Release Notes for the Cisco ASA Series, 9.6(x)

First Published: 2016-03-21

Last Modified: 2017-12-13

Release Notes for the Cisco ASA Series, 9.6(x)

This document contains release information for Cisco ASA software Version 9.6(x).

Important Notes

- Potential Traffic Outage (9.6(2.1) through 9.6(3))—Due to bug CSCvd78303, the ASA may stop passing traffic after 213 days of uptime. The effect on each network will be different, but it could range from an issue of limited connectivity to something more extensive like an outage. You must upgrade to a new version without this bug, when available. In the meantime, you can reboot the ASA to gain another 213 days of uptime. Other workarounds may be available. See Field Notice FN-64291 for affected versions and more information.
- 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).
- ASDM 7.6(2) supports AnyConnect Client profiles in multiple context mode. This feature requires AnyConnect Version 4.2.00748 or 4.3.03013 and later.
- (ASA 9.6.2) Upgrade impact when using multiple-mode configuration—When upgrading from 9.5.2 to 9.6.1 and then subsequently to 9.6.2, any existing RAVPN for multiple-mode configuration will stop working. Post upgrade to the 9.6.2 image, a reconfiguration to give each context a storage space and to get new AnyConnect images in all of the contexts is required.
- (ASA 9.6(2)) Upgrade impact when using SSH public key authentication—Due to updates to SSH authentication, additional configuration is required to enable SSH public key authentication; as a result, existing SSH configurations using public key authentication no longer work after upgrading. Public key authentication is the default for the ASAv on Amazon Web Services (AWS), so AWS users will see this issue. To avoid loss of SSH connectivity, you can update your configuration *before* you upgrade. Or you can use ASDM after you upgrade (if you enabled ASDM access) to fix the configuration.

  Sample original configuration for a username "admin":

  ```
  username admin nopassword privilege 15
  username admin attributes
    ssh authentication publickey 55:06:47:eb:13:75:fc:5c:a8:c1:2c:bb:
    07:80:3a:fc:d9:08:a9:1f:34:76:31:ed:ab:bd:3a:9e:03:14:1e:1b hashed
  ```

  To use the **ssh authentication** command, before you upgrade, enter the following commands:

  ```
  aaa authentication ssh console LOCAL
  ```

```
username admin password <password> privilege 15
```

We recommend setting a password for the username as opposed to keeping the **nopassword** keyword, if present. The **nopassword** keyword means that *any* password can be entered, not that *no* password can be entered. Prior to 9.6(2), the **aaa** command was not required for SSH public key authentication, so the **nopassword** keyword was not triggered. Now that the **aaa** command is required, it automatically also allows regular password authentication for a **username** if the **password** (or **nopassword**) keyword is present.

After you upgrade, the **username** command no longer requires the **password** or **nopassword** keyword; you can require that a user cannot enter a password. Therefore, to force public key authentication only, re-enter the **username** command:

```
username admin privilege 15
```

- Upgrade impact when upgrading the ASA on the Firepower 9300— Due to license entitlement naming changes on the back-end, when you upgrade to ASA 9.6(1)/FXOS 1.1.4, the startup configuration may not parse correctly upon the initial reload; configuration that corresponds to add-on entitlements is rejected.

  For a standalone ASA, after the unit reloads with the new version, wait until all the entitlements are processed and are in an "Authorized" state (**show license all**), and simply reload again (**reload**) *without* saving the configuration. After the reload, the startup configuration will be parsed correctly.

  For a failover pair if you have any add-on entitlements, follow the upgrade procedure in the FXOS release notes, but reset failover after you reload each unit (**failover reset**).

  For a cluster, follow the upgrade procedure in the FXOS release notes; no additional action is required.

- ASA 5508-X and 5516-X upgrade issue when upgrading to 9.5(x) or later—Before you upgrade to ASA Version 9.5(x) or later, if you never enabled jumbo frame reservation then you must check the maximum memory footprint. Due to a manufacturing defect, an incorrect software memory limit might have been applied. If you upgrade to 9.5(x) or later before performing the below fix, then your device will crash on bootup; in this case, you must downgrade to 9.4 using ROMMON (Load an Image for the ASA 5500-X Series Using ROMMON), perform the below procedure, and then upgrade again.

  1. Enter the following command to check for the failure condition:

     ```
     ciscoasa# show memory detail | include Max memory footprint
     Max memory footprint        =    456384512
     Max memory footprint        =            0
     Max memory footprint        =    456384512
     ```

     If a value less than **456,384,512** is returned for “Max memory footprint,” then the failure condition is present, and you must complete the remaining steps before you upgrade. If the memory shown is 456,384,512 or greater, then you can skip the rest of this procedure and upgrade as normal.

  2. Enter global configuration mode:

     ```
     ciscoasa# configure terminal
     ciscoasa(config)#
     ```

  3. Temporarily enable jumbo frame reservation:

```
ciscoasa(config)# jumbo-frame reservation
WARNING: This command will take effect after the running-config
is saved and the system has been rebooted. Command accepted.
INFO: Interface MTU should be increased to avoid fragmenting
jumbo frames during transmit
```

Note Do not reload the ASA.

4. Save the configuration:

```
ciscoasa(config)# write memory
Building configuration...
Cryptochecksum: b511ec95 6c90cadb aaf6b306 41579572
14437 bytes copied in 1.320 secs (14437 bytes/sec)
[OK]
```

5. Disable jumbo frame reservation:

```
ciscoasa(config)# no jumbo-frame reservation
WARNING: This command will take effect after the running-config is saved and
the system has been rebooted. Command accepted.
```

Note Do not reload the ASA.

6. Save the configuration again:

```
ciscoasa(config)# write memory
Building configuration...
Cryptochecksum: b511ec95 6c90cadb aaf6b306 41579572
14437 bytes copied in 1.320 secs (14437 bytes/sec)
[OK]
```

7. You can now upgrade to Version 9.5(x) or later.

- The RSA toolkit version used in ASA 9.x is different from what was used in ASA 8.4, which causes differences in PKI behavior between these two versions.

  For example, ASAs running 9.x software allow you to import certificates with an Organizational Name Value (OU) field length of 73 characters. ASAs running 8.4 software allow you to import certificates with an OU field name of 60 characters. Because of this difference, certificates that can be imported in ASA 9.x will fail to be imported to ASA 8.4. If you try to import an ASA 9.x certificate to an ASA running version 8.4, you will likely receive the error, "ERROR: Import PKCS12 operation failed.

System Requirements

This section lists the system requirements to run this release.

ASA and ASDM Compatibility

For information about ASA/ASDM software and hardware requirements and compatibility, including module compatibility, see Cisco ASA Compatibility.

VPN Compatibility

For VPN compatibility, see Supported VPN Platforms, Cisco ASA 5500 Series.

New Features

This section lists new features for each release.

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

New Features in ASA 9.6(4)

Released: December 13, 2017

There are no new features in this release.

New Features in ASA 9.6(3.1)

Released: April 3, 2017

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

Feature	Description
AAA Features	
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.

New Features in ASA 9.6(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.
Hot Plug Interfaces on the ASAv	You can add and remove Virtio virtual interfaces on the ASAv while the system is active. When you add a new interface to the ASAv, 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 ASAv runs as a guest in the Microsoft Azure environment of the Hyper V Hypervisor. The ASAv 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).*
Through traffic support on the Management 0/0 interface for the ASAv	You can now allow through traffic on the Management 0/0 interface on the ASAv. Previously, only the ASAv on Microsoft Azure supported through traffic; now all ASAvs 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	

Feature	Description
DNS over TCP inspection	You can now inspect DNS over TCP traffic (TCP/53). We added the following command: **tcp-inspection**
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**
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**
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**
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** *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**

Feature	Description
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.
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**
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**
Remote Access Features	
Pre-fill/Username-from-cert feature for multiple context mode	AnyConnect 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.
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**
AnyConnect client profiles supported in multiple context mode	AnyConnect client profiles are supported in multiple context mode. To add a new profile using ASDM, you must have the AnyConnect Secure Mobility Client release 4.2.00748 or 4.3.03013 and later.
Stateful failover for AnyConnect connections in multiple context mode	Stateful failover is now supported for AnyConnect connections in multiple context mode. We did not modify any commands.
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.

Feature	Description
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.
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.
Umbrella Roaming Security module support	You can choose to configure the AnyConnect Secure Mobility Client's Umbrella Roaming Security module for additional DNS-layer security when no VPN is active. We did not modify any commands.
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**
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**
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.
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**

Feature	Description
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**
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**
Interface Features	
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**
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**

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**
High Availability and Scalability Features	
Improved sync time for dynamic ACLs from AnyConnect when using Active/Standby failover	When you use AnyConnect 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.
Licensing Features	
Permanent License Reservation for the ASAv	For highly secure environments where communication with the Cisco Smart Software Manager is not allowed, you can request a permanent license for the ASAv. In 9.6(2), we also added support for this feature for the ASAv 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** *Also in 9.5(2.200).*
Satellite Server support for the ASAv	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.

Feature	Description
Permanent License Reservation for the ASAv 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.
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.
Smart Agent Upgrade for ASAv 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 ASAv does not retain the licensing registration state. You need to re-register with the **license smart register idtoken** *id_token* **force** command; 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** *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**
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**
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.

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** *Also in 9.4(3).*

New Features in ASA 9.6(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.
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.
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**.
Firewall Features	
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**.

Feature	Description
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.
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**.
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**.
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.
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 AnyConnect client. We introduced the following commands: **crypto ikev2 fragmentation**, **show running-config crypto ikev2**, **show crypto ikev2 sa detail**
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**
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**. *Also available in 9.1(7), 9.4(3), and 9.5(3).*

Feature	Description
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** *Also available in 9.1(7) and 9.4(3).*
Routing Features	
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.**
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**
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**

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. *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.

Upgrade the Software

This section provides the upgrade path information and a link to complete your upgrade.

ASA Upgrade Path

To view your current version and model, use one of the following methods:

- CLI—Use the **show version** command.
- ASDM—Choose **Home** > **Device Dashboard** > **Device Information**.

See the following table for the upgrade path for your version. Some older versions require an intermediate upgrade before you can upgrade to a newer version. Recommended versions are in **bold**.

