the File Transfer dialog box. To access this dialog box, go to **File Management**, and then click **File Transfer**.
Clear ACL Hit Counters	Added functionality enabling users to clear ACL hit counters. See the **Firewall > Advanced Manager** panel.
Renaming ACLs	Added the ability to rename ACLs from ASDM. See the **Firewall > Advanced > ACL Manager** panel.
Combine ASDM/HTTPS, SSH, Telnet into One Panel	ASDM has combined the ASDM, HTTPS, SSH, Telnet into one panel. See the **Monitoring > > Device Access > ASDM/HTTPS/Telnet/SSH Sessions** panel.
Display all standard ACLs in ACL Manager	Added functionality enabling users to display all standard ACL in the ACL Manager. See the **Firewall > Advanced > ACL Manager** panel.

[1] (1) This feature is not supported on the PIX security appliance.

New Features in ASA 8.0(3)/ASDM 6.0(3)

Released: November 7, 2007

Feature	Description
VPN Features	

Feature	Description
AnyConnect RSA SoftID API Integration	Provides support for AnyConnect VPN clients to communicate directly with R obtaining user token codes. It also provides the ability to specify SoftID messa a connection profile (tunnel group), and the ability to configure SDI messages o appliance that match SDI messages received through a RADIUS proxy. This fe the prompts displayed to the remote client user are appropriate for the action re authentication and the AnyConnect client responds successfully to authenticati
IP Address Reuse Delay	Delays the reuse of an IP address after it has been returned to the IP address po the delay prevents problems the security appliance may experience when an IP returned to the pool and reassigned quickly. In ASDM, see **Configure > Remote Access VPN > Network (Client) Access Assignment > Assignment Policy**.
Clientless SSL VPN Caching Static Content Enhancement	There are two changes to the clientless SSL VPN caching commands: The **cache-compressed** command is deprecated. The new **cache-static-content** command configures the ASA to cache all static c means all cacheable Web objects that are not subject to SSL VPN rewriting. Th content such as images and PDF files. The syntax of the command is **cache-static-content** {**enable** | **disable**}. By de content caching is disabled. Example: `hostname (config) # webvpn` `hostname (config-webvpn) # cache` `hostname (config-webvpn-cache) # cache-static-content enable` hostname (config-webvpn-cache) # In ASDM, see **Configuration > Remote Access VPN > Clientless SSL VPN Advanced > Content Cache**. *Also available in Version 7.2(3).*
Smart Card Removal Disconnect	This feature allows the central site administrator to configure remote client polic active tunnels when a Smart Card is removed. The Cisco VPN Remote Access So (both IPSec and SSL) will, by default, tear down existing VPN tunnels when the the Smart Card used for authentication. The following cli command disconnects tunnels when a smart card is removed: **smartcard-removal-disconnect** {**enab** This option is enabled by default. In ASDM, see **Configuration > Remote Access VPN > Network (Client) Ac Policies > Add/Edit Internal/External Group Policies > More Options**. *Also available in Version 7.2(3).*

Feature	Description
WebVPN load Balancing	The adaptive security appliance now supports the use of FQDNs for load balancing. T WebVPN load balancing using FQDNs, you must enable the use of FQDNs for load enter the **redirect-fqdn enable** command. Then add an entry for each of your adapti appliance outside interfaces into your DNS server if not already present. Each adapti appliance outside IP address should have a DNS entry associated with it for looku DNS entries must also be enabled for reverse lookup. Enable DNS lookups on you security appliance with the **dns domain-lookup inside** command (or whichever int a route to your DNS server). Finally, you must define the ip address, of your DNS the adaptive security appliance. Following is the new CLI associated with this enh **redirect-fqdn** {**enable** | **disable**}. In ASDM, see **Configuration > VPN > Load Balancing**. *Also available in Version 7.2(3).*
Application Inspection Features	
WAAS and ASA Interoperability	The **inspect waas** command is added to enable WAAS inspection in the policy-ma configuration mode. This CLI is integrated into Modular Policy Framework for ma flexibility in configuring the feature. The [no] inspect waas command can be configu a default inspection class and under a custom class-map. This inspection service is n by default. The keyword option waas is added to the **show service-policy inspect** command t WAAS statistics. `show service-policy inspect waas` A new system log message is generated when WAAS optimization is detected on a c All L7 inspection services including IPS are bypassed on WAAS optimized conne System Log Number and Format: %ASA-6-428001: WAAS confirmed from in_interface:src_ip_addr/src_port to out_interface:dest_ip_addr/dest_port, inspection services bypassed on this connect A new connection flag "W" is added in the WAAS connection. The **show conn detail** is updated to reflect the new flag. In ASDM, see **Configuration > Firewall > Service Policy Rules > Add/Edit Serv Rule > Rule Actions > Protocol Inspection**. *Also available in Version 7.2(3).*
DNS Guard Enhancement	Added an option to enable or disable DNS guard. When enabled, this feature allow DNS response back from a DNS request. In ASDM, see **Configuration > Firewall > Objects > Inspect maps > DNS**. *Also available in Version 7.2(3).*

Feature	Description
Support for ESMTP over TLS	This enhancement adds the configuration parameter **allow-tls** [**action log**] in the map. By default, this parameter is not enabled. When it is enabled, ESMTP insp not mask the 250-STARTTLS echo reply from the server nor the STARTTLS c the client. After the server replies with the 220 reply code, the ESMTP inspectio itself; the ESMTP traffic on that session is no longer inspected. If the **allow-tls** parameter is configured, the syslog message ASA-6-108007 is generated when on an ESMTP session. `policy-map type inspect esmtp esmtp_map` `parameters` `allow-tls [action log]` A new line for displaying counters associated with the **allow-tls** parameter is a show service-policy inspect esmtp command. It is only present if **allow-tls** is c the policy map. By default, this parameter is not enabled. `show service-policy inspect esmtp` `allow-tls, count 0, log 0` This enhancement adds a new system log message for the **allow-tls** parameter. an esmtp session the server has responded with a 220 reply code to the client S command. The ESMTP inspection engine will no longer inspect the traffic on th System log Number and Format: %ASA-6-108007: TLS started on ESMTP session between client <client-side interface-name>:<client IP address>/<client port> and server <server-side interface-name>:<server IP address>/<server port> In ASDM, see **Configuration > Firewall > Objects > Inspect Map > ESMTI** *Also available in Version 7.2(3).*
High Availability Features	
Added Dataplane Keepalive Mechanism	You can now configure the ASA so that a failover will not occur if the AIP SSM In previous releases when two ASAs with AIP SSMs are configured in failover SSM software is updated, the ASA triggers a failover, because the AIP SSM ne or restart for the software update to take effect. *Also available in Version 7.0(7) and 7.2(3)*
Fully Qualified Domain Name Support Enhancement	Added option in the **redirect-fqdn** command to send either the fully qualified (FQDN) or the IP address to the client in a VPN load balancing cluster. In ASDM, see **Configuration > Device Management >High Availability > V Balancing or Configuration > Remote Access VPN >Load Balancing**.
DHCP Features	

Feature	Description
DHCP client ID enhancement	If you enable the DHCP client for an interface using the **ip address dhcp** comman ISPs expect option 61 to be the interface MAC address. If the MAC address is not in the DHCP request packet, then an IP address will not be assigned. Use this new to include the interface MAC address for option 61. If you do not configure this co the client ID is as follows: cisco-<MAC>-<interface>-<hostname>. We introduced the following command: **dhcp-client client-id interface** *interface_* We modified the following screen: **Configuration > Device Management > DHCI Server**; then click **Advanced**. *Also available in Version 7.2(3).*
DHCP client broadcast flag	If you enable the DHCP client for an interface using the **ip address dhcp** command can use this command to set the broadcast flag to 1 in the DHCP packet header when client sends a discover requesting an IP address. The DHCP server listens to this b flag and broadcasts the reply packet if the flag is set to 1. If you enter the **no dhcp-client broadcast-flag** command, the broadcast flag is set the DHCP server unicasts the reply packets to the client with the offered IP addres The DHCP client can receive both broadcast and unicast offers from the DHCP se We introduced the following command: **dhcp-client broadcast-flag** We modified the following screen: **Configuration > Device Management > DHCI Server**; then click **Advanced**.
Platform Features	
ASA 5510 Security Plus License Allows Gigabit Ethernet for Port 0 and 1	The ASA 5510 ASA now has the security plus license to enable GE (Gigabit Ether port 0 and 1. If you upgrade the license from base to security plus, the capacity of th port Ethernet0/0 and Ethernet0/1 increases from the original FE (Fast Ethernet) (10 to GE (1000 Mbps). The interface names will remain Ethernet 0/0 and Ethernet 0/1 **speed** command to change the speed on the interface and use the **show interface** c to see what speed is currently configured for each interface. *Also available in Version 7.2(3).*
ASA 5505 Increased VLAN range	The ASA 5505 ASA now supports VLAN IDs between 1 and 4090. Originally, on IDs between 1 and 1001 were supported. *Also available in Version 7.2(3).*
Troubleshooting Features	
capture Command Enhancement	The enhancement to the capture command allows the user to capture traffic and dis real time. It also allows the user to specify command line options to filter traffic with to configure a separate access list. This enhancement adds the **real-time** and five-tup options. **capture** *cap_name* [**real-time**] [**dump**] [**detail** [**trace**] [**match** *prot* {**host** *ip* | *ip m* [{**eq** | **lt** | **gt**} *port*] {**host** *ip* | *ip mask* | **any**} [{**eq** | **lt** | **gt**} *port*]] *Also available in Version 7.2(3).*

Feature	Description
ASDM Features	
ASDM banner enhancement	The adaptive security appliance software supports an ASDM banner. If configu start ASDM, this banner text will appear in a dialog box with the option to con disconnect. The Continue option dismisses the banner and completes login as u the Disconnect option dismisses the banner and terminates the connection. This requires the customer to accept the terms of a written policy before connecting Following is the new CLI associated with this enhancement: **banner** {**exec** | **login** | **motd** | **asdm**} *text* **show banner** [**exec** | **login** | **motd** | **asdm**] **clear banner** In ASDM, see **Configuration > Properties > Device Administration > Bann** *Also available in Version 7.2(3).*
Localization Enhancement in ASDM	ASDM is now enhanced to supports AnyConnect Localization. See **Configurat Access VPN > Network (Client) Access > AnyConnect Customization,** or o **Configuration > RemoteAccess > Network Access > AnyConnect Customiz Configuration > RemoteAccess > Language Localization > MST Translati**
Time-based License Enhancement	On the Home page, the License tab of the Device Dashboard tab now includes days until a time-based license expires (if applicable).
Network Objects	You can now add true network objects that you can use in firewall rules. Objects and when you edit an object, the change is inherited wherever the object is use you create a rule, the networks that you specify in the rule are automatically ad network object list so you can reuse them elsewhere. You can name and edit th entries as well. See **Configuration > Firewall > Objects > Network Objects/**
Client Software Location Enhancement	Added support in Client Software Location list to allow client updates from Li systems. See **Configure > Remote Access VPN > Language Localization**. *Also available in Version 7.2(3).*
CSC Event and Statistic Reporting Enhancement	With the Cisco Content Security and Control (CSC) 6.2 software, ASDM provi statistics for the new Damage Cleanup Services (DCS) feature. DCS removes clients and servers and repairs system registries and memory.

New Features in ASA 8.0(2)/ASDM 6.0(2)

Released: June 18, 2007

Note There was no 8.0(1)/6.0(1) release.

Feature	Description
Routing Features	
EIGRP routing	The ASA supports EIGRP or EIGRP stub routing.
High Availability Features	
Remote command execution in Failover pairs	You can execute commands on the peer unit in a failover pair without having directly to the peer. This works for both Active/Standby and Active/Active fa
CSM configuration rollback support	Adds support for the Cisco Security Manager configuration rollback feature i configurations.
Failover pair Auto Update support	You can use an Auto Update server to update the platform image and configu failover pairs.
Stateful Failover for SIP signaling	SIP media and signaling connections are replicated to the standby unit.
Redundant interfaces	A logical redundant interface pairs an active and a standby physical interface. active interface fails, the standby interface becomes active and starts passing t can configure a redundant interface to increase the ASA reliability. This feature from device-level failover, but you can configure redundant interfaces as well if desired. You can configure up to eight redundant interface pairs.
Module Features	
Virtual IPS sensors with the AIP SSM	The AIP SSM running IPS software Version 6.0 and above can run multiple sensors, which means you can configure multiple security policies on the AIP can assign each context or single mode adaptive security appliance to one or m sensors, or you can assign multiple security contexts to the same virtual sens IPS documentation for more information about virtual sensors, including the number of sensors supported.
Password reset	You can reset the password on the SSM hardware module.
VPN Authentication Features[2]	
Combined certificate and username/password login	An administrator requires a username and password in addition to a certificat to SSL VPN connections.
Internal domain username/password	Provides a password for access to internal resources for users who log in with other than a domain username and password, for example, with a one-time pa This is a password in addition to the one a user enters when logging in.
Generic LDAP support	This includes OpenLDAP and Novell LDAP. Expands LDAP support availab authentication and authorization.
Onscreen keyboard	The ASA includes an onscreen keyboard option for the login page and subse authentication requests for internal resources. This provides additional protecti software-based keystroke loggers by requiring a user to use a mouse to click in an onscreen keyboard for authentication, rather than entering the character physical keyboard.

Feature	Description
SAML SSO verified with RSA Access Manager	The ASA supports Security Assertion Markup Language (SAML) protoc Sign On (SSO) with RSA Access Manager (Cleartrust and Federated Ident
NTLMv2	Version 8.0(2) adds support for NTLMv2 authentication for Windows-bas
Certificate Features	
Local certificate authority	Provides a certificate authority on the ASA for use with SSL VPN connec browser- and client-based.
OCSP CRL	Provides OCSP revocation checking for SSL VPN.
Cisco Secure Desktop Features	
Host Scan	As a condition for the completion of a Cisco AnyConnect or clientless SS connection, the remote computer scans for a greatly expanded collection of antispyware applications, firewalls, operating systems, and associated upd scans for any registry entries, filenames, and process names that you spec the scan results to the ASA. The ASA uses both the user login credentials computer scan results to assign a Dynamic Access Policy (DAP). With an Advanced Endpoint Assessment License, you can enhance Host configuring an attempt to update noncompliant computers to meet version Cisco can provide timely updates to the list of applications and versions t supports in a package that is separate from Cisco Secure Desktop.
Simplified prelogin assessment and periodic checks	Cisco Secure Desktop now simplifies the configuration of prelogin and pe to perform on remote Microsoft Windows computers. Cisco Secure Deskt add, modify, remove, and place conditions on endpoint checking criteria u simplified, graphical view of the checks. As you use this graphical view t sequences of checks, link them to branches, deny logins, and assign endp Cisco Secure Desktop Manager records the changes to an XML file. You the ASA to use returned results in combination with many other types of the connection type and multiple group settings, to generate and apply a D session.
VPN Access Policy Features	

Feature	Description
Dynamic access policies (DAP)	VPN gateways operate in dynamic environments. Multiple variables can affe VPN connection, for example, intranet configurations that frequently change, t roles each user may inhabit within an organization, and logins from remote a with different configurations and levels of security. The task of authorizing use more complicated in a VPN environment than it is in a network with a static con Dynamic Access Policies (DAP) on the ASA let you configure authorization that these many variables. You create a dynamic access policy by setting a collection control attributes that you associate with a specific user tunnel or session. These address issues of multiple group membership and endpoint security. That is, t grants access to a particular user for a particular session based on the policies y It generates a DAP at the time the user connects by selecting and/or aggregating from one or more DAP records. It selects these DAP records based on the en security information of the remote device and the AAA authorization informa the authenticated user. It then applies the DAP record to the user tunnel or se
Administrator differentiation	Lets you differentiate regular remote access users and administrative users ur same database, either RADIUS or LDAP. You can create and restrict access to t via various methods (TELNET and SSH, for example) to administrators only. on the IETF RADIUS service-type attribute.
Platform Enhancements	
VLAN support for remote access VPN connections	Provides support for mapping (tagging) of client traffic at the group or user le feature is compatible with clientless as well as IPsec and SSL tunnel-based co
VPN load balancing for the ASA 5510	Extends load balancing support to ASA 5510 adaptive security appliances tha Security Plus license.
Crypto conditional debug	Lets users debug an IPsec tunnel on the basis of predefined crypto conditions the peer IP address, connection-ID of a crypto engine, and security parameter (SPI). By limiting debug messages to specific IPSec operations and reducing t of debug output, you can better troubleshoot the ASA with a large number of
Browser-based SSL VPN Features	
Enhanced portal design	Version 8.0(2) includes an enhanced end user interface that is more cleanly o and visually appealing.
Customization	Supports administrator-defined customization of all user-visible content.
Support for FTP	You can provide file access via FTP in additional to CIFS (Windows-based).
Plugin applets	Version 8.0(2) adds a framework for supporting TCP-based applications withou a pre-installed client application. Java applets let users access these applicatio the browser-enabled SSL VPN portal. Initial support is for TELNET, SSH, R VNC.

