Release Notes for the Cisco ASA Series, Version 9.1(x)

First Published: December 3, 2012
Last Updated: March 30, 2017

This document contains release information for Cisco ASA software Version 9.1(1) through 9.1(7.4). This document includes the following sections:

Important Notes

- Potential Traffic Outage (9.1(7.9) through 9.1(7.15))--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 reload 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.
- Cisco ASA Clientless SSL VPN Portal Customization Integrity Vulnerability—Multiple vulnerabilities have been fixed for clientless SSL VPN in ASA software, so you should upgrade your software to a fixed version. See http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20141008-asa for details about the vulnerability and a list of fixed ASA versions. Also, if you ever ran an earlier ASA version that had a vulnerable configuration, then regardless of the version you are currently running, you should verify that the portal customization was not compromised. If an attacker compromised a customization object in the past, then the compromised object stays persistent after you upgrade the ASA to a fixed version. Upgrading the ASA prevents this vulnerability from being exploited further, but it will not modify any customization objects that were already compromised and are still present on the system.
- EtherChannel configuration on the 4GE SSM disallowed—Interfaces on the 4GE SSM, including the built-in module on the ASA 5550 (GigabitEthernet 1/*x*), are not supported as members of EtherChannels. However, although not supported, configuration was not disallowed until 9.0(1). If you configured any 4GE SSM interfaces as EtherChannel members, then upgrading to 9.0(1) or later will remove the channel-group membership configuration from those interfaces. You must alter your interface configuration to comply with supported interface types. (CSCtq62715)

- ASA 9.1(3) features for the ASA CX require ASA CX Version 9.2(1).
- Upgrading ASA Clustering from 9.0(1) or 9.1(1)—Due to many bug fixes, we recommend the 9.0(2) or 9.1(2) release or later for ASA clustering. If you are running 9.0(1) or 9.1(1), you should upgrade to 9.0(2) or 9.1(2) or later. Note that due to CSCue72961, hitless upgrading is not supported.
- Upgrading to 9.1(2.8) or 9.1(3) or later—See Upgrading the Software, page 17.
- ASA CX software module SSD—An SSD is required to install the ASA CX software module on the ASA 5500-X series. Non-Cisco SSDs are not supported.

Limitations and Restrictions

- Downgrading from 9.1(4) and later with failover and VPN using inner IPv6 with IKEv2—If you want to downgrade your failover pair, and you are using the 9.1(4) inner IPv6 VPN feature, then you must disconnect the connection before downgrading. If you downgrade without disconnecting, then any new AnyConnect connection that is assigned the same IP address as the previous connection will fail. (CSCul56646)
- Clientless SSL VPN with a self-signed certificate on the ASA—When the ASA uses a self-signed certificate or an untrusted certificate, Firefox 4 and later and Safari are unable to add security exceptions when browsing using an IPv6 address HTTPS URL (FQDN URL is OK): the "Confirm Security Exception" button is disabled. See https://bugzilla.mozilla.org/show_bug.cgi?id=633001. This bug affects all SSL connections originating from Firefox or Safari to the ASA (including clientless SSL VPN connections, and ASDM connections). To avoid this bug, configure a proper certificate for the ASA that is issued by a trusted certificate authority. For Internet Explorer 9 and later, use compatibility mode.
- When configuring for IKEv2, for security reasons you should use groups 21, 20, 19, 24, 14, and 5. We do not recommend Diffie Hellman Group1 or Group2. For example, use

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

- With a heavy load of users (around 150 or more) using a WebVPN plugin, you may experience large delays because of the processing overload. Using Citrix web interface reduces the ASA rewrite overhead. To track the progress of the enhancement request to allow WebVPN plug files to be cached on the ASA, refer to CSCud11756.
- (ASA 5510, ASA 5520, ASA 5540, and ASA 5550 only) We strongly recommend that you enable hardware processing using the **crypto engine large-mod-accel** command instead of software for large modulus operations such as 2048-bit certificates and DH5 keys. If you continue to use software processing for large keys, you could experience significant performance degradation due to slow session establishment for IPsec and SSL VPN connections. We recommend that you initially enable hardware processing during a low-use or maintenance period to minimize a temporary packet loss that can occur during the transition of processing from software to hardware.

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

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

System Requirements

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

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

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

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

New Features

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

New Features in Version 9.1(7.4)

Released: February 19, 2016

The following table lists the new features for ASA Version 9.1(7.4).

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

Table 1 New Features for ASA Version 9.1(7.4)

Feature	Description
Remote Access Features	
Clientless SSL VPN session cookie access restriction	You can now prevent a Clientless SSL VPN session cookie from being accessed by a third party through a client-side script such as Javascript. **Note:** Use this feature only if Cisco TAC advises you to do so. Enabling this command presents a security risk because the following Clientless SSL VPN features will not work without any warning. ■ Java plug-ins ■ Java rewriter ■ Port forwarding ■ File browser ■ Sharepoint features that require desktop applications (for example, MS Office applications) ■ AnyConnect Web launch ■ Citrix Receiver, XenDesktop, and Xenon ■ Other non-browser-based and browser plugin-based applications We introduced the following command: **http-only-cookie**. *This feature is also in 9.2(3) and 9.4(1).*
Configurable SSH encryption and HMAC algorithm	Users can select cipher modes when doing SSH encryption management and can configure HMAC and encryption for varying key exchange algorithms. We introduced the following commands: **ssh cipher encryption** and **ssh cipher integrity.**

Clientless SSL VPN cache disabled by default	The clientless SSL VPN cache is now disabled by default. Disabling the clientless SSL VPN cache provides better stability. If you want to enable the cache, you must manually enable it.
	`webvpn`
	`    cache`
	`      no disable`
	We modified the following command: **cache**
	Also available in 9.5(2).

HTTP redirect support for IPv6	When you enable HTTP redirect to HTTPS for ASDM access or clientless SSL VPN, you can now redirect traffic sent an to IPv6 address. We added functionality to the following command: **http redirect**

Table 1 New Features for ASA Version 9.1(7.4) (continued)

Feature	Description
Administrative Features	
show tech support enhancements	The **show tech support** command now: - Includes **dir all-filesystems** output—This output can be helpful in the following cases: – SSL VPN configuration: check if the required resources are on the ASA – Crash: check for the date timestamp and presence of a crash file - Includes **show resource usage count all 1** output—Includes information about xlates, conns, inspects, syslogs, and so on. This information is helpful for diagnosing performance issues. - Removes the **show kernel cgroup-controller detail** output—This command output will remain in the output of **show tech-support detail**. We modified the following command: **show tech support**
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.

New Features in Version 9.1(6)

Released: March 2, 2015

The following table lists the new features for ASA Version 9.1(6).

Table 2 New Features for ASA Version 9.1(6)

Feature	Description
Interface Features	
Maximum MTU is now 9198 bytes	The maximum MTU that the ASA can use is 9198 bytes (check for your model's exact limit at the CLI help). This value does not include the Layer 2 header. Formerly, the ASA let you specify the maximum MTU as 65535 bytes, which was inaccurate and could cause problems. If your MTU was set to a value higher than 9198, then the MTU is automatically lowered when you upgrade. In some cases, this MTU change can cause an MTU mismatch; be sure to set any connecting equipment to use the new MTU value. We modified the following command: **mtu**

New Features in Version 9.1(5)

Released: March 31, 2014

Table 3 lists the new features for ASA Version 9.1(5).

Table 3 New Features for ASA Version 9.1(5)

Feature	Description
Administrative Features	
Secure Copy client	The ASA now supports the Secure Copy (SCP) client to transfer files to and from a SCP server. We introduced the following commands: **ssh pubkey-chain**, **server (ssh pubkey-chain)**, **key-string**, **key-hash**, **ssh stricthostkeycheck**. We modified the following command: **copy scp**.
Improved one-time password authentication	Administrators who have sufficient authorization privileges may enter privileged EXEC mode by entering their authentication credentials once. The **auto-enable** option was added to the **aaa authorization exec** command. We modified the following command: **aaa authorization exec**.
Firewall Features	
Transactional Commit Model on rule engine for access groups	When enabled, a rule update is applied after the rule compilation is completed; without affecting the rule matching performance. We introduced the following comands: **asp rule-engine transactional-commit**, **show running-config asp rule-engine transactional-commit**, **clear configure asp rule-engine transactional-commit**.
Monitoring Features	
SNMP hosts, host groups, and user lists	You can now add up to 4000 hosts. The number of supported active polling destinations is 128. You can specify a network object to indicate the individual hosts that you want to add as a host group. You can associate more than one user with one host. We introduced or modified the following commands: **snmp-server host-group**, **snmp-server user-list**, **show running-config snmp-server**, **clear configure snmp-server**.
Monitoring Features	
NAT-MIB cnatAddrBindNumberOfEntries and cnatAddrBindSessionCount OIDs to allow polling for Xlate count.	Support was added for the NAT-MIB cnatAddrBindNumberOfEntries and cnatAddrBindSessionCount OIDs to support xlate_count and max_xlate_count for SNMP. This data is equivalent to the **show xlate count** command. *Also available in 8.4(5).*

Table 3 New Features for ASA Version 9.1(5) (continued)

Feature	Description
Remote Access Features	
AnyConnect DTLS Single session Performance Improvement	UDP traffic, such as streaming media, was being affected by a high number of dropped packets when sent over an AnyConnect DTLS connection. For example, this could result in streaming video playing poorly or cease streaming completely. The reason for this was the relatively small size of the flow control queue. We increased the DTLS flow-control queue size and offset this by reducing the admin crypto queue size. For TLS sessions, the priority of the crypto command was increased to high to compensated for this change. For both DTLS and TLS sessions, the session will now persist even if packets are dropped. This will prevent media streams from closing and ensure that the number of dropped packets is comparable with other connection methods. We did not modify any commands.
Webtype ACL enhancements	We introduced URL normalization. URL normalization is an additional security feature that includes path normalization, case normalization and scheme normalization. URLs specified in an ACE and portal address bar are normalized before comparison; for making decisions on webvpn traffic filtering. For example, if you have an https://calo.cisco.com/checkout/Devices/ bookmark, an https://calo.cisco.com/checkout/Devices/* under web type acl seems to match. However, since URL normalization has been introduced, both bookmark URL and web type ACL are normalized before comparison. In this example, https://calo.cisco.com/checkout/Devices is normalized to https://calo.cisco.com/checkout/Devices, and https://calo.cisco.com/checkout.Devices/* stays the same, so the two do not match. You must configure the following to meet the requirement: ■ To permit the bookmark URL (https://calo.cisco.com/checkout/Devices), configure the ACL to permit that URL ■ To permit the URLs within the Devices folder, configure the ACL to permit https://calo.cisco.com/checkout/Devices/* We did not modify any commands.

New Features in Version 9.1(4)

Released: December 9, 2013

Table 4 lists the new features for ASA Version 9.1(4).

Table 4 New Features for ASA Version 9.1(4)

Feature	Description
Remote Access Features	
HTML5 WebSocket proxying	HTML5 WebSockets provide persistent connections between clients and servers. During the establishment of the clientless SSL VPN connection, the handshake appears to the server as an HTTP Upgrade request. The ASA will now proxy this request to the backend and provide a relay after the handshake is complete. Gateway mode is not currently supported. We did not modify any commands.
Inner IPv6 for IKEv2	IPv6 traffic can now be tunneled through IPsec/IKEv2 tunnels. This makes the ASA to AnyConnect VPN connections fully IPv6 compliant. GRE is used when both IPv4 and IPv6 traffic are being tunneled, and when both the client and headend support GRE. For a single traffic type, or when GRE is not supported by the client or the headend, we use straight IPsec. **Note** This feature requires AnyConnect Client Version 3.1.05 or later. Output of the **show ipsec sa** and **show vpn-sessiondb detail anyconnect** commands has been updated to reflect the assigned IPv6 address, and to indicate the GRE Transport Mode security association when doing IKEv2 dual traffic. The **vpn-filter** command must now be used for both IPv4 and IPv6 ACLs. If the depracated **ipv6-vpn-filter** command is used to configure IPv6 ACLs the connection will be terminated.
Mobile Devices running Citrix Server Mobile have additional connection options	Support for mobile devices connecting to Citrix server through the ASA now includes selection of a tunnel-group, and RSA Securid for authorization. Allowing mobile users to select different tunnel-groups allows the administrator to use different authentication methods. We introduced the **application-type** command to configure the default tunnel group for VDI connections when a Citrix Receiver user does not choose a tunnel-group. A **none** action was added to the **vdi** command to disable VDI configuration for a particular group policy or user.
Split-tunneling supports exclude ACLs	Split-tunneling of VPN traffic has been enhanced to support both exclude and include ACLs. Exclude ACLs were previously ignored. **Note** This feature requires AnyConnect Client Version 3.1.03103 or later. We did not modify any commands.
High Availability and Scalability Features	
ASA 5500-X support for clustering	The ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, and ASA 5555-X now support 2-unit clusters. Clustering for 2 units is enabled by default in the base license; for the ASA 5512-X, you need the Security Plus license. We did not modify any commands.