Current Version	Interim Upgrade Version	Target Version
9.3(x)	—	Any of the following: → 9.4(x) → 9.3(x)
9.2(x)	—	Any of the following: → 9.4(x) → 9.3(x) → 9.2(x)
9.1(2), 9.1(3), 9.1(4), 9.1(5), 9.1(6), or 9.1(7.4)	—	Any of the following: → 9.4(x) → 9.3(x) → 9.2(x) → 9.1(3), 9.1(4), 9.1(5), 9.1(6), 9.1(7.4)

Current Version	Interim Upgrade Version	Target Version
9.1(1)	→ 9.1(2)	Any of the following: → 9.4(x) → 9.3(x) → 9.2(x) → 9.1(3), 9.1(4), 9.1(5), 9.1(6), 9.1(7.4)
9.0(2), 9.0(3), or 9.0(4)	—	Any of the following: → 9.4(x) → 9.3(x) → 9.2(x) → 9.1(3), 9.1(4), 9.1(5), 9.1(6), 9.1(7.4)
9.0(1)	→ 9.0(2), 9.0(3), or 9.0(4)	Any of the following: → 9.4(x) → 9.3(x) → 9.2(x) → 9.1(3), 9.1(4), 9.1(5), 9.1(6), 9.1(7.4)
8.6(1)	→ 9.0(2), 9.0(3), or 9.0(4)	Any of the following: → 9.4(x) → 9.3(x) → 9.2(x) → 9.1(3), 9.1(4), 9.1(5), 9.1(6), 9.1(7.4)
8.5(1)	→ 9.0(2), 9.0(3), or 9.0(4)	Any of the following: → 9.4(x) → 9.3(x) → 9.2(x) → 9.1(3), 9.1(4), 9.1(5), 9.1(6), 9.1(7.4)

Current Version	Interim Upgrade Version	Target Version
8.4(5+)	—	Any of the following: → 9.4(x) → 9.3(x) → 9.2(x) → 9.1(3), 9.1(4), 9.1(5), 9.1(6), 9.1(7.4)
8.4(1) through 8.4(4)	Any of the following: → 9.0(2), 9.0(3), or 9.0(4) → 8.4(6)	→ 9.4(x) → 9.3(x) → 9.2(x) → 9.1(3), 9.1(4), 9.1(5), 9.1(6), 9.1(7.4)
8.3(x)	→ 8.4(6)	Any of the following: → 9.4(x) → 9.3(x) → 9.2(x) → 9.1(3), 9.1(4), 9.1(5), 9.1(6), 9.1(7.4)
8.2(x) and earlier	→ 8.4(6)	Any of the following: → 9.4(x) → 9.3(x) → 9.2(x) → 9.1(3), 9.1(4), 9.1(5), 9.1(6), 9.1(7.4)

Upgrade Link

To complete your upgrade, see the ASA upgrade guide.

Open and Resolved Bugs

The open and resolved bugs for this release are accessible through the Cisco Bug Search Tool. This web-based tool provides you with access to the Cisco bug tracking system, which maintains information about bugs and vulnerabilities in this product and other Cisco hardware and software products.

Note You must have a Cisco.com account to log in and access the Cisco Bug Search Tool. If you do not have one, you can register for an account. If you do not have a Cisco support contract, you can only look up bugs by ID; you cannot run searches.

For more information about the Cisco Bug Search Tool, see the Bug Search Tool Help & FAQ.

Open Bugs in Version 9.6(x)

The following table lists select open bugs at the time of this Release Note publication.

Caveat ID Number	Description
CSCvb72148	ASAv5 - Cannot re-enable http after reducing memory from 2GB to 1G and upgrade from 9.4.1 to 9.6.2
CSCvb95568	DOC: Document all ASA SCH commands in Command Reference
CSCvd21406	Multiple PAT rules with "any" and named interface cause 305006 "portmap translation creation failed"
CSCve72751	ASA traceback with thread name: DATAPATH
CSCve78652	ASA Crash on Thread Name:CTM message handler
CSCve95924	ASA doesn't boot after a reload unless accessed with console connection
CSCvf10327	ENH: Unique IPv6 link-local addresses assigned when sub-interface is being created
CSCvf20094	"management-access <interface>" will open all management sockets on that int.
CSCvf30738	Active ASA Crashing on DATAPATH
CSCvf39539	Netflow Returns Large Values for Bytes Sent/Received and IP address switch
CSCvf43974	Rest-API queries returns "Resource-not-found" for existing resources
CSCvf70284	Connection table not synchronized during upgrade in failover environment.
CSCvf81672	ASA Routes flushed after failover when etherchannel fails
CSCvf84839	Incorrect sequence numbers in selective ACKs with SSL decrypt/resign
CSCvg00265	ASA fails to rejoin the failover HA Or a cluster with insufficient memory error, OGS enabled
CSCvg05368	Upon joining cluster slave unit generates ASA-3-202010: NAT/PAT pool exhausted for all PAT'd conns
CSCvg15947	ASA WebVPN Smart-tunnel: DNS resolution failing on Windows 8 and Windows 10
CSCvg32530	ASA broadcasting packets sent to subnet address as destination IP
CSCvg39694	FP4120 / ASA 9.6(3)230 "established tcp" not working anymore after SW upgrade

Caveat ID Number	Description
CSCvg40735	GTP inspection may spike cpu usage
CSCvg53904	OSPF Not So Stubby Area Type 7 are not converted to Type 5
CSCvg58385	ASA reports incorrectly double input packets traffic on PPPoe/VPDN interface
CSCvg69028	ASA traceback in Thread name: idfw_proc on running "show access-list"
CSCvg69301	Traceback when ACL and NAT objects changed from IP to FQDN objects
CSCvg69380	ASA - rare cp processing corruption causes console lock
CSCvg73584	Heavy utilization in SNP APP ID
CSCvg74220	ASA Traceback in spin_lock_fair_mode_enqueue: Lock (np_conn_shrlock_t)
CSCvg74549	Traceback when trying to save/view access-list with object groups (display_hole_og)
CSCvg82650	RDP session does not establish after changing SSL certificate on ASA.
CSCvg83588	DOC: IPsec over NAT-T enabled by default
CSCvg91150	ASA Traceback in Assert "0" failed: file "timer_services.c"
CSCvg93503	On ASA "show module" not showing correct BIOS version
CSCvg95033	traceback in IKE Reciver Thread when "wr standby" is used
CSCvg95284	Reverse Route fails to install after crypto map enabled interface on ASA undergoes a shut/no shut
CSCvg95648	ASA: several ipv6 packets drop during failover when using sub-interface
CSCvg97594	Next Registration Attempt shows wrong time and it stops to register when ntp is configured
CSCvg98106	ASA ping to IPv6 address selects egress interface source IP instead of specified source IP
CSCvh02975	Inspect SIP is not handling the RTCP attribute in the SDP header
CSCvh07457	Traceback when configuring/modifying time range objects and acls
CSCvh08040	ACL hitcount is not increasing even though ACE hitcount is being increased.
CSCvh11175	Failover delay with coredump configured

Resolved Bugs

This section lists resolved bugs per release.

Resolved Bugs in Version 9.6(4)

The following table lists select resolved bugs at the time of this Release Note publication.

Caveat ID Number	Description
CSCto19051	Resolve any vulnerabilities in ASA/FTD lina Heimdal Kerberos code
CSCua53312	FQDN ACL entries might be incomplete if DNS response from server is large and truncated
CSCuj69650	ASA block new conns with "logging permit-hostdown" & TCP syslog is down
CSCuj98977	ASA Traceback in thread SSH when ran "show service set conn detail"
CSCuu90811	TLS CTP does not work in TLSv1.2 when GCM ciphers are used
CSCuv63875	ASA traceback in Thread Name:ci/console while running show ospf commands
CSCuw37752	FTP data conn scaling fails with dynamic PAT
CSCuz22961	Support for more than 255 characters for Split DNS value
CSCuz52474	Evaluation of pix-asa for OpenSSL May 2016
CSCuz72137	ASA dropping packets with "novalid adjacency" though valid ARP entry avail
CSCuz77293	OSPF multicast filter rules missing in cluster slave
CSCva42669	Huge Byte Count seen on IP protocol 97 flows with SFR
CSCva92997	9.7.1 traceback in snp_fp_qos
CSCvb28491	Unable to run show counters protocol ip
CSCvb53233	ASA 9.1(7)9 Traceback with %ASA-1-199010 and %ASA-1-716528 syslog messages
CSCvb75685	EZVPN NEM client can't reconnect after "no vpnclient enable" is entered
CSCvb81438	TCP connections might fail through a FTD cluster with inline mode interfaces
CSCvb91810	ASA - Incorrect interface-based route-lookup if more specific route exist out different interface
CSCvb97470	asa Rest-api - component monitoring - empty value/blank value
CSCvc07112	Implement detection and auto-fix capability for scheduler corruption problems
CSCvc24380	Traceback on thread name IKE Daemon at mqc_enable_qos_for_tunnel
CSCvc27704	Logs lost when TCP is used as transport protocol for Syslogs
CSCvc56526	CEP records edit page take minutes to load
CSCvc56919	Traffic drops for reverse UDP/TCP IPv6 traffic over IPv4 tunnel
CSCvc82270	ASA 1550 block gradual depletion
CSCvc83462	gzip compression not working via Webvpn
CSCvc85369	ASA does not respond to IPv6 MLD Query.

