Release Notes for the Cisco ASA Series, Version 9.0(x)

Released: October 29, 2012
Updated: May 10, 2018

This document contains release information for Cisco ASA software Version 9.0(1) through 9.0(4). This document includes the following sections:

Important Notes

- Cisco ASA Clientless SSL VPN Portal Customization Integrity Vulnerability—Multiple vulnerabilities have been fixed for clientless SSL VPN in ASA software, so you should upgrade your software to a fixed version. See http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20141008-asa for details about the vulnerability and a list of fixed ASA versions. Also, if you ever ran an earlier ASA version that had a vulnerable configuration, then regardless of the version you are currently running, you should verify that the portal customization was not compromised. If an attacker compromised a customization object in the past, then the compromised object stays persistent after you upgrade

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

the ASA to a fixed version. Upgrading the ASA prevents this vulnerability from being exploited further, but it will not modify any customization objects that were already compromised and are still present on the system.

- Microsoft Kerberos Constrained Delegation support over clientless SSL VPN is limited to the following Web applications:
  - Microsoft Outlook Web Access
  - Microsoft SharePoint
  - Microsoft Internet Information Services
- EtherChannel configuration on the 4GE SSM disallowed—Interfaces on the 4GE SSM, including the built-in module on the ASA 5550 (GigabitEthernet 1/*x*), are not supported as members of EtherChannels. However, although not supported, configuration was not disallowed until 9.0(1). If you configured any 4GE SSM interfaces as EtherChannel members, then upgrading to 9.0(1) or later will remove the channel-group membership configuration from those interfaces. You must alter your interface configuration to comply with supported interface types. (CSCtq62715)
- ASA Clustering—Due to many caveat fixes, we recommend the 9.0(2) release or later for ASA clustering. If you are running 9.0(1) or 9.1(1), you should upgrade to 9.0(2) or later. Note that due to CSCue72961, hitless upgrading is not supported.
- Downgrading issues:
  - Upgrading to Version 9.0 includes ACL migration (see the 9.0 upgrade guide). Therefore, you cannot downgrade from 9.0 with a migrated configuration. Be sure to make a backup copy of your configuration before you upgrade so you can downgrade using the old configuration if required.
  - For the ASA 5512-X through ASA 5555-X, you cannot perform a hitless downgrade for a failover pair from 9.0(x) to 9.0(1); the ASA perceives a hardware mismatch. You can successfully downgrade from 9.1 and later to 9.0(1).
- Per-session PAT disabled when upgrading— Starting in Version 9.0, by default, all TCP PAT traffic and all UDP DNS traffic use per-session PAT (see the **xlate per-session** command in the command reference). If you upgrade to Version 9.0 from an earlier release, to maintain the existing functionality of multi-session PAT, the per-session PAT feature is disabled during configuration migration. The ASA adds the following deny rules:

```
xlate per-session deny tcp any4 any4
xlate per-session deny tcp any4 any6
xlate per-session deny tcp any6 any4
xlate per-session deny tcp any6 any6
xlate per-session deny udp any4 any4 eq domain
xlate per-session deny udp any4 any6 eq domain
xlate per-session deny udp any6 any4 eq domain
xlate per-session deny udp any6 any6 eq domain
```

  To enable per-session PAT after you upgrade, enter:

```
clear configure xlate
```

  The above deny rules are cleared so that only the default permit rules are still in place, which enables per-session PAT.
- No Payload Encryption for export—You can purchase some models with No Payload Encryption. For export to some countries, payload encryption cannot be enabled on the Cisco ASA series. The ASA software senses a 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 management connections and encrypted route messages for OSPFv3. For example, you can use ASDM HTTPS/SSL, SSHv2, Telnet and SNMPv3. You can also download the dynamic database for the Botnet Traffic Filer (which uses SSL) and redirect traffic to Cloud Web Security.

- Two ASA caches are used for processing server certificate verification information. The global cache is 30 seconds while the session cache is 30 minutes, although the cache timeout values are not configurable.
- Static NAT-with-port-translation requirement before upgrading—In Version 9.0 and later, static NAT-with-port-translation rules limit access to the destination IP address for the specified port only. If you try to access the destination IP address on a different port not covered by a NAT rule, then the connection is blocked. This behavior is also true for Twice NAT. Moreover, traffic that does not match the source IP address of the Twice NAT rule will be dropped if it matches the destination IP address, regardless of the destination port. Therefore, before you upgrade, you must add additional rules for all other traffic allowed to the destination IP address.

  For example, you have the following Object NAT rule to translate HTTP traffic to the inside server between port 80 and port 8080:

  ```
  object network my-http-server
      host 10.10.10.1
      nat (inside,outside) static 192.168.1.1 80 8080
  ```

  If you want any other services to reach the server, such as FTP, then you must explicitly allow them:

  ```
  object network my-ftp-server
      host 10.10.10.1
      nat (inside,outside) static 192.168.1.1 ftp ftp
  ```

  Or, to allow traffic to other ports of the server, you can add a general static NAT rule that will match all other ports:

  ```
  object network my-server-1
      host 10.10.10.1
      nat (inside,outside) static 192.168.1.1
  ```

  For Twice NAT, you have the following rule to allow HTTP traffic from 192.168.1.0/24 to the inside server and translate between port 80 and port 8080:

  ```
  object network my-real-server
      host 10.10.10.1
  object network my-mapped-server
      host 192.168.1.1
  object network outside-real-hosts
      subnet 192.168.1.0 255.255.255.0
  object network outside-mapped-hosts
      subnet 10.10.11.0 255.255.255.0
  object service http-real
      service tcp destination eq 80
  object service http-mapped
      service tcp destination eq 8080
  object service ftp-real
      service tcp destination eq 21
  nat (outside,inside) source static outside-real-hosts outside-mapped-hosts destination
  static my-mapped-server my-real-server service http-mapped http-real
  ```

  If you want the outside hosts to reach another service on the inside server, add another NAT rule for the service, for example FTP:

  ```
  nat (outside,inside) source static outside-real-hosts outside-mapped-hosts destination
  static my-mapped-server my-real-server ftp-real ftp-real
  ```

If you want other source addresses to reach the inside server on any other ports, you can add another NAT rule for that specific IP address or for any source IP address. Make sure the general rule is ordered after the specific rule.

```
nat (outside,inside) source static any any destination static my-mapped-server
my-real-server
```

Limitations and Restrictions

- Clientless SSL VPN with a self-signed certificate on the ASA—When the ASA uses a self-signed certificate or an untrusted certificate, Firefox 4 and later and Safari are unable to add security exceptions when browsing using an IPv6 address HTTPS URL (FQDN URL is OK): the “Confirm Security Exception” button is disabled. See https://bugzilla.mozilla.org/show_bug.cgi?id=633001. This caveat affects all SSL connections originating from Firefox or Safari to the ASA (including clientless SSL VPN connections, and ASDM connections). To avoid this caveat, configure a proper certificate for the ASA that is issued by a trusted certificate authority. For Internet Explorer 9 and later, use compatibility mode.
- Citrix Mobile Receiver and accessing Virtual Desktop Infrastructure (VDI):
  - CSD is not supported.
  - HTTP redirect is not supported.
  - Using Citrix Receiver mobile clients to access web interface of Citrix servers is not supported.
  - Certificate or smart card authentication is not supported as a means of auto sign-on.
  - You must install the XML service and configure it on XenApp and XenDesktop servers.
  - Make sure that the ports 443, 1494, 2598, and 80 are open on any intermediate firewalls between the ASA and the XenApp/XenDesktop server.
  - The password-expire-in-days notification on a tunnel group that is used by VDI is not supported.
- When configuring for IKEv2, for security reasons, you should use groups 21, 20, 19, 24, 14, and 5. We do not recommend Diffie Hellman Group1 or Group2. For example, use

  ```
  crypto ikev2 policy 10
  group 21 20 19 24 14 5
  ```

- With a heavy load of users (around 150 or more) using a WebVPN plugin, you may experience large delays because of the processing overload. Using Citrix web interface reduces the ASA rewrite overhead. To track the progress of the enhancement request to allow WebVPN plug files to be cached on the ASA, refer to CSCud11756.
- Inter-context OSPF adjacency is not supported. To work around this, use the **point-to-point non-broadcast** options under the interface configuration and the **neighbor** command under the **router ospf** section. See the following example for reference:

  ```
  interface Redundant1.189
   description to core
   nameif core
   security-level 0
   ip address 172.18.0.2 255.255.255.0
   ospf network point-to-point non-broadcast

   router ospf 1
   router-id 172.18.0.2
   network 172.18.0.0 255.255.255.0 area 0
  ```

```
log-adj-changes
neighbor 172.18.0.7 interface core
```

- (ASA 5510, ASA 5520, ASA 5540, and ASA 5550 only) We strongly recommend that you enable hardware processing using the **crypto engine large-mod-accel** command instead of software for large modulus operations such as 2048-bit certificates and DH5 keys. If you continue to use software processing for large keys, you could experience significant performance degradation due to slow session establishment for IPsec and SSL VPN connections. We recommend that you initially enable hardware processing during a low-use or maintenance period to minimize a temporary packet loss that can occur during the transition of processing from software to hardware.

  Note For the ASA 5540 and ASA 5550 using SSL VPN, in specific load conditions, you may want to continue to use software processing for large keys. If VPN sessions are added very slowly and the ASA runs at capacity, then the negative impact to data throughput is larger than the positive impact for session establishment.

  The ASA 5580/5585-X platforms already integrate this capability; therefore, **crypto engine** commands are not applicable on these platforms.

- Only users with a privilege level of 15 may copy files to the ASA using the secure copy protocol (SCP).