Table 4 New Features for ASA Version 9.1(4) (continued)

Feature	Description
Improved VSS and vPC support for health check monitoring	If you configure the cluster control link as an EtherChannel (recommended), and it is connected to a VSS or vPC pair, you can now increase stability with health check monitoring. For some switches, such as the Nexus 5000, when one unit in the VSS/vPC is shutting down or booting up, EtherChannel member interfaces connected to that switch may appear to be Up to the ASA, but they are not passing traffic on the switch side. The ASA can be erroneously removed from the cluster if you set the ASA holdtime timeout to a low value (such as .8 seconds), and the ASA sends keepalive messages on one of these EtherChannel interfaces. When you enable the VSS/vPC health check feature, the ASA floods the keepalive messages on all EtherChannel interfaces in the cluster control link to ensure that at least one of the switches can receive them. We modified the following command: **health-check** [**vss-enabled**]
Support for cluster members at different geographical locations (inter-site); Individual Interface mode only	You can now place cluster members at different geographical locations when using individual interface mode. See the configuration guide for inter-site guidelines. We did not modify any commands.
Support for clustering with the Cisco Nexus 5000 and Cisco Catalyst 3750-X	The ASA supports clustering when connected to the Cisco Nexus 5000 and Cisco Catalyst 3750-X. We modified the following command: **health-check** [**vss-enabled**]
Basic Operation Features	
DHCP rebind function	During the DHCP rebind phase, the client now attempts to rebind to other DHCP servers in the tunnel group list. Prior to this release, the client did not rebind to an alternate server, when the DHCP lease fails to renew. We introduced the following commands: **show ip address dhcp lease proxy**, **show ip address dhcp lease summary**, and **show ip address dhcp lease server**.
Troubleshooting Features	
Crashinfo dumps include AK47 framework information	Application Kernel Layer 4 to 7 (AK47) framework-related information is now available in crashinfo dumps. A new option, **ak47**, has been added to the **debug menu** command to help in debugging AK47 framework issues. The framework-related information in the crashinfo dump includes the following: ■ Creating an AK47 instance. ■ Destroying an AK47 instance. ■ Generating an crashinfo with a memory manager frame. ■ Generating a crashinfo after fiber stack overflow. ■ Generating a crashinfo after a local variable overflow. ■ Generating a crashinfo after an exception has occurred.

New Features in Version 9.1(3)

Released: September 18, 2013

Table 5 lists the new features for ASA Version 9.1(3).

Table 5 New Features for ASA Version 9.1(3)

Feature	Description
Module Features	
Support for the ASA CX module in multiple context mode	You can now configure ASA CX service policies per context on the ASA. **Note** Although you can configure per context ASA service policies, the ASA CX module itself (configured in PRSM) is a single context mode device; the context-specific traffic coming from the ASA is checked against the common ASA CX policy. Requires ASA CX 9.2(1) or later. We did not modify any commands.
ASA 5585-X with SSP-40 and -60 support for the ASA CX SSP-40 and -60	ASA CX SSP-40 and -60 modules can be used with the matching level ASA 5585-X with SSP-40 and -60. Requires ASA CX 9.2(1) or later. We did not modify any commands.
Filtering packets captured on the ASA CX backplane	You can now filter packets that have been captured on the ASA CX backplane using the **match** or **access-list** keyword with the **capture interface asa_dataplane** command. Control traffic specific to the ASA CX module is not affected by the access-list or match filtering; the ASA captures all control traffic. In multiple context mode, configure the packet capture per context. Note that all control traffic in multiple context mode goes only to the system execution space. Because only control traffic cannot be filtered using an access list or match, these options are not available in the system execution space. Requires ASA CX 9.2(1) or later. We modified the following command: **capture interface asa_dataplane**.
Monitoring Features	
Ability to view top 10 memory users	You can now view the top bin sizes allocated and the top 10 PCs for each allocated bin size. Previously, you had to enter multiple commands to see this information (the **show memory detail** command and the **show memory binsize** command); the new command provides for quicker analysis of memory issues. We introduced the following command: **show memory top-usage**. *Also available in 8.4(6).*

Table 5 New Features for ASA Version 9.1(3) (continued)

Feature	Description
Smart Call Home	We added a new type of Smart Call Home message to support ASA clustering. A Smart Call Home clustering message is sent for only the following three events: ■ When a unit joins the cluster ■ When a unit leaves the cluster ■ When a cluster unit becomes the cluster master Each message that is sent includes the following information: ■ The active cluster member count ■ The output of the **show cluster info** command and the **show cluster history** command on the cluster master We modified the following commands: **show call-home, show running-config call-home**. *Also available in 9.0(3).*
Remote Access Features	
user-storage value command password is now encrypted in **show** commands	The password in the **user-storage value** command is now encrypted when you enter **show running-config**. We modified the following command: **user-storage value**. *Also available in 8.4(6).*

New Features in Version 9.1(2)

Released: May 14, 2013

Table 6 lists the new features for ASA Version 9.1(2).

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

Table 6 New Features for ASA Version 9.1(2)

Feature	Description
Certification Features	
FIPS and Common Criteria certifications	The FIPS 140-2 Non-Proprietary Security Policy was updated as part of the Level 2 FIPS 140-2 validation for the Cisco ASA series, which includes the Cisco ASA 5505, ASA 5510, ASA 5520, ASA 5540, ASA 5550, ASA 5580, ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X, ASA 5585-X, and the ASA Services Module. The Common Criteria Evaluation Assurance Level 4 (EAL4) was updated, which provides the basis for a specific Target of Evaluation (TOE) of the Cisco ASA and VPN platform solutions.
Encryption Features	

Table 6 New Features for ASA Version 9.1(2) (continued)

Feature	Description
Support for IPsec LAN-to-LAN tunnels to encrypt failover and state link communications	Instead of using the proprietary encryption for the failover key (the **failover key** command), you can now use an IPsec LAN-to-LAN tunnel for failover and state link encryption. **Note** Failover LAN-to-LAN tunnels do not count against the IPsec (Other VPN) license. We introduced or modified the following commands: **failover ipsec pre-shared-key**, **show vpn-sessiondb**.

Additional ephemeral Diffie-Hellman ciphers for SSL encryption	The ASA now supports the following ephemeral Diffie-Hellman (DHE) SSL cipher suites:
	- DHE-AES128-SHA1
	- DHE-AES256-SHA1
	These cipher suites are specified in RFC 3268, *Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS*).
	When supported by the client, DHE is the preferred cipher because it provides Perfect Forward Secrecy. See the following limitations:
	- DHE is not supported on SSL 3.0 connections, so make sure to also enable TLS 1.0 for the SSL server.
	`!! set server version`
	`hostname(config)# ssl server-version tlsv1 sslv3`
	`!! set client version`
	`hostname(config) # ssl client-version any`
	- Some popular applications do not support DHE, so include at least one other SSL encryption method to ensure that a cipher suite common to both the SSL client and server can be used.
	- Some clients may not support DHE, including AnyConnect 2.5 and 3.0, Cisco Secure Desktop, and Internet Explorer 9.0.
	We modified the following command: **ssl encryption**.
	Also available in 8.4(4.1).

Management Features	
Support for administrator password policy when using the local database	When you configure authentication for CLI or ASDM access using the local database, you can configure a password policy that requires a user to change their password after a specified amount of time and also requires password standards such as a minimum length and the minimum number of changed characters. We introduced the following commands: **change-password, password-policy lifetime**, **password-policy minimum changes**, **password-policy minimum-length**, **password-policy minimum-lowercase**, **password-policy minimum-uppercase**, **password-policy minimum-numeric**, **password-policy minimum-special**, **password-policy authenticate enable**, **clear configure password-policy**, **show running-config password-policy**. *Also available in 8.4(4.1).*

Table 6 New Features for ASA Version 9.1(2) (continued)

Feature	Description
Support for SSH public key authentication	You can now enable public key authentication for SSH connections to the ASA on a per-user basis. You can specify a public key file (PKF) formatted key or a Base64 key. The PKF key can be up to 4096 bits. Use PKF format for keys that are too large to for the ASA support of the Base64 format (up to 2048 bits). We introduced the following commands: **ssh authentication**. *Also available in 8.4(4.1); PKF key format support is only in 9.1(2).*
AES-CTR encryption for SSH	The SSH server implementation in the ASA now supports AES-CTR mode encryption.
Improved SSH rekey interval	An SSH connection is rekeyed after 60 minutes of connection time or 1 GB of data traffic. We introduced the following command: **show ssh sessions detail**.
Support for Diffie-Hellman Group 14 for the SSH Key Exchange	Support for Diffie-Hellman Group 14 for SSH Key Exchange was added. Formerly, only Group 1 was supported. We introduced the following command: **ssh key-exchange**. *Also available in 8.4(4.1).*
Support for a maximum number of management sessions	You can set the maximum number of simultaneous ASDM, SSH, and Telnet sessions. We introduced the following commands: **quota management-session**, **show running-config quota management-session**, **show quota management-session**. *Also available in 8.4(4.1).*
The default Telnet password was removed	To improve security for management access to the ASA, the default login password for Telnet was removed; you must manually set the password before you can log in using Telnet. **Note**: The login password is only used for Telnet if you do not configure Telnet user authentication (the **aaa authentication telnet console** command). Formerly, when you cleared the password, the ASA restored the default of "cisco." Now when you clear the password, the password is removed. The login password is also used for Telnet sessions from the switch to the ASASM (see the **session** command). For initial ASASM access, you must use the **service-module session** command, until you set a login password. We modified the following command: **passwd**. *Also available in 9.0(2).*
Platform Features	
Support for Power-On Self-Test (POST)	The ASA runs its power-on self-test at boot time even if it is not running in FIPS 140-2-compliant mode. Additional tests have been added to the POST to address the changes in the AES-GCM/GMAC algorithms, ECDSA algorithms, PRNG, and Deterministic Random Bit Generator Validation System (DRBGVS).
Improved pseudo-random number generation (PRNG)	The X9.31 implementation has been upgraded to use AES-256 encryption instead of 3DES encryption to comply with the Network Device Protection Profile (NDPP) in single-core ASAs.
Support for image verification	Support for SHA-512 image integrity checking was added. We modified the following command: **verify**. *Also available in 8.4(4.1).*

Table 6 New Features for ASA Version 9.1(2) (continued)