Caveat ID Number	Description
CSCvc91839	Unable to deploy policy on FTD devices due to wrong XML parsing
CSCvc96614	ASA: IKEv2 ipsec-proposal command removed if more than 9 proposals configured in single command
CSCvd00293	VTI - Some sessions do not get cleared from vpn-sessiondb
CSCvd01130	ASA TCP SIP inspection translation not working when IP phone is behind VPN tunnel
CSCvd08200	Slow Memory leak in ASA
CSCvd14266	ASA traceback in DATAPATH-41-16976 thread
CSCvd15843	Port Forwarding Session times out due to "vpn-idle-timeout" in group-policy while passing data
CSCvd17581	ASA IKEv1: Set non-zero SPI in INVALID_ID_INFO Notify
CSCvd20013	Traceback in "Thread Name: IPsec message handler" on EZVPN client
CSCvd20408	FTD: Interface capture on lina CLI causes all traffic to be dropped on data-plane
CSCvd21458	RSA keys may fail to synchronize between contexts in cluster setup
CSCvd24066	ASA drops web traffic when IM inspection is enabled.
CSCvd26699	ASA erroneously triggers syslog ID 201011
CSCvd26939	SNMP lists same Hostname for all Firepower Threat Defense managed devices
CSCvd29150	Mgmt route deletion removes data plane route too.
CSCvd33044	FTD traceback at "cli_xmlserver_thread" while deploying access-control policy
CSCvd33602	ASA does not send Epoch on TACACS Auditing packet
CSCvd33787	Assertion in syslog.c due to uauth
CSCvd35811	Traceback in thread name DATAPATH
CSCvd36992	Ether-channel: 5585-60 LACP state shows SYSTEM ID of old neighbor on interface which is in disabled
CSCvd37850	9.6.2 DHCPRA: Maximum relay bindings (500) exceeded
CSCvd43309	Access-lists not being matched for a newly created object-group
CSCvd47888	Cisco Adaptive Security Appliance Username Enumeration Information Disclosure Vuln.
CSCvd49262	Traceback when trying to save/view access-list with giant object groups (display_hole_og)

Caveat ID Number	Description
CSCvd49550	ASA with 9.5.1 and above does not show SXP socket when managment0/0 is used as src-ip
CSCvd50107	ASA traceback in Thread name: idfw_proc on running "show access-list", while displaying remark
CSCvd50389	RT#687120: Bookmark Issue with clientless VPN - SAML
CSCvd53381	ASA Traceback when saving/viewing the configuration due to time-range ACLs
CSCvd55115	ASA in cluster results in incorrect user group mappings between the Master and Slave
CSCvd55999	%ASA-3-216001: internal error in ci_cons_shell: thread data misuse
CSCvd58094	ASA traceback in ARP thread, PBR configured
CSCvd58321	Web folder filebrowser applet code signing certificate expired
CSCvd58417	DCERPC inspection drops packets and breaks communication
CSCvd61308	ASA backup in multicontext fails due to [Running Configurations] ERROR
CSCvd62509	ASA traceback in Thread Name: accept/http when ASDM is displaying "Access Rules"
CSCvd64416	ASA All contexts use the same EIGRP router-ID upon a reload
CSCvd64693	EIGRP routes wrongly being advertising on mgmt routing table vrf after disabling and enabling EIGRP
CSCvd65797	ASA may traceback when changing a NAT related object to fqdn
CSCvd66303	Error deploying ASAv on ESXi vCenter 6.5
CSCvd68518	Traceback in Thread Name: Unicorn Admin Handler
CSCvd69551	ASA fails to contact the secondary LDAP server with reactivation mode timed configured
CSCvd69804	ASA - Interface status change causes VPN traffic disconnect while using ipsec inner-routing-lookup
CSCvd71473	ASA: slow memory leak when using many DNS queries
CSCvd73468	Cluster director connection gets timed out with reason idle timeout
CSCvd76821	tcp-options md5 allow is pushed to slave units as tcp-options md5 clear
CSCvd76939	ASA policy-map configuration is not replicated to cluster slave
CSCvd77893	ASA may generate an assert traceback while modifying access-group
CSCvd78303	ARP functions fail after 213 days of uptime, drop with error 'punt-rate-limit-exceeded'

Caveat ID Number	Description
CSCvd79797	ASA local dns resolution fails when dns server is reachable through a site to site ipsec tunnel
CSCvd79863	FTD OSPF with ECMP, packets are sent to peer in down state for existing connections
CSCvd80721	In security context, cannot generate the SNMP events trap.
CSCvd80740	FTD-VPN: VPN RRI not getting synced between Master and Slave units
CSCvd82064	Cisco Adaptive Security Appliance Authenticated Cross-Site Scripting Vulnerability
CSCvd82265	Increase memory allocated to rest-agent on ASAv5
CSCvd86411	ASA 9.6.2.11 - Intermittent authentication with CTP uauth in cluster
CSCvd87211	ASA traceback when trying to remove configured capture
CSCvd87647	ASA traceback in Thread Name: fover_parse performing upgrade from 9.1.5 to 9.4.3
CSCvd89003	ASA traceback observed in Datapath due to SIP inspection
CSCvd89925	Unable to switch standby unit of the failover pair to active
CSCvd90096	WebVPN forces IE to use IE8 mode
CSCvd92423	ASA Traceback in Unicorn Proxy Thread
CSCvd92489	L2TP/IPsec fails when transform-set with mode transport is 11th in dynamic-map
CSCvd97249	Cisco Firepower Detection Engine SSL Decryption Memory Consumption Denial of Service Vulnerability
CSCvd97568	FTD traceback observed during failover synchronization.
CSCvd99476	The interactive icons on internal bookmark site not showing properly (+CSCO+0undefined)
CSCvd99859	ASA may drop DNS reply containing only additional RR of type TXT
CSCve02469	ASA Issue with bgp route summarization(auto-summary)and route advertisement
CSCve02854	SFR Backplane is pulling the public address for policy match instead of ASA inside address
CSCve03387	Proxy ARP information for SSH NLP NAT is not updating on the FTD upon failover
CSCve03974	ASA with FirePOWER services module generates traceback and reload
CSCve04326	Slave should have use CCL to forward traffic instead of blackholing when egress interface is down
CSCve05841	ASA reloaded while joining cluster and active as slave
CSCve06367	Show Crypto Acclerator shows status as booting for hardware devices

Caveat ID Number	Description
CSCve06436	Routes do not sync properly between different minor versions during hitless upgrade
CSCve07856	CRL verification fails due to incorrect KU after CSCvd41423
CSCve08664	Dist-S2S: tunnels stay up even after passing vpn idle timeout in Multimode
CSCve08898	Memory leak with capture with trace and clear capture
CSCve08947	In multi-context ASA drops traffic sourced from certain ports when interface PAT is used
CSCve09249	ASA: Active FTP not working with extended keyword in NAT.
CSCve12654	ASA clustering to support rollback feature with CSM
CSCve13410	Upgrading the ASA results in No Valid adjacency due to track configure on the route
CSCve15873	ASA: Multicast packets getting dropped starting code 9.6.3
CSCve18293	ASA traceback observed in datapath
CSCve18880	Username is not fetched from certificate when certificate map is used in clientless portal
CSCve19179	Cisco Adaptive Security Appliance WebVPN Cross-Site Scripting Vulnerability
CSCve20346	ASA SNI connection fails after upgrade - no shared cipher
CSCve20438	"activate-tunnel-group-scripts" not available in 9.6.3.1
CSCve20980	CSCOGet_origin wrapper doesn't handle 'origin' property if it belongs to Location object
CSCve23033	ICMP Unreachables (PMTU) dropped indicating "Routing failed to locate next hop"
CSCve23091	Auto-RP packet is dropped due to no-route - No route to host
CSCve23155	BTF not supported on ASA application on FXOS Chassis, but smart licensing show this feature enabled.
CSCve23784	ASA may traceback on displaying access-list config or saving running config
CSCve24088	Smart Licensing ID cert renewal failure should not deregister product instance
CSCve24299	Traceback in Thread Name: IP RIB Update when routes are redistributed
CSCve25577	Interfaces on SLAVES in shutdown if FMC deployment results in failure
CSCve28027	Calls not working with CUCI Lync version 11.6.3 on ASA
CSCve29989	ASA - Traceback in DATAPATH during PAT pool socket allocation
CSCve31809	ASA corrupt dst mac address of return traffic from l2tp client

Caveat ID Number	Description
CSCve31880	network_udpmod_get not releasing shr_lock in rare error case
CSCve35799	CPU Hog CI_CONSOLE Traceback During Configuration
CSCve37948	ASA does not install routes learned via OSPF over IPSec using UDP/4500
CSCve42460	"NSF IETF/CISCO" commands getting removed on reload
CSCve42583	ASA: IPv6 protocol X rule for passing through FW is dropping packets with Invalid IP length message
CSCve43146	AnyConnect new customization creation fails on ASDM for all ASA versions above 9.5(3)
CSCve44561	ASA sends the ICMP unreachable type 3 code 4 in the wrong direction when SFR redirection enabled
CSCve46883	FTD Diagnostic Interface does Proxy ARP for br1 management subnet
CSCve47393	OSPF Rogue LSA with maximum sequence number vulnerability
CSCve48105	Slave reports Master's interface status as "init" while it is up
CSCve50118	ASA Memory Leak - RSA toolkit
CSCve53582	SSH Connections to ASA fail with SLA monitoring & nonzero floating-conn timeout
CSCve53783	"service resetoutside" impacts to-the-device traffic on all interfaces, behaves different on Standby
CSCve57150	vpn vlan mapping issue
CSCve57375	CPU hog in CP Processing thread due to huge number of sunrpc sessions
CSCve57548	ASA- Traceback in 'Thread Name : Datapath' on crypto_SSL functions
CSCve58709	ASA 9.5.1 onwards, Traffic incorrectly routed instead of management interface
CSCve60829	ASA Cluster : Potential UDP loop on cluster link with PAT pool
CSCve61284	ASA Log message 414003 may be generated with bogus IP data when TCP Syslog Server down
CSCve62358	ASA 2048 block depletion when PBR next-hop is interface address
CSCve63762	ASASM: Interface vlans going to admin down after reload.
CSCve71712	webvpn-l7-rewriter: Jira 7.3.0's login page through WebVPN portal does not render completely
CSCve72155	Memory leak at location "snp_fp_encrypt" when syslog server is reachable over the VPN tunnel
CSCve72201	ASA Webvpn Rewritter issue. Unable to browse tabs of WebSite over Clientless VPN

Caveat ID Number	Description
CSCve72227	IPsec SA fail to come up and flap with more than 1000 IPsec SA count in ASA5506/5508/5516
CSCve72964	Traceback in DATAPATH-1-2084 ASA 9.(8)1
CSCve73025	All 1700 "4 byte blocks" were depleted after a weekend VPN load test.
CSCve73556	ASA traceback on websns_rcv_tcp
CSCve75132	Start of Flow Block event has incorrect number of Initiator Bytes
CSCve77440	Traceback in Unicorn Proxy Thread due to Webvpn
CSCve78986	ASA/ 9.6.3 // WebVPN Smart tunnel works but floods windows with event viewer
CSCve85698	ASA WebVPN Rewriter: WebVPN bookmark scholar.google.com not properly written
CSCve91068	Cisco Adaptive Security Appliance HREF Cross Site Scripting Vulnerability
CSCve91223	Standby ASA rejects NAT rule when dest overlaps with interface IP, Active allows this
CSCve94349	SNMP::User is not added to a user-list or host ,after reconfigure it.
CSCve94886	Traceback on ASA with Firepower Services during NAT rule changes and packet capture enabled
CSCve95969	Unable to scale the flash virtualisation feature up to 250 contexts
CSCve97831	CDA agent stucks in 'Probing' when domain-lookup is enable
CSCve97844	ASA OSPF interface gets stuck in State DOWN (waiting for NSF) after 3rd failover
CSCve97874	ASA: Low free DMA Memory on versions 9.6 and later
CSCvf01762	Evaluation for the vulnerabilities CVE-2017-1000364 and CVE-2017-1000366
CSCvf01873	Regex is not matching for HTTP argument field
CSCvf03676	Ports not getting reserved on ASA after adding snmp configuration.
CSCvf07075	ASA - Crypto accelerator traceback in a loop
CSCvf11695	Duplicate host entries in flow-export action cause traceback after policy deployment
CSCvf14391	multicast traffic sourced from anyconnect pool dropped due to reverse path checked.
CSCvf16142	ASA-5-720012:(VPN-Secondary)Failed to update IPSec failover runtime data in ASA cluster environment
CSCvf16310	IPv6 Addresses intermittently assigned to AnyConnect clients
CSCvf16429	Ikev2 Remote Access client sessions stuck in Delete state