System Requirements

For information about ASA/ASDM requirements and compatibility, see *Cisco ASA Compatibility*:

http://www.cisco.com/en/US/docs/security/asa/compatibility/asamatrx.html

For VPN compatibility, see the *Supported VPN Platforms, Cisco ASA 5500 Series*:

http://www.cisco.com/en/US/docs/security/asa/compatibility/asa-vpn-compatibility.html

New Features

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

New Features in Version 9.0(4)

Released: December 5, 2013

There are no new features in Version 9.0(4).

New Features in Version 9.0(3)

Released: July 22, 2013

Table 1 lists the new features for ASA Version 9.0(3).

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.

Table 1 New Features for ASA Version 9.0(3)

Feature	Description
Monitoring Features	
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** command on the cluster master

New Features in Version 9.0(2)

Released: February 25, 2013

Table 2 lists the new features for ASA Version 9.0(2).

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.

Table 2 New Features for ASA Version 9.0(2)

Feature	Description
Remote Access Features	
Clientless SSL VPN: Windows 8 Support	This release adds support for Windows 8 x86 (32-bit) and Windows 8 x64 (64-bit) 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 you add the ASA to the trusted zone. – If you enable Enhanced Protected Mode, Smart Tunnel and Port Forwarder are not supported. • A Java Remote Desktop Protocol (RDP) plugin connection to a Windows 8 PC is not supported.
Cisco Secure Desktop: Windows 8 Support	CSD 3.6.6215 was updated to enable selection of Windows 8 in the Prelogin Policy operating system check. See the following limitations: • Secure Desktop (Vault) is not supported with Windows 8.
Management Features	
The default Telnet password was removed	To improve security for management access to the ASA, the default login password for Telnet was removed; you must manually set the password before you can log in using Telnet. **Note**: The login password is only used for Telnet if you do not configure Telnet user authentication (the **aaa authentication telnet console** command). Formerly, when you cleared the password, the ASA restored the default of "cisco." Now when you clear the password, the password is removed. The login password is also used for Telnet sessions from the switch to the ASASM (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**.

New Features in Version 9.0(1)

Released: October 29, 2012

Table 3 lists the new features for ASA Version 9.0(1).

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.

Table 3 New Features for ASA Version 9.0(1)

Feature	Description
Firewall Features	
Cisco TrustSec integration	Cisco TrustSec provides an access-control solution that builds upon an existing identity-aware infrastructure to ensure data confidentiality between network devices and integrate security access services on one platform. In the Cisco TrustSec solution, enforcement devices utilize a combination of user attributes and end-point attributes to make role-based and identity-based access control decisions. In this release, the ASA integrates with Cisco TrustSec to provide security group based policy enforcement. Access policies within the Cisco TrustSec domain are topology-independent, based on the roles of source and destination devices rather than on network IP addresses. The ASA can utilize the Cisco TrustSec solution for other types of security group based policies, such as application inspection; for example, you can configure a class map containing an access policy based on a security group. We introduced or modified the following commands: **access-list extended**, **cts sxp enable**, **cts server-group**, **cts sxp default**, **cts sxp retry period**, **cts sxp reconcile period**, **cts sxp connection peer**, **cts import-pac**, **cts refresh environment-data**, **object-group security**, **security-group**, **show running-config cts**, **show running-config object-group**, **clear configure cts**, **clear configure object-group**, **show cts**, **show object-group**, **show conn security-group**, **clear cts**, **debug cts**. We introduced the following MIB: CISCO-TRUSTSEC-SXP-MIB.
Cisco Cloud Web Security (ScanSafe)	Cisco Cloud Web Security provides content scanning and other malware protection service for web traffic. It can also redirect and report about web traffic based on user identity. **Note** Clientless SSL VPN is not supported with Cloud Web Security; be sure to exempt any clientless SSL VPN traffic from the ASA service policy for Cloud Web Security. We introduced or modified the following commands: **class-map type inspect scansafe**, **default user group**, **http**[**s**] (parameters), **inspect scansafe**, **license**, **match user group**, **policy-map type inspect scansafe**, **retry-count**, **scansafe**, **scansafe general-options**, **server** {**primary** | **backup**}, **show conn scansafe**, **show scansafe server**, **show scansafe statistics**, **user-identity monitor**, **whitelist**.

Table 3 New Features for ASA Version 9.0(1) (continued)

Feature	Description
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 extended**, **service-object**, **service**.
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 lookups when using IPv4 NAT, IPv6 NAT, and NAT64 with DNS inspection enabled for the NAT rule.
Per-session PAT	The per-session PAT feature improves the scalability of PAT and, for ASA clustering, allows each member unit to own PAT connections; multi-session PAT connections have to be forwarded to and owned by the master unit. At the end of a per-session PAT session, the ASA sends a reset and immediately removes the xlate. This reset causes the end node to immediately release the connection, avoiding the TIME_WAIT state. Multi-session PAT, on the other hand, uses the PAT timeout, by default 30 seconds. For "hit-and-run" traffic, such as HTTP or HTTPS, the per-session feature can dramatically increase the connection rate supported by one address. Without the per-session feature, the maximum connection rate for one address for an IP protocol is approximately 2000 per second. With the per-session 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 PAT xlate. For traffic that can benefit from multi-session PAT, such as H.323, SIP, or Skinny, you can disable per-session PAT by creating a per-session deny rule. We introduced the following commands: **xlate per-session**, **clear configure xlate**, **show running-config xlate**.
ARP cache additions for non-connected subnets	The ASA ARP cache only contains entries from directly-connected subnets by default. You can now enable the ARP cache to also include non-directly-connected subnets. We do not recommend enabling this feature unless you know the security risks. This feature could facilitate denial of service (DoS) attack against the ASA; a user on any interface could send out many ARP replies and overload 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**. *Also available in 8.4(5).*

Table 3 New Features for ASA Version 9.0(1) (continued)

Feature	Description
SunRPC change from dynamic ACL to pin-hole mechanism	Previously, Sun RPC inspection does not support outbound access lists because the inspection engine uses dynamic access lists instead of secondary connections. In this release, when you configure dynamic access lists on the ASA, they are supported on the ingress direction only and the ASA drops egress traffic destined to dynamic ports. Therefore, Sun RPC inspection implements a pinhole mechanism to support egress traffic. Sun RPC inspection uses this pinhole mechanism to support outbound dynamic access lists. *Also available in 8.4(4.1).*
Inspection reset action change	Previously, when the ASA dropped a packet due to an inspection engine rule, the ASA sent only one RST to the source device of the dropped packet. This behavior could cause resource issues. In this release, when you configure an inspection engine to use a reset action and a packet triggers 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** command is enabled. (The **service resetoutbound** command is disabled by default.) • The ASA sends a TCP reset to the outside host when the **service resetinbound** command is 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 inside servers; therefore countering denial of service attacks. For outside hosts, the ASA does not send a reset by default and information is not revealed through 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 increased from 65535 to 2000000. We modified the following commands: **set connection conn-max**, **set connection embryonic-conn-max**, **set connection per-client-embryonic-max**, **set connection per-client-max**. *Also available in 8.4(5)*
High Availability and Scalability Features	

Table 3 New Features for ASA Version 9.0(1) (continued)

Feature	Description
ASA Clustering for the ASA 5580 and 5585-X	ASA Clustering lets you group multiple ASAs together as a single logical device. A cluster provides all the convenience of a single device (management, integration into a network) while achieving the increased throughput and redundancy of multiple devices. ASA clustering is supported for the ASA 5580 and the ASA 5585-X; all units in a cluster must be the same model with the same hardware specifications. See the configuration guide for a list of unsupported features when clustering is enabled. We introduced or modified the following commands: **channel-group**, **clacp system-mac**, **clear cluster info**, **clear configure cluster**, **cluster exec**, **cluster group**, **cluster interface-mode**, **cluster-interface**, **conn-rebalance, console-replicate**, **cluster master unit**, **cluster remove unit**, **debug cluster**, **debug lacp cluster**, **enable** (cluster group), **health-check**, **ip address**, **ipv6 address**, **key** (cluster group), **local-unit, mac-address** (interface), **mac-address pool**, **mtu cluster, port-channel span-cluster, priority** (cluster group), **prompt cluster-unit**, **show asp cluster counter**, **show asp table cluster chash-table**, **show cluster**, **show cluster info**, **show cluster user-identity**, **show lacp cluster**, **show running-config cluster**.
OSPF, EIGRP, and Multicast for clustering	For OSPFv2 and OSPFv3, bulk synchronization, route synchronization, and spanned EtherChannels are supported in the clustering environment. For EIGRP, bulk synchronization, route synchronization, and spanned EtherChannels are supported in the clustering environment. Multicast routing supports clustering. We introduced or modified the following commands: **show route cluster**, **debug route cluster**, **show mfib cluster**, **debug mfib cluster**.
Packet capture for clustering	To support cluster-wide troubleshooting, you can enable capture of cluster-specific traffic on the master unit using the **cluster exec capture** command, which is then automatically enabled on all of the slave units in the cluster. The **cluster exec** keywords are the new keywords that you place in front of the **capture** command to enable cluster-wide capture. We modified the following commands: **capture**, **show capture**.
Logging for clustering	Each unit in the cluster generates syslog messages independently. You can use the **logging device-id** command to generate syslog messages with identical or different device IDs to make messages appear to come from the same or different units in the cluster. We modified the following command: **logging device-id**.