Feature	Description
Support for private VLANs on the ASA Services Module	You can use private VLANs with the ASASM. Assign the primary VLAN to the ASASM; the ASASM automatically handles secondary VLAN traffic. There is no configuration required on the ASASM for this feature; see the switch configuration guide for more information.
CPU profile enhancements	The **cpu profile activate** command now supports the following: - Delayed start of the profiler until triggered (global or specific thread CPU%) - Sampling of a single thread We modified the following command: **cpu profile activate** [*n-samples*] [**sample-process** *process-name*] [**trigger cpu-usage** *cpu%* [*process-name*]. *Also available in 8.4(6).*
DHCP Features	
DHCP relay servers per interface (IPv4 only)	You can now configure DHCP relay servers per-interface, so requests that enter a given interface are relayed only to servers specified for that interface. IPv6 is not supported for per-interface DHCP relay. We introduced or modified the following commands: **dhcprelay server** (interface config mode), **clear configure dhcprelay**, **show running-config dhcprelay**.
DHCP trusted interfaces	You can now configure interfaces as trusted interfaces to preserve DHCP Option 82. DHCP Option 82 is used by downstream switches and routers for DHCP snooping and IP Source Guard. Normally, if the ASA DHCP relay agent receives a DHCP packet with Option 82 already set, but the giaddr field (which specifies the DHCP relay agent address that is set by the relay agent before it forwards the packet to the server) is set to 0, then the ASA will drop that packet by default. You can now preserve Option 82 and forward the packet by identifying an interface as a trusted interface. We introduced or modified the following commands: **dhcprelay information trusted**, **dhcprelay informarion trust-all**, **show running-config dhcprelay**.
Module Features	
ASA 5585-X support for network modules	The ASA 5585-X now supports additional interfaces on network modules in slot 1. You can install one or two of the following optional network modules: - ASA 4-port 10G Network Module - ASA 8-port 10G Network Module - ASA 20-port 1G Network Module *Also available in 8.4(4.1).*
ASA 5585-X DC power supply support	Support was added for the ASA 5585-X DC power supply. *Also available in 8.4(5).*

Table 6 New Features for ASA Version 9.1(2) (continued)

Feature	Description
Support for ASA CX monitor-only mode for demonstration purposes	For demonstration purposes only, you can enable monitor-only mode for the service policy, which forwards a copy of traffic to the ASA CX module, while the original traffic remains unaffected. Another option for demonstration purposes is to configure a traffic-forwarding interface instead of a service policy in monitor-only mode. The traffic-forwarding interface sends all traffic directly to the ASA CX module, bypassing the ASA. We modified or introduced the following commands: **cxsc** {**fail-close** | **fail-open**} **monitor-only**, **traffic-forward cxsc monitor-only**.
Support for the ASA CX module and NAT 64	You can now use NAT 64 in conjunction with the ASA CX module. We did not modify any commands.
NetFlow Features	
Support for NetFlow flow-update events and an expanded set of NetFlow templates	In addition to adding the flow-update events, there are now NetFlow templates that allow you to track flows that experience a change to their IP version with NAT, as well as IPv6 flows that remain IPv6 after NAT. Two new fields were added for IPv6 translation support. Several NetFlow field IDs were changed to their IPFIX equivalents. For more information, see the *Cisco ASA Implementation Note for NetFlow Collectors*.
Firewall Features	
EtherType ACL support for IS-IS traffic (transparent firewall mode)	In transparent firewall mode, the ASA can now pass IS-IS traffic using an EtherType ACL. We modified the following command: **access-list ethertype** {**permit** | **deny**} **is-is**. *Also available in 8.4(5).*
Decreased the half-closed timeout minimum value to 30 seconds	The half-closed timeout minimum value for both the global timeout and connection timeout was lowered from 5 minutes to 30 seconds to provide better DoS protection. We modified the following commands: **set connection timeout half-closed**, **timeout half-closed**.
Remote Access Features	

Table 6 New Features for ASA Version 9.1(2) (continued)

Feature	Description
IKE security and performance improvements	The number of IPsec-IKE security associations (SAs) can be limited for IKE v1 now, as well as IKE v2. We modified the following command: **crypto ikev1 limit**.
	The IKE v2 Nonce size has been increased to 64 bytes. There are no ASDM screen or CLI changes.
	For IKE v2 on Site-to-Site, a new algorithm ensures that the encryption algorithm used by child IPsec SAs is not higher strength than the parent IKE. Higher strength algorithms will be downgraded to the IKE level. This new algorithm is enabled by default. We recommend that you do not disable this feature. We introduced the following command: **crypto ipsec ikev2 sa-strength-enforcement**.
	For Site-to-Site, IPsec data-based rekeying can be disabled. We modified the following command: **crypto ipsec security-association**.
Improved Host Scan and ASA Interoperability	Host Scan and the ASA use an improved process to transfer posture attributes from the client to the ASA. This gives the ASA more time to establish a VPN connection with the client and apply a dynamic access policy. *Also available in 8.4(5).*
Clientless SSL VPN: Windows 8 Support	This release adds support for Windows 8 x86 (32-bit) and Windows 8 x64 (64-bit) operating systems. We support the following browsers on Windows 8: ■ Internet Explorer 10 (desktop only) ■ Firefox (all supported Windows 8 versions) ■ Chrome (all supported Windows 8 versions) See the following limitations: ■ Internet Explorer 10: – The Modern (AKA Metro) browser is not supported. – If you enable Enhanced Protected Mode, we recommend that you add the ASA to the trusted zone. – If you enable Enhanced Protected Mode, Smart Tunnel and Port Forwarder are not supported. ■ A Java Remote Desktop Protocol (RDP) plugin connection to a Windows 8 PC is not supported. *Also available in 9.0(2).*

Table 6 New Features for ASA Version 9.1(2) (continued)

Feature	Description
Cisco Secure Desktop: Windows 8 Support	CSD 3.6.6215 was updated to enable selection of Windows 8 in the Prelogin Policy operating system check. See the following limitations: ■ Secure Desktop (Vault) is not supported with Windows 8. *Also available in 9.0(2).*
Monitoring Features	
NSEL	Flow-update events have been introduced to provide periodic byte counters for flow traffic. You can change the time interval at which flow-update events are sent to the NetFlow collector. You can filter to which collectors flow-update records will be sent. We introduced or modified the following commands: **flow-export active refresh-interval**, **flow-export event-type**. *Also available in 8.4(5).*

New Features in Version 9.1(1)

Released: December 3, 2012

Table 7 lists the new features for ASA Version 9.1(1).

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

Table 7 New Features for ASA Version 9.1(1)

Feature	Description
Module Features	
Support for the ASA CX SSP for the ASA 5512-X through ASA 5555-X	We introduced support for the ASA CX SSP software module for the ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, and ASA 5555-X. The ASA CX software module requires a Cisco solid state drive (SSD) on the ASA. For more information about the SSD, see the ASA 5500-X hardware guide. We modified the following commands: **session cxsc**, **show module cxsc**, **sw-module cxsc**.

Upgrading the Software

See the following table for the upgrade path for your version. Some versions require an interim upgrade before you can upgrade to the latest version.

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

- Upgrading ASA clustering from 9.0(1) or 9.1(1): due to CSCue72961, hitless upgrading is not supported.

- Upgrade issues with 8.4(6), 9.0(2), and 9.1(2) for failover—Due to CSCug88962, you cannot perform a Zero Downtime Upgrade to 8.4(6), 9.0(2), or 9.1(3). You should instead upgrade to 8.4(5) or 9.0(3) or later. To upgrade 9.1(1), you cannot upgrade directly to the 9.1(3) release due to CSCuh25271, so there is no workaround for a Zero Downtime Upgrade; you must upgrade to 9.1(2) before you upgrade to 9.1(3) or later.

Current ASA Version	First Upgrade to:	Then Upgrade to:
8.2(x) and earlier	8.4(5)	9.1(3) or later
8.3(x)	8.4(5)	9.1(3) or later
8.4(1) through 8.4(4)	8.4(5) or 9.0(4)	9.1(3) or later
8.4(5) and later	—	9.1(3) or later
8.5(1)	9.0(4)	9.1(3) or later
8.6(1)	9.0(4)	9.1(3) or later
9.0(1)	9.0(4)	9.1(3) or later
9.0(2) or later	—	9.1(3) or later
9.1(1)	9.1(2)	9.1(3) or later
9.1(2) or later	—	9.1(3) or later

For detailed steps about upgrading, see the 9.1 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, page 18
- Resolved Bugs, page 20

Open Bugs

If you have a Cisco support contract, use the following dynamic search for open bugs for Version 9.1:

- 9.1 open bug search

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

Table 8 Open Bugs in ASA Version 9.1

Bug	Description
CSCug24468	Unable to associate PRSM with AD_Realm.
CSCuh20157	http server session timeout issue
CSCuh37933	ASA behavior is not consistant when configuring traffic forwarding to CX
CSCui10122	object nat 4 to 6 translation incorrect on capture
CSCui22231	LU Updates during config sync in a clustered environment cause traceback
CSCui30278	ASA will traceback if anyconnect configuration is deleted
CSCui36851	ASA Client proxy creates leases without VPN connection
CSCui43057	WebVPN: IPv6 address is padded with zeros in FF browser 3.6
CSCui74211	Client lease not renewed and expired, entry not purged in secondary unit
CSCuj23106	ASA 9.1 Crash in NTP when issuing clear config all
CSCuj39089	asdm_handler session does not timeout after idle-timeout expires
CSCul18248	Configuration Migration Requires Reload in Multiple-Context Mode
CSCul24557	TFW Dropping fragmented V6 mcast traffic with 3 intf in a bridge group
CSCul30082	Flipping FO unit will create stale dhcp lease entries on Fo units.
CSCul34972	DHCP Client Proxy doesn't disable after FO units are flipped
CSCul64645	WebVpn: d3 library is not working
CSCun10751	ASA: SNMPv3 localized strings replicated during failover
CSCun88687	policing not done properly when there are multiple connections
CSCun91099	Clustering- IPv6 address is not shown for Inside and Outside Interfaces.
CSCun98137	FW Perf tests will have degradation after first reboot test run
CSCuo31318	ASA WebVPN JavaScript Content Rewrite Fails with an exception
CSCup23982	ASA permits dynamic ACLs (DAP/DACL) to be modified
CSCup37416	Stale VPN Context entries cause ASA to stop encrypting traffic
CSCup44613	ASA- interface name mismatches between CLI ind MIB
CSCuq58646	L2 cluster slave unit exiting cluster while sending multicast traffic
CSCuq66344	Personal bookmarks get overwritten after failover and addtion
CSCuq71100	Can't set crypto map pfs group > 5 with phase1-mode aggressive
CSCur77397	Firepower on Kenton: Unable to generate alerts for Chunked and GZIP pkts
CSCur80885	ASA-SM device is getting disconnected after confguring ip for vlan
CSCus09743	ICMPv6 packet too big passed through ASA though connection is teardown
CSCus29600	dhcprelay interface doesn't change by changing route
CSCus63115	ASA drops packet-too-big when icmp inspection is on (traffic thru ASA)
CSCus93565	XenDesktop 7.x access through HTML5 receiver fails for Chrome v40
CSCut12172	Unable to observe any DHCP lease information using the show command
CSCut63916	[ASA] CTP not working if proxyACL port_argument is eq
CSCuu80180	High cpu on cluster units due to looping of UDP packets
CSCuv20449	Traceback in Thread Name: ssh when using capture or continuous ping
CSCuv61791	CWS redirection on ASA may corrupt sequence numbers with https traffic

Table 8 Open Bugs in ASA Version 9.1 (continued)

Bug	Description
CSCuv73636	ASA: Traceback seen on L2 Cluster in multimode with large NAT configs
CSCuw48061	" your certificate is invalid for the selected group" when accessing ASDM
CSCuw51576	SSH connections are not timed out on Standby ASA (stuck in rtcli)
CSCuw71147	Traceback in Unicorn Proxy Thread, in http_header_by_name
CSCux29678	ASA 9.1.7: IE 11 Clientless SSL VPN cannot login to CIFS share
CSCux33726	ASA traceback - WebVPN CIFS_file_rename_remove operations
CSCux34679	ASA: Traceback with " clear conf router" on ASA Multiple Context
CSCux36742	ASA: Neighbor command not being removed on clearing interface config
CSCux42700	WebVPN HTTP-IPv6 redirect to port 9000 fails
CSCux43333	coredump completion reported when failure is due to insuff filesys size
CSCux43460	http://ASDM fails to redirect to https://ASDM:non-default-server-port
CSCux45179	WebVPN login page stopped displaying .../logon.html?fcadbadd=1
CSCux58172	DAP: debug dap trace not fully shown after +1600 lines
CSCux63990	ASA - Peak Concurrent sessions more than available addresses in pool
CSCux66866	Traffic drop due to constant amount of arp on ASASM
CSCux68948	ASA cluster master unit crash in DATAPATH-0-1292 after slave upgrade
CSCux70993	ASA unable to add policy NAT which is overlapping with ip local pool
CSCux71674	ASA: Traceback with Thread name Unicorn Admin Handler due to ACL config