Caveat ID Number	Description
CSCvf16808	Unable to SSH to Active Unit//TCP connection Limit Exceeded
CSCvf17214	ASA Exports ECDSA as corrupted PKCS12
CSCvf17222	SAML 2.0 || (5525) 9.7.1 ASA : ASA compiler not taking the sign-in URL for SAML authentication.
CSCvf21556	ASA: SNMP Host Group not working as required for multi context configuration.
CSCvf22190	ASA memory leak - DTLS sessions
CSCvf24063	ASA5585 traceback in DATAPATH - snp_vpn_process_natt_pkt
CSCvf24387	EC Certificates that are imported to the ASA in PKCS12s cannot be used for SSL
CSCvf25666	An ASA with low free memory fails to join existing cluster and could traceback and reload
CSCvf28292	DAP config restored but inactive after backup restore
CSCvf28749	ASA not sending register stop when mroute is configured
CSCvf31539	ASA Connections stuck in idle state with DCD enabled
CSCvf34791	Install 6.2.2-1290 sfr on a ASA with firepower - asa cores
CSCvf38655	ASA traceback in fover_parse after version up
CSCvf39679	Unable to add new networks to existing EIGRP configuration
CSCvf41547	traceback in watchdog process
CSCvf43019	Webvpn rewriter failing for internal URL
CSCvf43150	ASA// 9.6 // FTP inspection does not allocate new NAT entrie for DATA traffic on Active FTP with PAT
CSCvf43650	OSPF route not getting installed on peer devices when an ASA failover happens with NSF enabled
CSCvf44142	ASA 9.x: DNS inspection appending "0" on PTR query
CSCvf44950	iOS and OS X IKEv2 Native Clients unable to connect to ASA with EAP-TLS
CSCvf46732	Contexts are missing on ASA once Chassis reloads after becoming Master on 9.6 code
CSCvf49899	ENH: GOID allocation and sync cleanup
CSCvf51066	ASA on FXOS is sending SNMP Ifspeed OID (1.3.6.1.2.1.2.2.1.5) response value = 0
CSCvf54081	TLS version 1.1 connection failed no shared signature algorithms@t1_lib.c:3106
CSCvf54981	ASA - 80 Byte memory block depletion

Caveat ID Number	Description
CSCvf56506	ASA 9.6(2), 9.6(3) traceback in DataPath
CSCvf56917	ASA doesn't send LACP PDU during port flap in port-channel
CSCvf57908	Transparent Firewall: Ethertype ACLs installed with incorrect DSAP value
CSCvf61419	Traceback in thread DATAPATH due to NAT
CSCvf62365	ASA: entConfigChange is unexpectedly sent when secondary ASA is reloaded
CSCvf63108	ASA drops the IGMP Report packet which has Source IP address 0.0.0.0
CSCvf64643	ERROR: Captive-portal port not available. Try again
CSCvf72068	FXOS - ASA/FTD standby unit in transparent mode may still traffic for offloaded flows
CSCvf74218	ASAv image in AWS GovCloud not working in Hourly Billing Mode
CSCvf76281	IKEv2 RA cert auth. Unable to allocate new session. Max sessions reached
CSCvf77377	Hostscan: Errors in cscan.log downloading Microsoft and Panda .dll files
CSCvf79262	OpenSSL CVE-2017-3735 "incorrect text display of the certificate"
CSCvf80539	management-only comes back after reboot
CSCvf81222	Memory leak in 112 byte bin when packet hits PBR and connection is built
CSCvf81932	'Incomplete command' error with some inspects due to K7 license
CSCvf82733	"crypto ikev1 enable" command not installed on FTD CLI
CSCvf83709	Slave kicked out due to CCL link failure and rejoins, but loses v3 user in multiple context mode
CSCvf85065	ASA: Traceback by Thread Name idfw_proc
CSCvf87899	ASA - rare scheduler corruption causes console lock
CSCvf89504	ASA cluster intermittently drop IP fragments when NAT is involved
CSCvf90278	ASA/FTD traceback when clearing capture - assertion "0" failed: file "mps_hash_table_debug.c"
CSCvf94973	ASA on FP 2100 traceback when uploading AnyConnect image via ASDM
CSCvg01016	ASA does not create pinholes for DCERPC inspection, debug dcerpc shows "MEOW not found".
CSCvg01132	ASA : After upgrading from 9.2(4) to 9.2(4)18 serial connection hangs
CSCvg05250	"clear local-host <IP>" deletes all stub flows present in the entire ASA cluster for all hosts/conns

Caveat ID Number	Description
CSCvg08891	iPhone IKEv2 PKI leaks over Wi-Fi using local certificate authentication on ASA 5555 9.6.3
CSCvg09778	ASA-SSP HA reload in CP Processing due to DNS inspect
CSCvg17478	traceback with Show OSPF Database Commands
CSCvg20796	ASA local DNS resolution fails when DNS server is reachable over a site to site sec VPN tunnel
CSCvg21077	One node rejoined and traffic restarted will cause the unit 100% CPU due to snpi_untranslate
CSCvg25175	ASA getting stuck in hung state because of STATIC NAT configuration for SNMP ports
CSCvg25538	FORWARD PORT: 1550/2048/9344 byte memory block depletion due to identity UDP traffic
CSCvg25694	Assert Traceback, thread name : cli_xml_server
CSCvg30391	ASA SNMP OID for ifInDiscards always 0
CSCvg32179	Javascript elmements rewriter issue
CSCvg33669	"OCTEON:DROQ[8] idx: 494 len:0" message appearing on console access of the device
CSCvg33985	ASA Webvpn Username field should not accept XSS executable scripts.
CSCvg38437	ASA AC client PKI username from cert longer than 64 characters - radius username is cut short to 64
CSCvg45952	ASA traceback: thread name scansafe
CSCvg51984	High CPU in IKE Daemon causing slow convergence of VPN tunnels in a scaled environment
CSCvg52995	Unable to save configuration in system context after enabling password encryption in ASA
CSCvg53981	"dir /recursive cache:/stc" and "dir cache:stc/2/" list AnyConnect.xsd differently on ASA9.8.2
CSCvg57954	Modifying service object-groups (add and remove objects) removes ACE
CSCvg61829	SSH/Telnet Traffic, 3-WHS, ACK packets with data is getting dropped - reason (intercept-unexpected)
CSCvg66606	GTP echo response is dropped in ASA cluster
CSCvg67135	ASA backs out of connection when it receives Server Key exchange with named curve as x25519

Caveat ID Number	Description
CSCvg82932	Memory Leaking on ASA with vpnfol_memory_allocate and vpnfol_data_dyn_string_allocator
CSCvg89102	ASA:multi-session command being configured after write erase

Resolved Bugs in Version 9.6(3.1)

The following table lists select resolved bugs at the time of this Release Note publication.

Caveat ID Number	Description
CSCuj69650	ASA block new conns with "logging permit-hostdown" & TCP syslog is down
CSCum28756	ASA: Auth failures for SNMPv3 polling after unit rejoins cluster
CSCum74032	ASA traceback on standby when SNMP polling
CSCup37416	Stale VPN Context entries cause ASA to stop encrypting traffic
CSCuq80704	ASA classifies TCP packets as PAWS failure incorrectly
CSCus29600	dhcprelay interface doesn't change by changing route
CSCut07712	ASA - TO the box traffic break due to int. missing in asp table routing
CSCuu50708	ASA Traceback on 9.1.5.19
CSCuv61791	CWS redirection on ASA may corrupt sequence numbers with https traffic
CSCuv86562	Traceback: ASA crash in thread name fover_health_monitoring_thread
CSCuw71147	Traceback in Unicorn Proxy Thread, in http_header_by_name
CSCuw88759	ASA: Protocol and Status showing UP without connecting the interface
CSCuw95262	After some time flash operations fail and configuration can not be saved
CSCux17527	ASA memory leak related to Botnet
CSCux92157	ASA Traceback Assert in Thread Name: ssh_init with component ssh
CSCux98029	ASA reloads with traceback in thread name DATAPATH or CP Processing
CSCuy22155	ASA generates unexpected syslog messages with mcast routing disabled
CSCuy43438	L2TP over IPSec can not be connected after disconnection from client.
CSCuy47545	http config missing in multicontext after reload of stdby 916.9 or later
CSCuy55468	Unicorn Proxy Thread causing CP contention
CSCuy89288	AnyConnect DTLS on-demand DPDs are not sent intermittently
CSCuz09255	ASA does not respond to NS in Active/Active HA

Caveat ID Number	Description
CSCuz42390	ASA Stateful failover for DRP works intermittently
CSCuz44968	Commands not installed on Standby due to parser switch
CSCuz64603	GTP traceback at gtp_update_sig_conn_timestamp while processing data
CSCuz72244	Error Indication dropped with Null TID MBReq dropped with no Ctrl F-TEID
CSCuz77293	OSPF multicast filter rules missing in cluster slave
CSCuz80281	IPv6 neighbor discovery packet processing behavior
CSCuz87146	nat-t-disable feature is not working for ikev2
CSCuz89989	Ikev1 tunnel drops with reason " Peer Address Changed"
CSCuz90648	2048/1550/9344 Byte block leak cause traffic disruption & module failure
CSCuz92074	ASA with PAT fails to untranslate SIP Via field that doesnt contain port
CSCuz94158	Hash miscalculation for "Any" address on inside
CSCuz94862	IKEv2: Data rekey collisions can cause inactive IPsec SAs to get stuck
CSCuz94890	ASAv ACKs FIN before all data is received during smart licensing exch
CSCuz95703	management-only cli not available in user context of QP-D
CSCuz98704	Traceback in CP Processing thread after upgrade
CSCva00190	ASA 9.4.2.6 High CPU due to CTM message handler due to chip resets
CSCva00939	Remove ACL warning messages in show access-list when FQDN is resolved
CSCva01570	Unexpected end of file logon.html in WebVPN
CSCva02655	ASA sends invalid interface id to SFR for clientless VPN traffic
CSCva02817	ASA not rate limiting with DSCP bit set from the Server
CSCva03607	show service-policy output reporting incorrect values
CSCva05513	ASA: SLA Monitor not working with floating timeout configured to nonzero
CSCva07268	Unable to auth a 2nd time via clientless after ASA upgrade
CSCva10054	ASA ASSERT traceback in DATAPATH due to sctp inspection
CSCva12520	snmpwalk not working for some NAT OIDs
CSCva15911	On reloading the ASA, ASA mounts SSD as disk 0, instead of the flash.
CSCva16471	IPv6 OSPF routes do not update when a lower metric route is advertised
CSCva22048	ASA: SIP Call Drops with PAT when same media port used in multiple calls