Table 3 New Features for ASA Version 9.0(1) (continued)

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 unit when using Stateful Failover. By default, connections are replicated to the standby unit during a 15 second period. However, when a bulk sync occurs (for example, when you first enable failover), 15 seconds may not be long enough to sync large numbers of connections due to a limit on the maximum connections per second. For example, the maximum connections on the ASA is 8 million; replicating 8 million connections in 15 seconds means creating 533 K connections per second. However, the maximum connections allowed per second is 300 K. You can now specify the rate of replication to be less than or equal to the maximum connections per second, and the sync period will be adjusted until all the connections 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	
IPv6 Support on the ASA's outside interface for VPN Features.	This release of the ASA adds support for IPv6 VPN connections to its outside interface using SSL and IKEv2/IPsec protocols. This release of the ASA continues to support IPv6 VPN traffic on its inside interface using the SSL protocol as it has in the past. This release does not provide 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 address, or both an IPv4 and an IPv6 address to an AnyConnect client by creating internal pools of addresses on the ASA or by assigning a dedicated address to a local user on the ASA. The endpoint must have the dual-stack protocol implemented in its operating system to be assigned both types of addresses. Assigning an IPv6 address to the client is supported for the SSL protocol. This feature is not supported for the IKEv2/IPsec protocol. We introduced the following commands: **ipv6-vpn-addr-assign**, **vpn-framed-ipv6-address**.
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 group policy on the ASA. You can specify up to four DNS server addresses including up to two IPv4 addresses and up to two IPv6 addresses. DNS servers with IPv6 addresses can be reached by VPN clients when they are configured to use the SSL protocol. This feature is not supported for clients configured to use the IKEv2/IPsec protocol. We modified the following command: **dns-server value**.

Table 3 New Features for ASA Version 9.0(1) (continued)

Feature	Description
Remote Access VPN support for IPv6: Split tunneling	Split tunneling enables you to route some network traffic through the VPN tunnel (encrypted) and to route other network traffic outside the VPN tunnel (unencrypted or "in the clear"). You can now perform split tunneling on IPv6 network traffic by defining an IPv6 policy which specifies a unified access control rule. IPv6 split tunneling is reported with the telemetric data sent by the Smart Call Home feature. If either IPv4 or IPv6 split tunneling is enabled, Smart Call Home reports split tunneling as "enabled." For telemetric data, the VPN session database displays the IPv6 data typically reported with session management. You can include or exclude IPv6 traffic from the VPN "tunnel" for VPN clients configured to use the SSL protocol. This feature is not supported for the IKEv2/IPsec protocol. We introduced the following command: **ipv6-split-tunnel-policy**.
Remote Access VPN support for IPv6: AnyConnect Client Firewall Rules	Access control rules for client firewalls support access list entries for both IPv4 and IPv6 addresses. ACLs containing IPv6 addresses can be applied to clients configured to use the SSL protocol. This feature is not supported for the IKEv2/IPsec protocol. We modified the following command: **anyconnect firewall-rule**.
Remote Access VPN support for IPv6: Client Protocol Bypass	The Client Protocol Bypass feature allows you to configure how the ASA manages IPv4 traffic when it is expecting only IPv6 traffic or how it manages IPv6 traffic when it is expecting only IPv4 traffic. When the AnyConnect client makes a VPN connection to the ASA, the ASA could assign it an IPv4, IPv6, or both an IPv4 and IPv6 address. If the ASA assigns the AnyConnect connection only an IPv4 address or only an IPv6 address, you can now configure the Client Bypass Protocol to drop network traffic for which the ASA did not assign an IP address, or allow that traffic to bypass the ASA and be sent from the client unencrypted or "in the clear." For example, assume that the ASA assigns only an IPv4 address to an AnyConnect connection and the endpoint is dual stacked. When the endpoint attempts to reach an IPv6 address, if Client Bypass Protocol is disabled, the IPv6 traffic is dropped; however, if Client Bypass Protocol is enabled, the IPv6 traffic is sent from the client in the clear. This feature can be used by clients configured to use the SSL or IKEv2/IPsec protocol. We introduced the following command: **client-bypass-protocol**.

Table 3 New Features for ASA Version 9.0(1) (continued)

Feature	Description
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 feature is not supported for the IKEv2/IPsec protocol. We introduced the following command: **vpn-framed-ipv6-address**.
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 facilitate load balancing and session roaming. This feature can be used by clients configured to use the SSL or IKEv2/IPsec protocol. We introduced the following command: **gateway-fqdn**.
Remote Access VPN support for IPv6: ASA VPN Load Balancing	Clients with IPv6 addresses can make AnyConnect connections through the public-facing IPv6 address of the ASA cluster or through a GSS server. Likewise, clients with IPv6 addresses can make AnyConnect VPN connections through the public-facing IPv4 address of the ASA cluster or through a GSS server. Either type of connection can be load-balanced within the ASA cluster. For clients with IPv6 addresses to successfully connect to the ASAs public-facing IPv4 address, a device that can perform network address translation from IPv6 to IPv4 needs to be in the network. This feature can be used by clients configured to use the SSL or IKEv2/IPsec protocol. We modified the following commands: **show run vpn load-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 specify these 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/IPsec protocol.
Remote Access VPN support for IPv6: Session Management	Session management output displays the IPv6 addresses in Public/Assigned address fields for AnyConnect connections, site-to-site VPN connections, and Clientless SSL VPN connections. You can add new filter keywords to support filtering the output to show only IPv6 (outside or inside) connections. No changes to IPv6 User Filters exist. This feature can be used by clients configured to use the SSL protocol. This feature does not support IKEv2/IPsec protocol. We modified the following command: **show vpn-sessiondb**.

Table 3 New Features for ASA Version 9.0(1) (continued)

Feature	Description
NAT support for IPv6	NAT now supports IPv6 traffic, as well as translating between IPv4 and IPv6 (NAT64). Translating between IPv4 and IPv6 is not supported in transparent mode. We modified the following commands: **nat** (in global and object network configuration mode), **show conn**, **show nat**, **show nat pool**, **show xlate**.
DHCPv6 relay	DHCP relay is supported for IPv6. We introduced the following commands: **ipv6 dhcprelay server**, **ipv6 dhcprelay enable**, **ipv6 dhcprelay timeout**, **clear config ipv6 dhcprelay**, **ipv6 nd managed-config-flag**, **ipv6 nd other-config-flag**, **debug ipv6 dhcp**, **debug ipv6 dhcprelay**, **show ipv6 dhcprelay binding**, **clear ipv6 dhcprelay binding**, **show ipv6 dhcprelay statistics**, and **clear ipv6 dhcprelay statistics**.

Table 3 New Features for ASA Version 9.0(1) (continued)

Feature	Description
OSPFv3	OSPFv3 routing is supported for IPv6. Note the following additional guidelines and limitations for OSPFv2 and OSPFv3: **Clustering** • OSPFv2 and OSPFv3 support clustering. • When clustering is configured, OSPFv3 encryption is not supported. An error message appears if you try to configure OSPFv3 encryption in a clustering environment. • When using individual interfaces, make sure that you establish the master and slave units as either OSPFv2 or OSPFv3 neighbors. • When using individual interfaces, OSPFv2 adjacencies can only be established between two contexts on a shared interface on the master unit. Configuring static neighbors is supported only on point-to-point links; therefore, only one neighbor statement is allowed on an interface. **Other** • OSPFv2 and OSPFv3 support multiple instances on an interface. • The ESP and AH protocol is supported for OSPFv3 authentication. • OSPFv3 supports Non-Payload Encryption. We introduced or modified the following commands: **ipv6 ospf cost, ipv6 ospf database-filter all out**, **ipv6 ospf dead-interval**, **ipv6 ospf hello-interval**, **ipv6 ospf mtu-ignore**, **ipv6 ospf neighbor**, **ipv6 ospf network**, **ipv6 ospf priority**, **ipv6 ospf retransmit-interval**, **ipv6 ospf transmit-delay**, **ipv6 router ospf**, **ipv6 router ospf area**, **ipv6 router ospf default**, **ipv6 router ospf default-information**, **ipv6 router ospf distance**, **ipv6 router ospf exit**, **ipv6 router ospf ignore**, **ipv6 router ospf log-adjacency-changes**, **ipv6 router ospf no**, **ipv6 router ospf redistribute**, **ipv6 router ospf router-id**, **ipv6 router ospf summary-prefix**, **ipv6 router ospf timers**, **area range**, **area virtual-link**, **default**, **default-information originate**, **distance**, **ignore lsa mospf**, **log-adjacency-changes**, **redistribute**, **router-id**, **summary-prefix**, **timers lsa arrival**, **timers pacing flood**, **timers pacing lsa-group**, **timers pacing retransmission**, **show ipv6 ospf**, **show ipv6 ospf border-routers**, **show ipv6 ospf database-filter**, **show ipv6 ospf flood-list**, **show ipv6 ospf interface**, **show ipv6 ospf neighbor**, **show ipv6 ospf request-list**, **show ipv6 ospf retransmission-list**, **show ipv6 ospf summary-prefix**, **show ipv6 ospf virtual-links**, **show ospf**, **show run ipv6 router**, **clear ipv6 ospf**, **clear configure ipv6 router**, **debug ospfv3**.