Resolved Bugs

Resolved Bugs in Version 9.1(7.4)

If you have a Cisco support contract, use the following search for resolved bugs:

9.1(7.4) fixed bug search

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

Table 9 Resolved Bugs in ASA Version 9.1(7.4)

Bug	Description
CSCtg74172	Can get around dynamic-filter by using caps in domain name
CSCti05769	Migration of max_conn/em_limit to MPF is completely wrong in 8.3
CSCtx43501	CPU hog due to snmp polling of ASA memory pool information
CSCuc11186	ARP: Proxy IP traffic is hijacked.
CSCuf31658	Linux Kernel nfs_readdata_release() and nfs_writedata_release() Functi
CSCuf31803	Linux Kernel nfs_wait_on_request() Local Denial of Service Vulnerabili
CSCui41969	Authentication is successful, but http browser with error msg displayed
CSCul02601	Cisco ASA SNMP Denial of Service Vulnerability
CSCul16778	vpn load-balancing configuration exits sub-command menu unexpectedly
CSCum03212	URLF: Websense v4 message length calculation is incorrect by 2 bytes
CSCum77083	traceback in Thread Name: IKEv2 Daemon
CSCun66179	ASA558560 traceback tmatch_release+46 spin_lock.h:317 in cps IPV6 tests
CSCuo08193	Traceback in Thread Name: DATAPATH-1-1382 while processing nat-t packet
CSCuo58584	Cisco ASA fix for CSCun56954
CSCuo58823	A traceback may happen while processing crypto commands
CSCuq10239	Windows 8 with new JRE, IE is not gaining access to smart tunnel
CSCuq27342	Traceback and reload triggered by failover configuration
CSCuq57307	ASA 8.4 Memory leak due to duplicate entries in ASP table
CSCuq97035	WEBVPN: Citrix 5/6 application doesn't launch with IE10/Windows 7
CSCur07369	SXP Version Mismatch Between ASA & N7K with clustering
CSCur09141	RRI static routing changes not updated in routing table
CSCur20461	ASA Threat detection adds Shun entry for attacker based on routing table
CSCus10787	Transactional ACL commit will bypass security policy during compilation
CSCus11465	ASA teardown connection after receiving same direction fins
CSCus15721	ASA: ICMP loop when cluster member rejoins the cluster.
CSCus16416	Share licenses are not activated on failover pair after power cycle
CSCus23416	ASA traceback in DATAPATH-1-2414 after software upgrade
CSCus30833	ASA: Page fault traceback in SXP CORE thread
CSCus46895	WebVPN Rewriter: " parse" method returns curly brace instead of semicolon
CSCus47259	Cisco ASA XAUTH Bypass Vulnerability
CSCus51289	ASA: Traceback when removing manual NAT rule
CSCus53692	ASA traceback in Thread Name: fover_parse
CSCus56590	ASA - Traceback in Thread Name: fover_parse
CSCus57142	Cisco ASA DHCPv6 Relay Denial of Service Vulnerability
CSCus62884	ASA 9.1.5 does not always drop connections after receiving RST+ACK flag
CSCus64082	ASA fails to sync objects with name ANY after upgrade from 8.4 to 9.x
CSCus71190	LDAP over SSL fails when using TLS1.2 on ASA
CSCus76632	assertion " mh->mh_mem_pool > MEMPOOL_UNDEFINED && mh->mh_mem_pool < MEMP

Table 9 Resolved Bugs in ASA Version 9.1(7.4) (continued)

Bug	Description
CSCus78450	ASA cert validation fails when suitable TP is above the resident CA cert
CSCus91407	Network Object NAT is not working when config-register == 0x41
CSCus91636	Adding subnet(s) to the object group for NAT causes high CPU
CSCus92856	ASA traceback in DATAPATH Thread due to Double Block Free
CSCus94026	Cisco ASA ISAKMP Denial of Service Vulnerability
CSCus97061	ASA Cluster member traceback in DATAPATH
CSCut01856	ASA dropping traffic with TCP syslog configured in multicontext mode
CSCut03495	Cisco ASA DNS Denial of Service Vulnerability
CSCut10078	Standby ASA does not apply OSPF route after config replication
CSCut11895	Failover assembly remained in active-active state permanantly
CSCut12513	ASA allows citrix ICA connection without authentication
CSCut15570	Anyconnect SSL VPN certificate authentication fails o ASA
CSCut28217	Active ASA in failover setup reboots on its own
CSCut30741	ASA redirection to Scansafe tower fails with log id " 775002" in syslog
CSCut36927	Cluster destabilizes when contexts are removed
CSCut39985	Per-session PAT RST sent to incorrect direction after closing session
CSCut44075	Traceback in snp_cluster_get_buffer
CSCut45114	2048-byte block leak if DNS server replies with " No such name"
CSCut46019	MARCH 2015 OpenSSL Vulnerabilities
CSCut47204	Clustering: Eigrp RIB not replicated to slave node
CSCut48009	Traceback in thread CP Processing
CSCut49034	ASA: High CPU on standby due to RDP conn to AC client from CL SSL portal
CSCut49111	ASA traceback because of TD tcp-intercept feature
CSCut71095	ASA WebVPN clientless cookie authentication bypass
CSCut75983	ASA Traceback in PPP
CSCut88287	ASA Traceback in vpnfol_thread_msg
CSCut92194	ASA traceback in Thread Name: CP Processing
CSCut95793	ASA: Anyconnect IPv6 Traceroute does not work as expected
CSCuu04012	ASA CX - Data Plane marked as DOWN untill ASA reload.
CSCuu07799	Cisco ASA DNS Denial of Service Vulnerability
CSCuu18989	ASA %ASA-3-201011: Connection limit exceeded when not hitting max limit
CSCuu27334	ASA: Traceback with Thread Name - AAA
CSCuu28909	ASA cluster: ICMP loop on CCL for ICMP packet destined to the VPN tunnel
CSCuu32905	ASA WebVPN: Javascript fails to execute when accessing internal portal
CSCuu39636	Cert Auth fails with 'max simultaneous-login restriction' error
CSCuu45812	asa Traceback with Thread Name idfw_proc
CSCuu45813	ASA Name Constraints dirName improperly verified
CSCuu46569	ASA CA certificate import fails with different types of Name Constraints

Table 9 Resolved Bugs in ASA Version 9.1(7.4) (continued)

Bug	Description
CSCuu48197	ASA: Stuck uauth entry rejects AnyConnect user connections
CSCuu56912	ASA change non-default port to 443 for https traffic redirected to CWS
CSCuu61573	9.5.2 Gold Setup - Traceback in DATAPATH-6-2596 snp_fp_get_frag_chain
CSCuu73395	Auth-prompt configured in one context appears in another context
CSCuu75901	ASA failover due to issue show local-host command make CPU-hog
CSCuu78835	Webvpn rewrite issues for Confluence - by atlassian on latest v6.4.5
CSCuu83280	Evaluation of OpenSSL June 2015
CSCuu84085	DHCP-DHCP Proxy thread traceback shortly after failover and reload
CSCuu84697	ASA Traceback in Thread Name ssh/client
CSCuu91304	Immediate FIN from client after GET breaks scansafe connection
CSCuu94945	ASA: Traceback while copying file using SCP on ASA
CSCuv01177	ASA: traceback in IDFW AD agent
CSCuv05386	Clientless webvpn on ASA does not display asmx files
CSCuv07106	ASATraceback in ssh whilst adding new line to extended ACL
CSCuv10258	ASA5505 permanent base license, temp secplus, failover, vlan count issue
CSCuv12564	Memory leak @regcomp_unicorn with APCF configured
CSCuv12884	Unable to authenticate with remove aaa-server from different context
CSCuv30184	AddThis widget is not shown causing Traceback in Unicorn Proxy Thread
CSCuv32615	ASA: LDAP over SSL Authentication failure
CSCuv38654	rewriter returns 302 for a file download
CSCuv39775	ASA cluster-Incorrect "current conns" counter in service-policy
CSCuv45756	ASA may tracebeck when displaying packet capture with trace option
CSCuv49446	ASA traceback on Standby device during config sync in thread DATAPATH
CSCuv57389	ASA PKI: cert auth fails after upgrade to 9.1(6.4) / 9.1(6.6) / 9.1(6.8)
CSCuv58559	Traceback in Thread Name: DATAPATH on modifying "set connection" in MPF
CSCuv66333	ASA picks incorrect trustpoint to verify OCSP Response
CSCuv70932	FO: ASAv crashed while syncing during upgrade from 9.4.1 to 9.5.1
CSCuv79552	Standby traceback during config replication with customization export
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
CSCuw09578	ASA 9.3.3.224 traceback in ak47_platform.c with WebVPN stress test
CSCuw14334	Trace back with Thread Name: IP Address Assign
CSCuw15615	Backup unknown with dynamic pat pool
CSCuw17930	Improper S2S IPSec Datapath Selection for Remote Overlapping Networks

Table 9 Resolved Bugs in ASA Version 9.1(7.4) (continued)

Bug	Description
CSCuw19671	ASA crashes while restoring backup configuration from ASDM
CSCuw22130	ASA traceback when removing dynamic PAT statement from cluster
CSCuw24664	ASA:Traceback in Thread Name:- netfs_thread_init
CSCuw28735	Cisco ASA Software Version Information Disclosure Vulnerability
CSCuw36853	ASA: ICMP error loop on cluster CCL with Interface PAT
CSCuw41548	DNS Traceback in channel_put()
CSCuw66397	DHCP Server Process stuck if dhcpd auto_config already enabled from CLI
CSCuw87910	PCP 10.6 Clientless VPN Access is Denied when accessing Pages
CSCuw97445	clustering nat : Observing crash on blade after disabling cluster on uut
CSCux07002	ASA: assertion "pp->pd == pd" failed: file "main.c", line 192
CSCux09310	ASA traceback when using an ECDSA certificate
CSCux20913	Clustering NAT: ASA crash during NAT configuration
CSCux29978	Cisco ASA IKEv1 and IKEv2 Buffer Overflow Vulnerability
CSCux35538	Traceback in ctm_ssl_generate_key with DHE ciphers SSL VPN scaled test
CSCux37442	Cisco signed certificate expired for WebVpn Port Forward Binary on ASA
CSCux41145	Evaluation of pix-asa for OpenSSL December 2015 Vulnerabilities
CSCux42019	Cisco ASA IKEv1 and IKEv2 Buffer Overflow Vulnerability
CSCux43345	Allow a larger (4GB) coredump filesystem to be configured on ASA
CSCux45179	SSL sessions stop processing -"Unable to create session directory" error
CSCux46192	ASA coredumped after enable,disable webvpn on interface
CSCux56111	"no ipv6-vpn-addr-assign" CLI not working
CSCux58016	AnyConnect sessions fail due to IPv6 address assignment failure.
CSCux63770	IPAA needs improved debugging - Part 2- add Syslogs 737034-737036
CSCuy03024	ASA Crashes and reloads citing Thread Name: idfw_proc
CSCuy27428	ASA traceback in thread name snmp after upgrade to 9.1(7)

Resolved Bugs in Version 9.1(6)

If you have a Cisco support contract, use the following search for resolved bugs:

9.1(6) fixed bug search

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

Table 10 Resolved Bugs in ASA Version 9.1(6)

Bug	**Description**
CSCun78551	Cisco ASA Information Disclosure Vulnerability
CSCur10595	ASA cut-through proxy limiting authentication attempts from user
CSCui41969	Authentication is successful, but http browser with error msg displayed
CSCuc80004	Traceback seen when editing ACL configured in AAA UAuth
CSCuo19916	ASA - Cut Through Proxy sends empty redirect w/ Virtual HTTP and Telnet

Table 10 Resolved Bugs in ASA Version 9.1(6) (continued)