Caveat ID Number	Description
CSCva24799	TLS Proxy feature missing client trust-point command
CSCva24924	ASA SM on 9300 reloads multi-context over SSH when config-url is entered
CSCva26771	ASA : PBR Mem leak as packet dropped
CSCva31378	ASA treaceback at Thread Name: rtcli async executor process
CSCva32092	OSPFv3/IPv6 flapping every 30 min between ASA cluster and 4500
CSCva35439	ASA DATAPATH traceback (Cluster)
CSCva36202	BGP Socket not open in ASA after reload
CSCva36884	Cisco ASA Cross Site Scripting SSLVPN Vulnerability
CSCva38556	Cisco ASA Input Validation File Injection Vulnerability
CSCva39094	ASA traceback in CLI thread while making MPF changes
CSCva39804	Interfaces get deleted on SFR during cluster rejoining
CSCva40844	Crypto accelerator ring timeout causes packet drops
CSCva43746	ASA 'show inventory' shows 'Driver Error, invalid query ready'
CSCva43992	IKEv2 RA cert auth. Unable to allocate new session. Max sessions reached
CSCva45590	ASA OSPFv3 interface ID changes upon disabling/enabling failover
CSCva46920	Traceback in Thread Name: ssh when issuing show tls-proxy session detail
CSCva47608	SCTP MH:pin hole removed and added freq on standby with dual nat
CSCva49256	memory leak in ssh
CSCva50554	ASA uses "::" for host IP addresses if booted with an improper config
CSCva50838	ASA capture type isakmp not saving reassembled rfc7383 IKEv2 packets
CSCva52514	ASAv-Azure: waagent may reload when asav deployed with load balancer
CSCva53581	Increasing the global ARP request pool
CSCva56114	CISCO-MEMORY-POOL-MIB returns incorrect values for heapcache
CSCva56343	Clustering: TFW asynchronous flow packet drop due to L2 entry timeout
CSCva60283	Two Upstream Kernel Patches for ASAv in Azure
CSCva62667	Shut down interfaces shows up in ASP routing table
CSCva62861	uauth is failed after failover
CSCva66278	SmartLic: Inter-chassis master switchover license race condition

Caveat ID Number	Description
CSCva68364	SNMPv3 active engineID is not reset when ASA is replaced
CSCva68987	ASA drops ICMP request packets when ICMP inspection is disabled
CSCva69346	Unable to relay DHCP discover packet from ASA when NAT is matched
CSCva69584	OSPF generates Type-5 LSA with incorrect mask, which gets stuck in LSDB
CSCva69799	ASA stuck in boot loop due to FIPS Self-Test failure
CSCva70095	ASA negotiates TLS1.2 when server in tls-proxy
CSCva70979	failover descriptor is not updated in Port Channel interfaces
CSCva71783	ICMP error packets in response to reply packets are dropped
CSCva76568	ASA : Enabling IKEv1/IKEv2 opens RADIUS ports
CSCva77852	ipsecvpn-ikev2_oth: 5525 9.4.2.11 traceback in Thread Name: IKEv2 Daemon
CSCva81412	ASR9000 BGP Graceful Restart doesnt work as expected
CSCva81749	IPV6 address not assigned when connecting via IPSEC protocol
CSCva84079	ASAv hangs often during reboot
CSCva84625	ASAv show hostname generates smart licensing authorization request
CSCva84635	ASA: CHILD_SA collision brings down IKEv2 SA
CSCva85382	ASA memory leak for CTS SGT mappings
CSCva85933	FTD - 6.1 - redistribute connected is redistributing Internal-Data (NLP)
CSCva86626	HTML5: Guacamole server requires page refresh
CSCva87077	GTP traceback at gtpv1_process_msg for echo response
CSCva87160	OTP authentication is not working for clientless ssl vpn
CSCva88796	AnyConnect Sessions Cannot Connect Due to Stuck L2TP Uauth Sessions
CSCva90419	issuer-name falsely detecting duplicates in certificate map using attr
CSCva90806	ASA Traceback when issue 'show asp table classify domain permit'
CSCva91420	ASA Traceback in CTM Message Handler
CSCva92151	Cisco ASA SNMP Remote Code Execution Vulnerability
CSCva92813	ASA Cluster DHCP Relay doesn't forward the server replies to the client
CSCva92975	ASA 5585-60 dropping out of cluster with traceback
CSCva94702	Enqueue failures on DP-CP queue may stall inspected TCP connection

Caveat ID Number	Description
CSCva95686	FTD: 9k byte block depletion leads to dropped traffic
CSCva97863	971 EST - Console hang on show capture
CSCva98240	SIP: Address from Route: header not translated correctly
CSCva98532	FTD inline is not blocking MPLS-switched TCP session it should block
CSCvb03994	Traceback in IKE_DBG
CSCvb04685	Unable to delete the SNMP config
CSCvb05667	H.323 inspection causes Traceback in Thread Name: CP Processing
CSCvb05787	traceback in network udpmod_get after anyconnect test load application
CSCvb08776	Internal ATA Compact Flash size is incorrectly shown in "show version"
CSCvb13690	ASA : Botnet update fails with a lot of Errors
CSCvb13737	wr mem/ wr standby is not syncing configs on standby
CSCvb14997	ASA DHCP Relay rewrites netmask and gw received as part of DHCP Offer
CSCvb15265	ASA Page fault traceback in Thread Name: DATAPATH
CSCvb19251	ASA as DHCP relay drops DHCP 150 Inform message
CSCvb19843	Buffer Overflow in ASA Leads to Remote Code Execution
CSCvb20256	Sweet32 Vulnerability in ASA's SSH Implementation
CSCvb21922	Remove ACL warning messages in show access-list when FQDN is unresolved
CSCvb22435	ASA Traceback in thread name CP Processing due to DCERPC inspection
CSCvb22848	ASA 9.1.7-9 crash in Thread Name: NIC status poll
CSCvb25139	IPv6 DNS packets getting malformed when DNS inspection is enabled.
CSCvb26119	Webvpn rewriter failing on matterport.com
CSCvb27868	ASA 1550 block depletion with multi-context transparent firewall
CSCvb28491	Unable to run show counters protocol ip
CSCvb29411	AAA authentication/authorization fails if only accessible via mgmt vrf
CSCvb29688	Stale VPN Context entries cause ASA to stop encrypting traffic despite fix for CSCup37416
CSCvb30445	ASA may generate DATAPATH Traceback with policy-based routing enabled
CSCvb31055	ASA Multiple Context SNMP PAT Interface Missing

Caveat ID Number	Description
CSCvb31833	Traceback : ASA with Threadname: DATAPATH-0-1790
CSCvb32297	WebVPN:VNC plugin:Java:Connection reset by peer: socket write error
CSCvb32341	ASA traceback with passive-interface default on 9.6(2)
CSCvb33009	Cisco ASA Signature Verification Misleading Digital Signing Text On Boot
CSCvb33013	Cisco ASA Remove Mis-leading Secure Boot commands on non-SB hardware
CSCvb36199	Thread Name: snmp ASA5585-SSP-2 running 9.6.2 traceback
CSCvb37456	Failover after IKE rekey fails to initiate ph1 rekey on act device
CSCvb38522	ASA PKI OCSP failing - CRYPTO_PKI: failed to decode OCSP response data.
CSCvb39147	Lower NFS throughput rate on Cisco ASA platform
CSCvb40417	nlp_int_tap routes seen in ASA "sh route" command
CSCvb40818	nlp information seen in ipv6 commands
CSCvb40847	ASA not sending Authen Session End log if user logs out manually
CSCvb41097	GTPv2 Dropping instance 1 handoffs
CSCvb43120	ASA Traceback in Checkheaps Thread
CSCvb45039	ASA traceback with Thread Name aaa_shim_thread
CSCvb46531	ASDM : memory usage reading incorrect for ASAv 9.6.2
CSCvb47006	ASA traceback observed on auto-update thread.
CSCvb48640	Evaluation of pix-asa for Openssl September 2016
CSCvb49264	Delete Bearer Req fails to delete second default bearer after v2 Handoff callflow.
CSCvb49273	Traceback triggered by CoA on ASA when sending/receiving to/from ISE
CSCvb49445	IKEv2: It is NOT cleaning the sessions after disconnected from the client.
CSCvb50301	ASA traceback at Thread Name: rtcli
CSCvb50609	RADIUS authorization request does not send Called-Station-ID attribute
CSCvb50750	Lina core during failover with sip traffic
CSCvb52157	viewer_dart.js file not loading correctly
CSCvb52492	VPN tunnels are lost after failover due to OSPF route issue
CSCvb52988	ASA Traceback Thread Name: emweb/https
CSCvb53094	ASA : Discrepancy in used memory calculation for Multiple context firewall