Feature	Description
Smart tunnels	A smart tunnel is a connection between an application and a remote site, u browser-based SSL VPN session with the ASA as the pathway. Version 8 identify the applications to which you want to grant smart tunnel access, a specify the path to the application and the SHA-1 hash of its checksum to granting it access. Lotus SameTime and Microsoft Outlook Express are e applications to which you might want to grant smart tunnel access. The remote host originating the smart tunnel connection must be running Windows Vista, Windows XP, or Windows 2000, and the browser must be Java, Microsoft ActiveX, or both.
RSS newsfeed	Administrators can populate the clientless portal with RSS newsfeed infor lets company news or other information display on a user screen.
Personal bookmark support	Users can define their own bookmarks. These bookmarks are stored on a
Transformation enhancements	Adds support for several complex forms of web content over clientless co including Adobe flash and Java WebStart.
IPv6	Allows access to IPv6 resources over a public IPv4 connection.
Web folders	Lets browser-based SSL VPN users connecting from Windows operating sy shared file systems and perform the following operations: view folders, vi file properties, create, move, copy, copy from the local host to the remote from the remote host to the local host, and delete. Internet Explorer indica web folder is accessible. Accessing this folder launches another window, view of the shared folder, on which users can perform web folder functio the properties of the folders and documents permit them.
Microsoft Sharepoint enhancement	Extends Web Access support for Microsoft Sharepoint, integrating Micro applications available on the machine with the browser to view, change, a documents shared on a server. Version 8.0(2) supports Windows Sharepo 2.0 in Windows Server 2003.
HTTP/HTTPS Proxy Features	
PAC support	Lets you specify the URL of a proxy autoconfiguration file (PAC) to dow browser. Once downloaded, the PAC file uses a JavaScript function to ide for each URL.
Proxy exclusion list	Lets you configure a list of URLs to exclude from the HTTP requests the A to an external proxy server.
VPN Network Access Control Features	
SSL VPN tunnel support	The ASA provides NAC posture validation of endpoints that establish Any client sessions.

Feature	Description
Support for audit services	You can configure the ASA to pass the IP address of the client to an optional au if the client does not respond to a posture validation request. The audit server host IP address to challenge the host directly to assess its health. For example challenge the host to determine whether its virus checking software is active up-to-date. After the audit server completes its interaction with the remote hos a token to the posture validation server, indicating the health of the remote ho token indicates the remote host is healthy, the posture validation server sends access policy to the ASA for application to the traffic on the tunnel.
Application Inspection Features	
Modular policy framework inspect class map	Traffic can match one of multiple match commands in an inspect class map; traffic had to match all match commands in a class map to match the class ma
AIC for encrypted streams and AIC Arch changes	Provides HTTP inspection into TLS, which allows AIC/MPF inspection in W HTTP and HTTPS streams.
TLS Proxy for SCCP and SIP[3]	Enables inspection of encrypted traffic. Implementations include SSL encryp signaling, namely Skinny and SIP, interacting with the Cisco CallManager.
SIP enhancements for CCM	Improves interoperability with CCM 5.0 and 6.x with respect to signaling pir
IPv6 support for SIP	The SIP inspection engine supports IPv6 addresses. IPv6 addresses can be used in the Via header field, and SDP fields.
Full RTSP PAT support	Provides TCP fragment reassembly support, a scalable parsing routine on RT security enhancements that protect RTSP traffic.
Access List Features	
Enhanced service object group	Lets you configure a service object group that contains a mix of TCP services services, ICMP-type services, and any protocol. It removes the need for a spe ICMP-type object group and protocol object group. The enhanced service ob also specifies both source and destination services. The access list CLI now su behavior.
Ability to rename access list	Lets you rename an access list.
Live access list hit counts	Includes the hit count for ACEs from multiple access lists. The hit count value how many times traffic hits a particular access rule.
Attack Prevention Features	
Set connection limits for management traffic to the adaptive security appliance	For a Layer 3/4 management class map, you can specify the **set connection** c
Threat detection	You can enable basic threat detection and scanning threat detection to monito such as DoS attacks and scanning attacks. For scanning attacks, you can auto shun attacking hosts. You can also enable scan threat statistics to monitor both invalid traffic for hosts, ports, protocols, and access lists.
NAT Features	

Feature	Description
Transparent firewall NAT support	You can configure NAT for a transparent firewall.
Monitoring Features	
Secure logging	You can enable secure connections to the syslog server using SSL or TLS and encrypted system log message content. Not supported on the PIX seri security appliance.
ASDM Features	
Redesigned Interface	Reorganizes information to provide greater logical consistency and ease o
Expanded onscreen help	ASDM describes features and configuration options on screen, which red to consult other information sources.
Visual policy editor	The visual policy editor lets an administrator configure access control polici checking.
Firewall Dashboard	From the home page, you can now track threats to your network by monit that exceeds rate limits, as well as allowed and dropped traffic by host, ac or protocol.
Accessibility Features	Features such as keyboard navigation, alternate text for graphics, and imp reader support have been added.
Complex Configuration Support	You can move between panes without applying changes, allowing you to en configurations before applying that configuration to the device.
Device List	ASDM maintains a list of recently accessed devices, allowing you to swit devices and contexts.
SSL VPN configuration wizard	The new SSL VPN configuration wizard provides step-by-step guidance i basic SSL VPN connections.
Startup Wizard Enhancement	The Startup Wizard now allows you to configure the adaptive ASA to pas installed CSC SSM.
ASDM Assistant Enhancements‘	An assistant for configuring Secure Voice was added.
Packet Capture Wizard	The Packet Capture Wizard assists you in obtaining and downloading sni PCAP format.
Service Policy Rule Wizard	Updated to support IPS Virtualization.
Certificate Management Enhancements	The certificate management GUI is reorganized and simplified.

[2] (1) Clientless SSL VPN features are not supported on the PIX security appliance.
[3] (2) TLS proxy is not supported on the PIX security appliance.

New Features in Version 7.2

New Features in ASA 7.2(5)/ASDM 5.2(5)

Released: May 11, 2010

There were no new features in ASA 7.2(5)/ASDM 5.2(5)

New Features in ASA 7.2(4)/ASDM 5.2(4)

Released: April 7, 2008

Feature	Description
Remote Access Features	
Local Address Pool Edit	Address pools can be edited without affecting the desired connection. If an address in us being eliminated from the pool, the connection is not affected. However, if the address i being eliminated from the pool, the connection is brought down. *Also available in Version 7.0(8) and 8.0(4).*
Routing Features	
IPv6 Multicast Listener Discovery Protocol v2 Support	The ASA now supports the Multicast Listener Discovery Protocol (MLD) Version 2, to the presence of multicast address listeners on their directly attached links, and to discover s which multicast addresses are of interest to those neighboring nodes. The ASA becomes address listener, or a host, but not a a multicast router, and responds to Multicast Listene and sends Multicast Listener Reports only. The following commands support this feature: • **clear ipv6 mld traffic** The clear ipv6 mld traffic command allows you to reset all the Multicast Listener D traffic counters. • **show ipv6 mld traffic** The show ipv6 mld command allows you to display all the Multicast Listener Discov counters. • **debug ipv6 mld** The enhancement to the debug ipv6 command allows the user to display the debug for MLD, to see whether the MLD protocol activities are working properly. • **show debug ipv6 mld** The enhancement to the show debug ipv6 command allows the user to display whet ipv6 mld is enabled or disabled. *Also available in Version 8.0(4).*

Feature	Description
Platform Features	
Native VLAN Support on ASA 5505 Trunk Ports	You can now allow native VLANs on a trunk port (see the **switchport trunk native vla** In ASDM, see **Configuration > Device Setup > Interfaces > Switch Ports > Edit** o *Also available in Version 8.0(4).*
Connection Features	
clear conn Command	The **clear conn** command was added to remove connections. *Also available in Version 7.0(8) and 8.0(4).*
Fragment full reassembly	The **fragment** command was enhanced with the **reassembly full** keywords to enable fu for fragments that are routed through the device. Fragments that terminate at the devi fully reassembled. *Also available in Version 7.0(8) and 8.0(4).*
QoS Traffic Shaping	If you have a device that transmits packets at a high speed, such as the ASA with Fast it is connected to a low speed device such as a cable modem, then the cable modem i at which packets are frequently dropped. To manage networks with differing line spe configure the security appliance to transmit packets at a fixed slower rate. See the **sha** See also the **crypto ipsec security-association replay** command, which lets you confi anti-replay window size. One side-effect of priority queueing is packet re-ordering. For IPSec packets, out-of- that are not within the anti-replay window generate warning syslog messages. These become false alarms in the case of priority queueing. This new feature avoids possibl In ASDM, see **Configuration > Firewall > Security Policy > Service Policy Rules Service Policy Rule > Rule Actions > QoS**. Note that the only traffic class supporte shaping is class-default, which matches all traffic. *Also available in Version 8.0(4).*
Firewall Features	

Feature	Description
TCP Normalization Enhancements	You can now configure TCP normalization actions for certain packet types. Previously, t actions for these kinds of packets was to drop the packet. Now you can set the TCP norm allow the packets. • TCP invalid ACK check (the **invalid-ack** command) • TCP packet sequence past window check (the **seq-past-window** command) • TCP SYN-ACK with data check (the **synack-data** command) You can also set the TCP out-of-order packet buffer timeout (the **queue** command **timeout** Previously, the timeout was 4 seconds. You can now set the timeout to another value. The default action for packets that exceed MSS has changed from drop to allow (the **exc** command). The following non-configurable actions have changed from drop to clear for these packe • Bad option length in TCP • TCP Window scale on non-SYN • Bad TCP window scale value • Bad TCP SACK ALLOW option In ASDM, see the **Configuration > Global Objects > TCP Maps** pane. *Also available in Version 8.0(4).*
Timeout for SIP Provisional Media	You can now configure the timeout for SIP provisional media using the **timeout sip-provisional-media** command. In ASDM, see the **Configuration > Properties > Timeouts** pane. *Also available in Version 8.0(4).*
Ethertype ACL MAC Enhancement	EtherType ACLs have been enhanced to allow non-standard MACs. Existing default rul retained, but no new ones need to be added. *Also available in Version 7.0(8) and 8.0(4).*
Troubleshooting and Monitoring Features	
capture command Enhancement	The **capture type asp-drop** *drop_code* command now accepts **all** as the *drop_code*, so y now capture all packets that the ASA drops, including those dropped due to security che *Also available in Version 7.0(8) and 8.0(4).*
MIB Enhancement	The CISCO-REMOTE-ACCESS-MONITOR-MIB is implemented more completely. *Also available in 8.0(4).*
show asp drop Command Enhancement	Output now includes a timestamp indicating when the counters were last cleared (see the **drop** command). It also displays the drop reason keywords next to the description, so you use the **capture asp-drop** command using the keyword. *Also available in Version 7.0(8) and 8.0(4).*

Feature	Description
clear asp table Command	Added the **clear asp table** command to clear the hits output by the **show asp table** c *Also available in Version 7.0(8) and 8.0(4).*
show asp table classify hits Command Enhancement	The hits option was added to the **show asp table classify** command, showing the timesta the last time the asp table counters were cleared. It also shows rules with hits values zero. This permits users to quickly see what rules are being hit, especially since a simple may end up with hundreds of entries in the **show asp table classify** command. *Also available in Version 7.0(8) and 8.0(4).*
show perfmon Command	Added the following rate outputs: TCP Intercept Connections Established, TCP Interc TCP Embryonic Connections Timeout, and Valid Connections Rate in TCP Intercept *Also available in Version 7.0(8) and 8.0(4).*
memory tracking Commands	The following new commands are introduced in this release: • **memory tracking enable**–This command enables the tracking of heap memory • **no memory tracking enable**–This command disables tracking of heap memory re up all currently gathered information, and returns all heap memory used by the the system. • **clear memory tracking**–This command clears out all currently gathered inform continues to track further memory requests. • **show memory tracking**–This command shows currently allocated memory trac tool, broken down by the topmost caller function address. • **show memory tracking address**–This command shows currently allocated me down by each individual piece of memory. The output lists the size, location, and function of each currently allocated piece memory tracked by the tool. • **show memory tracking dump**–This command shows the size, location, partial a memory dump of the given memory address. • **show memory tracking detail**–This command shows various internal details to gaining insight into the internal behavior of the tool. *Also available in Version 7.0(8) and 8.0(4).*
Failover Features	
failover timeout Command	The **failover timeout** command no longer requires a failover license for use with the feature. *Also available in Version 7.0(8) and 8.0(4).*
ASDM Features	

Feature	Description
Network Objects	You can now add true network objects that you can use in firewall rules. Objects can be n when you edit an object, the change is inherited wherever the object is used. Also, when a rule, the networks that you specify in the rule are automatically added to the network o so you can reuse them elsewhere. You can name and edit these automatic entries as well Configuration > Objects > Network Objects/Groups.
Enhanced ASDM Rule Table	The ASDM rule tables have been redesigned to streamline policy creation.