Bug	Description
CSCun26772	Invalid user names are logged in syslogs
CSCup59774	No syslogs for ASDM or clientless access with blank username/password
CSCur94645	ASA - Additional empty fields in RADIUS Access-Request packet
CSCun69561	ASA Crafted Radius DoS Vulnerability
CSCuq38807	ASA Radius Access-Request contains both User-Password and CHAP-Password
CSCuq65542	Cisco ASA Software Version Information Disclosure Vulnerability
CSCur69803	acl rules are not removed when service object-group entry is deleted.
CSCup59017	ASA with ACL optimization crashing in "fover_parse" thread
CSCup28968	When ACL optimization is enabled, wrong rules get deleted
CSCuo09383	ASA WebVPN Memory leak leading to Blank Portal Page/AnyConnect failure
CSCtz53586	ASA: Crash when out of stack memory with call-home configured
CSCun43072	ASA5585-SSP60 Traceback in Thread Name SSH on Capture Command
CSCuh84378	ASA: Last packet in PCAP capture file not readable
CSCum77758	capture type tls-proxy no longer works
CSCuq59114	ASA traceback in cluster with DATAPATH thread
CSCuq75981	ASA traceback in DATAPATH-0-2078 thread
CSCun21186	ASA traceback when retrieving idfw topn user from slave
CSCuq66078	Traceback in clacp_enforce_load_balance with ASA Clustering
CSCup26347	ASA Panic: CP Processing - ERROR: shrlock_join_domain
CSCun12838	ASA Traceback in DATAPATH-1-1400 with error message shrlock_join_domain
CSCuq91793	ASA: RST packet forwarded with non-zero ACK number (and ACK flag clear)
CSCum35118	ASA:Traceback in Thread Name: DATAPATH-23-2334
CSCum70178	Datapath:Observing Deadlock in different DATAPATH threads
CSCur45455	ASA crashes in DHCPV6 Relay agent feature Functionality
CSCuq62597	ASA L2TP Split-Tunnel DHCPC: DHCP daemon got msg for uninitialized
CSCur16308	DHCP Relay reloads after changing server interface
CSCuo42563	Traceback DHCP 'IP Address Assign' while upgrading ASAs in Failover
CSCup07330	ASA: no auth prompt when accessing internet website using ASA-CX
CSCur71254	ASA crash loop while upgrading when FIPS enabled
CSCun64754	ASA may traceback when "write standby" command is entered twice
CSCuj79509	ASA Physical Interface Failure Does not Trigger Failover
CSCur98502	ASA: 'no monitor-interface service-module' command gone after reload.
CSCur07061	Traceback on standby ASA during hitless upgrade
CSCum80899	ASA: Watchdog traceback in Unicorn Admin Handler with TopN host stats
CSCur25431	ASA assert traceback on Standby Unit in c_idfw.c
CSCuq77228	ASA Cluster: IDFW traceback inThread Name: DATAPATH-3-132
CSCup50857	ASA traceback in thread name idfw_adagent
CSCur59704	ASA: Traceback in idfw_proc

Table 10 Resolved Bugs in ASA Version 9.1(6) (continued)

Bug	Description
CSCuj98221	IDFW: user-group is not deactivated even if IDFW ACL is removed
CSCul22215	Traceback when using IDFW ACL's with VPN crypto maps
CSCup47885	ASA: Page fault traceback in DATAPATH when DNS inspection is enabled
CSCuo68327	Cisco ASA DNS Inspection Engine Denial of Service Vulnerability
CSCum56399	Cisco ASA GTP Inspection Engine Denial of Service Vulnerability
CSCum46027	Cisco ASA SQL*NET Inspection Engine Denial of Service Vulnerability
CSCur66635	ASA Traceback in Thread Name: DATAPATH-3-1274
CSCuo33186	Traceback with thread DATAPATH-2-1181
CSCuo23892	ASA SIP Inspect:'From: header' in the INVITE not NATed for outbound flow
CSCuq99821	ASA/ASASM drops SIP invite packets with From field containing " " and
CSCun11074	Cisco ASA SunRPC Inspection Denial of Service Vulnerability
CSCuq59667	ASA tracebacks in Thread Name: ssh due to watchdog
CSCuq77655	Cisco ASA DNS Memory Exhaustion Vulnerability
CSCur41860	HTTP and FTP Copy operations exposes sensitive information in syslogs
CSCuq22357	SCP copy operations exposes sensitive information in syslogs
CSCup16419	Traceback in Thread Name: ssh_init
CSCum70258	ASA crashes w/ syslog 702307 & syslogs sent over ipsec conn w/ load
CSCun66613	ASA stops decrypting certain L2L traffic after working for some time
CSCur64659	ASA Traceback in Thread Name: DATAPATH-6-2544
CSCuq28582	Cisco ASA VPN Failover Commands Injection Vulnerability
CSCul61545	ASA Page Fault Traceback in 'vpnfol_thread_msg' Thread
CSCup00433	Failover Standby unit has higher memory utilization
CSCul36176	Cisco ASA VPN Denial of Service Vulnerability
CSCum91360	Aborted AnyConnect Authentications can cause resource leak
CSCuo58411	ASA IKEv2 "Duplicate entry in tunnel manager" (post 9.1.5)
CSCun31725	ASA using IKEv2 rejects multiple NAT_DETECTION_SOURCE_IP payloads
CSCum96401	Cisco ASA IKEv2 Denial of Service Vulnerability
CSCun45787	Duplicated CHILD SAs in 1 IKEv2 SA, traffic dropped vpn-overlap-conflict
CSCuo26501	ASA: Traceback in Thread Name: Dispatch Unit when enable debug ppp int
CSCuo45321	ASA allows IKEv1 clients to bypass address assignment, causing conflict
CSCun88276	High CPU with IKE daemon Process
CSCum88762	VPN Filter missing from standby session
CSCun45520	Cisco ASA DHCPv6 Denial of Service Vulnerability
CSCuq62164	IPv6 stateless autoconfiguration fails if managed config flag in RA
CSCuq42475	IPv6 tunneled route on link-local interfaces
CSCty22380	USG-IPv6 / ReadyLogo P2 Conformance Bug NA changes Running Config
CSCuo27866	Traceback on DATAPATH-7-1524 Generating Botnet Filter Syslog
CSCur81376	ASA traceback in Thread Name: ci/console, assertion "snp_sp_action.c"

Table 10 Resolved Bugs in ASA Version 9.1(6) (continued)

Bug	Description
CSCus06652	ASA5580-20 8.4.7.23: Traceback in Thread Name: ssh
CSCur42907	Failed to allocate global ID when adding service-policy
CSCuo49385	Multicast - ASA doesn't populate mroutes after failover
CSCub53088	Arsenal:twice NAT with service type ftp not working.
CSCuq26046	ASA - Traceback in thread name SSH while changing NAT configuration
CSCun32324	ASA Cluster ICMP with PAT not functional on reload
CSCuo88253	ASA NAT: Some NAT removed after upgrade from 8.6.1.5 to 9.x
CSCup43257	ASA Traceback in Thread name: ci/console while modifying an object-group
CSCue51351	ASA: Huge NAT config causes traceback due to unbalanced p3 tree
CSCur65317	NAT pool address distribution fails,with NATtransactional-commit enabled
CSCuo37603	object nat config getting deleted after reloaded with vpdn config
CSCtz98516	Observed Traceback in SNMP while querying GET BULK for 'xlate count'
CSCup74532	ASA failover standby device reboots due to delays in config replication
CSCuf31654	Linux Kernel GUID Partition Tables Handling Arbitrary Code Execution V
CSCuf31607	Linux Kernel Invalid fs and gs Registry KVM Denial of Service Vulnerab
CSCuq62925	ASA: standby traceback during replication of specific privilege command
CSCur25542	Traceback: pki-crl: Thread Name: Crypto CA with traffic through VPN L2L
CSCun10916	Cisco ASA SCH Digital Certificate Validation Vulnerability
CSCum00360	ASA - DHCP Discover Sent out during boot process
CSCup47195	ASA - Traceback in DATAPATH-0-1275
CSCuo48593	ASA with SFP+4GE-SSM sends flow-control packets at line rate
CSCuo58584	Cisco ASA fix for CSCun56954
CSCup81146	jumbo frame enabled will cause ASA5585-20 in boot loop from 9.3.0.101
CSCup98176	Jumbo Frame is not support in the ASA558560 due to wrong bigphys size
CSCuo00627	Saleen copper module port speed/duplex changes ineffective
CSCup48979	ASA - Permitting/blocking traffic based on wrong IPs in ACL
CSCup48772	ASA - Wrong object-group migration during upgrade from 8.2
CSCul05079	ASA Memory usage in a context rises
CSCuq68271	ASA Cluster slave unit loses default route due to sla monitor
CSCul02052	ASA fails to set forward address in OSPF route redistrubution
CSCup16512	ASA traceback in Thread Name : Checkheaps when snmp config is cleared
CSCus27696	ASA:- SSH un-authenticated connections are not timing out
CSCur23709	ASA : evaluation of SSLv3 POODLE vulnerability
CSCug51375	ASA SSL: Continues to accept SSLv3 during TLSv1 only mode
CSCus08101	ASA: evaluation of Poodle Bites in TLSv1
CSCuq34213	Double Free when processing DTLS packets
CSCup22532	Multiple Vulnerabilities in OpenSSL - June 2014
CSCuq34226	OpenSSL Zero-Length Fragments DTLS Memory Leak Denial of Service Vuln

Table 10 Resolved Bugs in ASA Version 9.1(6) (continued)

Bug	Description
CSCuo44216	ASA traceback (Page fault) during xlate replication in a failover setup
CSCuo78285	ASA Traceback while running L2 BGP Adjacency in f/o during config sync
CSCuh01570	Dropped packets/Retries/Timeout on applying a huge ACL on existing acl
CSCuo68647	Traceback when no failover then clear conf all during xlate replication
CSCus30833	ASA: Page fault traceback in SXP CORE thread
CSCuq36615	Traceback caused by WCCP
CSCun11323	ASA: Traceback in aware_http_server_thread after upgrade
CSCuo08511	ASA 9.0.4.1 traceback in webvpn datapath
CSCup35713	ASA tmatch_summary_alloc block leak in binsize 1024
CSCur64589	DATAPATH Traceback in snp_mp_svc_udp_upstream_data function
CSCuq50366	Traceback may occur on bring up of multiple SSL sessions w/DHE
CSCup55377	ASA: Traceback Page Fault in vpnfol_thread_msg on Standby ASA
CSCuo93225	Traceback during AnyConnect IPv6 TLS TPS Test
CSCuq20396	Traceback when executing " show crypto accelerator load-balance"
CSCuo95074	ASA AnyConnect failure or crash in SSL Client compression with low mem
CSCug25761	ASA has inefficient memory use when cumulative AnyConnect session grows
CSCus95290	Cisco ASA VPN XML Parser Denial of Service Vulnerability
CSCun26381	ASA crashes in stress testing with user-storage enabled
CSCul04263	ASA Webvpn CIFS vnode_create: VNODE ALLOCATION LIMIT 100000 REACHED!
CSCuq47381	DMA memory leak in 256 byte fragments with nbns-server config
CSCuq24404	traceback in thread name: netfs_thread_init
CSCus14009	ASA WebVPN Citrix SSO: Chrome does not skip to login on external page
CSCuq29136	Cisco ASA SSL VPN Info Disclosure and DoS Vulnerability
CSCup36829	Cisco ASA SSL VPN Portal Customization Integrity Vulnerability
CSCuo54393	ASA: HTTP searchPendingOrders.do function failing over WebVPN
CSCup54184	Cisco ASA SharePoint RAMFS Integrity and Lua Injection Vulnerability
CSCur17483	nested custom write functions causing blank page through rewriter
CSCur49086	Traceback due to fiber_create failure in unicorn remove session dir

Resolved Bugs in Version 9.1(5)

Table 11 contains select resolved bugs in ASA Version 9.1(5).