Table 3 New Features for ASA Version 9.0(1) (continued)

Feature	Description
Unified ACL for IPv4 and IPv6	ACLs now support IPv4 and IPv6 addresses. You can also specify a mix of IPv4 and IPv6 addresses for the source and destination. The IPv6-specific ACLs are deprecated. Existing IPv6 ACLs are migrated to extended ACLs. ACLs containing IPv6 addresses can be applied to clients configured to use the SSL protocol. This feature is not supported for the IKEv2/IPsec protocol. We modified the following commands: **access-list extended**, **access-list webtype**. We removed the following commands: **ipv6 access-list**, **ipv6 access-list webtype**, **ipv6-vpn-filter**.
Mixed IPv4 and IPv6 object groups	Previously, network object groups could only contain all IPv4 addresses or all IPv6 addresses. Now network object groups can support a mix of both IPv4 and IPv6 addresses. **Note** You cannot use a mixed object group for NAT. We modified the following command: **object-group network**.
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**.
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 inspections: • DNS • FTP • HTTP • ICMP You can now also configure the service policy to generate a syslog message (767001) when unsupported inspections receive and drop IPv6 traffic. We modified the following command: **service-policy fail-close**.
Remote Access Features	
Clientless SSL VPN: Additional Support	We have added additional support for these browsers, operating systems, web technologies and applications: **Internet browser support**: Microsoft Internet Explorer 9, Firefox 4, 5, 6, 7, and 8 **Operating system support**: Mac OS X 10.7 **Web technology support**: HTML 5 **Application Support**: Sharepoint 2010

Table 3 New Features for ASA Version 9.0(1) (continued)

Feature	Description
Clientless SSL VPN: Enhanced quality for rewriter engines	The clientless SSL VPN rewriter engines were significantly improved to provide better quality and efficacy. As a result, you can expect a better end-user experience for clientless SSL VPN users. We did not add or modify any commands 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 applications running on mobile devices to XenApp and XenDesktop VDI servers through the ASA. For the ASA to proxy Citrix Receiver to a Citrix Server, when users try to connect to Citrix virtualized resource, instead of providing the Citrix Server's address and credentials, users enter the ASA's SSL VPN IP address and credentials. We modified the following command: **vdi**.
Clientless SSL VPN: Enhanced Auto-sign-on	This feature improves support for web applications that require dynamic parameters for authentication.
Clientless SSL VPN: Clientless Java Rewriter Proxy Support	This feature provides proxy support for clientless Java plug-ins when a proxy is configured in client machines' browsers. We did not add or modify any commands for this feature.
Clientless SSL VPN: Remote File Explorer	The Remote File Explorer provides users with a way to browse the corporate network from their web browser. When users click the Remote File System icon on the Cisco SSL VPN portal page, an applet is launched on the user's system displaying the remote file system in a tree and folder view. We did not add or modify any commands for this feature.
Clientless SSL VPN: Server Certificate Validation	This feature enhances clientless SSL VPN support to enable SSL server certificate verification for remote HTTPS sites against a list of trusted CA certificates. We modified the following commands: **ssl-server-check**, **crypto**, **crypto ca trustpool**, **crl**, **certificate**, **revocation-check**.
AnyConnect Performance Improvements	This feature improves throughput performance for AnyConnect TLS/DTLS traffic in multi-core platforms. It accelerates the SSL VPN datapath and provides customer-visible performance gains in AnyConnect, smart tunnels, and port forwarding. We modified the following commands: **crypto engine accelerator-bias** and **show crypto accelerator**.

Table 3 New Features for ASA Version 9.0(1) (continued)

Feature	Description
Custom Attributes	Custom attributes define and configure AnyConnect features that have not yet been added to ASDM. You add custom attributes to a group policy, and define values for those attributes. For AnyConnect 3.1, custom attributes are available to support AnyConnect Deferred Upgrade. Custom attributes can benefit AnyConnect clients configured for either IKEv2/IPsec or SSL protocols. We added the following command: **anyconnect-custom-attr**.

Table 3 New Features for ASA Version 9.0(1) (continued)

Feature	Description
Next Generation Encryption	The National Standards Association (NSA) specified a set of cryptographic algorithms that devices must support to meet U.S. federal standards for cryptographic strength. RFC 6379 defines the Suite B cryptographic suites. Because the collective set of algorithms defined as NSA Suite B are becoming a standard, the AnyConnect IPsec VPN (IKEv2 only) and public key infrastructure (PKI) subsystems now support them. The next generation encryption (NGE) includes a larger superset of this set adding cryptographic algorithms for IPsec V3 VPN, Diffie-Hellman Groups 14 and 24 for IKEv2, and RSA certificates with 4096 bit keys for DTLS and IKEv2. The following functionality is added to ASA to support the Suite B algorithms: • 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 platforms • 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 Premium license for IKEv2 remote access connections, but Suite B usage for other connections or purposes (such as PKI) has no limitations. IPsecV3 has no licensing restrictions. We introduced or modified the following commands: **crypto ikev2 policy**, **crypto ipsec ikev2 ipsec-proposal**, **crypto key generate**, **crypto key zeroize**, **show crypto key mypubkey**, **show vpn-sessiondb**.
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 mode.

Table 3 New Features for ASA Version 9.0(1) (continued)

Feature	Description
New resource type for site-to-site VPN tunnels	New resource types, vpn other and vpn burst other, were created to set the maximum number of site-to-site VPN tunnels in each context. We modified the following commands: **limit-resource**, **show resource types**, **show resource usage**, **show resource allocation**.
Dynamic routing in Security Contexts	EIGRP and OSPFv2 dynamic routing protocols are now supported in multiple 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 number of routing table entries in each context. We modified the following commands: **limit-resource**, **show resource types**, **show resource usage**, **show resource allocation**.
Mixed firewall mode support in multiple context mode	You can set the firewall mode independently for each security context in multiple context mode, so some can run in transparent mode while others run in routed mode. We modified the following command: **firewall transparent**. *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 hardware and software requirements, see: http://www.cisco.com/en/US/docs/security/asa/compatibility/asamatrx.html.
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 situation. This context includes the identity of the user (who), the application or website that the user is trying to access (what), the origin of the access attempt (where), the time of the attempted access (when), and the properties of the device used for the access (how). With the ASA CX module, you can extract the full context of a flow and enforce granular policies such as permitting access to Facebook but denying access to games on Facebook or permitting finance employees access to a sensitive enterprise database but denying the same to other employees. We introduced or modified the following commands: **capture**, **cxsc**, **cxsc auth-proxy**, **debug cxsc**, **hw-module module password-reset**, **hw-module module reload**, **hw-module module reset**, **hw-module module shutdown**, **session do setup host ip**, **session do get-config**, **session do password-reset**, **show asp table classify domain cxsc**, **show asp table classify domain cxsc-auth-proxy**, **show capture**, **show conn**, **show module**, **show service-policy**. *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 can use two SSPs of the same level in the same chassis). VPN is now supported when using dual SSPs. We did not modify any commands.

Upgrading the Software

See the following table for the upgrade path for your version. Some versions require an interim upgrade before you can upgrade to the latest version. Important fixes were added to Version 9.0(3) that make it possible to upgrade easily to later versions, so we recommend upgrading to 9.0(3) or later.

Note There are no special requirements for Zero Downtime Upgrades for failover and ASA clustering with the following exceptions:

- Upgrading ASA clustering from 9.0(1) to 9.0(2) or later: due to CSCue72961, a Zero Downtime Upgrade is not supported.
- Upgrading issues with 8.4(6) and 9.0(2) for failover: due to CSCug88962, you cannot perform a Zero Downtime Upgrade to 8.4(6) or 9.0(2). You should instead upgrade to 8.4(5) or to 9.0(3) or later.

Current ASA Version	First Upgrade to:	Then Upgrade to:
8.2(x) and earlier	8.4(5)	9.0(3) or later
8.3(x)	8.4(5)	9.0(3) or later
8.4(x)	—	9.0(3) or later
8.5(1)	—	9.0(3) or later
8.6(1)	—	9.0(3) or later
9.0(1) or later	—	9.0(3) or later

For detailed steps about upgrading and configuration migration, see the 9.0 upgrade guide.

Open Caveats

Table 4 contains open caveats in the latest maintenance release.

If you are running an older release, and you need to determine the open caveats for your release, then add the caveats in this section to the resolved caveats from later releases. For example, if you are running Version 9.0(1), then you need to add the caveats in this section to the resolved caveats from 9.0(2) and higher to determine the complete list of open caveats.

If you are a registered Cisco.com user, view more information about each caveat using the Bug Search at the following website:

https://tools.cisco.com/bugsearch

Table 4 Open Caveats in ASA Version 9.0(x)

Caveat	Description
CSCtb64709	RRI Fails to Install Routes After Tunnel Flap
CSCtg78775	asa passes the first packet but denies the rest in pim bidir mode
CSCtn53325	5505 w/ 256MB unable to load anyconnect pkg file
CSCtr67875	HW accelerator error PKCS1 v1.5 RSA - cert auth fails with certain certs
CSCts25553	Directly connected host not reachable for 30 sec after Po is UP
CSCty80078	ASASM shows duplicate link local address on failover
CSCub53088	Arsenal:twice NAT with service type ftp not working.
CSCuc80004	Traceback seen when editing ACL configured in AAA UAuth
CSCug69697	Extended Egress Drops on Etherchannel Members After LACP Reconvergence
CSCui32791	WebVPN: Can't upload slides on SP 2010 server on Windows 8
CSCuj50870	ASA in failover pair may panic in shrlock_unjoin
CSCuj83344	ASA traceback in Thread name - netfs_thread_init
CSCuj99176	Make ASA-SSM cplane keepalives more tolerable to communication delays
CSCul00624	ASA: ARP Fails for Subinterface Allocated to Multiple Contexts on Gi0/6
CSCul02052	ASA fails to set forward address in OSPF route redistrubution
CSCul07504	Scansafe: ASA forwards https packets to SS tower in wrong sequence
CSCul33381	ASA 5505 SIP packets may have extra padding one egress of 5505
CSCul34702	ASA Unicorn rewriter memory corruption
CSCul47395	ASA should allow out-of-order traffic through nromalizer for ScanSafe
CSCul61231	VPN Load-Balancing does not use configured ID certificate for cluster-IP
CSCul62357	ASA fails to perform KCD SSO when web server listens on non-default port
CSCul68246	ASA TCP Normalizer does not handle OOO TCP ACKs to the box
CSCul68363	EIGRP: Auth key with space replicates to Secondary with no space
CSCul70712	ASA: ACL CLI not converting 0.0.0.0 0.0.0.0 to any4
CSCul77465	BPDUs on egress from ASA-SM dropped on backplane
CSCul84216	ASA - "Failed to update IPSec failover runtime data" msg on standby unit

Resolved Caveats

Resolved Caveats in Version 9.0(4)

Table 5 contains resolved caveats in ASA software Version 9.0(4).