New Features in ASA 7.2(3)/ASDM 5.2(3)

Released: August 15, 2007

Feature	Description
Remote Access Features	
WebVPN load Balancing	The adaptive security appliance now supports the use of FQDNs for load balancing. To WebVPN load balancing using FQDNs, you must enable the use of FQDNs for load balan the **redirect-fqdn enable** command. Then add an entry for each of your adaptive security outside interfaces into your DNS server if not already present. Each adaptive security ap outside IP address should have a DNS entry associated with it for lookups. These DNS en also be enabled for reverse lookup. Enable DNS lookups on your adaptive security appli the **dns domain-lookup inside** command (or whichever interface has a route to your DN Finally, you must define the ip address, of your DNS server on the adaptive security app Following is the new CLI associated with this enhancement: **redirect-fqdn** {**enable** | **dis** In ASDM, see **Configuration > VPN > Load Balancing**. *Also available in Version 8.0(3).*
Clientless SSL VPN Caching Static Content Enhancement	There are two changes to the clientless SSL VPN caching commands: The **cache-compressed** command is deprecated. The new **cache-static-content** command configures the ASA to cache all static content, means all cacheable Web objects that are not subject to SSL VPN rewriting. This include such as images and PDF files. The syntax of the command is **cache-static-content** {**enable** | **disable**}. By default, stati caching is disabled. Example: `hostname (config) # webvpn` `hostname (config-webvpn) # cache` `hostname (config-webvpn-cache) # cache-static-content enable` hostname (config-webvpn-cache) # In ASDM, see **Configuration > Remote Access VPN > Clientless SSL VPN Access > > Content Cache**. *Also available in Version 8.0(3).*

Feature	Description
Smart Card Removal Disconnect	This feature allows the central site administrator to configure remote client policy for d tunnels when a Smart Card is removed. The Cisco VPN Remote Access Software clien and SSL) will, by default, tear down existing VPN tunnels when the user removes th used for authentication. The following cli command disconnects existing VPN tunnels card is removed: **smartcard-removal-disconnect** {**enable** | **disable**}. This option is default. In ASDM, see **Configuration > Remote Access VPN > Network (Client) Access > G > Add/Edit Internal/External Group Policies > More Options**. *Also available in Version 8.0(3).*
Platform Features	
ASA 5510 Security Plus License Allows Gigabit Ethernet for Port 0 and 1	The ASA 5510 ASA now has the security plus license to enable GE (Gigabit Etherne and 1. If you upgrade the license from base to security plus, the capacity of the exter Ethernet0/0 and Ethernet0/1 increases from the original FE (Fast Ethernet) (100 Mbps Mbps). The interface names will remain Ethernet 0/0 and Ethernet 0/1. Use the **speed** change the speed on the interface and use the show interface command to see what spe configured for each interface. *Also available in Version 8.0(3).*
ASA 5505 Increased VLAN range	The ASA 5505 ASA now supports VLAN IDs between 1 and 4090. Originally, only between 1 and 1001 were supported. *Also available in Version 8.0(3).*
Troubleshooting Features	
capture Command Enhancement	The enhancement to the **capture** command allows the user to capture traffic and disp time. It also allows the user to specify command line options to filter traffic without configure a separate access list. This enhancement adds the **real-time** and five-tupple **m** **capture** *cap_name* [**real-time**] [**dump**] [**detail** [**trace**] [**match** *prot* {**host** *ip* | *ip mas* | **lt** | **gt**} *port*] {**host** *ip* | *ip mask* | **any**} [{**eq** | **lt** | **gt**} *port*]] *Also available in Version 8.0(3).*
Application Inspection Features	

Feature	Description
Support for ESMTP over TLS	This enhancement adds the configuration parameter **allow-tls** [**action log**] in the esmtp p By default, this parameter is not enabled. When it is enabled, ESMTP inspection would the 250-STARTTLS echo reply from the server nor the **STARTTLS** command from the After the server replies with the 220 reply code, the ESMTP inspection turns off by itself; t traffic on that session is no longer inspected. If the **allow-tls action log** parameter is conf syslog message ASA-6-108007 is generated when TLS is started on an ESMTP session. `policy-map type inspect esmtp esmtp_map` `parameters` `allow-tls [action log]` A new line for displaying counters associated with the **allow-tls** parameter is added to th **service-policy inspect esmtp** command. It is only present if **allow-tls** is configured in t map. By default, this parameter is not enabled. `show service-policy inspect esmtp` `allow-tls, count 0, log 0` This enhancement adds a new system log message for the **allow-tls** parameter. It indicat esmtp session the server has responded with a 220 reply code to the client **STARTTLS** The ESMTP inspection engine will no longer inspect the traffic on this connection. System log Number and Format: %ASA-6-108007: TLS started on ESMTP session between client *<client-side interface-name>:<client IP address>/<client port> and server <server-side interface-name IP address>/<server port>* In ASDM, see **Configuration > Firewall > Objects > Inspect Map > ESMTP**. *Also available in Version 8.0(3).*
DNS Guard Enhancement	Added an option to enable or disable DNS guard. When enabled, this feature allows only response back from a DNS request. In ASDM, see **Configuration > Firewall > Objects > Inspect maps > DNS**. *Also available in Version 8.0(3).*

Feature	Description
WAAS and ASA Interoperability	The **inspect waas** command is added to enable WAAS inspection in the policy-map configuration mode. This CLI is integrated into Modular Policy Framework for maxim in configuring the feature. The **[no] inspect waas** command can be configured under inspection class and under a custom class-map. This inspection service is not enabled The keyword option waas is added to the **show service-policy inspect** command to d statistics. `show service-policy inspect waas` A new system log message is generated when WAAS optimization is detected on a co L7 inspection services including IPS are bypassed on WAAS optimized connections. System Log Number and Format: %ASA-6-428001: WAAS confirmed from in_interface:src_ip_addr/src_port to out_interface:dest_ip_addr/dest_port, inspection services bypassed on this connectio A new connection flag "W" is added in the WAAS connection. The show conn detail updated to reflect the new flag. In ASDM, see **Configuration > Firewall > Service Policy Rules > Add/Edit Servic > Rule Actions > Protocol Inspection**. *Also available in Version 8.0(3).*
DHCP Features	
DHCP client ID enhancement	If you enable the DHCP client for an interface using the **ip address dhcp** command, expect option 61 to be the interface MAC address. If the MAC address is not included request packet, then an IP address will not be assigned. Use this new command to includ MAC address for option 61. If you do not configure this command, the client ID is a cisco-<MAC>-<interface>-<hostname>. We introduced the following command: **dhcp-client client-id interface** *interface_na* We modified the following screen: **Configuration > Device Management > DHCP Server**; then click **Advanced**. *Also available in Version 8.0(3).*
Module Features	
Added Dataplane Keepalive Mechanism	You can now configure the ASA so that a failover will not occur if the AIP SSM is u previous releases when two ASAs with AIP SSMs are configured in failover and the software is updated, the ASA triggers a failover, because the AIP SSM needs to rebo for the software update to take effect. *Also available in Version 7.0(7) and 8.0(3)*
ASDM Features	

Feature	Description
ASDM banner enhancement	The adaptive security appliance software supports an ASDM banner. If configured, whe ASDM, this banner text will appear in a dialog box with the option to continue or disco Continue option dismisses the banner and completes login as usual whereas, the Disconn dismisses the banner and terminates the connection. This enhancement requires the cust accept the terms of a written policy before connecting. Following is the new CLI associated with this enhancement: **banner** {**exec** | **login** | **motd** | **asdm**} *text* **show banner** [**exec** | **login** | **motd** | **asdm**] **clear banner** In ASDM, see **Configuration > Properties > Device Administration > Banner**. *Also available in Version 8.0(3).*
Cisco Content Security and Control (CSC) Damage Cleanup Services (DCS) feature events and statistics	With the Cisco Content Security and Control (CSC) 6.2 software, ASDM provides even statistics for the new Damage Cleanup Services (DCS) feature. DCS removes malware fr and servers and repairs system registries and memory.
Client Software Location	Added support in Client Software Location list to allow client updates from Linux or Ma In ASDM, see **Configuration > Remote Access VPN > Network (Client) Access > Ac IPSec > Upload Software > Client Software**. *Also available in Version 8.0(3).*

New Features in ASA 7.2(2)/ASDM 5.2(2)

Released: November 22, 2006

Feature	Description
Module Features	
Password reset on SSMs	You can reset the password on the AIP-SSM and CSC-SSM of user 'cisco' back to the de 'cisco'. We added the following command: **hw-module module password-reset**.
AAA Features	

Feature	Description
HTTP(S) authentication challenge flexible configuration	The new **aaa authentication listener** command enables the ASA to authenticate we select the form-based redirection approach that is currently used in Version 7.2(1). 7.2(2) reintroduces the choice to use basic HTTP authentication that was available b Basic HTTP and HTTPS authentication generates custom login windows. You can us authentication if: • You do not want the adaptive security appliance to open listening ports • You use NAT on a router and you do not want to create a translation rule for the served by the adaptive security appliance • Basic HTTP authentication might work better with your network. For example applications, like when a URL is embedded in email, might be more compatible authentication. **Note** By default the the **aaa authentication listener** command is not pre configuration, making Version 7.1 aaa behavior the default for 7.2(when a Version 7.2(1) configuration is upgraded to Version 7.2(2), th **aaa authentication listener** commands are added to the configurati **aaa** behavior will not be changed by the upgrade. To support basic HTTP, the **virtual http** command was restored. This is needed with authentication when you have cascading authentication requests. In Version 7.2(1), basic authentication was replaced by a form based authentication ap HTTP and HTTPS connections are redirected to authentication pages that are served f After successful authentication, the browser is again redirected to the originally-intend was done to provide: • More graceful support authentication challenge processing • An identical authentication experience for http and https users A persistent logon/logoff URL for network users This approach does require listenin opened on the ASA on each interface on which **aaa authentication** was enabled.
Interface Features	
Maximum number of VLANs increased	The maximum number of VLANs for the Security Plus license on the ASA 5505 ada appliance was increased from 5 (3 fully functional; 1 failover; one restricted to a bac to 20 fully functional interfaces. In addition, the number of trunk ports was increased Now there are 20 fully functional interfaces, you do not need to use the **backup interf** to cripple a backup ISP interface; you can use a fully-functional interface for it. The ba command is still useful for an Easy VPN configuration. VLAN limits were also increased for the ASA 5510 adaptive security appliance (fro the Base license, and from 25 to 100 for the Security Plus license), the ASA 5520 ada appliance (from 100 to 150), the ASA 5550 adaptive security appliance (from 200 to
Increased physical interfaces on the ASA 5510 base license	On the ASA Model 5510, the maximum number of physical interfaces available has from 3+1 to unlimited (5).
Certification Features	

Feature	Description
FIPS 140-2	7.2(2) has been submitted for FIPS 140 Level 2 validation.
ASDM Features	
Multicast support	Support for the following multicast commands has been added: • **mfib forwarding** • **multicast boundary** • **pim bidir-neighbor-filter** • **pim neighbor-filter** • **pim old-register-checksum**
Local demo mode	ASDM works when it is connected to a device in a local demo mode.

New Features in ASA 7.2(1)/ASDM 5.2(1)

Released: May 31, 2006

Feature	Description
Platform Features	
ASA 5505 support	The ASA 5505 was introduced in this release. The ASA 5505 is a new model for small of office, enterprise teleworker environments, includes a built-in 8-port Fast Ethernet switc supports Easy VPN, Dual ISP, and has many more features The ASA 5505 has Power over Ethernet (PoE) switch ports that can be used for PoE dev as IP phones. However, these ports are not restricted to that use. They can also be used a switch ports. If a PoE device is not attached, power is not supplied to the port.
ASA 5550 support	The ASA 5550 delivers gigabit-class security services and enables Active/Active high a for large enterprise and service-provider networks in a reliable, 1RU form-factor. Providi connectivity in the form of both Ethernet- and Fiber-based interfaces with high-density V integration, the ASA 5550 enables businesses to segment their networks into numerous high-performance zones for improved security.
Easy VPN Features (ASA 5505 Only)	
Client Mode (also called Port Address Translation) and Network Extension Mode	• Client Mode—Hides the IP addresses of devices on the ASA 5505 private network, traffic from the ASA 5505 private network arrives on the private network of the cer ASA with a single-source, assigned IP address. You cannot ping or access a device o 5505 private network from the central site, but you can access the assigned IP addr • Network Extension Mode—Permits devices behind the ASA to have direct access t on the ASA 5505 private network only through the tunnel. You can ping or access a the ASA 5505 network from the central site. The ASA 5505 does not have a default mode; you must specify the one that you want to

Feature	Description
Automatic Tunnel Initiation	Supports NEM, but not Client Mode. It uses a group name, username, and password configuration to initiate the tunnel.
IKE and IPsec Support	The ASA 5505 supports preshared keys and certificates (RSA-SIG). The ASA uses IK Mode for preshared keys and IKE Main Mode for RSA-SIG based key exchange. Cis can initiate IPsec, IPsec over NAT-T, and IPsec over cTCP sessions.
Secure Unit Authentication (SUA)	Supports the ASA 5505 authentication with dynamically generated authentication cr with static credentials to be entered at tunnel initiation. With SUA enabled, the user m trigger the IKE tunnel using a browser or an interactive CLI.
Individual User Authentication (IUA)	Enables static and one-time password authentication of individual clients on the insid IUA and SUA are independent of each other; they work in combination or isolation fr
Token-Based Authentication	Supports Security Dynamics (SDI) SecurID one-time passwords.
Authentication by HTTP Redirection	Redirects unauthenticated HTTP traffic to a login page if SUA or a username and pas configured or if IUA is disabled.
Load Balancing	An ASA 5505 configured with dual ISP backup supports cluster-based VPN load ba the two Ethernet ports available in the Internet zone. The load-balancing scheme invo director" IP address that is the destination of incoming client connections. The serve virtual director IP address form a cluster, where one cluster member acts as the clust master receives a request sent to the virtual director and redirects the client, using a pr notify message, to the optimal server in the cluster. The current ISAKMP session ter new session is attempted to the optimal server. If the connection to the optimal server fails, the client reconnects to the primary server director IP address of the cluster) and repeats the load-balancing procedure. If the con primary server fails, the client rolls over to the next configured backup server, which master of another cluster.
Failover (using Backup Server List)	You can configure a list of 10 backup servers in addition to the primary server. The A attempts to establish a tunnel with the primary server. If that attempt fails, the ASA 5 to establish a tunnel with other specified servers in the backup server list in sequence
Device Pass-Through	Encompasses both IP Phone Pass Through and LEAP Pass Through features. Certain devices, such as printers and Cisco IP phones, are incapable of performing au so they cannot participate in IUA. With device pass-through enabled, the ASA 5505 devices from authentication if IAU is enabled. The Easy VPN Remote feature identifies the devices to exempt, based on a configure addresses. A related issue exists with wireless devices such as wireless access points nodes. These devices require LEAP/PEAP authentication to let wireless nodes partic network. It is only after the LEAP/PEAP authentication stage that the wireless nodes IUA. The ASA 5505 also bypasses LEAP/PEAP packets when you enable Device Pa so that the wireless nodes can participate in IUA.
IKE Mode Configuration	You can set the attribute values that the ASA 5505 requests after IKE Phase I and XA device at the central site downloads the VPN policy and the ASA 5505 dynamically c features based on the security values. Except for SUA, the Clear Save password, and concentrator list, the dynamic feature configuration lasts only while the tunnel is up.

Feature	Description
Remote Management	Supports management of the ASA 5505 over the tunnel to the outside interface with NEM c and in the clear to the outside interface.
DNS Resolution of Easy VPN Peer Names	The ASA 5505 resolves the Easy VPN peer names with the DNS server. You can specify name of the server/client in the CLI.
Split tunneling	Allows the client decide which traffic to send over the tunnel, based on a configured list o accessible by tunneling to the central site. Traffic destined to a network other than those the split tunnel network list is sent out in the clear. A zero-length list indicates no split tu and all traffic travels over the tunnel.
Push Banner	Allows you to configure a 491-byte banner message to display in HTTP form to individu who try to authenticate using IUA.
Application Inspection Features	
Enhanced ESMTP Inspection	This feature allows you to detect attacks, including spam, phising, malformed message at buffer overflow and underflow attacks. It also provides support for application security an conformance, which enforce the sanity of the ESMTP messages as well as detects severa blocks senders and receivers, and blocks mail relay.
DCERPC Inspection	This feature allows you to change the default configuration values used for DCERPC ap inspection using a DCERPC inspect map. DCERPC is a protocol used by Microsoft distributed client and server applications that a software clients to execute programs on a server remotely. Typically, a client queries a server called the Endpoint Mapper (EPM) that listens on a w port number for the dynamically allocated network information of a required service. Th then sets up a secondary connection to the server instance that provides the service. The appliance allows the appropriate port number and network address and also applies NAT if needed, for the secondary connection.
Enhanced NetBIOS Inspection	This feature allows you to change the default configuration values used for NetBIOS app inspection. NetBIOS application inspection performs NAT for the embedded IP address in the NetB service packets and NetBIOS datagram services packets. It also enforces protocol confo checking the various count and length fields for consistency.
Enhanced H.323 Inspection	This feature allows you to change the default configuration values used for H.323 applic inspection. H.323 inspection supports RAS, H.225, and H.245, and its functionality translates all em addresses and ports. It performs state tracking and filtering and can do a cascade of inspec activation. H.323 inspection supports phone number filtering, dynamic T.120 control, H.245 control, protocol state tracking, H.323 call duration enforcement, and audio and video co
Enhanced DNS Inspection	This feature allows you to specify actions when a message violates a parameter that uses inspection policy map. DNS application inspection supports DNS message controls that protection against DNS spoofing and cache poisoning. User configurable rules allow filte on the DNS header, domain name, and resource record TYPE and CLASS.