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

https://tools.cisco.com/bugsearch

Table 11 Resolved Bugs in ASA Version 9.1(5)

Bug	Description
CSCsq82949	Algorithm ID encoding error causes CA cert to be unimportable on to ASA
CSCtb71323	Cisco ASA Webtype ACL By-Pass Vulnerability
CSCtc18329	ACL renamed but syslog doesn't reflect new name
CSCtk66541	ENH: ASA drops ICMP Error Reply for uni-directional SCTP Traffic
CSCtn30286	DHCP Relay needs to handle DHCPREQUEST differently
CSCtz92586	A warning message is needed when a new encryption license is applied
CSCua92694	Traceback on Configuration Manipulation over Telnet/SSH Sessions
CSCud24785	Slow throughput of AnyConnect client w/DTLS compared to IPSec IKEv1
CSCue51351	ASA: Huge NAT config causes traceback due to unbalanced p3 tree
CSCug49382	IKEv2 : L2L tunnel fails with error " Duplicate entry in Tunnel Manager"
CSCug87445	SVC_UDP Module is in flow control with a SINGLE DTLS tunnel
CSCuh61321	AC 3.1:ASA incorrectly handles alternate DTLS port,causes reconnect
CSCui04520	WebVpn: javascript parser error while rewriting libmin.js
CSCui30677	ENH - SCP Support on the ASA
CSCui44095	ASA 9.1: timer app id was corrupted causing to Dispatch Unit traceback
CSCui53710	ACL Migration to 8.3+ Software Unnecessarily Expands Object Groups
CSCui56863	ASA may reload with traceback in Thread Name: vpnfol_thread_msg
CSCui63001	ASA traceback in Thread Name: fover_parse during command replication
CSCui79979	ASA 9.1.2 - Traceback in Thread Name: fover_parse during configuration
CSCuj10294	CSCul37888Traceback in DATAPATH caused by HTTP Inspection
CSCuj23318	ASA 9.1 enabling IKE on one interface reserves UDP 500 on ALL interfaces
CSCuj26816	ENH - ASA and AAA Operations
CSCuj35576	ASA OSPF route stuck in database and routing table
CSCuj45406	ASA: Page fault traceback with 'show dynamic-filter dns-snoop detail'
CSCuj50870	ASA in failover pair may panic in shrlock_unjoin
CSCuj54639	ASA drops inspected HTTP when unrelated service-policy is removed
CSCuj59545	SSL connectivity to ASA stops working on failover
CSCuj62146	RU : Traceback on Thread Name : Cluster show config
CSCuj68055	ASA traceback in Thread Name: ssh on modifying service object
CSCuj68420	ASA SMR: Multicast traffic for some groups stops flowing after failover
CSCuj69650	ASA block new conns with " logging permit-hostdown" & TCP syslog is down
CSCuj71626	ST not injected in mstsc.exe on 64-bit Win 8 IE 10 when started TSWebApp
CSCuj72638	ASA-SM - TFW Dropping jumbo mcast traffic with 3 intf in a bridge group
CSCuj77219	ASA KCD traceback during domain leave or join
CSCuj82692	ASA 8.4.7 - Traceback with assertion in thread name Dispatch Unit
CSCuj83344	ASA traceback in Thread name - netfs_thread_init
CSCuj94335	watchdog at ci_delayed_acl_elem_addition when object-group-search access
CSCul00624	ASA: ARP Fails for Subinterface Allocated to Multiple Contexts on Gi0/6

Table 11 Resolved Bugs in ASA Version 9.1(5) (continued)

Bug	Description
CSCul05200	Webvpn rewriter some links from steal.js are mangled incorrectly
CSCul08896	ASA Webvpn: Rewriter issue with dynamic iframes
CSCul11741	Removing ports from service object-group does not remove from the ACL
CSCul13258	ASA rejects certificates with NULL param in ECDSA/SHA signature alg
CSCul17354	Traceback after upgrade from pre-8.3 to 8.3 and above
CSCul18059	Object Group Search may cause ACL to be matched incorrectly
CSCul22237	ASA may drop all traffic with Hierarchical priority queuing
CSCul25576	ASA: Page fault traceback after running show asp table socket
CSCul26755	INSPECT ICMP ERROR ICMP HEADER AFTER UN_NAT DOES NOT MATCH IP DST ADDR
CSCul28082	ASA traceback in Thread Name: DATAPATH due to double block free
CSCul33074	ASA: Hitless upgrade fails with port-channels
CSCul34143	ENH: Need to optimize messages printed on upgrade from 8.2- to 8.3+
CSCul37560	ASA traceback when uploading an image using FTP
CSCul41183	ASA 5585 High Memory due to dACLs installed from cut-through-proxy
CSCul41447	ASA: Memory leak with WebVPN and HTTP server enabled simultaneously
CSCul41718	traceback on master VPNLB ASA after switch port failure conditions
CSCul46000	2048 byte block depletion with Smart-Tunnel Application
CSCul46582	ASA: Out of order Fin packet leaves connection half closed
CSCul47395	ASA should allow out-of-order traffic through normalizer for ScanSafe
CSCul47481	ASA WebVPN Login portal returns to login page after successful login
CSCul48261	Cannot enable IPSEC encrypted failover without Stateful link
CSCul49796	ASA Tranparent A/A - Replicated MAC addresses not deleted after timeout
CSCul52942	ASA failover cluster traceback when replicating the configuration
CSCul60058	Case sensitivity check missing for Web Type ACL and Access-group
CSCul60950	IPSEC VPN - One crypto ACE mismatch terminates all Phase2 with that peer
CSCul61939	Webvpn: ASA fails to rewrite javascript tag correctly
CSCul62357	ASA fails to perform KCD SSO when web server listens on non-default port
CSCul64980	Acct-stop for VPN session doesn't send out when failover occurred
CSCul65069	ASA Assert Traceback in Dispatch Unit during LU Xlate replication
CSCul67705	ASA sends RST to both ends when CX policy denies based on destination IP
CSCul68363	EIGRP: Auth key with space replicates to Secondary with no space
CSCul70712	ASA: ACL CLI not converting 0.0.0.0 0.0.0.0 to any4
CSCul74286	ASA: Phy setting change on member interfaces not seen on port-channel
CSCul77465	BPDUs on egress from ASA-SM dropped on backplane
CSCul82354	ASA should not forward multicast packets to the CX - Multicast Drops
CSCul83331	Redundant IFC not Switching Back
CSCul84216	ASA - Remote access VPN sessions are not replicated to Standby unit
CSCul90151	ASA EIGRP redistribute static shows up as internal route

Table 11 Resolved Bugs in ASA Version 9.1(5) (continued)

Bug	Description
CSCul95239	Copying configuration to running-config fails
CSCul96580	ASA tears down SIP signaling conn w/ reason Connection timeout
CSCul96864	ASA translates the source address of OSPF hello packets
CSCul98420	'Route-Lookup' Behavior Assumed for Twice NAT with Identity Destination
CSCum00556	Page fault traceback in DATAPATH under DoS, rip qos_topn_hosts_db_reset
CSCum00826	ASA reloads on Thread name: idfw_proc
CSCum01313	ASA drops DHCP Offer packet in ASP when nat configured with " Any"
CSCum06272	ASA reloads due to SSL processing
CSCum16576	ASA not allowing AC IKEv2 Suite-B with default Premium Peer license
CSCum16787	SSH: ASA 9.1.3 rare traceback observed during ping command
CSCum23018	ASA traceback with Thread Name: IKE Common thread
CSCum24634	IKEv1 - Send INVALID_ID_INFO when received P2 ID's not in crypto map
CSCum26955	Webvpn: Add permissions attribute to portforwarder jar file
CSCum26963	Webvpn: Add permissions attribute to mac smart-tunnel jar
CSCum37080	Traceback in IKEv2 Daemon with AnyConnect Failure
CSCum39328	uauth session considered inactive when inspect icmp is enabled
CSCum39333	idle time field is missing in show uauth output
CSCum44040	Anyconnect wrong User Messages printed after weblaunch RE-DAP
CSCum47174	WebVPN configs not synchronized when configured in certain order-v3
CSCum54163	IKEv2 leaks embryonic SAs during child SA negotiation with PFS mismatch
CSCum60784	ASA traceback on NAT assert on file nat_conf.c
CSCum65278	ASA 5500-X: Chassis Serial Number missing in entity MIB
CSCum68923	Webvpn: connecting to oracle network SSO returns error
CSCum69144	HTTP redirect to the VPNLB address using HTTPS fails in 9.1.4/9.0.4.x
CSCum82840	ASA: Traceback in pix_flash_config_thread when upgrading with names
CSCun48868	ASA changes to improve CX throughput and prevent unnecessary failovers
CSCun53447	Enhance the Host Group configuration to allow upto 4K snmp polling hosts

Resolved Bugs in Version 9.1(4)

Table 12 contains select resolved bugs in ASA Version 9.1(4).

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

https://tools.cisco.com/bugsearch

Table 12 Resolved Bugs in ASA Version 9.1(4)

Bug	Description
CSCtd57392	Unable to create policy map depending on existing maps and name
CSCtg31077	DHCP relay binding limit of 100 should be increased to 500
CSCtg63826	ASA: multicast 80-byte block leak in combination with phone-proxy
CSCtr80800	Improve HTTP inspection's logging of proxied HTTP GETs
CSCtu37460	Backup Shared License Server unable to open Socket
CSCtw82904	ESP packet drop due to failed anti-replay checking after HA failovered
CSCty13865	ASA DHCP proxy for VPN clients should use ARP cache to reach server
CSCtz70573	SMP ASA traceback on periodic_handler for inspecting icmp or dns trafic
CSCub43580	Traceback during child SA rekey
CSCud16208	ASA 8.4.4.5 - Traceback in Thread Name: Dispatch Unit
CSCue33632	ASA 5500x on 9.1.1 IPS SW module reset causes ASA to reload.
CSCug33233	ASA Management lost after a few days of uptime
CSCug48732	Crash when loading configuration from TFTP multiple contexts
CSCug97772	Watchdog due to access-list change during uauth
CSCuh03193	ASA - Not all GRE connections are replicated to the standby unit
CSCuh12279	ASA: Data packets with urgent pointer dropped with IPS as bad-tcp-cksum
CSCuh21682	ASA traceback with less PAT with huge traffic
CSCuh32106	ASA KCD is broken in 8.4.5 onwards
CSCuh38785	Improve ScanSafe handling of Segment HTTP requests
CSCuh70040	Renew SmartTunnel Web Start .jnlp Certificate 9/7/2013
CSCui00618	ASA does not send Gratuitous ARP(GARP) when booting
CSCui01258	limitation of session-threshold-exceeded value is incorrect
CSCui06108	LU allocate xlate failed after Standby ASA traceback
CSCui08074	ak47 instance got destroyed issue
CSCui12430	ASA: SIP inspection always chooses hairpin NAT/PAT for payload rewrite
CSCui19504	ASA: HA state progression failure after reload of both units in HA
CSCui20216	ASA CX Fail-Open Drops traffic during reload
CSCui20346	ASA: Watchdog traceback in DATAPATH thread
CSCui22862	ASA traceback when using " Capture Wizard" on ASDM
CSCui24669	ASA PAT rules are not applied to outbound SIP traffic version 8.4.5/6
CSCui25277	ASA TFW doesn't rewrite VLAN in BPDU packets containing Ethernet trailer
CSCui36033	PP: VoIP interface fails replication on standby due to address overlap
CSCui36550	ASA crashes in Thread Name: https_proxy
CSCui38495	ASA Assert in Checkheaps chunk create internal
CSCui41794	ASA A/A fover automatic MAC address change causes i/f monitoring to fail
CSCui45340	ASA-SM assert traceback in timer-infra
CSCui45606	ASA traceback upon resetting conn due to filter and inspect overlap
CSCui51199	Cisco ASA Clientless SSL VPN Rewriter Denial of Service

Table 12 Resolved Bugs in ASA Version 9.1(4) (continued)