If you are a registered Cisco.com user, view more information about each caveat using the Bug Search at the following website:

https://tools.cisco.com/bugsearch

Table 5 Resolved Caveats in ASA Version 9.0(4)

Caveat	Description
CSCsq82949	Algorithm ID encoding error causes CA cert to be unimportable on to ASA
CSCtd57392	Unable to create policy map depending on existing maps and name
CSCtg31077	DHCP relay binding limit of 100 should be increased to 500
CSCtu37460	Backup Shared License Server unable to open Socket
CSCua69937	Traceback in DATAPATH-1-1143 thread: abort with unknown reason
CSCub43580	Traceback during child SA rekey
CSCub52207	Nested Traceback from Watchdog in tmatch_release_recursive_locks()
CSCud37992	HTTP Deep Packet Inspection Denial of Service Vulnerability
CSCud84290	ASA: Random traceback with HA setup with 9.1.(1)
CSCue27223	Standby sends proxy neighbor advertisements after failover
CSCue34342	Cisco ASA IPv6 NAT Denial of Service Vulnerability
CSCue45615	Portchannel keeps sending packets through down/down interface
CSCuf31253	Floating route takes priority over the OSPF routes after failover
CSCuf93071	ASA 8.4.4.1 traceback in threadname Datapath
CSCug03975	ASA DNS Inspection Denial of Service Vulnerability
CSCug30043	revocation-check crl none does not seems to download CRL's properly
CSCug31704	ASA - "Show Memory" Output From Admin Context is Invalid
CSCug33233	ASA Management lost after a few days of uptime
CSCug39080	HA sync configuration stuck -"Unable to sync configuration from Active"
CSCug48732	Crash when loading configuration from TFTP multiple contexts
CSCug55657	ASA does not assign MTU to AnyConnect client in case of IKEv2
CSCug64098	ASA 9.1.1-7 traceback with Checkheaps thread
CSCug76763	Cannot login webvpn portal when Passwd mgmt is enabled for Radius server
CSCug77782	ASA5585 - 9.1.1 - Traceback on IKEv2Daemon Thread

Table 5 Resolved Caveats in ASA Version 9.0(4) (continued)

Caveat	Description
CSCug78561	ASA Priority traffic not subject to shaping in Hierarchical QoS
CSCug79778	ASA standby traceback in fover_parse when upgrading to 9.0.2
CSCug82031	ASA traceback in Thread Name: DATAPATH-4-2318
CSCug83080	Cross-site scripting vulnerability
CSCug83401	ASA Remote Access VPN Authentication Bypass Vulnerability
CSCug90225	ASA: EIGRP Route Is Not Updated When Manually Adding Delay on Neighbor
CSCug97772	Watchdog due to access-list change during uauth
CSCug99467	ASA: Fover downgrade from 9.1 to 9.0 causes HA state progression failure
CSCuh03193	ASA - Not all GRE connections are replicated to the standby unit
CSCuh05791	Single Sign On with BASIC authentication does not work
CSCuh08432	Anyconnect sessions do not connect due to uauth failure
CSCuh08651	UDP ports 500/4500 not reserved from PAT on multicontext ASA for IKEv1
CSCuh09400	ASA OSPF route stuck in database and routing table
CSCuh12279	ASA: Data packets with urgent pointer dropped with IPS as bad-tcp-cksum
CSCuh12375	ASA multicontext transparent mode incorrectly handles multicast IPv6
CSCuh13899	ASA protcol inspection connection table fill up DOS Vulnerability
CSCuh20716	Re-transmitted FIN not allowed through with sysopt connection timewait
CSCuh21682	ASA traceback with less PAT with huge traffic
CSCuh22344	ASA: WebVPN rewriter fails to match opening and closing parentheses
CSCuh23347	ASA:Traffic denied 'licensed host limit of 0 exceeded
CSCuh27912	ASA does not obfuscate aaa-server key when timeout is configured.
CSCuh32106	ASA KCD is broken in 8.4.5 onwards
CSCuh34147	ASA memory leaks 3K bytes each time executing the show tech-support.
CSCuh40372	ASA Round-Robin PAT doesn't work under load
CSCuh45559	ASA: Page fault traceback when changing ASP drop capture buffer size
CSCuh48005	ASA doesn't send NS to stale IPv6 neighbor after failback
CSCuh48577	Slow memory leak on ASA due to SNMP
CSCuh49686	slow memory leak due to webvpn cache
CSCuh52326	ASA: Service object-group not expanded in show access-list for IDFW ACLs
CSCuh56559	ASA removed from cluster when updating IPS signatures
CSCuh58576	Different SNMPv3 Engine Time and Engine Boots in ASA active / standby
CSCuh66892	ASA: Unable to apply "http redirect <interface_name> 80" for webvpn
CSCuh69818	ASA 9.1.2 traceback in Thread Name ssh
CSCuh70040	Renew SmartTunnel Web Start .jnlp Certificate 9/7/2013
CSCuh72888	ASA SSLVPN Java RDP Plugin issues when connecting through group-urls
CSCuh74597	ASA-SM multicast boundary command disappears after write standby

Table 5 Resolved Caveats in ASA Version 9.0(4) (continued)

Caveat	Description
CSCuh78110	Incorrect substitution of 'CSCO_WEBVPN_INTERNAL_PASSWORD' value in SSO
CSCuh80522	nat config is missing after csm rollback operation.
CSCuh90740	WebVPN configs not synchronized when configured in certain order 2
CSCuh90799	ASA 5505 Ezvpn Client fails to connect to Load Balance VIP on ASA server
CSCuh94732	Traceback in DATAPATH-1-2533 after a reboot in a clustered environment
CSCuh95321	Not all contexts successfully replicated to standby ASA-SM
CSCui00618	ASA does not send Gratuitous ARP(GARP) when booting
CSCui01258	limitation of session-threshold-exceeded value is incorrect
CSCui04520	WebVpn: javascript parser error while rewriting libmin.js
CSCui08074	ak47 instance got destroyed issue
CSCui10904	Macro substitution fails on External portal page customization
CSCui12430	ASA: SIP inspection always chooses hairpin NAT/PAT for payload rewrite
CSCui13436	ASA-SM can't change firewall mode using session from switch
CSCui15881	ASA Cluster - Loss of CCL link causes clustering to become unstable
CSCui17249	ASA SNMPv2-MIB ColdStart trap not sent on reload
CSCui19504	ASA: HA state progression failure after reload of both units in HA
CSCui20346	ASA: Watchdog traceback in DATAPATH thread
CSCui22862	ASA traceback when using "Capture Wizard" on ASDM
CSCui24669	ASA PAT rules are not applied to outbound SIP traffic version 8.4.5/6
CSCui25277	ASA TFW doesn't rewrite VLAN in BPDU packets containing Ethernet trailer
CSCui27831	Nested Traceback with No Crashinfo File Recorded on ACL Manipulation
CSCui38495	ASA Assert in Checkheaps chunk create internal
CSCui41794	ASA A/A fover automatic MAC address change causes i/f monitoring to fail
CSCui45340	ASA-SM assert traceback in timer-infra
CSCui45606	ASA traceback upon resetting conn due to filter and inspect overlap
CSCui48221	ASA removes RRI-injected route when object-group is used in crypto ACL
CSCui51199	Cisco ASA Clientless SSL VPN Rewriter Denial of Service
CSCui55190	Failover cluster traceback while modifying object groups via SSH
CSCui55510	ASA traceback in Thread Name: DATAPATH-2-1140
CSCui60514	ASA 5585 SSP-IPS 9.x Gig interfaces do not come up after module reset
CSCui61335	Traceback in Thread: DATAPATH-3-1281 Page fault: Address not mapped
CSCui61822	ASA 5585 - traceback after reconnect failover link and 'show run route'
CSCui63322	ASA Traceback When Debug Crypto Archives with Negative Pointers
CSCui65495	ASA 5512 - Temporary security plus license does not add security context
CSCui66657	Safari crashes when use scroll in safari on MAC 10.8 with smart-tunnel
CSCui70562	AnyConnect Copyright Panel and Logon Form message removed after upgrade

Table 5 Resolved Caveats in ASA Version 9.0(4) (continued)

Caveat	Description
CSCui75284	ASA: Summary IPv6 range not advertised by ABR for OSPFv3
CSCui76124	ASA telnet limit reached 9.0.3
CSCui77398	Cisco ASA Crafted ICMP Packet Denial of Service Vulnerability
CSCui78992	ASA after fover may not flush routes for an active grp in active/standby
CSCui80059	ASA traceback in pix_startup_thread
CSCui80835	ASA drops packet as PAWS failure after incorrect TSecr is seen
CSCui85750	ASA SCH Inventory message incorrectly set at Severity 10
CSCui88578	Failure when accessing CIFS share with period character in username
CSCui91247	ASA does not pass calling-station-id when doing cert base authentication
CSCui94757	ASA tears down SIP signaling conn w/ reason Connection timeout
CSCui98879	Clientless SSL VPN:Unable to translate for Japanese
CSCuj06865	ASA traceback when removing more than 210 CA certificates at once
CSCuj08004	AnyConnect states: "VPN configuration received... has an invalid format"
CSCuj10559	ASA 5505: License Host limit counts non-existent hosts
CSCuj13728	ASA unable to remove ipv6 address from BVI interface
CSCuj16320	ASA 8.4.7 Multi Context TFW not generating any syslog data
CSCuj23632	Certificate CN and ASA FQDN mismatch causes ICA to fail.
CSCuj26709	ASA crashes on access attempt via Citrix Receiver
CSCuj28701	ASA - Default OSPF/EIGRP route gone in Active unit
CSCuj28861	Cisco ASA Malformed DNS Reply Denial of Service Vulnerability
CSCuj28871	ASA WebVPN: Rewriter doesn't work well with Base path and HTTP POST
CSCuj29434	ASA5505 - Max Conn Limit Does Not Update When Adding Temp Sec Plus Key
CSCuj34124	Sustained high cpu usage in Unicorn proxy thread with jar file rewrite
CSCuj34241	no debug all, undebug all CLI commands doesnt reset unicorn debug level
CSCuj39040	syslog 402123 CRYPTO: The ASA hardware accelerator encountered an error
CSCuj42515	ASA reloads on Thread name: idfw_proc
CSCuj43339	Add X-Frame-Options: SAMEORIGIN to ASDM HTTP response
CSCuj44998	ASA drops inbound traffic from AnyConnect Clients
CSCuj47104	EIGRP routes on the active ASA getting deleted after the ASA failover
CSCuj49690	ikev2 L2L cannot be established between contexts on the same ASA
CSCuj50376	ASA/Access is denied to the webfolder applet for a permitted cifs share
CSCuj54287	ASA ACL not applied object-group-search enabled & first line is remark
CSCuj58096	Crypto chip resets with large SRTP payload on 5555
CSCuj58670	Local CA server doesn't notify the first time allowed user
CSCuj60572	Unable to assign ip address from the local pool due to 'Duplicate local'
CSCuj62146	RU : Traceback on Thread Name : Cluster show config