Feature	Description
Enhanced FTP Inspection	This feature allows you to change the default configuration values used for FTP applicat FTP command filtering and security checks are provided using strict FTP inspection security and control. Protocol conformance includes packet length checks, delimiters format checks, command terminator checks, and command validation. Blocking FTP based on user values is also supported so that it is possible for FTP sit for download but restrict access to certain users. You can block FTP connections base server name, and other attributes. System message logs are generated if an FTP connec after inspection.
Enhanced HTTP Inspection	This feature allows you to change the default configuration values used for HTTP ap inspection. HTTP application inspection scans HTTP headers and body and performs various ch data. These checks prevent various HTTP constructs, content types, and tunneling ar protocols from traversing the security appliance. HTTP application inspection can block tunneled applications and non-ASCII charact requests and responses, preventing malicious content from reaching the web server. S of various elements in HTTP request and response headers, URL blocking, and HTTP type spoofing are also supported.
Enhanced Skinny (SCCP) Inspection	This feature allows you to change the default configuration values used for SCCP (Skinn inspection. Skinny application inspection performs translation of embedded IP address and port nu the packet data and dynamic opening of pinholes. It also performs additional protocol checks and basic state tracking.
Enhanced SIP Inspection	This feature allows you to change the default configuration values used for SIP applicati SIP is a widely used protocol for Internet conferencing, telephony, events notificatio messaging. Partially because of its text-based nature and partially because of its flexi networks are subject to a large number of security threats. SIP application inspection provides address translation in the message header and bo opening of ports, and basic sanity checks. It also supports application security and pr conformance, which enforces the sanity of the SIP messages, as well as detects SIP-b
Instant Messaging (IM) Inspection	This feature allows you to change the default configuration values used for Instant M application inspection. Instant Messaging (IM) application inspection provides detailed access control to co usage. It also helps stop leakage of confidential data and propagations of network thre expression database search that represents various patterns for Instant Messaging (IM be filtered is applied. A syslog is generated if the flow is not recognized. The scope can be limited by using an access list to specify any traffic streams to be i UDP messages, a corresponding UDP port number is also configurable. Inspection o Messenger and MSN Messenger instant messages are supported.

Feature	Description
MPF-Based Regular Expression Classification Map	This feature allows you to define regular expressions in Modular Policy Framework class match a group of regular expressions that has the **match-any** attribute. You can use a reg expression class map to match the content of certain traffic; for example, you can match U inside HTTP packets.
Radius Accounting Inspection	This feature allows you to protect against an over-billing attack in the Mobile Billing Infr The **policy-map type inspect radius-accounting** command was introduced in this versi
GKRCS Support for H.323	Two control signaling methods are described in the ITU-T H.323 recommendation: Gate Routed Control Signaling (GKRCS) and Direct Call Signalling (DCS). DCS is supporte Cisco IOS gatekeeper. This feature adds Gatekeeper Routed Control Signaling (GKRCS signaling method support.
Skinny Video Support	This feature adds SCCP version 4.1.2 message support to print the message name proces inspect feature when **debug skinny** is enabled. CCM 4.0.1 messages are supported.
SIP IP Address Privacy	This feature allows you to retain the outside IP addresses embedded in inbound SIP pack transactions, except REGISTER (because it is exchanged between the proxy and the phon the real IP address of the phone. The REGISTER message and the response to REGISTE will be exempt from this operation because this message is exchanged between the phon proxy. When this feature is enabled, the outside IP addresses in the SIP header and SDP data of SIP packets will be retained. Use the **ip-address-privacy** command to turn on this featu
RTP/RTCP Inspection	This feature NATs embedded IP addresses and opens pinholes for RTP and RTCP traffic feature ensures that only RTP packets flow on the pinholes opened by Inspects SIP, Skin H.323. To prevent a malicious application from sending UDP traffic to make use of the p created on the ASA, this feature allows you to monitor RTP and RTCP traffic and to enf validity of RTP and RTCP packets.
Remote Access and Site-to-Site VPN Features	

Feature	Description
Network Admission Control	Network Admission Control (NAC) allows you to validate a peer based on its state. T referred to as posture validation (PV). PV can include verifying that the peer is runnin with the latest patches, and ensuring that the antivirus files, personal firewall rules, o protection software that runs on the remote host are up to date. An Access Control Server (ACS) must be configured for Network Admission Contro configure NAC on the ASA. As a NAC authenticator, the ASA does the following: • Initiates the initial exchange of credentials based on IPsec session establishmen exchanges thereafter. • Relays credential requests and responses between the peer and the ACS. • Enforces the network access policy for an IPsec session based on results from th • Supports a local exception list based on the peer operating system, and optional • (Optional) Requests access policies from the ACS server for a clientless host. As an ACS client, the ASA supports the following: • EAP/RADIUS • RADIUS attributes required for NAC NAC on the ASA differs from NAC on Cisco IOS Layer 3 devices (such as routers) trigger PV based on routed traffic. The ASA enabled with NAC uses an IPsec VPN s trigger for PV. Cisco IOS routers configured with NAC use an Intercept ACL to trigg on traffic destined for certain networks. Because external devices cannot access the ne the ASA without starting a VPN session, the ASA does not need an intercept ACL as During PV, all IPsec traffic from the peer is subject to the default ACL configured fo group. Unlike the Cisco VPN 3000 Concentrator Series, NAC on the ASA supports stateles initialization of all NAC sessions in a tunnel group, revalidation of all NAC sessions group, and posture validation exemption lists configured for each tunnel group. NAC does not support non-VPN traffic, IPv6, security contexts, and WebVPN. By default, NAC is disabled. You can enable it on a group policy basis.

Feature	Description
L2TP Over IPsec	Layer 2 Tunneling Protocol (L2TP) is a VPN tunneling protocol that allows remote clien the public IP network to communicate securely with private corporate network servers. I PPP over UDP (port 1701) to tunnel the data. L2TP is based on the client/server model. Th is divided between the L2TP Network Server (LNS), and the L2TP Access Concentrator The LNS typically runs on a network gateway such as a router, while the LAC can be a Network Access Server (NAS), or a PC with a bundled L2TP client such as Microsoft W 2000. L2TP/IPsec provides the capability to deploy and administer an L2TP VPN solution alo IPsec VPN and firewall services in a single platform. The primary benefit of configuring L2TP with IPsec in a remote access scenario is that re can access a VPN over a public IP network without a gateway or a dedicated line, enabli access from virtually anyplace with POTS. An additional benefit is that the only client re for VPN access is the use of Windows 2000 with Microsoft Dial-Up Networking (DUN additional client software, such as Cisco VPN client software, is required.
OCSP Support	The Online Certificate Status Protocol (OCSP) provides an alternative to CRL for obtain revocation status of X.509 digital certificates. Rather than requiring a client to download a and often large certificate revocation list, OCSP localizes the certificate status on a Valid Authority, which it queries for the status of a specific certificate.
Multiple L2TP Over IPsec Clients Behind NAT	The security appliance can successfully establish remote-access L2TP-over-IPsec conne more than one client behind one or more NAT devices. This enhances the reliability of L IPsec connections in typical SOHO/branch office environment environments, where mult over IPsec clients must communicate securely with a central office.
Nokia Mobile Authentication Support	You can establish a VPN using a handheld Nokia 92xx Communicator series cellular de remote access. The authentication protocol that these devices use is the IKE Challenge/R for Authenticated Cryptographic Keys (CRACK) protocol.
Zonelabs Integrity Server	You can configure the ASA in a network that deploys the Zone Labs Integrity System to security policies on remote VPN clients. In this case, the ASA is an edge gateway betwee Labs Integrity server and the remote clients. The Zone Labs Integrity server and the Zon Personal Firewall on the remote client ensure that a remote client complies with a centrally security policy before the client can access private network resources. You configure the pass security policy information between the server and clients to maintain or close client co to prevent a server connection failure, and to optionally, require SSL certificate authenti both the Integrity server and the ASA.
Hybrid XAUTH	You can configure hybrid authentication to enhance the IKE security between the ASA a users. With this feature, IKE Phase I requires two steps. The ASA first authenticates to t VPN user with standard public key techniques and establishes an IKE security associatio unidirectionally authenticated. An XAUTH exchange then authenticates the remote VPN extended authentication can use any one of the supported authentication methods. Hybri allows you to use digital certificates for ASA authentication and a different method for re user authentication, such as RADIUS, TACACS+ or SecurID.
IPsec Fragmentation and Reassembly Statistics	You can monitor additional IPsec fragmentation and reassembly statistics that help to de IPsec-related fragmentation and reassembly issues. The new statistics provide informatio fragmentation and reassembly both before and after IPsec processing.

Feature	Description
Inspection IPS, CSC and URL Filtering for WebVPN	This feature adds support for inspection, IPS, and Trend Micro for WebVPN traffic i mode and port forwarding mode. Support for SVC mode is preexisting. In all of the Trend Micro and the IPS engines will be triggered (if configured). URL/FTP/HTTPS/Java/Activex filtering using WebSense and N2H2 support has also DNS inspect will be triggered for the DNS requests. In port forwarding mode, HTTP, SMTP, FTP, and DNS inspections with the filtering using WebSense and N2H2 support has been added.
Routing Features	
Active RIP Support	The ASA supports RIP Version 1 and RIP Version 2. You can only enable one RIP ro on the ASA. When you enable the RIP routing process, RIP is enabled on all interface the security appliance sends RIP Version 1 updates and accepts RIP Version 1 and Vers To specify the version of RIP accepted on an interface, use the **rip receive version** c interface configuration mode.
Standby ISP Support	This feature allows you to configure a link standby ISP if the link to your primary IS static routing and object tracking to determine the availability of the primary route an the secondary route when the primary route fails.
PPPoE Client	Point-to-Point Protocol over Ethernet (PPPoE) combines two widely accepted standa and PPP, to provide an authenticated method of assigning IP addresses to client syste clients are typically personal computers connected to an ISP over a remote broadban such as DSL or cable service. ISPs deploy PPPoE because it supports high-speed broa using their existing remote access infrastructure and because it is easier for customer
Dynamic DNS Support	You can create dynamic DNS (DDNS) update methods and configure them to update Records (RRs) on the DNS server at whatever frequency you need. DDNS complements DHCP, which enables users to dynamically and transparently as IP addresses to clients. DDNS then provides dynamic updating and synchronizing of the address and the address to the name mappings on the DNS server. With this versi supports the IETF standard for DNS record updates.
Static Route Tracking	The static route tracking feature provides a method for tracking the availability of a st installing a backup route if the primary route should fail. We introduced the following commands: **clear configure sla, frequency, num-pack request-data-size, show sla monitor, show running-config sla, sla monitor, sla mon threshold, timeout, tos, track rtr** We introduced or modified the following screens: **Configuration > Device Setup > Routing > Static Routes > Add Static Route Co Device Setup > Routing > Static Routes > Add Static Route > Route Monitoring**
Multicast Routing Enhancements	Multicast routing enhancements allows you to define multicast boundaries so that do RPs that have the same IP address do not leak into each other, to filter PIM neighbor control the PIM process, and to filter PIM bidir neighbors to support mixed bidirecti sparse-mode networks.

Feature	Description
Expanded DNS Domain Name Usage	You can use DNS domain names, such as www.example.com, when configuring AAA s also with the **ping**, **traceroute**, and **copy** commands.
Intra-Interface Communication for Clear Traffic	You can now allow any traffic to enter and exit the same interface, and not just VPN traf
IPv6 Security Enforcement of IPv6 Addresses	This feature allows you to configure the security appliance to require that IPv6 addresses f connected hosts use the Modified EUI-64 format for the interface identifier portion of th
Multiple Context Mode Features	
Private and Automatic MAC Address Assignments and Generation for Multiple Context Mode	You can assign a private MAC address (both active and standby for failover) for each inte multiple context mode, you can automatically generate unique MAC addresses for share interfaces, which makes classifying packets into contexts more reliable. The new **mac-address auto** command allows you to automatically assign private MAC to each shared context interface.
Resource Management for Security Contexts	If you find that one or more contexts use too many resources, and they cause other conte denied connections, for example, then you can configure resource management to limit t resources per context.
Save All Context Configurations from the System	You can now save all context configurations at once from the system execution space us **write memory all** command.
High Availability Features	
Sub-second Failover	This feature allows you to configure failover to detect and respond to failures in under a
Configurable Prompt	With this feature, the user can see the failover status of the security appliance without ha enter the **show failover** command and parse the output. This feature allows users to see t slot number of the failover unit. Previously, the prompt reflected just the hostname, securi and configuration mode. The prompt command provides support for this feature.
Firewall Features	
Generic Input Rate Limiting	This feature prevents denial of service (DoS) attacks on a ASA or on certain inspection e a firewall. The 7.0 release supports egress rate-limiting (police) functionality and in this input rate-limiting functionality extends the current egress policing functionality. The **police** command is extended for this functionality.
Authentication for Through Traffic and Management Access Supports All Servers Previously Supported for VPN Clients	All server types can be used for firewall authentication with the following exceptions: H protocol supports single sign-on authentication for WebVPN users only and SDI is not s for HTTP administrative access.

Feature	Description
Dead Connection Detection (DCD)	This feature allows the adaptive security appliance to automatically detect and expire connections. In previous versions, dead connections never timed out; they were give timeout. Manual intervention was required to ensure that the number of dead connec overwhelm the security appliance. With this feature, dead connections are detected a automatically, without interfering with connections that can still handle traffic. The s timeout and show service-policy commands provide DCD support.
WCCP	The Web Cache Communication Protocol (WCCP) feature allows you to specify WC groups and redirect web cache traffic. The feature transparently redirects selected typ a group of web cache engines to optimize resource usage and lower response times.
Filtering Features	
URL Filtering Enhancements for Secure Computing (N2H2)	This feature allows you to enable long URL, HTTPS, and FTP filtering by using both (the current vendor) and N2H2 (a vendor that has been purchased by Secure Computing the code only enabled the vendor Websense to provide this type of filtering. The url-blo and filter commands provide support for this feature.
Management and Troubleshooting Features	
Auto Update	The security appliance can now be configured as an Auto Update server in addition t configured as an Auto Update client. The existing client-update command (which is update VPN clients) is enhanced to support the new Auto Update server functionality new keywords and arguments that the security appliance needs to update security app configured as clients. For the security appliance configured as an Auto Update client, th command continues to be the command used to configure the parameters that the secu needs to communicate with the Auto Update server.
Modular Policy Framework Support for Management Traffic	You can now define a Layer 3/4 class map for to-the-security-appliance traffic, so yo special actions on management traffic. For this version, you can inspect RADIUS acco
Traceroute	The **traceroute** command allows you to trace the route of a packet to its destination.
Packet Tracer	The packet tracer tool allows you to trace the life span of a packet through the ASA t behaving as expected. The **packet-tracer** command provides detailed information about the packets and ho processed by the security appliance. If a command from the configuration did not ca to drop, the **packet-tracer** command will provide information about the cause. The new patent-pending Packet Tracer tool in ASDM lets you easily trace the life sp through the ASA in an animated packet flow model to see if it is behaving as expected troubleshooting no matter how complex the network design. The tool provides the at packet such as source and destination IP addresses with a visual representation of the di of the packet and the relevant configuration, which is accessible with a single click. F it displays whether the packet is dropped or allowed.
ASDM Features	

Feature	Description
Enhanced ASDM rules table	The ASDM rule tables have been redesigned to streamline policy creation. In addition to rule creation that maps more closely with CLI, the rule tables support most configuration including super-netting and using an object group that is associated to more than interfac of ASDM location and ASDM group was removed to simplify the creation of rules. You the ability to: • Create objects, object-groups and rules from a single panel • Filter on interfaces, source, destination or services • Policy query in the rule tbale for advanced filtering using multiple conditions • Show logs for a particular access rule in the real time log viewer • Select a rule and packet trace with a single click which will populate with appropria attributes • Easily organize and move up and down in the table to change the order of access lis • Expand and display elements in an object group • See attributes of a object or memebers of a group via tooltips
High Availability and Scalability Wizard	The High Availability and Scalability Wizard is used to simplify configuration of Active Active/Standy failover and VPN Load balancing. The wizard also intelligently configure device.
Syslog enhancements	Enhancements to the syslog features include: • Syslog parsing to display source IP, destination IP, syslog ID, date and time into dif columns • Integrated syslog references with explanations and recommended actionss for each s a single click • Syslog coloring based on severity level • A brief explanation of the syslogs as a tool tip in the log viewer
NAT rules	The creation of NAT rules is simplified.
Object group support	There is now full ASDM support of network, service, protocol and ICMP-type object gr
Named IP addresses	The ability to create a name to be associated with an IP Address now exists.
ASDM Assistant	The new ASDM Assistant provides task-oriented guidance to configuring features such server, logging filters, SSL VPN Client, and others features. You can also upload new gu
Context management	Context management is improved, including context caching and better scalability.
Inspection maps	Predefined low, medium and high security settings simplify creation and management of maps.