Caveat ID Number	Description
CSCvb55721	GARP flood done by ASAs in multi-site cluster using the site-ip address
CSCvb57817	EIGRP: Need to add large number error handling when getting scaled bandwidth
CSCvb58087	Object-group-search redundant service group objects are incorrectly removed
CSCvb63503	AAA session handle leak with IKEv2 when denied due to time range
CSCvb63819	ASA-SM traceback with Thread : fover_parse during upgrade OS 9.1.6 to 9.4.3
CSCvb64161	ASA fairly infrequently rewrites the dest MAC address of multicast packet for client
CSCvb66593	webvpn_state cookie information disclosure in url
CSCvb68766	ASA traceback at Thread Name: IKE Daemon.
CSCvb74084	SCP fails in 962
CSCvb74249	ASA dropping traffic with TCP syslog configured in multicontext mode
CSCvb75266	ASA - ACL remark displayed incorrectly in the Packet Tracer tool's XML output
CSCvb75685	EZVPN NEM client can't reconnect after "no vpnclient enable" is entered
CSCvb78614	4GE-SSM RJ45 interface may drop traffic due to interface "rate limit drops"
CSCvb83446	v1 PDP may get deleted on parse IE failure
CSCvb85624	Evaluation of pix-asa for CVE-2016-5195 (DIRTY CoW)
CSCvb87586	Failed to ssh management interface after failover and plug-in/out
CSCvb88126	ASA: Stuck uauth entry rejects AnyConnect connection despite fix for CSCuu48197
CSCvb88358	webvpn-l7-rewriter: 5515 9.1.6 Content Rewrite Problem for ASA Web Bookmark
CSCvb89988	WebVPN: Internal page login button not working through rewriter
CSCvb92125	ASA drops DNS PTR Reply with reason Label length exceeded during rewrite
CSCvb92417	Cluster ASA drops to-the-box ICMP replies with reason "inspect-icmp-seq-num-not-matched"
CSCvb92548	ASA matches incorrect ACL with object-group-search enabled
CSCvb92823	ASA SIP inspection may delay transmission of 200 OK when embedded with NOTIFY
CSCvc00015	Incorrect behaviour when SNMP polling is done on virtual IP of an ASA cluster.
CSCvc00689	ASA : memory leak due to ikev2
CSCvc00760	RDP Plugin Connection failed with error
CSCvc01685	PLR: ASAv generates invalid reservation code

Caveat ID Number	Description
CSCvc04741	ASA DHCP relay is incompatible with intercept-dhcp feature
CSCvc05005	ASA cluster TCP/SSL ports are not displayed on LISTEN state
CSCvc06150	ASA unable to add multiple attribute entries in a certificate map
CSCvc07112	Implement detection and auto-fix capability for scheduler corruption problems
CSCvc07330	ASAv may crash when running webvpn
CSCvc14190	ASA fails SSL VPN session establishment with EC under load
CSCvc14448	9.6.2 - Traceback during AnyConnect IKEv2 Performance Test
CSCvc14502	ASA multicontext disallowing new conns with TCP syslog unreachable and logging permit-hostdown set
CSCvc16330	ASA-SM 9.5.2 inspect-sctp licensing breaks existing deployments
CSCvc19318	ASA traceback at Thread Name: sch_syslog
CSCvc22193	DSCP Markings Not Copied to Outer IP Header With IPsec Encapsulation
CSCvc23838	Cisco ASA Heap Overflow in Webvpn CIFS
CSCvc24380	Traceback on thread name IKE Daemon at mqc_enable_qos_for_tunnel
CSCvc24657	MIB object cempMemPoolHCUsed disappeared
CSCvc24788	ASA: OspfV3 routes are not getting installed
CSCvc25195	ASA portal reveals that multiple context is configured when anyconnect is deployed.
CSCvc25281	Error synchronizing the SNMPv3 user after rebooting a cluster unit
CSCvc25409	ASA memory leak in CloneOctetString when using SNMP polling
CSCvc33796	Implement speed improvements for ACL and NAT table compilation
CSCvc36535	ASA traceback in Thread Name: ssh, rip igb_disable_rx_queues after no shutdown of interface
CSCvc36805	Firepower Threat Defense (FTD) IKEv2 NAT-T gets disabled after reboot
CSCvc37557	SSL connection hangs between ASA and backend server in clientless WebVPN
CSCvc38425	ASA with FirePOWER module generates traceback and reloads or causes process not running
CSCvc39121	Anyconnect address assignment fails using external DHCP server when ASA is in Multi-context Mode
CSCvc44240	ASA clustering: mac-address cmd is ignored on spanned port-channel interface in 9.6.2

Caveat ID Number	Description
CSCvc48640	ASA not update access-list dynamically when forward-reference enable is configured
CSCvc52072	Webvpn portal not displayed corrrectly for connections landing on default webvpn group.
CSCvc52272	ASA inspection-MPF ACL changes are not getting ordered correctly in the ASP Table
CSCvc52504	ASA may traceback with Thread Name: Unicorn Admin Handler
CSCvc52879	Reloading Active unit in Active/Standby ASA failover pair is not triggering a failover.
CSCvc55674	ASA: IPSec SA failed to come up
CSCvc55974	ikev2 handles get leaked in a L2L setup
CSCvc58272	ASA incorrectly processing negative numbers in wrappers, resulting in graphical webvpn issue
CSCvc60254	SIP: 200 OK messages with multiple seqments not reassembled correctly
CSCvc60964	ASA L3 Cluster: DHCP relay drops DHCPOFFER in case of asymmetric routing
CSCvc61818	CTP after failed attempt sends the domain along with the username
CSCvc61845	RDP plugin activex Full Screen option is not available with ASA 9.6.2 version
CSCvc62252	Tracking route is up while the reachability is down
CSCvc62556	Traceback in ASA Cluster Thread Name: qos_metric_daemon
CSCvc65409	Traceback observed on gtpv2_process_msg on cluster
CSCvc68229	BGP's BFD support code opens tcp/udp 3784 and 3785 to bypass access-lists
CSCvc79077	ASA watchdog traceback during cluster config sync with rest-api enabled
CSCvc79371	ASA nat pool not getting updated correctly.
CSCvc79454	Unable to configure ssh public auth for script users
CSCvc79569	mac-address auto command uses default prefix of 1 on ASA5585-X
CSCvc82146	ASA traceback in threadname Datapath
CSCvc86554	Traceback: ASA 9.5(2)11 crash Active
CSCvc87914	ASA traceback and Reload on Config Sync Failure
CSCvc88115	ASA Clustering IDFW not updating user mappings
CSCvc88411	1550-byte block depletion seen due to Radius Accounting packets
CSCvc91839	Unable to deploy policy on FTD devices due to wrong XML parsing
CSCvc93947	ASA(9.1.7.12):Connection entries created for multicast streams through standby ASA.

Caveat ID Number	Description
CSCvc97734	Deployment fails when management-only enabled on port-channel interface
CSCvd01736	L2TP connects only sometimes when DHCP used
CSCvd03261	ASAv Goes Unresponsive / VPN fails to function after restart
CSCvd03343	Unable to configure SSH public key auth for non-system contexts
CSCvd06022	ASA-FP9300 Crashed in thread name IPSEC MESSAGE HANDLER after upgrade
CSCvd06527	SNMPv3 linkup/linkdown should be generated through admin context
CSCvd08200	Slow Memory leak in ASA
CSCvd08479	ACL last hit-cnt counter shows incorrect time
CSCvd08709	asymetric path icmp traffic fails through distributed clustering
CSCvd14266	ASA traceback in DATAPATH-41-16976 thread
CSCvd15843	Port Forwarding Session times out due to "vpn-idle-timeout" in group-policy while passing data
CSCvd21154	5585 does not unbundle its data intfs for 30 seconds after leaving cluste
CSCvd21541	Cannot delete port-object once created under the Service object group in ASA 944
CSCvd21665	ASA w/ RRI and OSPF : Fails to flush route from ASP routing table
CSCvd23016	ASA may traceback when copying capture out using tftp
CSCvd23471	ASA may traceback while loading a large context config during bootup
CSCvd24066	ASA drops web traffic when IM inspection is enabled.
CSCvd26939	SNMP lists same Hostname for all FTD managed devices
CSCvd28859	ASA: PBR Memory leak for ICMP traffic
CSCvd29150	Mgmt route deletion removes data plane route too.
CSCvd33044	FTD crash at "cli_xmlserver_thread" while deploying access-control policy
CSCvd33787	Assertion in syslog.c due to uauth
CSCvd39113	Cluster C-Hash table is updated with one more unit despite the new unit didn't join the setup
CSCvd41052	Scheduler Queue Corruption leads to connectivity failures or failover problems after 9.6(2)
CSCvd41423	CRL must be signed by certificate containing cRLSign key usage
CSCvd43309	Access-lists not being matched for a newly created object-group

Caveat ID Number	Description
CSCvd47781	ASA traceback while doing in-service upgrade
CSCvd49262	Traceback when trying to save/view access-list with giant object groups (display_hole_og)
CSCvd49550	ASA with 9.5.1 and above does not show SXP socket when managment0/0 is used as src-ip
CSCvd50389	RT#687120: Bookmark Issue with clientless VPN - SAML
CSCvd53884	Firepower (SFR) module data plane down after reload of module
CSCvd55983	Traceback in Thread Name: dhcp_daemon
CSCvd58417	DCERPC inspection drops packets and breaks communication
CSCvd61308	ASA backup in multicontext fails due to [Running Configurations] ERROR
CSCvd62509	ASA traceback in Thread Name: accept/http when ASDM is displaying "Access Rules"
CSCvd63718	ASA-FP9300 Crashed in thread name IPSEC MESSAGE HANDLER
CSCvd64416	ASA All contexts use the same EIGRP router-ID upon a reload
CSCvd64693	EIGRP routes wrongly being advertising on mgmt routing table vrf after disabling and enabling EIGRP
CSCvd65797	ASA May crash when changing a NAT related object to fqdn
CSCvd66303	Error deploying ASAv on ESXi vCenter 6.5
CSCvd69804	ASA - Interface status change causes VPN traffic disconnect while using ipsec inner-routing-lookup
CSCvd73468	Cluster director connection gets timed out with reason idle timeout
CSCvd76939	ASA policy-map configuration is not replicated to cluster slave
CSCvd77893	ASA may generate an assert traceback while modifying access-group
CSCvd78303	ARP functions fail after 213 days of uptime, drop with error 'punt-rate-limit-exceeded'

Resolved Bugs in Version 9.6(2)

The following table lists select resolved bugs at the time of this Release Note publication.