Table 5 Resolved Caveats in ASA Version 9.0(4) (continued)

Caveat	Description
CSCuj68055	ASA crashes under Thread Name: ssh on modifying service object
CSCuj74318	ASA: crypto engine large-mod-accel support in multple context
CSCuj81046	ASA defaults to incorrect max in-negotiation SA limit
CSCuj81157	ASA does not enforce max in-negotiation SA limit
CSCuj85424	Transparent ASA in Failover : Management L2L VPN termination fails
CSCuj88114	WebVPN Java rewriter issue: Java Plugins fail after upgrade to Java 7u45
CSCuj95555	SNMP: ccaAcclEntity MIB info for 5585 not consistent with CLI
CSCuj97361	DNS request failing with debugs "unable to allocate a handle"
CSCuj99263	Wrong ACL seq & remarks shown when using Range object w/ object-group
CSCul00917	SNMP: ccaGlobalStats values do not include SW crypto engine
CSCul19727	NPE: Querying unsupported IKEv2 MIB causes crash
CSCul35600	WebVPN: sharepoint 2007/2010 and Office2007 can't download/edit pictures
CSCul41718	traceback on master VPNLB ASA after switch port failure conditions

Resolved Caveats in Version 9.0(3)

Table 6 contains resolved caveats in ASA software Version 9.0(3).

If you are a registered Cisco.com user, view more information about each caveat using the Bug Search at the following website:

https://tools.cisco.com/bugsearch

Table 6 Resolved Caveats in ASA Version 9.0(3)

Caveat	Description
CSCee19547	show failover does not show interface shutdown status
CSCsk06824	Syslog 103005 should include reason for failure
CSCsv41155	reload due to block depletion needs post-event detection mechanism
CSCsz75702	ENH: ASA8.1 - show environment should be included in show tech
CSCtf59088	Active LED stays green without active failover group
CSCth40232	ASA IKE "debug menu ike" command available for customer use
CSCti07431	1/5 minute input rate and output rate are always 0 with user context.
CSCtn15254	Message: 'Link is down as 10Gbps support is not licensed' always shown
CSCto50963	ASA SIP inspection - To: in INVITE not translated after 8.3/8.4 upgrade
CSCtq12090	ACL remark line is missing when range object is configured in ACL
CSCtr04553	Traceback while cleaning up portlist w/ clear conf all or write standby
CSCtr65927	dynamic policy PAT fails with FTP data due to latter static NAT entry
CSCtx32727	GTP inspect not working in Asymmetric Routing Envirement with ASR group:
CSCtx49751	nat command allows the interface keyword to be chosen as a pat-pool

Table 6 Resolved Caveats in ASA Version 9.0(3) (continued)

Caveat	Description
CSCtx55513	ASA: Packet loss during phase 2 rekey
CSCty59567	Observing traceback @ ipigrp2_redist_metric_incompatible+88
CSCty85328	PPPOE manual address allocation changes subnet into /32
CSCty91030	Snmp-server:wr standby is not copying one of the trap
CSCtz70573	SMP ASA traceback on periodic_handler for inspecting icmp or dns trafic
CSCua13405	Failover Unit Stuck in Cold Standby After Boot Up
CSCua22709	ASA traceback in Unicorn Proxy Thread while processing lua
CSCua51319	simultaneous config-changes on multiple contexts can't be synchronized
CSCua69937	Traceback in DATAPATH-1-1143 thread: abort with unknown reason
CSCua75298	RADIUS Class attribute in accounting stop is missing after ASA failover
CSCua98219	Traceback in ci/console during context creation - ssl configuration
CSCub13022	ASA updates arp entry with an invalid GARP
CSCub50435	Proxy ARP Generated for Identity NAT Configuration in Transparent Mode
CSCub52102	ASA 8.3.2 'name' command is not mapped to 'show crypto ipsec sa' output
CSCub56239	ASA Auth-Proxy should reject aaa listner if port already in use
CSCub58996	Cisco ASA Clientless SSLVPN CIFS Vulnerability
CSCub63148	With inline IPS and heavy load ASA could drop ICMP or DNS replies
CSCub75595	ASA-SM does not allow slot number in prompt
CSCub98434	ASA: Nested traceback in Thread Dispatch Unit - cause: SQLNet Inspection
CSCuc14644	SIP inspect NATs Call-ID in one direction only
CSCuc40450	error 'Drop-reason: (punt-no-mem) Punt no memory' need to be specific
CSCuc44179	Static routes not getting redistributed into EIGRP table via prefixlist
CSCuc46561	OWA doesn't work after the ASA upgrade
CSCuc55719	Destination NAT with non single service (range, gt, lt) not working
CSCuc65775	ASA CIFS UNC Input Validation Issue
CSCuc66362	CP Processing hogs in SMP platform causing failover problems, overruns
CSCuc74333	EZVPN: User gets unexpected IUA prompt
CSCuc74758	Traceback: deadlock between syslog lock and host lock
CSCuc92292	ASA may not establish EIGRP adjacency with router due to version issues
CSCuc95774	access-group commands removed on upgrade to 9.0(1)
CSCuc96911	ASASM platform is not exempt from MAC move wait timer
CSCuc98398	ASA writes past end of file system then can't boot
CSCud00451	L2 learning/ARP DOS attack possible
CSCud13053	NAT64 error message for manual NAT is too vague
CSCud20080	ASA Allows duplicate xlate-persession config lines
CSCud21307	Traceroute through the ASA does not work properly, always shows dest IP

Table 6 Resolved Caveats in ASA Version 9.0(3) (continued)

Caveat	Description
CSCud21714	BTF traceback in datapth when apply l4tm rule
CSCud28106	IKEv2: ASA does not clear entry from asp table classify crypto
CSCud32111	Deny rules in crypto acl blocks inbound traffic after tunnel formed
CSCud34973	ASA stops decrypting traffic after phase2 rekey under certain conditions
CSCud40898	TLS-Proxy does not Send issuer name in the certificate
CSCud41507	Traffic destined for L2L tunnels can prevent valid L2L from establishing
CSCud42001	Smart Tunnel hangs when list contains more than 80 entries
CSCud43999	Prioritize Failover Control Packets on ASA5585-X CPU Uplinks
CSCud50997	ASA IKEv2 fails to accept incoming IKEV2 connections
CSCud57759	DAP: debug dap trace not fully shown after +1000 lines
CSCud62661	STI Flash write failure corrupts large files
CSCud64725	VPNLB: Lost packet during IKEv1 not retransmitted
CSCud64817	ASA 9.x dropping case sensitive DNS PTR requests
CSCud65506	ASA5585: Traceback in Thread Name:DATAPATH when accessing webvpn urls
CSCud67392	ASA hitless upgrade from 8.2 to 8.4 - ERROR: unable to download policy
CSCud69251	traceback in ospf_get_authtype
CSCud69535	OSPF routes were missing on the Active Firewall after the failover
CSCud70273	ASA may generate Traceback while running packet-tracer
CSCud74941	ASA LDAP Mapping should not map 0 to values with no match
CSCud76481	ASA 8.6/9.x : Fails to parse symbols in LDAP attribute name
CSCud77352	Upgrade ASA causes traceback with assert during spinlock
CSCud80242	UDP port 10000 reserved without any crypto configured
CSCud81304	TRACEBACK, DATAPATH-8-2268, Multicast
CSCud84290	ASA: Random traceback with HA setup with 9.1.(1)
CSCud84827	ASA 5580 running 8.2(5)13 traceback
CSCud85382	Threat Detection Syslogs from System Context in Multi-context Mode
CSCud85831	Netbios insp translating ip in answer field to mapped ip of WINS server
CSCud86142	Anyconnect using Ikev2 is missing username in syslog messages
CSCud90534	ASA traceback with Checkheaps thread
CSCud92021	ASA: Mixed-mode transparent context can't change allocated interf. name
CSCud98298	ASA doesn't stop overlapping subnets on physical interfaces
CSCud98455	ASA: 256 byte blocks depleted when syslog server unreachable across VPN
CSCud99081	Control-plane access-list doesn't filter Anyconnect traffic
CSCue00850	Traceback: snp_syslog fails to recognise parent syslog flow
CSCue01840	ASA-1-743002 message is seen without prior ASA-1-743001 message
CSCue02226	ASA 9.1.1 - WCCPv2 return packets are dropped

Table 6 Resolved Caveats in ASA Version 9.0(3) (continued)