New Features in Version 7.1

New Features in ASA 7.1(2)/ASDM 5.1(2)

Released: March 15, 2006

There were no new features in ASA 7.1(2)/ASDM 5.1(2)

New Features in ASA 7.1(1)/ASDM 5.1(1)

Released: February 6, 2006

Feature	Description
Platform Features	

Feature	Description
Support for the Content Security and Control (CSC) SSM	The CSC SSM, an integral part of Cisco's Anti-X solution, delivers industry-leading threat and content control at the Internet edge providing comprehensive antivirus, anti-spyware blocking, anti-spam, anti-phising, URL blocking and filtering, and content filtering servi CSC SSM services module helps businesses more effectively protect their networks, increas availability, and increase employee productivity through the following key elements: • Antivirus—Market leading antivirus, from Trend Micro, shields your internal network from both known and unknown virus attacks, at the most effective point in your infra the Internet gateway. By cleaning your email and web traffic at the perimeter, it elim need for resource intensive malware infection clean-ups and ensures business conti • Anti-Spyware—Blocks spyware from entering your network through web traffic (H FTP) and email traffic. Frees-up IT support resources from costly spyware removal p and improves employee productivity by blocking spyware at the gateway. • Anti-Spam—Effective blocking of spam with very low false positives helps to resto effectiveness of your email communications, so contact with customers, vendors, an continues uninterrupted. • Anti-Phishing—Identity theft protection guards against phishing attacks thereby pr employees inadvertently disclosing company or personal details which could lead to loss. • Automatic Updates from TrendLabs—The solution is backed and supported by one largest teams of virus, spyware and spam experts in the industry working 24x7 to en your solution is providing the most up to date protection – automatically. • Central Administration—Easy, set-and-forget administration through a remotely ac web-console and automated updates reduces IT support costs. • Real-time protection for Web access, Mail (SMTP & POP3) and FTP (file transfer) the company mail is already protected, many employees will access their own private from their company PCs or laptops introducing yet another entry point for internet bor Similarly, employees may directly download programs of files which may be simila contaminated. Real-time protection of all web traffic at the internet gateway greatly this often over-looked point of vulnerability. • Full URL filtering capability with categories, scheduling and cache—URL filtering c to control employee internet usage by blocking access to inappropriate or non-work websites improving employee productivity and limiting the risk of legal action bein employees exposed to offensive web content. • Email Content Filtering—Email filtering minimizes legal liability for offensive mat transferred by email and enforces regulatory compliance, helping organizations me requirements of legislation such as GLB and the Data Protection Act.
General VPN Features	

Feature	Description
Cisco Secure Desktop	Cisco Secure Desktop (CSD) is an optional Windows software package you can insta to validate the security of client computers requesting access to your SSL VPN, ensu secure while they are connected, and remove all traces of the session after they disco After a remote PC running Microsoft Windows connects to the ASA, CSD installs it the IP address and presence of specific files, registry keys, and certificates to identify location from which the PC is connecting. Following user authentication, CSD uses op as conditions for granting access rights. These criteria include the operating system, anti antispyware, and personal firewall running on the PC. To ensure security while a PC is connected to your network, the Secure Desktop, a CS that runs on Microsoft Windows XP and Windows 2000 clients, limits the operations the user during the session. For remote users with administrator privileges, Secure De 168-bit Triple Data Encryption Standard (3DES) to encrypt the data and files associa downloaded during an SSL VPN session. For remote users with lesser privileges, it u Cipher 4 (RC4) encryption algorithm. When the session closes, Secure Desktop over removes all data from the remote PC using the U.S. Department of Defense (DoD) sec for securely deleting files. This cleanup ensures that cookies, browser history, tempo downloaded content do not remain after a remote user logs out or an SSL VPN sessi CSD also uninstalls itself from the client PC. Cache Cleaner, which wipes out the client cache when the session ends, supports Wi Windows 2000, Windows 9x, Linux, and Apple Macintosh OS X clients.
Customized Access Control Based on CSD Host Checking	Adaptive security appliances with Cisco Secure Desktop installed can specify an alte policy. The ASA uses this attribute to limit access rights to remote CSD clients as fo • Always use it if you set the VPN feature policy to “Use Failure Group-Policy.” • Use it if you set the VPN feature policy to “Use Success Group-Policy, if criteri the criteria then fail to match. This attribute specifies the name of the alternative group policy to apply. Choose a g differentiate access rights from those associated with the default group policy. The d DfltGrpPolicy. **Note** The ASA does not use this attribute if you set the VPN feature policy to Success Group-Policy.”
SSL VPN Client	SSL VPN client is a VPN tunneling technology that gives remote users the connectiv an IPSec VPN client without the need for network administrators to install and confi VPN clients on remote computers. SVC uses the SSL encryption that is already present computer as well as the WebVPN login and authentication of the ASA. To establish an SVC session, the remote user enters the IP address of a WebVPN inte ASA in the browser, and the browser connects to that interface and displays the Web screen. If the user satisfies the login and authentication, and the ASA identifies the use the SVC, the ASA downloads the SVC to the remote computer. If the ASA identifies having the *option* to use the SVC, the ASA downloads the SVC to the remote compu presenting a link on the user screen to skip the SVC installation. After downloading, the SVC installs and configures itself, When the connection term either remains or uninstalls itself (depending on the configuration) from the remote c

Feature	Description
WebVPN Functions and Performance Optimizations	This version enhances WebVPN performance and functions through the following comp • Flexible content transformation/rewriting that includes complex JavaScript, VBScrip • Server-side and browser caching • Compression • Proxy bypass • Application Profile Customization Framework support • Application keep-alive and timeout handling • Support for logical (VLAN) interfaces
Citrix Support for WebVPN	WebVPN users can now use a connection to the ASA to access Citrix MetaFrame servic configuration, the ASA functions as the Citrix secure gateway. Therefore you must conf Citrix Web Interface software to operate in a mode that does not use the Citrix secure ga Install an SSL certificate onto the ASA interface to which remote users use a fully qualifi name (FQDN) to connect; this function does not work if you specify an IP address as th name (CN) for the SSL certificate. The remote user attempts to use the FQDN to commun the ASA. The remote PC must be able to use DNS or an entry in the System32\drivers\etc to resolve the FQDN. Finally, use the **functions** command to enable Citrix.
PDA Support for WebVPN	You can access WebVPN from your Pocket PC 2003 or Windows Mobile X. If you are a this makes accessing your private network more convenient. This feature requires no con
WebVPN Support of Character Encoding for CIFS Files	WebVPN now supports optional character encoding of portal pages to ensure proper ren Common Internet File System files in the intended language. The character encoding su character sets identified on the following Web page, including Japanese Shift-JIS charac http://www.iana.org/assignments/character-sets Use the **character-encoding** command to specify the character set to encode in WebVPI pages to be delivered to remote users. By default, the encoding type set on the remote br determines the character set for WebVPN portal pages. The character-encoding attribute is a global setting that, by default, all WebVPN portal pag However, you can use the **file-encoding** command to specify the encoding for WebVPN pages from specific CIFS servers. Thus, you can use different file-encoding values for CI that require different character encodings. The mapping of CIFS servers to their appropriate character encoding, globally with the character-encoding attribute, and individually with file-encoding overrides, provides for th handling and display of CIFS pages when the proper rendering of file names or directory well as pages, are an issue. **Tip** The character-encoding and file-encoding values do not exclude the font fa used by the browser. You need to complement the setting of one these value **page style** command in webvpn customization command mode to replace th family if you are using Japanese Shift_JIS character encoding, or enter the **n style** command in webvpn customization command mode to remove the for

Feature	Description
Compression for WebVPN and SSL VPN Client Connections	Compression can reduce the size of the transferring packets and increase the commu performance, especially for connections with bandwidth limitations, such as with dia and handheld devices used for remote access. Compression is enabled by default, for both WebVPN and SVC connections. You ca compression using ASDM or CLI commands. You can disable compression for all WebVPN or SVC connections with the **compress** from global configuration mode. You can disable compression for a specific group or user for WebVPN connections with command, or for SVC connections with the **svc compression** command, in the group username webvpn modes.
Active/Standby Stateful Failover for WebVPN and SVC Connections	During a failover, WebVPN and SVC connections, as well as IPSec connections, are with the secondary, standby security appliance for uninterrupted service. Active/stan requires a one-to-one active/standby match for each connection. A security appliance configured for failover shares authentication information about W with the standby security appliance. Therefore, after a failover, WebVPN users do no reauthenticate. For SVC connections, after a failover, the SVC reconnects automatically with the sta appliance.
WebVPN Customization	You can customize the WebVPN page that users see when they connect to the securit and you can customize the WebVPN home page on a per-user, per-group, or per-tunne Users or groups see the custom WebVPN home page after the security appliance authe You can use Cascading Style Sheet (CSS) parameters. To easily customize, we recom use ASDM, which has convenient features for configuring style elements, including c and preview capabilities.
Auto Applet Download	To run a remote application over WebVPN, a user clicks Start Application Access on homepage to download and start a port-forwarding Java applet. To simplify applicati shorten start time, you can now configure WebVPN to automatically download this po applet when the user first logs in to WebVPN.
Authentication and Authorization VPN Features	
Override Account Disabled	You can configure the ASA to override an account-disabled indication from a AAA se the user to log on anyway. We introduced the following command: **override account disabled.**
LDAP Support	You can configure the security appliance to authenticate and authorize IPSec VPN us clients, and WebVPN users to an LDAP directory server. During authentication, the secu acts as a client proxy to the LDAP server for the VPN user, and authenticates to the L in either plain text or using the Simple Authentication and Security Layer (SASL) pr security appliance supports any LDAP V3 or V2 compliant directory server. It suppo management features only on the Sun Microsystems Java System Directory Server and Active Directory server.

Feature	Description
Password Management	You can configure the ASA to warn end users when their passwords are about to expire. configure this feature, the ASA notifies the remote user at login that the current passwor to expire or has expired. The ASA then offers the user the opportunity to change the pas the current password has not yet expired, the user can still log in using that password. This is valid for AAA servers that support such notification; that is, RADIUS, RADIUS with server, and LDAP servers. The ASA ignores this command if RADIUS or LDAP authenti not been configured. Note that this command does not change the number of days before the password expires, specifies the number of days before expiration that the ASA starts warning the user that the is about to expire. The default value is 14 days. For LDAP server authentication only, you can specify a specific number of days before to begin warning the user about the pending expiration. We introduced the following command: **password management**.
Single sign-on (SSO)	Single sign-on (SSO) support lets WebVPN users enter a username and password only onc multiple protected services and web servers. You can choose among the following metho configure SSO: • Computer Associates eTrust SiteMinder SSO server (formerly Netegrity SiteMinde typically would choose to implement SSO with SiteMinder if your Web site securit infrastructure already incorporates SiteMinder. • HTTP Forms—A common and standard approach to SSO authentication that can al as a AAA method. You can use it with other AAA servers such as RADIUS or LDA • SSO with Basic HTTP and NTLM Authentication—The simplest of the three SSO passes WebVPN login credentials for authentication through to internal servers usin HTTP or NTLM authentication. This method does not require an external SSO serv
Tunnel Group and Group Policy VPN Features	
WebVPN Tunnel Group Type	This version adds a WebVPN tunnel group, which lets you configure a tunnel group with WebVPN-specific attributes, including the authentication method to use, the WebVPN cust to apply to the user GUI, the DNS group to use, alternative group names (aliases), group NBNS server to use for CIFS name resolution, and an alternative group policy to apply to to limit access rights to remote CSD clients.
Group-Based DNS Configuration for WebVPN	You can define a list of DNS servers under a group. The list of DNS servers available to depends on the group that the user is assigned to. You can specify the DNS server to use WebVPN tunnel group. The default value is DefaultDNS.
New Login Page Option for WebVPN Users	You can optionally configure WebVPN to display a user login page that offers the user the o to select the tunnel group to use for login. If you configure this option, the login page dis additional field offering a drop-down menu of groups from which to select. The user is aut against the selected group.

Feature	Description
Group Alias and Group URL	You can create one or more alternate names by which the user can refer to a tunnel g specifying one or more group aliases. The group aliases that you specify here appear in t list on the user login page. Each group can have multiple aliases or no alias. If you w name of the tunnel group to appear on this list, specify it as an alias. This feature is us same group is known by several common names, such as “Devtest” and “QA”. Specifying a group URL eliminates the need for the user to select a group at login. Wh in, the ASA looks for the user incoming URL in the tunnel-group-policy table. If it f and if this feature is enabled, then the ASA automatically selects the appropriate serve the user with only the username and password fields in the login window. If the URL the dropdown list of groups also appears, and the user must make the selection. You can configure multiple URLs (or no URLs) for a group. You can enable or disab individually. You must use a separate specification (**group-url** command) for each U specify the entire URL, which can use either the HTTP or HTTPS protocol. You cannot associate the same URL with multiple groups. The ASA verifies the unic URL before accepting the URL for a tunnel group.
ASDM Features	
Management and Monitoring Support for the CSC SSM	ASDM Version 5.1 delivers an industry-first solution that blends the simplicity of Tr HTML-based configuration panels with the ingenuity of ASDM. This helps ensure cor enforcement, and simplifies the complete provisioning, configuration, and monitoring the rich unified threat management functions offered by the CSC SSM. ASDM provi complementing monitoring solution with a new CSC SSM homepage and new monit Once a CSC SSM is installed, the main ASDM homepage is automatically updated to CSC SSM panel, which provides a historic view into threats, e-mail viruses, live eve module statistics such as last installed software/signature updates, system resources, Within the monitoring section of ASDM, a rich set of analysis tools provide detailed threats, software updates, resource graphs, and more. The Live Security Event Monit troubleshooting and monitoring tool that provides real-time updates regarding scanne e-mail messages, identified viruses/worms, detected attacks, and more. It gives admi option to filter messages using regular-expression string matching, so specific attack messages can be focused on and analyzed in detail.
Syslog to Access Rule Correlation	This ASDM release introduces a new Syslog to Access Rule Correlation tool that gre day-to-day security management and troubleshooting activities. With this dynamic to administrators can quickly resolve common configuration issues, along with most use connectivity problems. Users can select a syslog message within the Real-Time Sysl panel, and by simply clicking the Create button at the top of the panel, can invoke the a options for that specific syslog. Intelligent defaults help ensure that the configuration simple, which helps improve operational efficiency and response times for business-crit The Syslog to Access Rule Correlation tool also offers an intuitive view into syslog mes by user-configured access rules.
Customized Syslog Coloring	ASDM allows for rapid critical system message identification and convenient syslog m allowing the colored grouping of syslog messages according to syslog level. Users ca default coloring options, or create their own unique colored syslog profiles for ease of
ASDM and WebVPN interface	ASDM and WebVPN can now run on the same interface simultaneously.