Bug	Description
CSCui55190	Failover cluster traceback while modifying object groups via SSH
CSCui55510	ASA traceback in Thread Name: DATAPATH-2-1140
CSCui55978	ASA 8.2.5 snmpEngineTime displays incorrect values
CSCui57181	ASA/IKEv1-L2L: Do not allow two IPsec tunnels with identical proxy IDs
CSCui61335	Traceback in Thread: DATAPATH-3-1281 Page fault: Address not mapped
CSCui61822	ASA 5585 - traceback after reconnect failover link and 'show run route'
CSCui63322	ASA Traceback When Debug Crypto Archives with Negative Pointers
CSCui65495	ASA 5512 - Temporary security plus license does not add security context
CSCui66657	Safari crashes when use scroll in safari on MAC 10.8 with smart-tunnel
CSCui70562	AnyConnect Copyright Panel and Logon Form message removed after upgrade
CSCui75284	ASA: Summary IPv6 range not advertised by ABR for OSPFv3
CSCui76124	ASA telnet limit reached 9.0.3
CSCui78992	ASA after fover may not flush routes for an active grp in active/standby
CSCui80059	ASA traceback in pix_startup_thread
CSCui80835	ASA drops packet as PAWS failure after incorrect TSecr is seen
CSCui85750	ASA SCH Inventory message incorrectly set at Severity 10
CSCui88578	Failure when accessing CIFS share with period character in username
CSCui91247	ASA does not pass calling-station-id when doing cert base authentication
CSCui94757	ASA tears down SIP signaling conn w/ reason Connection timeout
CSCui98879	Clientless SSL VPN:Unable to translate for Japanese
CSCuj00614	SNMP environmental parameters oscillate on 5512,25,45 and 5550 platforms
CSCuj06865	ASA traceback when removing more than 210 CA certificates at once
CSCuj08004	AnyConnect states: " VPN configuration received... has an invalid format"
CSCuj10559	ASA 5505: License Host limit counts non-existent hosts
CSCuj13728	ASA unable to remove ipv6 address from BVI interface
CSCuj16320	ASA 8.4.7 Multi Context TFW not generating any syslog data
CSCuj23632	Certificate CN and ASA FQDN mismatch causes ICA to fail.
CSCuj26709	ASA crashes on access attempt via Citrix Receiver
CSCuj28701	ASA - Default OSPF/EIGRP route gone in Active unit
CSCuj28861	Cisco ASA Malformed DNS Reply Denial of Service Vulnerability
CSCuj28871	ASA WebVPN: Rewriter doesn't work well with Base path and HTTP POST
CSCuj29434	ASA5505 - Max Conn Limit Does Not Update When Adding Temp Sec Plus Key
CSCuj33401	vpn_sanity script ipv4 DTLS RA testing using load-balancing fails
CSCuj33701	traceback ABORT(-87): strcpy_s: source string too long for dest
CSCuj34124	Sustained high cpu usage in Unicorn proxy thread with jar file rewrite
CSCuj34241	no debug all, undebug all CLI commands doesnt reset unicorn debug level
CSCuj39040	syslog 402123 CRYPTO: The ASA hardware accelerator encountered an error
CSCuj39069	ASA:" IKEv2 Doesn't have a proposal specified" though IKEv2 is disabled

Table 12 Resolved Bugs in ASA Version 9.1(4) (continued)

Bug	Description
CSCuj39727	Unable to modify existing rules/network groups after few days up time
CSCuj42515	ASA reloads on Thread name: idfw_proc
CSCuj43339	Add X-Frame-Options: SAMEORIGIN to ASDM HTTP response
CSCuj44998	ASA drops inbound traffic from AnyConnect Clients
CSCuj47104	EIGRP routes on the active ASA getting deleted after the ASA failover
CSCuj49690	ikev2 L2L cannot be established between contexts on the same ASA
CSCuj50376	ASA/Access is denied to the webfolder applet for a permitted cifs share
CSCuj51075	Unable to launch ASDM with no username/password or with enable password
CSCuj54287	ASA ACL not applied object-group-search enabled & first line is remark
CSCuj58096	Crypto chip resets with large SRTP payload on 5555
CSCuj58670	Local CA server doesn't notify the first time allowed user
CSCuj60572	Unable to assign ip address from the local pool due to 'Duplicate local'
CSCuj62146	RU : Traceback on Thread Name : Cluster show config
CSCuj74318	ASA: crypto engine large-mod-accel support in multple context
CSCuj81046	ASA defaults to incorrect max in-negotiation SA limit
CSCuj81157	ASA does not enforce max in-negotiation SA limit
CSCuj85424	Transparent ASA in Failover : Management L2L VPN termination fails
CSCuj88114	WebVPN Java rewriter issue: Java Plugins fail after upgrade to Java 7u45
CSCuj95555	SNMP: ccaAcclEntity MIB info for 5585 not consistent with CLI
CSCuj97361	DNS request failing with debugs " unable to allocate a handle"
CSCuj99263	Wrong ACL seq & remarks shown when using Range object w/ object-group
CSCul00917	SNMP: ccaGlobalStats values do not include SW crypto engine
CSCul19727	NPE: Querying unsupported IKEv2 MIB causes crash
CSCul35600	WebVPN: sharepoint 2007/2010 and Office2007 can't download/edit pictures

Resolved Bugs in Version 9.1(3)

Table 13 contains select resolved bugs in ASA Version 9.1(3).

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

https://tools.cisco.com/bugsearch

Table 13 Resolved Bugs in ASA Version 9.1(3)

Bug	Description
CSCsv41155	reload due to block depletion needs post-event detection mechanism
CSCtg63826	ASA: multicast 80-byte block leak in combination with phone-proxy
CSCtw57080	Protocol Violation does not detect violation from client without a space
CSCua69937	Traceback in DATAPATH-1-1143 thread: abort with unknown reason
CSCua98219	Traceback in ci/console during context creation - ssl configuration

Table 13 Resolved Bugs in ASA Version 9.1(3) (continued)

Bug	Description
CSCub50435	Proxy ARP Generated for Identity NAT Configuration in Transparent Mode
CSCub52207	Nested Traceback from Watchdog in tmatch_release_recursive_locks()
CSCuc00279	ASA doesn't allow reuse of object when pat-pool keyword is configured
CSCuc66362	CP Processing hogs in SMP platform causing failover problems, overruns
CSCud05798	FIPS Self-Test failure,fips_continuous_rng_test [-1:8:0:4:4]
CSCud20080	ASA Allows duplicate xlate-persession config lines
CSCud21312	ASA verify /md5 shows incorrect sum for files
CSCud34973	ASA stops decrypting traffic after phase2 rekey under certain conditions
CSCud50997	ASA IKEv2 fails to accept incoming IKEV2 connections
CSCud76481	ASA 8.6/9.x : Fails to parse symbols in LDAP attribute name
CSCud84290	ASA: Random traceback with HA setup with 9.1.(1)
CSCud98455	ASA: 256 byte blocks depleted when syslog server unreachable across VPN
CSCue11738	ACL migration issues with NAT
CSCue27223	Standby sends proxy neighbor advertisements after failover
CSCue34342	ASA may traceback due to watchdog timer while getting mapped address
CSCue46275	Connections not timing out when the route changes on the ASA
CSCue46386	Cisco ASA Xlates Table Exhaustion Vulnerability
CSCue48432	Mem leak in PKI: crypto_get_DN_DER
CSCue51796	OSPF routes missing for 10 secs when we failover one of ospf neighbour
CSCue60069	ENH: Reload ASA when free memory is low
CSCue62422	Multicast,Broadcast traffic is corrupted on a shared interface on 5585
CSCue67198	Crypto accelerator resets with error code 23
CSCue78836	ASA removes TCP connection prematurely when RPC inspect is active
CSCue88423	ASA traceback in datapath thread with netflow enabled
CSCue90343	ASA 9.0.1 & 9.1.1 - 256 Byte Blocks depletion
CSCue95008	ASA - Threat detection doesn't parse network objects with IP 'range'
CSCue98716	move OSPF from the punt event queue to its own event queue
CSCuf07393	ASA assert traceback during xlate replication in a failover setup
CSCuf27008	Webvpn: Cifs SSO fails first attempt after AD password reset
CSCuf29783	ASA traceback in Thread Name: ci/console after write erase command
CSCuf31253	Floating route takes priority over the OSPF routes after failover
CSCuf31391	ASA failover standby unit keeps reloading while upgrade 8.4.5 to 9.0.1
CSCuf64977	No debug messages when DHCP OFFER packet dropped due to RFC violations
CSCuf67469	ASA sip inspection memory leak in binsize 136
CSCuf68858	ASA: Page fault traceback in dbgtrace when running debug in SSH session
CSCuf71119	Incorrect NAT rules picked up due to divert entries
CSCuf79091	Cisco ASA time-range object may have no effect
CSCuf85295	ASA changes user privilege by vpn tunnel configuration

Table 13 Resolved Bugs in ASA Version 9.1(3) (continued)

Bug	Description
CSCuf85524	Traceback when NULL pointer was passed to the l2p function
CSCuf90410	ASA LDAPS authorization fails intermittently
CSCuf92320	ASA-CX: Cosmetic parser error " 'sw-module cxsc recover configure image"
CSCuf93071	ASA 8.4.4.1 traceback in threadname Datapath
CSCuf93843	No value or incorrect value for SNMP OIDs needed to identify VPN clients
CSCug03975	ASA 9.1(1) Reboot while applying regex dns
CSCug08285	Webvpn: OWA 2010 fails to load when navigating between portal and OWA
CSCug10123	ASA sends ICMP Unreach. thro wrong intf. under certain condn.
CSCug13534	user-identity will not retain group names with spaces on reboot
CSCug23311	cannot access Oracle BI via clentless SSL VPN
CSCug25761	ASA has inefficient memory use when cumulative AnyConnect session grows
CSCug29809	Anyconnect IKEv2:Truncated/incomplete debugs,missing 3 payloads
CSCug31704	ASA - "Show Memory" Output From Admin Context is Invalid
CSCug33233	ASA Management lost after a few days of uptime
CSCug39080	HA sync configuration stuck -"Unable to sync configuration from Active"
CSCug45645	Standby ASA continues to forward Multicast Traffic after Failover
CSCug45674	ASA : HTTP Conn from the box, broken on enabling TCP-State-Bypass
CSCug51148	Responder uses pre-changed IP address of initiator in IKE negotiation
CSCug53708	Thread Name: Unicorn Proxy Thread
CSCug55657	ASA does not assign MTU to AnyConnect client in case of IKEv2
CSCug55969	ASA uses different mapped ports for SDP media port and RTP stream
CSCug56940	ASA Config Locked by another session prevents error responses.
CSCug58801	ASA upgrade from 8.4 to 9.0 changes context's mode to router
CSCug63063	ASA 9.x: DNS inspection corrupts RFC 2317 PTR query
CSCug64098	ASA 9.1.1-7 traceback with Checkheaps thread
CSCug66457	ASA : "ERROR:Unable to create router process" & routing conf is lost
CSCug71714	DHCPD appends trailing dot to option 12 [hostname] in DHCP ACK
CSCug72498	ASA scansafe redirection drops packets if tcp mss is not set
CSCug74860	Multiple concurrent write commands on ASA may cause failure
CSCug75709	ASA terminates SIP connections prematurely generating syslog FIN timeout
CSCug76763	Cannot login webvpn portal when Passwd mgmt is enabled for Radius server
CSCug77782	ASA5585 - 9.1.1 - Traceback on IKEv2Daemon Thread
CSCug78561	ASA Priority traffic not subject to shaping in Hierarchical QoS
CSCug79778	ASA standby traceback in fover_parse when upgrading to 9.0.2
CSCug82031	ASA traceback in Thread Name: DATAPATH-4-2318
CSCug83036	L2TP/IPSec traffic fails because UDP 1701 is not removed from PAT
CSCug83080	Cross-site scripting vulnerability
CSCug86386	Inconsistent behavior with dACL has syntax error

Table 13 Resolved Bugs in ASA Version 9.1(3) (continued)