Caveat	Description
CSCue02806	Removing IPv6 overlapping routes causes traffic failure
CSCue03220	Anyconnect mtu config at ASA not taking effect at client
CSCue04309	TCP connection to multicast MAC - unicast MAC S/ACK builds new TCP conn
CSCue05458	16k blocks near exhaustion - process emweb/https (webvpn)
CSCue09762	Revert change in subnetting rules for splittunnel policy for smarttunnel
CSCue11669	ASA 5505 not Forming EIGRP neighborship after failover
CSCue11738	ACL migration issues with NAT
CSCue15533	ASA:Traceback while deleting trustpoint
CSCue17876	Some java applets won't connect via smart tunnel on windows with jre1.7
CSCue18975	ASA: Assertion traceback in DATAPATH thread after upgrade
CSCue23700	ASA not in ha becomes pseudo standby after "no fail active"
CSCue25524	Webvpn: Javascript based applications not working
CSCue31622	Secondary Flows Lookup Denial of Service Vulnerability
CSCue32221	LU allocate xlate failed (for NAT with service port)
CSCue33354	Mac version Smart Tunnel with Safari 6.0.1/6.0.2 issue
CSCue34342	ASA may crash due to watchdog timer while getting mapped address
CSCue35150	ASA in multicontext mode provides incorrect SNMP status of failover
CSCue35343	Memory leak of 1024B blocks in webvpn failover code
CSCue36084	RADIUS Memory Leak on ASA using AD-Agent
CSCue41939	IKEv2 reply missing 4bytes of 0's after UDP header
CSCue46386	Cisco ASA Xlates Table Exhaustion Vulnerability
CSCue46757	Make default behavior for LZS compression the same for DTLS and TLS
CSCue47775	after-auto NAT rule (section 3) is not evaluated after double add/remove
CSCue48276	ASA drops packets with IP Options received via a VPN tunnel
CSCue49077	ASA: OSPF fails to install route into asp table after a LSA update
CSCue51796	OSPF routes missing for 10 secs when we failover one of ospf neighbour
CSCue54264	WebVPN: outside PC enabled webvpn to management-access inside interface
CSCue55461	ESMTP drops due to MIME filename length >255
CSCue56901	secondary-authentication-server-group cmd breaks Ikev1/IPsec RA VPN auth
CSCue59676	ASA shared port-channel subinterfaces and multicontext traffic failure
CSCue62422	Multicast,Broadcast traffic is corrupted on a shared interface on 5585
CSCue62470	mrib entries mayy not be seen upon failover initiated by auto-update
CSCue62691	ASASM Traceback when issue 'show asp table interface' command
CSCue63881	ASA SSHv2 Denial of Service Vulnerability
CSCue67198	Crypto accelerator resets with error code 23
CSCue67446	The ASA hardware accelerator encountered an error (Bad checksum)

Table 6 Resolved Caveats in ASA Version 9.0(3) (continued)

Caveat	Description
CSCue73708	Group enumeration still possible on ASA
CSCue74372	Anyconnect DTLS idle-timeout is being reset by transmit traffic only
CSCue74649	When specifying two same OID in GETBULK, reply has no duplicate OID
CSCue77969	Character encoding not visible on webvpn portal pages.
CSCue82544	ASA5585 8.4.2 Traceback in Thread Name aaa while accessing Uauth pointer
CSCue84586	re-write fails for javascript generated URL with "\"
CSCue88423	ASA traceback in datapath thread with netflow enabled
CSCue88560	ASA Traceback in Thread Name : CERT API
CSCue90343	ASA 9.0.1 & 9.1.1 - 256 Byte Blocks depletion
CSCue98716	move OSPF from the punt event queue to its own event queue
CSCue99041	Smart Call Home sends Environmental message every 5 seconds for 5500-X
CSCuf02988	ASA: Page fault traceback in aaa_shim_thread
CSCuf06633	ASA traceback in Thread Name: UserFromCert
CSCuf07810	DTLS drops tunnel on a crypto reset
CSCuf11285	ASA 9.x cut-through proxy ACL incorrectly evaluated
CSCuf16850	split-dns cli warning msg incorrect after client increasing the limit
CSCuf17375	Route Session for Stateful failover reports rerr for all updates
CSCuf27008	Webvpn: Cifs SSO fails first attempt after AD password reset
CSCuf27811	ASA: Pending DHCP relay requests not flushed from binding table
CSCuf29783	ASA traceback in Thread Name: ci/console after write erase command
CSCuf34123	ASA 8.3+ l2l tunnel-group name with a leading zero is changed to 0.0.0.0
CSCuf34754	Framed-IP-Address not sent with AC IKEv2 and INTERIM-ACCOUNTING-UPDATE
CSCuf47114	ASA 9.x: DNS inspection corrupts PTR query before forwarding packet
CSCuf52468	ASA Digital Certificate Authentication Bypass Vulnerability
CSCuf58624	snmp engineID abnormal for asa version 8.4.5 after secondary asa reload
CSCuf65912	IKEv2: VPN filter ACL lookup failure causing stale SAs and traceback
CSCuf71119	Incorrect NAT rules picked up due to divert entries
CSCuf77065	Arsenal: Single Core Saleen Admin Driver Fix Revert Bug
CSCuf77294	ASA traceback with Thread Name: DATAPATH-3-1041
CSCuf77606	ASA-SM traceback in Thread Name: accept/http
CSCuf79091	Cisco ASA time-range object may have no effect
CSCuf85295	ASA changes user privilege by vpn tunnel configuration
CSCuf85524	Traceback when NULL pointer was passed to the l2p function
CSCuf89220	ASA IDFW : Unable to handle contacts in DC user groups
CSCuf90410	ASA LDAPS authorization fails intermittently

Table 6 Resolved Caveats in ASA Version 9.0(3) (continued)

Caveat	Description
CSCuf93843	No value or incorrect value for SNMP OIDs needed to identify VPN clients
CSCug03975	ASA 9.1(1) Reboot while applying regex dns
CSCug08285	Webvpn: OWA 2010 fails to load when navigating between portal and OWA
CSCug10123	ASA sends ICMP Unreach. thro wrong intf. under certain condn.
CSCug13534	user-identity will not retain group names with spaces on reboot
CSCug14707	ASA 8.4.4.1 Keeps rebooting when FIPS is enabled: FIPS Self-Test failure
CSCug19491	ASA drops some CX/CSC inspected HTTP packets due to PAWS violation
CSCug22787	Change of behavior in Prefill username from certificate SER extraction
CSCug23031	Clientless plugins are not working
CSCug23311	cannot access Oracle BI via clentless SSL VPN
CSCug25761	ASA has inefficient memory use when cumulative AnyConnect session grows
CSCug29809	Anyconnect IKEv2:Truncated/incomplete debugs,missing 3 payloads
CSCug30086	ASA traceback on thread Session Manager
CSCug45645	Standby ASA continues to forward Multicast Traffic after Failover
CSCug45674	ASA : HTTP Conn from the box, broken on enabling TCP-State-Bypass
CSCug51148	Responder uses pre-changed IP address of initiator in IKE negotiation
CSCug53708	Thread Name: Unicorn Proxy Thread
CSCug56940	ASA Config Locked by another session prevents error responses.
CSCug58801	ASA upgrade from 8.4 to 9.0 changes context's mode to router
CSCug63063	ASA 9.x: DNS inspection corrupts RFC 2317 PTR query
CSCug66457	ASA : "ERROR:Unable to create router process" & routing conf is lost
CSCug71714	DHCPD appends trailing dot to option 12 [hostname] in DHCP ACK
CSCug72498	ASA scansafe redirection drops packets if tcp mss is not set
CSCug74860	Multiple concurrent write commands on ASA may cause failure
CSCug75709	ASA terminates SIP connections prematurely generating syslog FIN timeout
CSCug83036	L2TP/IPSec traffic fails because UDP 1701 is not removed from PAT
CSCug87747	WebVPN: login banner is shifted left
CSCug94308	ASA: "clear config all" does not clear the enable password
CSCug95287	ASA IDFW: idle users not marked as 'inactive' after default idle timeout
CSCug98852	Traceback when using VPN Load balancing feature
CSCug98894	Traceback in Thread Name: OSPF Router during interface removal
CSCuh01167	Unable to display webpage via WebVPN portal, ASA 9.0(2)9
CSCuh01983	ASA tearsdown TCP SIP phone registration conn due to SIP inspection
CSCuh05751	WebVPN configs not synchronized when configured in certain order
CSCuh10827	Cisco ASA config rollback via CSM doesnt work in multi context mode

Table 6 Resolved Caveats in ASA Version 9.0(3) (continued)

Caveat	Description
CSCuh19234	Traceback after upgrade from 8.2.5 to 8.4.6
CSCuh20372	ASA adds 'extended' keyword to static manual nat configuration line

Resolved Caveats in Version 9.0(2)

Table 7 contains resolved caveats in ASA software Version 9.0(2).

If you are a registered Cisco.com user, view more information about each caveat using the Bug Search at the following website:

https://tools.cisco.com/bugsearch

Table 7 Resolved Caveats in ASA Version 9.0(2)

Caveat	Description
CSCsr58601	SCCP does not handle new msg StartMediaTransmissionACK
CSCti14272	Time-based License Expires Pre-maturely
CSCti38856	Elements in the network object group are not converted to network object
CSCtj12159	ASA (8.3.2) traceback in Thread Name: DATAPATH-1-1295
CSCtj87870	Failover disabled due to license incompatible different Licensed cores
CSCtr17899	Some legitimate traffic may get denied with ACL optimization
CSCtr92976	ESMTP inspection corrupts data
CSCts15825	RRI routes are not injected after reload if IP SLA is configured.
CSCts50723	ASA: Builds conn for packets not destined to ASA's MAC in port-channel
CSCtw56859	Natted traffic not getting encrypted after reconfiguring the crypto ACL
CSCtx82335	Reserve 256 byte block pool for ARP processing
CSCty18976	ASA sends user passwords in AV as part of config command authorization.
CSCtz00381	RADIUS client too busy - try later
CSCtz04768	Emails from Smart Call Home are not RFC 2822 Section 2.3 compliant
CSCtz46845	ASA 5585 with IPS inline -VPN tunnel dropping fragmented packets
CSCtz47034	ASA 5585- 10 gig interfaces may not come up after asa reload
CSCtz56155	misreported high CPU
CSCtz64218	ASA may traceback when multiple users make simultaneous change to ACL
CSCtz78718	ASA: access-list with name "ext" is changed to "extended" on boot
CSCtz79578	Port-Channel Flaps at low traffic rate with single flow traffic
CSCtz94191	ASA cut-though proxy stops working if using FQDN ACL
CSCua20850	5500X Software IPS console too busy for irq can cause data plane down.
CSCua28838	ASA:IKEv2 tunnel failure due to IPsec rekey collision
CSCua35337	Local command auth not working for certain commands on priv 1
CSCua44723	ASA nat-pat: 8.4.4 assert crashes related to xlate timeout