Feature	Description
ASDM Demo Mode	ASDM Demo Mode initial support.

New Features in Version 7.0

New Features in ASA 7.0(8)/ASDM 5.0(8) and ASDM 5.0(9)

Released: June 2, 2008

Note ASDM 5.0(9) does not include any new features; it includes caveat fixes only.

Feature	Description
Firewall Features	
Ethertype ACL MAC Enhancement	EtherType ACLs have been enhanced to allow non-standard MACs. Existing default rul retained, but no new ones need to be added. *Also available in Version 7.2(4) and 8.0(4).*
Remote Access Features	
Local Address Pool Edit	Address pools can be edited without affecting the desired connection. If an address in us being eliminated from the pool, the connection is not affected. However, if the address i being eliminated from the pool, the connection is brought down. *Also available in Version 7.2(4) and 8.0(4).*
Connection Features	
clear conn Command	The **clear conn** command was added to remove connections. *Also available in Version 7.2(4) and 8.0(4).*
Fragment full reassembly	The **fragment** command was enhanced with the **reassembly full** keywords to enable full r for fragments that are routed through the device. Fragments that terminate at the device a fully reassembled. *Also available in Version 7.2(4) and 8.0(4).*
Troubleshooting and Monitoring Features	
capture command Enhancement	The **capture type asp-drop** *drop_code* command now accepts **all** as the *drop_code*, so y now capture all packets that the ASA drops, including those dropped due to security che *Also available in Version 7.2(4) and 8.0(4).*

Feature	Description
show asp drop Command Enhancement	Output now includes a timestamp indicating when the counters were last cleared (see **drop** command). It also displays the drop reason keywords next to the description, so use the **capture asp-drop** command using the keyword. *Also available in Version 7.2(4) and 8.0(4).*
clear asp table Command	Added the **clear asp table** command to clear the hits output by the **show asp table c** *Also available in Version 7.2(4) and 8.0(4).*
show asp table classify hits Command Enhancement	The hits option was added to the **show asp table classify** command, showing the timesta the last time the asp table counters were cleared. It also shows rules with hits values zero. This permits users to quickly see what rules are being hit, especially since a simple may end up with hundreds of entries in the **show asp table classify** command. *Also available in Version 7.2(4) and 8.0(4).*
show perfmon Command	Added the following rate outputs: TCP Intercept Connections Established, TCP Interc TCP Embryonic Connections Timeout, and Valid Connections Rate in TCP Intercept *Also available in Version 7.2(4) and 8.0(4).*
memory tracking Commands	The following new commands are introduced in this release: • **memory tracking enable**–This command enables the tracking of heap memory • **no memory tracking enable**–This command disables tracking of heap memory re up all currently gathered information, and returns all heap memory used by the the system. • **clear memory tracking**–This command clears out all currently gathered inform continues to track further memory requests. • **show memory tracking**–This command shows currently allocated memory trac tool, broken down by the topmost caller function address. • **show memory tracking address**–This command shows currently allocated me down by each individual piece of memory. The output lists the size, location, and function of each currently allocated piece memory tracked by the tool. • **show memory tracking dump**–This command shows the size, location, partial a memory dump of the given memory address. • **show memory tracking detail**–This command shows various internal details to gaining insight into the internal behavior of the tool. *Also available in Version 7.2(4) and 8.0(4).*
Failover Features	
failover timeout Command	The **failover timeout** command no longer requires a failover license for use with the feature. *Also available in Version 7.2(4) and 8.0(4).*
Usability Features	

Feature	Description
show access-list Output	Expanded access list output is indented to make it easier to read. *Also available in Version 7.2(4) and 8.0(4).*
show arp Output	In transparent firewall mode, you might need to know whether an ARP entry is statically c or dynamically learned. ARP inspection drops ARP replies from a legitimate host if a dyn entry has already been learned. ARP inspection only works with static ARP entries. The command now shows each entry with its age if it is dynamic, or no age if it is static. See **Monitoring > Interfaces > ARP Table**. *Also available in Version 7.2(4) and 8.0(4).*
show conn Command	The syntax was simplified to use source and destination concepts instead of "local" and In the new syntax, the source address is the first address entered and the destination is th address. The old syntax used keywords like foreign and port to determine the destinatior and port.
ASDM Features	
Support for fragment option	ASDM now supports a fragment option to reassemble packets routed through ASDM. To configure this feature, see **Configuration > Properties > Advanced > Fragment.**

New Features in ASA 7.0(7)/ASDM 5.0(7)

Released: July 9, 2007

Feature	Description
Module Features	
Added Dataplane Keepalive Mechanism	You can now configure the ASA so that a failover will not occur if the AIP SSM is upgr previous releases when two ASAs with AIP SSMs are configured in failover and the AI software is updated, the ASA triggers a failover, because the AIP SSM needs to reboot c for the software update to take effect. *Also available in Version 7.2(3) and 8.0(3)*

New Features in ASA 7.0(6)/ASDM 5.0(6)

Released: August 22, 2006

There were no new features in ASA 7.0(6)/ASDM 5.0(6)

New Features in ASA 7.0(5)/ASDM 5.0(5)

Released: April 14, 2006

Feature	Description
Application Inspection Features	
Command to Control DNS Guard	You can now control the DNS guard function. In releases prior to 7.0(5), the DNS gu are always enabled regardless of the configuration of DNS inspection: • Stateful tracking of the DNS response with DNS request to match the ID • Tearing down the DNS connection when all pending requests are responded This command is effective only on interfaces with DNS inspection disabled (**no inspe** DNS inspection is enabled, the DNS guard function is always performed. We introduced the following command: **dns guard**.
Enhanced IPSEC Inspection	The ability to open specific pinholes for ESP flows based on existence of an IKE flo by the enhanced IPSec inspect feature. This feature can be configured within the MPF along with other inspects. The idle-timeout on the resulting ESP flows is statically set There is no maximum limit on number of ESP flows that can be allowed. We introduced the following command: **inspect ipsec-pass-thru**.
Firewall Features	
Command to Disable RST for Denied TCP Packets	When a TCP packet is denied, the adaptive security appliance always sends a reset wh is going from a high security to a low security interface. The **service resetinbound** c used to enable or disable sending resets when a TCP packet is denied when going from to a high security interface. The **service resetinbound** command is introduced to con RESETs when a packet is denied when going from a high security to a low security i existing **service resetinbound** command is enhanced to take an additional interface We introduced the following commands: **service resetoutbound**, **service resetinbou**
Platform Features	
Increased Connections and VLANs	The maximum connections and VLANs is increased to the following numbers. • ASA5510 base license conns 32000->50000 vlans 0->10 • ASA5510 plus license conns 64000->130000 vlans 10->25 • ASA5520 conns 130000->280000 vlans 25->100 • ASA5540 conns 280000->400000 vlans 100->200
Management Features	
Password Increased in Local Database	Username and enable password length limits increased from 16 to 32 in the LOCAL

Feature	Description
Enhanced **show interface** and **show traffic** Commands	The traffic statistics displayed in both the **show interface** and **show traffic** commands no 1 minute rate and 5 minute rate for input, output and drop. The rate is calculated as the delt the last two sampling points. For a 1 minute rate and a 5 minute rate, a 1 minute timer and timer are run constantly for the rates respectively. An example of the new display follow `1 minute input rate 128 pkts/sec,  15600 bytes/sec` `1 minute output rate 118 pkts/sec,  13646 bytes/sec` `1 minute drop rate 12 pkts/sec` `5 minute input rate 112 pkts/sec,  13504 bytes/sec` `5 minute output rate 101 pkts/sec,  12104 bytes/sec` `5 minute drop rate 4 pkts/sec`

New Features in ASA 7.0(4)/ASDM 5.0(4)

Released: October 15, 2005

Note There was no 7.0(3)/5.0(3) release.

Feature	Description
Platform Features	
Support for the 4GE SSM	The 4GE Security Services Module (SSM) is an optional I/O card for the adaptive security The 4GE SSM expands the total number of ports available on the security appliance, prov additional ports with Ethernet (RJ-45) or SFP (fiber optic) connections.
VPN Features	
WebVPN Capture Feature	The WebVPN capture feature lets you log information about websites that do not displa over a WebVPN connection. You can enable the WebVPN capture feature with the capture but note that it has an adverse affect on the performance of the security appliance. So, be disable this feature after you have captured the information that you need for troublesho
Auto Update Over a VPN Tunnel	With this release, the **auto-update server** command has a new **source** argument that lets y an interface, such as a VPN tunnel used for management access and specified by the **management-access** command: **auto-update server** *url* [**source** *interface*] [*verify-certificate*]

Feature	Description
HTTP proxy applet	The HTTP proxy is an Internet Proxy, that supports both HTTP and HTTPS connectio proxy code modifies the browser proxy configuration dynamically to redirect all bro requests to the new proxy configuration. This allows the Java Applet to take over as the browser. HTTP Proxy can be used in conjunction with the Port Forwarding (Application Acce by itself. **Note** The HTTP proxy feature only works when using Internet Explorer. On some of the older computers, running Windows XP, the RunOnce Reg-Key is no causing the Port Forwarding HTTP-Proxy feature to fail when attempting to modify on Internet Explorer. You can mannually change the registry. Complete the following steps to change the regi **1.** Click **Start** | **Run**. **2.** Type **regedit** in the open text box, and click **OK**. **3.** Open this folder: HKEY_CURRENT_USER\Software\Microsoft\Windows\Curr **4.** Right click inside the CurrentVersion and select **New** | **Key**. **5.** Name the new key **RunOnce**. **6.** Click **OK**. To configure file access and file browsing, MAPI Proxy, HTTP Proxy, and URL entry for this user or group policy, use the **functions** command in WebVPN mode.
IPSec VPN: Add support for cascading ACLs	*Cascading ACLs* involves the insertion of deny ACEs to bypass evaluation against a resume evaluation against a subsequent ACL in the crypto map set. Because you can crypto map with different IPSec settings, you can use deny ACEs to exclude special further evaluation in the corresponding crypto map, and match the special traffic to per in another crypto map to provide or require different security. The sequence number a crypto ACL determines its position in the evaluation sequence within the crypto map
Troubleshooting and Monitoring Features	
Crashinfo Enhancement	Output from the **crashinfo** command might contain sensitive information that is inpp viewing by all users connected to the ASA. The new **crashinfo console disable** com suppress the output from displaying on the console.
Rate limiting of Syslog messages	The logging rate limit enables you to limit the rate at which system log messages are g can limit the number of system messages that are generated during a specified time i You can limit the message generation rate for all messages, a single message ID, a ran IDs, or all messages with a particular severity level. To limit the rate at which system are generated, use the **logging rate-limit** command.
Firewall Features	
Connection timeout using Modular Policy Framework	The new **set connection timeout** command lets you configure the timeout period, af idle TCP connection is disconnected.

Feature	Description
Downloadable ACL Enhancements	A new feature has been added to ensure that downloadable ACL requests sent to a RADI come from a valid source through the Message-Authenticator attribute. Upon receipt of a RADIUS authentication request that has a username attribute containing of a downloadable ACL, Cisco Secure ACS authenticates the request by checking the Message-Authenticator attribute. The presence of the Message-Authenticator attribute p malicious use of a downloadable ACL name to gain unauthorized network access. The Message-Authenticator attribute and its use are defined in RFC 2869, RADIUS Extensions at http://www.ietf.org.
Converting Wildcards to Network Mask in Downloadable ACL	Some Cisco products, such as the VPN 3000 concentrator and Cisco IOS routers, requir configure dowloadable ACLs with wildcards instead of network masks. The Cisco ASA adaptive security appliance, on the other hand, requires you to configure downloadable A network masks. This new feature allows the ASA to convert a wildcard to a netmask int Translation of wildcard netmask expressions means that downloadable ACLs written for C 3000 series concentrators can be used by the ASA without altering the configuration of t downloadable ACLs on the RADIUS server. You can configure ACL netmask conversion on a per-server basis, using the **acl-netmas** command, available in the AAA-server configuration mode.
Application Inspection Features	
Support GTP Load Balancing Across GSNs	If the ASA performs GTP inspection, by default the ASA drops GTP responses from GS were not specified in the GTP request. This situation occurs when you use load-balancin pool of GSNs to provide efficiency and scalability of GPRS. You can enable support for pooling by using the **permit response** command. This command configures the ASA to responses from any of a designated set of GSNs, regardless of the GSN to which a GTP re sent.

New Features in ASA 7.0(2)/ASDM 5.0(2)

Released: July 22, 2005

There were no new features in ASA 7.0(2)/ASDM 5.0(2)

New Features in ASA 7.0(1)/ASDM 5.0(1)

Released: May 31, 2005

Feature	Description
Platform Features	
Support for the ASA 5500 series	Support for the ASA 5500 series was introduced, including support for the following mo 5510, ASA 5520, and ASA 5540.
Firewall Features	

Feature	Description
Transparent Firewall (Layer 2 Firewall)	This feature has the ability to deploy the ASA in a secure bridging mode, similar to a L to provide rich Layer 2 – 7 firewall security services for the protected network. This businesses to deploy this ASA into existing network environments without requiring of the network. While the ASA can be completely "invisible" to devices on both sides network, administrators can manage it via a dedicated IP address (which can be hostec interface). Administrators have the ability to specify non-IP (EtherType) ACLs, in ac standard ACLs, for access control over Layer 2 devices and protocols. We introduced the following commands: **arp-inspection**, **firewall**, **mac-address-tab** **mac-learn**.
Security Contexts (Virtual Firewall)	This feature introduces the ability to create multiple security contexts (virtual firewal single appliance, with each context having its own set of security policies, logical int administrative domain. This provides businesses a convenient way of consolidating mu into a single physical appliance, yet retaining the ability to manage each of these virt separately. These capabilities are only available on ASA with either unrestricted (UR (FO) licenses. This is a licensed feature, with multiple tiers of supported security cont 20, and 50). We introduced the following commands: **admin-context**, **context** (and context subco **changeto**, and **mode**.
Outbound ACLs and	This feature gives administrators improved flexibility for defining access control polic support for outbound ACLs and time-based ACLs (building on top of our existing in support). Using these new capabilities, administrators can now apply access controls a an interface or exits an interface. Time-based access control lists provide administrat control over resource usage by defining when certain ACL entries are active. New con administrators to define time ranges, and then apply these time ranges to specific AC
Time-based ACLs	The existing versatile **access-list** global configuration command was extended with th command to specify a time-based policy defined using the **time-range** global configurat Additionally, the **access-group** global configuration command supports the out keywor an outbound ACL.
Enabling/Disabling of ACL Entries	This feature provides a convenient troubleshooting tool that allows administrators to tes ACLs, without the need to remove and replace ACL entries.
EtherType Access Control	This feature includes very powerful support for performing packet filtering and logg the EtherType of the packets. When operating as a transparent firewall, this provides flexibility for permitting or denying non-IP protocols.
Modular Policy Framework	This feature introduces a highly flexible and extensible next-generation modular polic It enables the construction of flow-based policies that identify specific flows based o administrator-defined conditions, and then apply a set of services to that flow (such a firewall/inspection policies, VPN policies, QoS policies, and more). This provides si improved granular control over traffic flows, and the services performed on them. This n also enables inspection engines to have flow-specific settings (which were global in prev We introduced the following commands: **class-map**, **policy-map**, and **service-policy**