Caveat ID Number	Description
CSCsh75522	Increase Content-length counter from 4 to 8 byte size
CSCtw90511	Packet captures cause CPU spike on Multi-Core platforms due to spin_lock
CSCuh89500	ASA: ifSpeed/ifHighSpeed not populated by SNMP for port-channel

Caveat ID Number	Description
CSCum70304	FIPS self test power on fails - fipsPostDrbgKat
CSCup37416	Stale VPN Context entries cause ASA to stop encrypting traffic
CSCuu40736	Capture <name> type inline-tag interface <name> defaults to tag value 0
CSCuv09640	ASA: "Auto-Enable" feature not working with SSH configured with PKF
CSCuw51576	SSH connections are not timed out on ASA (stuck in rtcli)
CSCuw55813	Standby ASA traceback in Thread Name: EIGRP-IPv4
CSCux08783	CWS: ASA does not append XSS headers
CSCux15273	show memory indicates inaccurate free memory available
CSCux29842	Primary and Secondary ASA in HA is traceback in Thread Name:DataPath
CSCux29929	ASA 9.4.2 traceback in DATAPATH
CSCux33726	ASA traceback - WebVPN CIFS_file_rename_remove operations
CSCux33974	ASA "show chunkstat | redirect" does not work
CSCux35538	Traceback in ctm_ssl_generate_key with DHE ciphers SSL VPN scaled test
CSCux39988	Different output of BVI address in transparent mode on failover pair
CSCux45179	SSL sessions stop processing -"Unable to create session directory" error
CSCux66866	Traffic drop due to constant amount of arp on ASASM
CSCux71197	"show resource usage" gives wrong number of routes after shut/no sh
CSCux82023	Stub Connections Torn Down due to Shun/Threat Detection in ASA Cluster
CSCux82835	Nat pool exhausted observed when enabling asp transactional-commit nat
CSCux83705	DNS Reply Modification for Dual-Stack does not work as expected
CSCux86769	VLAN mapping doesn't work when connection falls back to TLS
CSCux96716	Traceback when unit joins cluster
CSCux98029	ASA reloads with traceback in thread name DATAPATH or CP Processing
CSCux99392	Uploaded/downloaded files via CIFS have Zero Byte size (same WebFolder)
CSCuy00296	Traceback in Thread: IPsec message handler
CSCuy01438	ASA traceback with SIP inspection and SFR enabled in 9.5.2
CSCuy03024	ASA traceback and reload citing Thread Name: idfw_proc
CSCuy05949	ASA: MAC address changes on active context when WRITE STANDBY is issued

Caveat ID Number	Description
CSCuy07753	Smart tunnel does not work since Firefox 32bit version 43
CSCuy10665	HA: Number of interfaces mismatch after SFR module reload on both units
CSCuy11021	Webvpn bookmark subtitles not visible
CSCuy11281	ASA: Assert traceback in version 9.4.2
CSCuy11905	ASA 5585 traceback when the User name is mentioned in the Access list
CSCuy13937	ASA Watchdog traceback in CP Processing thread during TLS processing
CSCuy15798	Add support for IPv6 assigned address field in Radius Accounting packet
CSCuy18640	Potential deadlock between GTP msg process and pdp creation/deletion
CSCuy19933	ASA rewriter incorrectly handle HTML code of type <base>xxx</base>
CSCuy21206	Traceback when drop is enabled with diameter inspection and tls-proxy
CSCuy22561	VPN Load-Balancing does not send load-balancing cert for IPv6 Address
CSCuy25163	Cisco ASA ACL ICMP Echo Request Code Filtering Vulnerability
CSCuy27428	ASA traceback in thread name snmp after upgrade to 9.1(7)
CSCuy30069	ASA 9.5.2 does not send CERT_REQ for 512-bit certificate
CSCuy32321	Traceback in ldap_client_thread with ldap attr mapping and pw-mgmt
CSCuy32728	VPN LB stops working when cluster encryption is configured
CSCuy32964	inter chassises SSP ASA cluster Traceback during hitless fxos upgrade
CSCuy34265	ASA Access-list missing and losing elements after configuration change
CSCuy41986	OCSP validation fails when multiple certs in chain are verified
CSCuy42087	ASA: Not able to remove ACE with "log default" keyword
CSCuy42223	BGP:Deployment failed with reason supported on management-only interface
CSCuy43857	ASA WebVPN: Java Exception with Kronos application
CSCuy47706	Traceback at gtpv1_process_pdp_create_req
CSCuy48237	Clientless SSL VPN CIFS stress test: ramfs_webvpn_file_open traceback
CSCuy49902	inspect ip-option is not allowing "NOP" even when allowed
CSCuy50406	Crash in proxyi_rx_q_timeout_timer
CSCuy51918	Buffer overflow in RAMFS dirent structure causing traceback
CSCuy54567	Evaluation of pix-asa for OpenSSL March 2016

Caveat ID Number	Description
CSCuy58084	Unable to configure a user for ssh public auth only (tied w/ CSCuw90580)
CSCuy59460	SNMP poll is successful for invalid username for v3
CSCuy60320	IPv6 Routes not installed on QP
CSCuy62198	If FQDN is more than 64 chars then we redirect to ip instead of FQDN
CSCuy63642	ASA 9.1(6) traceback in webvpn-datapath : thread name "DATAPATH-2-1524"
CSCuy65416	assert "ctm->async_ref == 0" failed: file "ssl_common.c", line 193-part2
CSCuy65569	Coverity 114172: FORWARD_NULL in snp_fp_inspect_ip_options
CSCuy65571	Coverity 114170: SECURE_CODING in parser_interface_list_invalid
CSCuy67333	SIP call transfer fail due to differences b/w fixing CallId and Refer-To
CSCuy68174	Coverity 114166: NULL_RETURNS in ss_send_health_check_request
CSCuy71812	Coverity 114217: NULL_RETURNS in snp_fp_action_cap_construct_key
CSCuy72255	Coverity 114176: CHECKED_RETURN in oct_dbg_read_csr
CSCuy72257	Coverity 114177: CHECKED_RETURN in oct_dbg_write_csr
CSCuy73652	Traceback in thread name idfw when modifying object-group having FQDN
CSCuy74218	Assert Traceback in Thread Name: DATAPATH on clustered packet reassembly
CSCuy74362	WebVPN FTP client failing with "Error contacting host" message
CSCuy78802	orignial master not defending all GARP packets after cluster split brain
CSCuy80058	FO replication failed: cmd=no disable, when disabling webvpn-cache
CSCuy83792	Coverity 114304: CHECKED_RETURN in ProcessConfiguration(vdi::config::Adi
CSCuy84044	Rewriter error with webworker JS
CSCuy86333	BFD: ASA might traceback in snp_bfd_pp_process+101
CSCuy87597	ASA - Traceback in CP Processing Thread During Private Key Decryption
CSCuy88971	ASA does not suppress EIGRP candidate default route information
CSCuy89425	AAA: RSA/SDI unable to set new PIN
CSCuy91405	ASA should not load-balance same flow traffic over port-channel CCL
CSCuy91788	ASAv: Free memory is reported as negative in an OOM condition
CSCuy94787	Traceback in DATAPATH or Hi CPU usage due to Threat Detection
CSCuy95543	Improve efficiency of malloc_avail_freemem()

Caveat ID Number	Description
CSCuy96391	ASA clientless rewriter failure at 'CSCOPut_hash' function
CSCuy98769	Slow ASA OSPF interface transition from DOWN to WAITING after failover
CSCuy99280	ENH: ASAv should have a different pre-loaded cert
CSCuz00077	ASA 9.1.6.4 traceback with Thread Name: telnet/ci
CSCuz01658	Traceback in gtp_remove_request with duplicate requests
CSCuz06125	Active and Standby ASA use same MAC addr with only active MAC configured
CSCuz06499	WebVPN: Webpage not fully rewritten when ASA has the same FQDN as srv
CSCuz08625	ASA traceback in SSH thread
CSCuz09394	infinite loop in JS rewriter state machine when return followed by var
CSCuz10371	ASA Traceback and reload by strncpy_sx.c
CSCuz14600	Kenton 9.5.1'boot system/boot config' commands not retained after reload
CSCuz14808	5585-10 traceback in Thread Name: idfw_proc
CSCuz14875	ASA RIP crashes when using address-family subconfiguration
CSCuz16398	Incorrect modification of NAT divert table.
CSCuz16498	Error messages on console "ERROR: Problem with interface "
CSCuz18707	Intranet page does not load via WebVPN with JavaScript errors
CSCuz20742	AWS: ASAv not reachable if deployed with 2 interfaces
CSCuz21068	CSCOPut_hash can initiate unexepected requests
CSCuz21178	ASA traceback in threadname ssh
CSCuz23354	CPU usage is high after timer dequeue failed in GTP
CSCuz23576	Allocated memory showing high (invalid) values
CSCuz27165	BTF is not blocking blacklisted domain with more than 2 labels in it
CSCuz28000	Context config may get rejected if all the units in Cluster reloaded
CSCuz30425	Network command disappears from BGP after reload with name
CSCuz34753	ASA QOS fails to classify packets between priority and best effort queue
CSCuz36545	Drop down menu doesn't work on Simfosia web page
CSCuz36938	Traceback on editing a network object on exceeding the max snmp hosts
CSCuz38115	ASA Tback when large ACL applied to interface with object-group-search

Caveat ID Number	Description
CSCuz38180	ASA: Page Fault traceback in DATAPATH on standby ASA after booting up
CSCuz38888	WebVPN rewrite fails for MSCA Cert enrollment page / VBScript
CSCuz40081	ASA memory leak due to vpnfo
CSCuz40793	Interfaces get deleted on SFR during HA configuration sync
CSCuz41033	dynamic crypto map fails if named the same as static crypto map
CSCuz41308	zone keyword seen in show route interface
CSCuz42390	ASA Stateful failover for DRP works intermittently
CSCuz42986	ASA(HA) doesn't send RST packets when sfr module shutdown
CSCuz50929	Many "show blocks" outputs have truncated PC values with ASLR
CSCuz52474	Evaluation of pix-asa for OpenSSL May 2016
CSCuz52859	SNMPv3 noauth traps/poll not working when going from single to multimode
CSCuz53186	ASA AnyConnect CSTP Copyright message changed improperly
CSCuz54193	ASA: Traceback on ASA in Datapath as we enable SFR traffic redirection
CSCuz54545	ASA Address not mapped traceback - configuring snmp-server host
CSCuz58142	ASA Access-list missing and losing elements Warning Message enhancement
CSCuz60555	ASA-2-321006 May be received invalidly when memory is not high
CSCuz61092	Interface health-check failover causes OSPF not to advertise ASA as ABR
CSCuz63531	Observing Memory corruption, assert for debug ospf
CSCuz64603	GTP traceback at gtp_update_sig_conn_timestamp while processing data
CSCuz64784	ASA traceback in DATAPATH on all cluster units during context removal
CSCuz66269	SCP Client not allow to enter password with "no ssh stricthostkeycheck"
CSCuz66661	ASA Cut-through Proxy inactivity timeout not working
CSCuz67349	ASA Cluster fragments reassembled before transmission with no inspection
CSCuz67590	ASA may Traceback with Thread Name: cluster rx thread
CSCuz67596	ASA may Traceback with Thread Name: Unicorn Admin Handler
CSCuz70330	ASA: SSH being denied on the ASA device as the maximum limit is reached
CSCuz72244	Error Indication dropped with Null TID MBReq dropped with no Ctrl F-TEID
CSCuz72352	traceback during tls-proxy handshake