Table 7 Resolved Caveats in ASA Version 9.0(2) (continued)

Caveat	Description
CSCua50058	PP : TFTP ACK to last block dropped
CSCua60417	8.4.3 system log messages should appear in Admin context only
CSCua87170	Interface oversubscription on active causes standby to disable failover
CSCua88376	ASA vulnerable to CVE-2003-0001
CSCua91108	ASA unexpected system reboot with Thread Name: UserFromCert Thread
CSCua91189	Traceback in CP Processing when enabling H323 Debug
CSCua93764	ASA: Watchdog traceback from tmatch_element_release_actual
CSCua95621	ASA:write standby command brings down port-channel interface on standby
CSCua99003	WebVPN:"My Mail" option doesn't work for OWA2010
CSCua99091	ASA: Page fault traceback when copying new image to flash
CSCub04470	ASA: Crash in Dispatch Unit with HTTP inspect regex
CSCub08224	ASA 210005 and 210007 LU allocate xlate/conn failed with simple 1-1 NAT
CSCub11582	ASA5550 continous reboot with tls-proxy maximum session 4500
CSCub14196	FIFO queue oversubscription drops packets to free RX Rings
CSCub15394	unexpected policy-map is added on standby ASA when new context is made
CSCub16427	Standby ASA traceback while replicating flow from Active
CSCub16573	ASA: Memory leak due to SNP RT Inspect
CSCub23840	ASA crashes due to nested protocol object-group used in ACL
CSCub24113	ASA does not check aaa-server use before removing commands
CSCub28198	ASA Webvpn rewriter compression not working
CSCub28721	Standby ASA has duplicate ACEs for webtype ACLs after 'write standby'
CSCub31151	"idle-timeout = 0" is not able to configure with AnyConnect IKEv2
CSCub37882	Standby ASA allows L2 broadcast packets with asr-group command
CSCub39677	ASA Webvpn form POST is not rewritten 8.4.1.8 or later
CSCub40805	After some time "show inventory" fails to display Power Supply SN
CSCub59136	ASA: Manual NAT rules are not processed in order
CSCub59536	NAT Config Rejected on Upgrade when Objects Overlap with Failover IP
CSCub61578	ASA: Assert traceback in PIX Garbage Collector with GTP inspection
CSCub62584	ASA unexpectedly reloads with traceback in Thread Name: CP Processing
CSCub70946	ASA traceback under threadname Dispatch Unit due to multicast traffic
CSCub72545	syslog 113019 reports invalid address when VPN client disconnects.
CSCub72990	ASA is max-aging OSPF LSAs after 50 minutes
CSCub75522	ASA TFW sends broadcast arp traffic to all interfaces in the context
CSCub83472	VPNFO should return failure to HA FSM when control channel is down
CSCub84164	ASA traceback in threadname Logger
CSCub84711	OID used for authentication by EKU is trunkated

Table 7 Resolved Caveats in ASA Version 9.0(2) (continued)

Caveat	Description
CSCub89078	ASA standby produces traceback and reloads in IPsec message handler
CSCub94635	Deleting ip local pool cause disconnect of VPN session using other pools
CSCub97263	WebVpn PortForward code signning issue
CSCub99578	High CPU HOG when connnect/disconnect VPN with large ACL
CSCub99704	WebVPN - mishandling of request from Java applet
CSCuc04636	Traceback in Thread Name: accept/http
CSCuc04900	ASA doesn't prohibit changing password to ones previously used
CSCuc06857	Accounting STOP with caller ID 0.0.0.0 if admin session exits abnormally
CSCuc09055	Nas-Port attribute different for authentication/accounting Anyconnect
CSCuc12119	ASA: Webvpn cookie corruption with external cookie storage
CSCuc12967	OSPF routes were missing on the Standby Firewall after the failover
CSCuc14191	ASA: Webvpn rewriter not rewriting eval function call properly
CSCuc14255	Enhance RTCLI implementation of password type (BNF)
CSCuc15034	The "clear crypto ca crls <trustpoint>" command does not work
CSCuc16455	ASA packet transmission failure due to depletion of 1550 byte block
CSCuc16513	'clear config crypto ipsec ikev1' removes ikev2 proposals as well
CSCuc16670	ASA - VPN connection remains up when DHCP rebind fails
CSCuc17257	ASA Traceback - MD5_Update
CSCuc19882	Flash filesystem does not recognize filesnames > 63 characters
CSCuc23984	ASA: Port-channel config not loaded correctly when speed/duplex are set
CSCuc24547	TCP ts_val for an ACK packet sent by ASA for OOO packets is incorrect
CSCuc24919	ASA: May crash in Thread Name: fover_health_monitoring_thread
CSCuc25787	Per tunnel webvpn customizations ignored after ASA 8.2 upgraded to 8.4
CSCuc28903	ASA 8.4.4.6 and higher: no OSPF adj can be build with Portchannel port
CSCuc34345	Multi-Mode ASA crash on ci/console copying config tftp to running-config
CSCuc36831	Crash when removing group-policy
CSCuc40005	PRTG app Javascript as a stream (not content) fails through the rewriter
CSCuc45011	ASA may traceback while fetching personalized user information
CSCuc46026	ASA traceback: ASA reloaded when call home feature enabled
CSCuc46270	ASA never removes qos-per-class ASP rules when VPN disconnects
CSCuc46561	OWA doesn't work after the ASA upgrade
CSCuc48355	ASA webvpn - URLs are not rewritten through webvpn in 8.4(4)5
CSCuc50544	Error when connecting VPN: DTLS1_GET_RECORD Reason: wrong version number
CSCuc56078	Traceback in threadname CP Processing
CSCuc60478	Management access fails via L2TP VPN client on SMP platform
CSCuc60566	ASA IPSEC error: Internal Error, ike_lock trying to unlock bit

Table 7 Resolved Caveats in ASA Version 9.0(2) (continued)

Caveat	Description
CSCuc60950	ASA traceback in Dispatch Unit
CSCuc61985	distribute-list does not show in the router config.
CSCuc63592	HTTP inspection matches incorrect line when using header host regex
CSCuc64108	ASA:DAP User Messages is truncated when action is terminate
CSCuc66227	Port-channel config fails, Error: unable to get MCAST_MAC_TABLE_SIZE
CSCuc75090	Crypto IPSec SA's are created by dynamic crypto map for static peers
CSCuc75093	Log indicating syslog connectivity not created when server goes up/down
CSCuc78176	Cat6000/15.1(1)SY- ASASM/8.5(1.14) PwrDwn due to SW Version Mismatch
CSCuc79304	ASA 9.0:Clientless & anyconnect fail to group-url with port defined
CSCuc79825	5580 - Thread Name: CP Midpath Processing eip pkp_free_ssl_ctm
CSCuc83059	traceback in fover_health_monitoring_thread
CSCuc83170	ipsecvpn-ike:IKEv1 rekey fails when IPCOMP proposal is sent
CSCuc83323	XSS in SSLVPN
CSCuc83828	ASA Logging command submits invalid characters as port zero
CSCuc84079	ASA: Multiple context mode does not allow configuration of 'mount'
CSCuc89163	Race condition can result in stuck VPN context following a rekey
CSCuc97552	Deny rules in crypto acl blocks inbound traffic after tunnel formed
CSCud04867	Incorrect and duplicate logs about status change of port-channel intfs
CSCud07436	APCF Flag no-toolbar fails after upgrade to 8.4.4.9
CSCud07930	ASA webvpn plugin files Expires header incorrectly set
CSCud08203	Smart-tunnel failing to forward tcp connections for certain application
CSCud08385	Smart Tunnel failed for Safari 6.0.1/6.0.2 on OSX10.7 and 10.8
CSCud12924	CA certificates expiring after 2038 display wrong end date on 5500-X
CSCud16105	Called-Station-Id in RADIUS acct stop after failover is standby address.
CSCud17993	ASA-Traceback in Dispatch unit due to dcerpc inspection
CSCud20442	Sharepoint 2010 over clientless - file edition fails with Office 2010
CSCud24452	ASA TACACS authentication on Standby working incorrectly
CSCud29007	License server becomes unreachable due to "signature invalid" error
CSCud29045	ASASM forwards subnet directed bcast back onto that subnet
CSCud36686	Deny ACL lines in crypto-map add RRI routes
CSCud37992	SMP ASA traceback in periodic_handler in proxyi_rx
CSCud41670	ASA nested traceback with url-filtering policy during failover
CSCud46746	DNS resolution for "from-the-box" traffic not working with "names"
CSCud47900	ASA: adding nested object group fails with "IP version mismatch"
CSCud51281	"Failed to update IPSec failover runtime data" msg on the standby unit
CSCud51478	management access missing from multi cont vpn

Table 7 Resolved Caveats in ASA Version 9.0(2) (continued)

Caveat	Description
CSCud67282	data-path: ASA-SM: 8.5.1 traceback in Thread Name: SSH
CSCud72383	IKEV2-L2L: DH handle leak when PFS enabled only on one peer
CSCud89380	ASA: Username with ampersand disconnects ASDM Firewall Dashboards
CSCud89974	flash in ASA5505 got corrupted

End-User License Agreement

For information on the end-user license agreement, go to:

http://www.cisco.com/go/warranty

Related Documentation

For additional information on the ASA, see *Navigating the Cisco ASA Series Documentation*:

http://www.cisco.com/go/asadocs

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation* at: http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.