Feature	Description
TCP Security Engine	This feature introduces several new foundational capabilities to assist in detecting protoc application layer attacks. TCP stream reassembly helps detect attacks that are spread acro of packets by reassembling packets into a full packet stream and performing analysis of t TCP traffic normalization provides additional techniques to detect attacks including adv and option checking, detection of data tampering in retransmitted packets, TCP packet c verification, and more. You can configure the extensive TCP security policy using the **set connection advanced** in global configuration command and **tcp-map** global configuration command.
Outbound Low Latency Queuing (LLQ) and Policing	This feature supports applications with demanding quality of service (QoS) requirement support of Low Latency Queuing (LLQ) and Traffic Policing – supporting the ability to end-to-end network QoS policy. When enabled, each interface maintains two queues for traffic – one for latency-sensitive traffic (such as voice or market-data), and one for latenc traffic (such as file transfers). Queue performance can be optimized through a series of con parameters. The QoS functionality is managed using the following commands: **police**, **priority**, **priori** **queue-limit**, and **tx-ring-limit**.
Application Inspection Features	
Advanced HTTP Inspection Engine	This feature introduces deep analysis of web traffic, enabling granular control over HTT for improved protection from a wide range of web-based attacks. In addition, this new H inspection engine allows administrative control over instant messaging applications, pee file sharing applications, and applications that attempt to tunnel over port 80 or any port HTTP transactions. Capabilities provided include RFC compliance enforcement, HTTP authorization and enforcement, response validation, Multipurpose Internet Mail Extensio type validation and content control, Uniform Resource Identifier (URI) length enforcem more. A user can define the advanced HTTP Inspection policy using the **http-map** global conf command and then apply it to the **inspect http** configuration mode command that was e support the specification of a map name.
FTP Inspection Engine	This feature includes the FTP inspection engine which provides new command filtering Building upon the FTP security services previously supported, such as protocol anomaly protocol state tracking, NAT/PAT support, and dynamic port opening, Version 7.0 gives administrators granular control over the usage of 9 different FTP commands, enforcing c that users/groups can perform in FTP sessions. Version 7.0 also introduces FTP server c capabilities, hiding the type and version of the FTP server from those who access it throu
ESMTP Inspection Engine	This feature builds on the SMTP (RFC 821) feature with the addition of support for the (ESMTP) protocol, featuring a variety of commands defined in RFC 1869. Supported co include **AUTH**, **DATA**, **EHLO**, **ETRN**, **HELO**, **HELP**, **MAIL**, **NOOP**, **QUIT**, **RCPT** **SAML**, **SEND**, **SOML**, and **VRFY** (all other commands are automatically blocked to p additional level of security). The **inspect esmtp** global configuration command provides inspection services for SMT ESMTP traffic.

Feature	Description
SunRPC / NIS+ inspection engine	The SunRPC inspection engine provides better support for NIS+ and SunRPC servic enhancements include support for all three versions of the lookup service - Portmapp RPCBind v3 and v4. Use the **inspect sunrpc** and the **sunrpc-server** global configuration commands to co SunRPC / NIS+ inspection Engine.
ICMP Inspection Engine	This feature introduces an ICMP inspection engine. This engine enables secure usag providing stateful tracking for ICMP connections, matching echo requests with repli controls are available for ICMP error messages, which are only permitted for establishe This release introduces the ability to NAT ICMP error messages. Use the **inspect icmp** and the **inspect icmp error** commands to configure the ICMP engine.
GTP Inspection Engine for Mobile Wireless Environments	This feature introduces a new inspection engine for securing 3G Mobile Wireless envi provide packet switched data services using the GPRS Tunneling Protocol (GTP). Th advanced GTP inspection services permit mobile service providers secure interaction partners and provide mobile administrators robust filtering capabilities based on GTI parameters such as IMSI prefixes, APN values and more. This is a licensed feature. The **inspect gtp** command in the policy-map configuration mode and the **gtp-map** g configuration commands are new features introduced in Version 7.0. For more inform and detailed instructions for configuring your GTP inspection policy, see the "Manag Inspection" section in the CLI configuration guide. You may need to install a GTP ac using the **activation-key** exec command.
H.323 Inspection Engine	The H.323 inspection engine adds support for the T.38 protocol, an ITU standard tha secure transmission of Fax over IP (FoIP). Both real-time and store-and-forward FAX supported. The H.323 inspection engine supports Gatekeeper Routed Call Signaling addition to the Direct Call Signaling (DCS) method currently supported. GKRCS sup the ITU standard, now allows the ASA to handle call signaling messages exchanged dir H.323 Gatekeepers.
H.323 Version 3 and 4 Support	This release supports NAT and PAT for H.323 versions 3 and 4 messages, and in part H.323 v3 feature Multiple Calls on One Call Signaling Channel.
SIP Inspection Engine	This feature adds support for Session Initiation Protocol (SIP)-based instant messagin as Microsoft Windows Messenger. Enhancements include support for features descri 3428 and RFC 3265.
Support for Instant Messaging Using SIP	Fixup SIP now supports the Instant Messaging (IM) Chat feature on Windows XP us Messenger RTC client version 4.7.0105 only.
Configurable SIP UDP Inspection Engine	This provides a CLI-enabled solution for non-Session Information Protocol (SIP) pac through the ASA instead of being dropped when they use a SIP UDP port.
MGCP Inspection Engine	This feature includes an MGCP inspection engine that supports NAT and PAT for the protocol. This ensures seamless security integration in distributed call processing envi include MGCP Version 0.1 or 1.0 as the VoIP protocol. The **inspect mgcp** command in the policy-map configuration mode and the **mgcp-m** configuration command enables the user to configure MGCP inspection policy.

Feature	Description
RTSP Inspection Engine	This feature introduces NAT support for the Real Time Streaming Protocol (RTSP), whi streaming applications such as Cisco IP/TV, Apple Quicktime, and RealNetworks RealP operate transparently across NAT boundaries.
SNMP Inspection Engine	Similar to other new inspection engines, the inspect snmp command in policy-map confi mode and the snmp-map global configuration command enables the user to configure an inspection policy.
Port Address Translation (PAT) for H.323 and SIP Inspection Engines	This release enhances support for the existing H.323 and SIP inspection engines by addi for Port Address Translation (PAT). Adding support for PAT with H.323 and SIP enables customers to expand their network address space using a single global address.
PAT for Skinny	This feature allows Cisco IP Phones to communicate with Cisco CallManager across the A it is configured with PAT. This is particularly important in a remote access environment Skinny IP phones behind a ASA talk to the CallManager at the corporate site through a V
ILS Inspection Engine	This feature provides an Internet Locator Service (ILS) fixup to support NAT for ILS and L Directory Access Protocol (LDAP). Also, with the addition of this fixup, the ASA suppo session establishment by Microsoft NetMeeting. Microsoft NetMeeting, SiteServer, and Directory products leverage ILS, which is a directory service, to provide registration and of endpoints. ILS supports the LDAP protocol and is LDAPv2 compliant.
Configurable RAS Inspection Engine	This feature includes an option to turn off the H.323 RAS (Registration, Admission, and fixup and displays this option, when set, in the configuration. This enables customers to t RAS fixup if they do not have any RAS traffic, they do not want their RAS messages to be or if they have other applications that utilize the UDP ports 1718 and 1719.
CTIQBE Inspection Engine	Known also as TAPI/JTAPI Fixup, this feature incorporates a Computer Telephony Interf Buffer Encoding (CTIQBE) protocol inspection module that supports NAT, PAT, and bi-d NAT. This enables Cisco IP SoftPhone & other Cisco TAPI/JTAPI applications to work communicate successfully with Cisco CallManager for call setup and voice traffic across This release supports the **inspect ctiqbe 2748** command.
MGCP Inspection Engine	This release adds support for Media Gateway Control Protocol (MGCP) 1.0, enabling m between Call Agents and VoIP media gateways to pass through the ASA in a secure man See the **inspect mgcp** command.
Ability to Configure TFTP Inspection Engine	Ability to configure TFTP inspection engine inspects the TFTP protocol and dynamicall connection and xlate, if necessary, to permit file transfer between a TFTP client and serv Specifically, the fixup inspects TFTP read request (RRQ), write request (WRQ), and error m (ERROR). **Note** TFTP Fixup is enabled by default. TFTP Fixup must be enabled if static PA to redirect TFTP traffics.
Filtering Features	

Feature	Description
Improved URL Filtering Performance	This feature significantly increases the number of concurrent URLs that can be proce improving the communications channel between the ASA and the Websense servers. The existing **url-server** global configuration command now supports the **connection** specify the number of TCP connections in the pool that is used.
URL Filtering Enhancements	This release supports N2H2 URL filtering services for URLs up to 1159 bytes. For Websense, long URL filtering is supported for URLs up to 4096 bytes in length. Additionally, this release provides a configuration option to buffer the response from if its response is faster than the response from either an N2H2 or Websense filtering s This prevents the web server's response from being loaded twice.
IPSec VPN Features	
Incomplete Crypto Map Enhancements	Every static crypto map must define an access list and an IPSec peer. If either is missi map is considered incomplete and a warning message is printed. Traffic that has not to an complete crypto map is skipped, and the next entry is tried. Failover hello packe from the incomplete crypto map check.
Spoke-to-Spoke VPN Support	This feature improves support for spoke-to-spoke (and client-to-client) VPN commu providing the ability for encrypted traffic to enter and leave the same interface. Furth split-tunnel remote access connections can now be terminated on the outside interface allowing Internet-destined traffic from remote access user VPN tunnels to leave on the as it arrived (after firewall rules have been applied). The **same-security-traffic** command permits traffic to enter and exit the same interfa with the **intra-interface** keyword enabling spoke-to-spoke VPN support.
OSPF Dynamic Routing over VPN	Support for OSPF has been extended to support neighbors across an IPSec VPN tunne the ASA to support dynamic routing updates across a VPN tunnel to other OSPF peers are unicast and encrypted for transport down the tunnel to an identified neighbor in an R manner. The **ospf network point-to-point non-broadcast** command in interface configuration comprehensive OSPF dynamic routing services to support neighbors across IPSec V providing improved network reliability for VPN connected networks.
Remote Management Enhancements	This feature enables administrators to remotely manage firewalls over a VPN tunnel us interface IP address of the remote ASA. In fact, administrators can define any ASA i management-access. This feature supports ASDM, SSH, Telnet, SNMP, and so on, th dynamic IP address. This feature significantly benefits broadband environments.
X.509 Certificate Support	Support for X.509 certificates has been significantly improved in the ASA, adding sup certificate chaining (for environments with a multi-level certification authority hierar enrollment (for environments with offline certificate authorities), and support for 409 keys. Version 7.0 also includes support for the new certificate authority introduced in software, a lightweight X.509 certificate authority designed to simplify roll-out of PI site-to-site VPN environments.

Feature	Description
Easy VPN Server	This release supports Cisco Easy VPN server. Cisco Easy VPN server is designed to fun seamlessly with existing VPN headend configured to support Cisco VPN client and to mi administrative overhead for the client by centralizing VPN configuration at the Cisco Ea server. Examples of Cisco Easy VPN server products include the Cisco VPN client v3.x a and the Cisco VPN 3002 Hardware client. **Note** The ASA already acts as a central site VPN device and supports the termina remote access VPN clients.
Easy VPN Server Load Balancing Support	The ASA 5500 ASA can participate in cluster-based concentrator load balancing. It supp 3000 series concentrator load balancing with automatic redirection to the least utilized co
Dynamic Downloading of Backup Easy VPN Server Information	Support for downloading a list of backup concentrators defined on the headend. This feature supports the vpngroup group_name **backup-server** {{ip1 [*ip2... ip10*]} | **clear-** commands.
Easy VPN Internet Access Policy	The ASA changes the behavior of a ASA used as an Easy VPN remote device in regard access policy for users on the protected network. The new behavior occurs when split tu enabled on the Easy VPN server. Split tunneling is a feature that allows users connected the ASA to access the Internet in a clear text session, without using a VPN tunnel. The ASA used as an Easy VPN remote device downloads the split tunneling policy and its local Flash memory when it first connects to the Easy VPN server. If the policy enabl tunneling, users connected to the network protected by the ASA can connect to the Internet of the status of the VPN tunnel to the Easy VPN server.
Verify Certificate Distinguished Name	This feature enables the adaptive security appliances acting as either a VPN peer for site as the Easy VPN server in remote access deployments to validate matching of a certifica administrator specified criteria.
Easy VPN Web Interface for Manual Tunnel Control User Authentication and Tunnel Status	With the introduction of the User-Level Authentication and Secure Unit Authentication, the ASA delivers the ability to enter the credentials, connect/dis-connect the tunnel and m connection using new web pages served to users when attempting access to the VPN tun unprotected networks through the ASA. This is only applicable to the Easy VPN server
User-Level Authentication	Support for individually authenticating clients (IP address based) on the inside network o Both static and One Time Password (OTP) authentication mechanisms are supported. Th through a web-based interface. This feature adds support to the **vpn-group-policy** command.
Secure Unit Authentication	This feature provides the ability to use dynamically generated authentication credentials to a the Easy VPN remote (VPN Hardware client) device.
Flexible Easy VPN Management Solutions	Managing the ASA using the outside interface will not require the traffic to flow over th tunnel. You will have the flexibility to require all NMS traffic to flow over the tunnel or this policy.

Feature	Description
VPN Client Security Posture Enforcement	This feature introduces the ability to perform VPN client security posture checks wh connection is initiated. Capabilities include enforcing usage of authorized host-based sec (such as the Cisco Security Agent) and verifying its version number, policies, and sta (enabled/disabled). To set personal firewall policies that the security appliance pushes to the VPN client tunnel negotiation, use the **client-firewall** command in group-policy configuration m
VPN Client Update	To configure and change **client update** parameters, use the client-update command in ipsec-attributes configuration mode.
VPN Client Blocking by Operating System and Type	This feature adds the ability to restrict the different types of VPN clients (software cl VPN 3002, and PIX) that are allowed to connect based on type of client, operating sy installed, and VPN client software version. When non-compliant users attempt to con be directed to a group that specifically allows connections from non-compliant users To configure rules that limit the remote access client types and versions that can con through the ASA, use the **client-access-rule** command in group-policy configuration
Movian VPN Client Support	This feature introduces support for handheld (PocketPC and Palm) based Movian VP securely extending access to your network to mobile employees and business partner New support for Diffie-Hellman Group 7 (ECC) to negotiate perfect forward secrecy Version 7.0. This option is intended for use with the MovianVPN client, but can be us clients that support D-H Group 7 (ECC).
VPN NAT Transparency	This feature extends support for site-to-site and remote-access IPSec-based VPNs to environments that implement NAT or PAT, such as airports, hotels, wireless hot spots, a environments. Version 7.0 also adds support for Cisco TCP and User Datagram Proto NAT traversal methods as complementary methods to existing support for the IETF U mechanism for safe traversal through NAT/PAT boundaries. See the **isakmp** global configuration command for additional options when configur traversal policy.
IKE Syslog Support	This feature introduces a small enhancement to IKE syslogging support and a limited event tracing capabilities for scalable VPN troubleshooting. These enhancements hav to allow for new syslog message generation and improved ISAKMP command contr
Diffie-Hellman (DH) Group 5 Support	This release supports the 1536-bit MODP Group that has been given the group 5 iden
Advanced Encryption Standard (AES)	This feature adds support for securing site-to-site and remote access VPN connections international encryption standard. It also provides software-based AES support on all ASA models and hardware-accelerated AES via the new VAC+ card.
New Ability to Assign Netmasks with Address Pools	This feature introduces the ability to define a subnet mask for each address pool and information onto the client.
Cryptographic Engine Known Answer Test (KAT)	The function of KAT is to test the instantiation of the ASA crypto engine. The test will every time during the ASA boot up before the configuration is read from Flash mem be run for valid crypto algorithms for the current license on the ASA.