Caveat ID Number	Description
CSCuz77818	PIM BiDir DF Elections stuck in "offer" state on some interfaces
CSCuz79800	ASA cant delete ACL lines and remarks - Specified remark does not exist
CSCuz81922	SRTS: "type" option missing under "show cluster chassis xlate count"
CSCuz90648	2048/1550/9344 Byte block leak cause traffic disruption & module failure
CSCuz94862	IKEv2: Data rekey collisions can cause inactive IPsec SAs to get stuck
CSCuz98201	ASAv - High CPU utilization
CSCuz98220	ASA traceback with Thread Name: Dispatch Unit
CSCuz98704	Traceback in CP Processing thread after upgrade
CSCva00939	Remove ACL warning messages in show access-list when FQDN is resolved
CSCva01570	Unexpected end of file logon.html in WebVPN
CSCva02121	Traceback Thread Name: ci/console : debug menu ctm 103 crashes the ASA
CSCva02655	ASA sends invalid interface id to SFR for clientless VPN traffic
CSCva03982	ASA : Mem leak in cluster mode due to PBR lookup
CSCva11580	ASA9.(6)1 regression "internal error' instead of "maximum time exceeded"
CSCva12520	snmpwalk not working for some NAT OIDs
CSCva12598	CISCO-ENHANCED-MEMPOOL-MIB::cempMemPoolHCFree.1.1 = Counter64: 0 bytes
CSCva14545	Cannot bootup ASAv-KVM when deployed via oVirt
CSCva26771	ASA : PBR Mem leak as packet dropped
CSCva35439	ASA DATAPATH traceback (Cluster)
CSCva39804	Interfaces get deleted on SFR during cluster rejoining
CSCva40844	Crypto accelerator ring timeout causes packet drops
CSCva45590	ASA OSPFv3 interface ID changes upon disabling/enabling failover
CSCva62861	uauth is failed after failover
CSCva92151	Cisco ASA SNMP Remote Code Execution Vulnerability

Resolved Bugs in Version 9.6(1)

The following table lists select resolved bugs at the time of this Release Note publication.

Identifier	Description
CSCtz98516	Observed Traceback in SNMP while querying GET BULK for 'xlate count'
CSCuc11186	ARP: Proxy IP traffic is hijacked.
CSCun21186	ASA traceback when retrieving idfw topn user from slave
CSCuo08193	Traceback in Thread Name: DATAPATH-1-1382 while processing nat-t packet
CSCur46371	TLSv1.2 Client Cert Auth Connection Establishment Failure
CSCur87011	ASA low DMA memory on low end ASA-X -5512/5515 devices
CSCus10787	Transactional ACL commit will bypass security policy during compilation
CSCus16416	Share licenses are not activated on failover pair after power cycle
CSCus53126	ASA traffic not sent properly using 'traffic-forward sfr monitor-only'
CSCut40770	Interface TLV to SFR is corrupt when frame is longer than 2048 bytes
CSCut49034	ASA: High CPU on standby due to RDP conn to AC client from CL SSL portal
CSCut71095	ASA WebVPN clientless cookie authentication bypass
CSCuu02848	Disable ECDSA SSL Ciphers When Manually Configuring RSA Cert for SSL
CSCuu06081	ASAv licesing enforcement should not be CLI parser based
CSCuu48197	ASA: Stuck uauth entry rejects AnyConnect user connections
CSCuu82229	ikev2 with DH 19 and above fails to pass traffic after phase2 rekey
CSCuu91304	Immediate FIN from client after GET breaks scansafe connection
CSCuv20449	Traceback in Thread Name: ssh when using capture or continuous ping
CSCuv49446	ASA traceback on Standby device during config sync in thread DATAPATH
CSCuv50709	Standby ASA inside IP not reachable after Anyconnect disconnect
CSCuv58559	Traceback in Thread Name: DATAPATH on modifying "set connection" in MPF
CSCuv66333	ASA picks incorrect trustpoint to verify OCSP Response
CSCuv87150	ASA traceback in Thread Name: fover_parse (ak47/ramfs)
CSCuv87760	Unicorn proxy thread traceback with RAMFS processing
CSCuv92371	ASA traceback: SSH Thread: many users logged in and dACLs being modified
CSCuv92384	ASA TCP Normalizer sends PUSH ACK for invalid ACK for half-open CONNS
CSCuv94338	ASA traceback in Thread Name: CP Crypto Result Processing.
CSCuw02009	ASA - SSH sessions stuck in CLOSE_WAIT causing ASA to send RST

Identifier	Description
CSCuw09578	ASA 9.3.3.224 traceback in ak47_platform.c with WebVPN stress test
CSCuw14334	Trace back with Thread Name: IP Address Assign
CSCuw16607	ASA EIGRP does not send poison reverse for neighbors to remove route
CSCuw17930	Improper S2S IPSec Datapath Selection for Remote Overlapping Networks
CSCuw19671	ASA traceback while restoring backup configuration from ASDM
CSCuw22130	ASA traceback when removing dynamic PAT statement from cluster
CSCuw22886	Split-tunnel not working for EzVPN client on Kenton device (9.5.1)
CSCuw24664	ASA:Traceback in Thread Name:- netfs_thread_init
CSCuw26991	ASA: Traceback in Thread Unicorn Admin Handler due to Threat Detection
CSCuw28735	Cisco ASA Software Version Information Disclosure Vulnerability
CSCuw29566	ASA5585 9.5(1): Support Failover Lan on Management0/0 port
CSCuw33860	RA-VPN transactions are shown as 0 in PRSM Dashboard
CSCuw36853	ASA: ICMP error loop on cluster CCL with Interface PAT
CSCuw39685	filter sfr traffic may cause memory corruption
CSCuw41548	DNS Traceback in channel_put()
CSCuw44038	Watchdog traceback in ldap_client_thread with large number of ldap grps
CSCuw44744	Traceback in WebVPN rewriter
CSCuw48499	QEMU coredump: qemu_thread_create: Resource temporarily unavailable
CSCuw51576	SSH connections are not timed out on Standby ASA (stuck in rtcli)
CSCuw55813	Standby ASA traceback in Thread Name: EIGRP-IPv4
CSCuw59388	Unable to load ASDM to a Context in Multiple Context Mode
CSCuw66397	DHCP Server Process stuck if dhcpd auto_config already enabled from CLI
CSCuw85261	SAML won't be able select Oracle OAM tunnel group
CSCuw86069	ASAv Cannot remove/change default global_policy or inspection_default
CSCuw87331	ASA: Traceback in Thread name DATAPATH-7-1918
CSCuw87910	PCP 10.6 Clientless VPN Access is Denied when accessing Pages
CSCuw90116	ASA 9.4.1 traceback upon clearing and reconfiguring ACL
CSCuw92005	Thread Name: DATAPATH-17-3095: ASA in Cluster Reloads Unexpectedly

Identifier	Description
CSCux03626	Traceback in thread name: Unicorn Proxy Thread
CSCux05081	RSA 4096 key generation causes failover
CSCux07002	ASA: assertion "pp->pd == pd" failed: file "main.c", line 192
CSCux08783	CWS: ASA does not append XSS headers
CSCux09181	http-form authentication fails after 9.3.2
CSCux09310	ASA traceback when using an ECDSA certificate
CSCux15273	show memory indicates inaccurate free memory available
CSCux16427	PBR incorrect route selection for deny clause
CSCux20178	OSPF neighbor goes down after "reload in xx" commnad in 9.2 and later
CSCux21955	ASA: FAILOVER not working with password encryption.
CSCux23659	ASA 9.1.6.10 traceback after remove compact flash and execute dir cmd
CSCux29929	ASA 9.4.2 traceback in DATAPATH
CSCux30780	GTPv1 traceback in gtpv1_process_msg
CSCux36112	PBR: Mem leak in cluster mode due to policy based route
CSCux37303	Port-Channel Config on Gi 0/0 causes Boot Loop - FIPS related
CSCux37442	Cisco signed certificate expired for WebVpn Port Forward Binary on ASA
CSCux41145	Evaluation of pix-asa for OpenSSL December 2015 Vulnerabilities
CSCux42936	ASA 9.5.1 traceback in Threadname Datapath due to SIP Inspection
CSCux43978	DHCP Relay fails for cluster ASAs with long interface names
CSCux45179	SSL sessions stop processing -"Unable to create session directory" error
CSCux47195	ASA(9.5.2) changing the ACK number sent to client with SFR redirection
CSCux56111	"no ipv6-vpn-addr-assign" CLI not working
CSCux59122	ASA L7 policy-map comes into affect only if the inspection is re-applied
CSCux61257	ASA: Traceback in Thread IP Address Assign
CSCux69987	ASA: Traceback on ASA device after adding FQDN objects in NAT rule
CSCux70998	Reload in Thread Name: IKE Daemon
CSCux71197	"show resource usage" gives wrong number of routes after shut/no sh
CSCux72610	ASA TACACS+: process tacplus_snd uses large percentage of CPU

Identifier	Description
CSCux72835	ASA 9.5 - OCSP check using global routing table instead of management
CSCux81683	ASA Traceback on Thread Name: Unicorn Admin Handler
CSCux82835	Nat pool exhausted observed when enabling asp transactional-commit nat
CSCux86769	VLAN mapping doesn't work when connection falls back to TLS
CSCux87457	ASA traceback in Thread Name: https_proxy
CSCux88237	ASA traceback in DATAPATH thread
CSCux93751	Cisco ASA Linux Kernel Vulnerability - CVE-2016-0728
CSCuy01420	ASA traceback in Thread Name: Unicorn Proxy Thread.
CSCuy03024	ASA traceback and reload citing Thread Name: idfw_proc
CSCuy11905	ASA 5585 traceback when the User name is mentioned in the Access list
CSCuy13937	ASA Watchdog traceback in CP Processing thread during TLS processing
CSCuy22561	VPN Load-Balancing does not send load-balancing cert for IPv6 Address
CSCuy27428	ASA traceback in thread name snmp after upgrade to 9.1(7)
CSCuy32321	Traceback in ldap_client_thread with ldap attr mapping and pw-mgmt
CSCuy41986	OCSP validation fails when multiple certs in chain are verified
CSCuy47706	Traceback at gtpv1_process_pdp_create_req

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.