Feature	Description
Custom Backup Concentrator Timeout	This feature constitutes a configurable time out on the ASA connection attempts to a VPN thereby controlling the latency involved in rolling over to the next backup concentrator This feature supports the **vpngroup** command.
WebVPN Features	
Remote Access via Web Browser (WebVPN)	Version 7.0(1) supports WebVPN on ASA 5500 series security appliances in single, rout WebVPN lets users establish a secure, remote-access VPN tunnel to the security applian web browser. There is no need for either a software or hardware client. WebVPN provid access to abroad range of web resources and both web-enabled and legacy applications fr any computer that can reach HTTPS Internet sites. WebVPN uses Secure Sockets Layer and its successor, Transport Layer Security (SSL/TLS1) to provide a secure connection remote users and specific, supported internal resources that you configure at a central sit security appliance recognizes connections that need to be proxied, and the HTTP server with the authentication subsystem to authenticate users.
CIFS	WebVPN supports the Common Internet Files System, which lets remote users browse a preconfigured NT/Active Directory file servers and shares at a central site. CIFS runs ov and uses DNS and NetBIOS for name resolution.
Port Forwarding	WebVPN port forwarding, also called application access, lets remote users use TCP-app over an SSL VPN connection.
Email	WebVPN supports several ways of using email, including IMAP4S, POP3S, SMTPS, M Web Email. • IMAP4S, POP3S, SMTPS WebVPN lets remote users use the IMAP4, POP3, and SMTP email protocols over SSL co • MAPI Proxy WebVPN supports MAPI, which is remote access to e-mail via MS Outlook Exchange p forwarding. MS Outlook exchange must be installed on the remote computer. • Web Email Web email is MS Outlook Web Access for Exchange 2000, Exchange 5.5, and Exchange requires an MS Outlook Exchange Server at the central site.
Routing Features	
IPv6 Inspection, Access Control, and Management	This feature introduces support for IP version 6 (IPv6) inspection, access control, and ma Full stateful inspection is provided for through-the-box IPv6 traffic in both a dedicated I and in a dual-stack IPv4 / IPv6 mode. In addition, a ASA can be deployed in a pure IPv6 env supporting IPv6 to-the-box management traffic for protocols including SSHv2, Telnet, H ICMP. Inspection engines that support IPv6 traffic in Version 7.0 include HTTP, FTP, SM TCP and ICMP.

Feature	Description
DHCP Option 66 and 150 Support	This feature enhances the DHCP server on the inside interface of the ASA to provide information to the served DHCP clients. The implementation responds with one TFT DHCP option 66 requests and with, at most, two servers for DHCP option 150 reque DHCP options 66 and 150 simplify remote deployments of Cisco IP Phones and Cis by providing the Cisco CallManager contact information needed to download the rest c configuration.
DHCP Server Support on Multiple Interfaces	This release allows as many integrated Dynamic Host Configuration Protocol (DHC be configured as desired, and on any interface. DHCP client can be configured only interface, and DHCP relay agent can be configured on any interface. However, DHC DHCP relay agent cannot be configured concurrently on the same ASA, but DHCP cli relay agent can be configured concurrently. We modified the following command: **dhcpd address**.
Multicast Support	PIM sparse mode was added to allow direct participation in the creation of a multica PIM-SM. This capability extends existing multicast support for IGMP forwarding ar access control policies and ACLs. PIM-SM provides an alternative to transparent mo in multicast environments. The **pim** commands and the **multicast-routing** command added support to the new in addition to the **show mrib** EXEC command in this feature.
Interface Features	
Common Security-Level for Multiple Interfaces	This feature extends the security-level policy structure by enabling multiple interface common security level. This allows for simplified policy deployments by allowing i a common security policy (for example two ports connected into the same DMZ, or zones/departments within a network) to share a common security level. Communicat interfaces with the same security level is governed by the ACL on each interface. See the **same-security-traffic** command and the **inter-interface** keyword to enable t interfaces configured with the same security level.
show interface Command	The **show interface** command has display buffer counters.
Dedicated Out-of-Band Management Interface	The **management-only** configuration command has been introduced in the interface mode to enable dedicated out-of-band management access to the device.
Modification to GE Hardware Speed Settings	The Gigabit Ethernet cards can be configured by hardware in TBI or GMII mode. TE not support half duplex. GMII mode supports both half duplex and full duplex. All t controllers used in the ASAs are configured for TBI and thus cannot support half-du hence the half-duplex setting is removed.
VLAN-based virtual interfaces	802.1Q VLAN support provides flexibility in managing and provisioning the ASA. enables the decoupling of IP interfaces from physical interfaces (hence making it possib logical IP interfaces independent of the number of interface cards installed), and suppli handling for IEEE 802.1Q tags. We introduced the following command: **vlan**.
NAT Features	

Feature	Description
Optional Address Translation Services	This feature simplifies deployment of the ASA by eliminating previous requirement for translation policies to be in place before allowing network traffic to flow. Now, only hos networks that require address translation will need to have address translation policies co This feature introduces a new configuration option, “nat-control”, which allows NAT to b incrementally. Version 7.0 introduces the **nat-control** command and preserves the current behavior for upgrading from previous versions of the software. For new security appliances or device have their configurations cleared, the default will be to not require a NAT policy for traffic the security appliance.
High Availability Features	
Active/Active Failover with Asymmetric Routing Support	This feature builds upon the award-winning ASA high availability architecture, introduci for Active/Active failover. This enables two UR licensed or one UR and one FO-AA lice to act as a failover pair, both actively passing traffic at the same time, and with Asymmetr Support. The Active/Active failover feature leverages the security context feature of this release – where each ASA in a failover pair is active for one context and standby for the an inverse symmetric pair. Another key customer challenge that we are addressing in Ve is Asymmetric Routing Support. This will enable customers with advanced routing topolog packets may enter from one ISP and exit via another ISP, to deploy the ASA to protect th environments (leveraging the Asymmetric Routing Support introduced in Version 7.0). To support the Active/Active feature, the **failover active** command is extended with the keyword and this software release introduces the failover group configuration mode. In a the **asr-group** command in interface configuration mode extends the Active/Active solu environments with Asymmetric Routing.
VPN Stateful Failover	This feature introduces Stateful Failover for VPN connections, complementing the awar firewall failover services. All security association (SA) state information and key materi automatically synchronized between the failover pair members, providing a highly resili solution. The VPN Stateful Failover is enabled implicitly when the device operates in single routed addition to the **show failover** EXEC command, which includes a detailed view of VPN S Failover operations and statistics, the **show isakmp sa**, **show ipsec sa** and **show vpnd-s** commands have information about the tunnels on both the active and standby unit.
Failover Enhancements	This feature enhances failover functionality so that the standby unit in a ASA failover pa configured to use a virtual MAC address. This eliminates potential “stale” ARP entry iss devices connected to the ASA failover pair, in the unlikely event that both ASAs in a fai fail at the same time and only the standby unit remains operational.
show failover Command	This new feature enhances the **show failover** command to display the last occurrence of
Failover Support for HTTP	This feature supports the **failover replicate http** and **show failover** commands to allow t replication of HTTP sessions in a Stateful Failover environment: When HTTP replication is enabled, the **show failover** command displays the **failover re http** command.

Feature	Description
Zero-Downtime Software Upgrades	This feature introduces the ability for customers to perform software upgrades of fail without impacting network uptime or connections flowing through the units. Version the ability to do inter-version state sharing between ASA failover pairs, allowing cus perform software upgrades to maintenance releases (for example Version 7.0(1) upgra without impacting traffic flowing through the pair (in active/standby failover environ Active/Active environments where the pair is not oversubscribed – more that 50% loa member).
General High Availability Enhancements	This feature includes many significant enhancements to the Failover operation and co deliver faster Failover transitions, increased scalability and even further robustness i operation. The release introduces the following new commands: **failover interface-policy**, **failo** and **failover reload-standby**.
Troubleshooting and Monitoring Features	
Improved SNMP Support	This feature adds support for SNMPv2c, providing new services including 64-bit cou for packet counters on Gigabit Ethernet interfaces) and support for bulk MIB data tra Additionally, Version 7.0 includes SNMPv2 MIB (RFC 1907), and the IF-MIB (RFC 2233) and the Cisco IPSec Flow Monitoring MIB, giving complete visibility into VPN including tunnel uptime, bytes/packets transferred, and more.
CPU Utilization Monitoring Through SNMP	This feature supports monitoring of the ASA CPU usage through SNMP. CPU usage is still available directly on the ASA through the **show cpu** [**usage**] command, but SN integration with other network management software.
SNMP Enhancements	Support for the ASA platform-specific object IDs has been added to the **SNMP mib-2.system.sysObjectID** variable. This enables CiscoView Support on the ASA.
Stack Trace in Flash Memory	This feature enables the stack trace to be stored in non-volatile Flash Memory, so tha retrieved at a later time for debug/troubleshooting purposes.
ICMP Ping Services	This feature introduces several additions to ping (ICMP echo) services, including sup addresses. The **ping** command also supports extended options including data pattern, count, datagram size, interval, verbose output, and sweep range of sizes. The existing **ping** EXEC command has been extended with various keywords and par in troubleshooting network connectivity issues. It also provides support for an intera operation.
System Health Monitoring and Diagnostic Services	This feature provides improved monitoring of the system operation and to help isolat network and ASA issues. The **show resource** and **show counters** commands provide information about resource utilization for the appliance and security contexts as well statistics. To monitor the CPU utilization you may use the new **show cpu** EXEC com as the **show process cpu-hog** EXEC commands. To isolate potential software flaws introduces the **checkheaps** command and related show EXEC command. Finally, to understanding of the block (packet) utilization, the **show blocks** EXEC command prov analytical tools on block queuing and utilization in the system.

Feature	Description
Debug Services	The **debug** commands have been improved and many new features include to respective support. Furthermore, the debug output is now supported to all virtual terminals without re That is, when you enable debug output for a particular feature, you will be able to view t without any limitations. Clearly, the output will be restricted to the session where it was Finally, the user can send debug output over syslogs if your security policy allows it and to do so by leveraging the **logging** command.
SSL debug Support	Support for the Secure Sockets Layer (SSL) protocol is added to the **debug** command. S protocol for authenticated and encrypted communications between client and servers suc ASDM and the ASA.
Packet Capture	This release supports packet capture. The ASA packet capture provides the ability to sni any traffic accepted or blocked by the ASA. Once the packet information is captured, yo option of viewing it on the console, transferring it to a file over the network using a TFT or accessing it through a web browser using Secure HTTP. However, the ASA does not traffic unrelated to itself on the same network segment, and this packet capture feature d include file system, DNS name resolution, or promiscuous mode support. Users can now specify the **capture** command to store the packet capture in a circular bu capture will continue writing packets to the buffer until it is stopped by the administrator The ASA introduces additional support to improve the ability of the user to diagnose device by supporting the ability to capture ISAKMP traffic and only capture packets dropped b Accelerated Security Path (ASP). The existing **capture** command has been extended with a new **type** keyword and param capture ISAKMP, packet drops, and packet drops matching a specified reason string.
show tech Command	This feature enhances the current **show tech** command output to include additional diag information.
Management Features	
Storage of Multiple Configurations in Flash Memory	This release debuts a new Flash file system on the ASA enabling administrators to store configurations on the security appliance. This provides the ability to do configuration ro the event of a mis-configuration. Commands are introduced to manage files on this new f **Note** The new Flash file system is capable of storing not only configuration files multiple system images and multiple PIX images when their is adequate Fla available. The **boot config** global configuration command provides the ability to specify which con file should be used at start-up.
Secure Asset Recovery	This feature introduces the ability to prevent the recovery of configuration data, certificat material if the no **service password recovery** command is in a ASAs configuration (wh allowing customers to recover the asset). This feature is useful in environments where pl security may not be ideal, and to prevent nefarious individuals gaining access to sensitiv configuration data.
Scheduled System Reload (Reboot)	Administrators now have the ability to schedule a reload on a ASA either at a specific ti an offset from the current time, thus making it simpler to schedule network downtimes a remote access VPN users of an impending reboot.

Feature	Description
Command-Line Interface (CLI) Usability	This feature enhances the CLI "user experience" by incorporating many popular Cisco command-line services such as command completion, online help, and aliasing for in ease-of-use and common user experience.
Command-Line Interface (CLI) Activation Key Management	This feature lets you enter a new activation key through the ASA command-line inte without using the system monitor mode and having to TFTP a new image. Additiona CLI displays the currently running activation key when you enter the **show version** c
show version Command	The **show version** command output now has two interface-related lines, Max Physic and Max interfaces. Max interfaces is the total physical and virtual interfaces.
AAA Features	
AAA Integration	Version 7.0(1) native integration with authentication services including Kerberos, NT RSA SecurID (without requiring a separate RADIUS/TACACS+ server) for simplifi authentication. This release also introduces the ability to generate TACACS+AAA ac records for tracking administrative access to ASAs, as well as tracking all configurat that are made during an administrative session.
AAA Fallback for Administrative Access	This feature introduces the ability to authenticate and authorize requests to fall-back database on the ASA. The requirements and design will factor future compatibility w software-like "method list" support for the ASA, and deliver the addition of the LOC method.
AAA Integration Enhancements	This feature debuts native integration with authentication services including Kerbero RSA SecurID (without requiring a separate RADIUS/TACACS+ server) for simplifi administrator authentication. This feature also introduces the ability to generate TAC accounting records for tracking administrative access to ASAs, as well as tracking all changes that are made during an administrative session.
Secure HyperText Transfer Protocol (HTTPS) Authentication Proxy	This feature extends the capabilities of the ASA to securely authenticate HTTP sessi support for HTTPS Authentication Proxy. To configure secure authentication of HTT use the **aaa authentication secure-http-client** command. To configure secure authe HTTPS sessions, use the **aaa authentication include https** or the **aaa authentication** command. In this release configurations that include the **aaa authentication include tcp/0** com inherit the HTTPS Authentication Proxy feature, which is enabled by default with a c to Version 6.3 or later.
Downloadable Access Control Lists (ACLs)	This feature supports the download of ACLs to the ASA from an access control serve enables the configuration of per-user access lists on a AAA server, to provide per-us authorization, that are then downloadable through the ACS to the ASA. This feature is supported for RADIUS servers only and is not supported for TACACS
New Syslog Messaging for AAA authentication	This feature introduces a new AAA syslog message, which prompts users for their A before they can use a service port.

Feature	Description
Per-user-override	This feature allows users to specify a new keyword per-user-override to the **access-group** When this keyword is specified, it allows the permit/deny status from the per-user acces (downloaded via AAA authentication) that is associated to a user to override the permit/d from the access-group access-list.
Local User Authentication Database for Network and VPN Access	This feature allows cut-through and VPN (using xauth) traffic to be authenticated using local username database (as an alternative in addition to the existing authenticating via a AAA server). The server tag variable now accepts the value LOCAL to support cut-through proxy auth using Local Database.
ASDM Features	
Dynamic Dashboard (ASDM Home Page)	• Displays detailed device and licensing information for quick identification of syste resources available. • Displays real-time system and traffic profiling .
Real-time Log Viewer	• Displays real-time syslog messages. • Advanced filtering capabilities make it easy to focus on key events.
Improved Java Web-Based Architecture	• Accelerates the loading of ASDM with optimized applet caching capability. • Provides anytime, anywhere access to all management and monitoring features.
Downloadable ASDM Launcher (on Microsoft Windows 2000 or XP operating systems only)	• Lets you download and run ASDM locally on your PC. • Multiple instances of ASDM Launcher provide administrative access to multiple se appliances simultaneously, from the same management workstation. • Automatically updates the software based on the installed version on the appliance, consistent security management throughout the network.
Multiple Language Operating System Support	Supports both the English and Japanese versions of the Microsoft Windows operating sy