Bug	Description
CSCug87482	webvpn redirection fails when redirection FQDN is same as ASA FQDN
CSCug90225	ASA: EIGRP Route Is Not Updated When Manually Adding Delay on Neighbor
CSCug94308	ASA: " clear config all" does not clear the enable password
CSCug95287	ASA IDFW: idle users not marked as 'inactive' after default idle timeout
CSCug98852	Traceback when using VPN Load balancing feature
CSCug98894	Traceback in Thread Name: OSPF Router during interface removal
CSCuh01167	Unable to display webpage via WebVPN portal, ASA 9.0(2)9
CSCuh01983	ASA teardown TCP SIP phone registration conn due to SIP inspection
CSCuh05751	WebVPN configs not synchronized when configured in certain order
CSCuh05791	Single Sign On with BASIC authentication does not work
CSCuh08432	Anyconnect sessions do not connect due to uauth failure
CSCuh08651	UDP ports 500/4500 not reserved from PAT on multicontext ASA for IKEv1
CSCuh10076	Some interface TLVs are not sent in a bridge group in trans mode ASA
CSCuh10827	Cisco ASA config rollback via CSM doesnt work in multi context mode
CSCuh12375	ASA multicontext transparent mode incorrectly handles multicast IPv6
CSCuh13899	ASA protcol inspection connection table fill up DOS Vulnerability
CSCuh14302	quota management-session not working with ASDM
CSCuh19234	Traceback after upgrade from 8.2.5 to 8.4.6
CSCuh19462	ASA 9.1.2 - Memory corruptions in ctm hardware crypto code.
CSCuh20372	ASA adds 'extended' keyword to static manual nat configuration line
CSCuh20716	Re-transmitted FIN not allowed through with sysopt connection timewait
CSCuh22344	ASA: WebVPN rewriter fails to match opening and closing parentheses
CSCuh23347	ASA:Traffic denied 'licensed host limit of 0 exceeded
CSCuh27912	ASA does not obfuscate aaa-server key when timeout is configured.
CSCuh33570	ASA: Watchdog traceback in SSH thread
CSCuh34147	ASA memory leaks 3K bytes each time executing the show tech-support.
CSCuh40372	ASA Round-Robin PAT doesn't work under load
CSCuh45559	ASA: Page fault traceback when changing ASP drop capture buffer size
CSCuh48005	ASA doesn't send NS to stale IPv6 neighbor after failback
CSCuh48577	Slow memory leak on ASA due to SNMP
CSCuh49686	slow memory leak due to webvpn cache
CSCuh52326	ASA: Service object-group not expanded in show access-list for IDFW ACLs
CSCuh56559	ASA removed from cluster when updating IPS signatures
CSCuh58576	Different SNMPv3 Engine Time and Engine Boots in ASA active / standby
CSCuh66892	ASA: Unable to apply " http redirect <interface_name> 80" for webvpn
CSCuh69818	ASA 9.1.2 traceback in Thread Name ssh
CSCuh69931	ASA 5512 - 9.1.2 Traceback in Thread Name: ssh
CSCuh73195	Tunneled default route is being preferred for Botnet updates from ASA

Table 13 Resolved Bugs in ASA Version 9.1(3) (continued)

Bug	Description
CSCuh74597	ASA-SM multicast boundary command disappears after write standby
CSCuh78110	Incorrect substitution of 'CSCO_WEBVPN_INTERNAL_PASSWORD' value in SSO
CSCuh79288	ASA 9.1.2 DHCP - Wireless Apple devices are not getting an IP via DHCPD
CSCuh79587	ASA5585 SSM card health displays down in ASA version 9.1.2
CSCuh80522	nat config is missing after csm rollback operation.
CSCuh90799	ASA 5505 Ezvpn Client fails to connect to Load Balance VIP on ASA server
CSCuh94732	Traceback in DATAPATH-1-2533 after a reboot in a clustered environment
CSCuh95321	Not all contexts successfully replicated to standby ASA-SM
CSCui10904	Macro substitution fails on External portal page customization
CSCui13436	ASA-SM can't change firewall mode using session from switch
CSCui15881	ASA Cluster - Loss of CCL link causes clustering to become unstable
CSCui27831	Nested Traceback with No Crashinfo File Recorded on ACL Manipulation
CSCui42956	ASA registers incorrect username for SSHv2 Public Key Authenticated user
CSCui48221	ASA removes RRI-injected route when object-group is used in crypto ACL

Resolved Bugs in Version 9.1(2)

Table 14 contains select resolved bugs in ASA Version 9.1(2).

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

https://tools.cisco.com/bugsearch

Table 14 Resolved Bugs in ASA Version 9.1(2)

Bug	Description
CSCti07431	1/5 minute input rate and output rate are always 0 with user context.
CSCti38856	Elements in the network object group are not converted to network object
CSCtj87870	Failover disabled due to license incompatible different Licensed cores
CSCto50963	ASA SIP inspection - To: in INVITE not translated after 8.3/8.4 upgrade
CSCtr04553	Traceback while cleaning up portlist w/ clear conf all or write standby
CSCtr17899	Some legitimate traffic may get denied with ACL optimization
CSCtr65927	dynamic policy PAT fails with FTP data due to latter static NAT entry
CSCts15825	RRI routes are not injected after reload if IP SLA is configured.
CSCts50723	ASA: Builds conn for packets not destined to ASA's MAC in port-channel
CSCtw56859	Natted traffic not getting encrypted after reconfiguring the crypto ACL
CSCtx55513	ASA: Packet loss during phase 2 rekey
CSCty18976	ASA sends user passwords in AV as part of config command authorization.
CSCty59567	Observing traceback @ ipigrp2_redist_metric_incompatible+88
CSCtz46845	ASA 5585 with IPS inline -VPN tunnel dropping fragmented packets
CSCtz47034	ASA 5585- 10 gig interfaces may not come up after asa reload

Table 14 Resolved Bugs in ASA Version 9.1(2) (continued)

Bug	Description
CSCtz56155	misreported high CPU
CSCtz64218	ASA may traceback when multiple users make simultaneous change to ACL
CSCtz70573	SMP ASA traceback on periodic_handler for inspecting icmp or dns trafic
CSCtz79578	Port-Channel Flaps at low traffic rate with single flow traffic
CSCua13405	Failover Unit Stuck in Cold Standby After Boot Up
CSCua20850	5500X Software IPS console too busy for irq can cause data plane down.
CSCua22709	ASA traceback in Unicorn Proxy Thread while processing lua
CSCua35337	Local command auth not working for certain commands on priv 1
CSCua44723	ASA nat-pat: 8.4.4 assert traceback related to xlate timeout
CSCua60417	8.4.3 system log messages should appear in Admin context only
CSCua87170	Interface oversubscription on active causes standby to disable failover
CSCua91189	Traceback in CP Processing when enabling H323 Debug
CSCua93764	ASA: Watchdog traceback from tmatch_element_release_actual
CSCua99091	ASA: Page fault traceback when copying new image to flash
CSCub04470	ASA: Traceback in Dispatch Unit with HTTP inspect regex
CSCub08224	ASA 210005 and 210007 LU allocate xlate/conn failed with simple 1-1 NAT
CSCub11582	ASA5550 continous reboot with tls-proxy maximum session 4500
CSCub14196	FIFO queue oversubscription drops packets to free RX Rings
CSCub16427	Standby ASA traceback while replicating flow from Active
CSCub23840	ASA traceback due to nested protocol object-group used in ACL
CSCub37882	Standby ASA allows L2 broadcast packets with asr-group command
CSCub58996	Cisco ASA Clientless SSLVPN CIFS Vulnerability
CSCub61578	ASA: Assert traceback in PIX Garbage Collector with GTP inspection
CSCub62584	ASA unexpectedly reloads with traceback in Thread Name: CP Processing
CSCub63148	With inline IPS and heavy load ASA could drop ICMP or DNS replies
CSCub72545	syslog 113019 reports invalid address when VPN client disconnects.
CSCub75522	ASA TFW sends broadcast arp traffic to all interfaces in the context
CSCub83472	VPNFO should return failure to HA FSM when control channel is down
CSCub84164	ASA traceback in threadname Logger
CSCub89078	ASA standby produces traceback and reloads in IPsec message handler
CSCub98434	ASA: Nested Crash in Thread Dispatch Unit - cause: SQLNet Inspection
CSCub99578	High CPU HOG when connnect/disconnect VPN with large ACL
CSCub99704	WebVPN - mishandling of request from Java applet
CSCuc06857	Accounting STOP with caller ID 0.0.0.0 if admin session exits abnormally
CSCuc09055	Nas-Port attribute different for authentication/accounting Anyconnect
CSCuc12119	ASA: Webvpn cookie corruption with external cookie storage
CSCuc12967	OSPF routes were missing on the Standby Firewall after the failover
CSCuc14644	SIP inspect NATs Call-ID in one direction only

Table 14 Resolved Bugs in ASA Version 9.1(2) (continued)

Bug	Description
CSCuc16455	ASA packet transmission failure due to depletion of 1550 byte block
CSCuc16670	ASA - VPN connection remains up when DHCP rebind fails
CSCuc24547	TCP ts_val for an ACK packet sent by ASA for OOO packets is incorrect
CSCuc24919	ASA: May traceback in Thread Name: fover_health_monitoring_thread
CSCuc28903	ASA 8.4.4.6 and higher: no OSPF adj can be build with Portchannel port
CSCuc34345	Multi-Mode treceback on ci/console copying config tftp to running-config
CSCuc40450	error 'Drop-reason: (punt-no-mem) Punt no memory' need to be specific
CSCuc45011	ASA may traceback while fetching personalized user information
CSCuc46026	ASA traceback: ASA reloaded when call home feature enabled
CSCuc46270	ASA never removes qos-per-class ASP rules when VPN disconnects
CSCuc48355	ASA webvpn - URLs are not rewritten through webvpn in 8.4(4)5
CSCuc50544	Error when connecting VPN: DTLS1_GET_RECORD Reason: wrong version number
CSCuc55719	Destination NAT with non single service (range, gt, lt) not working
CSCuc56078	Traceback in threadname CP Processing
CSCuc60950	Traceback in snpi_divert with timeout floating-conn configured
CSCuc61985	distribute-list does not show in the router config.
CSCuc63592	HTTP inspection matches incorrect line when using header host regex
CSCuc65775	ASA CIFS UNC Input Validation Issue
CSCuc74488	ASA upgrade fails with large number of static policy-nat commands
CSCuc74758	Traceback: deadlock between syslog lock and host lock
CSCuc75090	Crypto IPSec SA's are created by dynamic crypto map for static peers
CSCuc75093	Log indicating syslog connectivity not created when server goes up/down
CSCuc78176	Cat6000/15.1(1)SY- ASASM/8.5(1.14) PwrDwn due to SW Version Mismatch
CSCuc79825	ASA: Traceback in Thread Name CP Midpath Processing eip pkp_free_ssl_ctm
CSCuc83059	traceback in fover_health_monitoring_thread
CSCuc83323	XSS in SSLVPN
CSCuc83828	ASA Logging command submits invalid characters as port zero
CSCuc89163	Race condition can result in stuck VPN context following a rekey
CSCuc92292	ASA may not establish EIGRP adjacency with router due to version issues
CSCuc95774	access-group commands removed on upgrade to 9.0(1)
CSCuc98398	ASA writes past end of file system then can't boot
CSCud02647	traffic is resetting uauth timer
CSCud16590	ASA may traceback in thread emweb/https
CSCud17993	ASA-Traceback in Dispatch unit due to dcerpc inspection
CSCud20887	ASA reloads after issuing " show inventory" command
CSCud21714	BTF traceback in datapth when apply l4tm rule
CSCud24452	ASA TACACS authentication on Standby working incorrectly
CSCud28106	IKEv2: ASA does not clear entry from asp table classify crypto

Table 14 Resolved Bugs in ASA Version 9.1(2) (continued)

Bug	Description
CSCud29045	ASASM forwards subnet directed bcast back onto that subnet
CSCud32111	Deny rules in crypto acl blocks inbound traffic after tunnel formed
CSCud36686	Deny ACL lines in crypto-map add RRI routes
CSCud37992	SMP ASA traceback in periodic_handler in proxyi_rx
CSCud41507	Traffic destined for L2L tunnels can prevent valid L2L from establishing
CSCud41670	ASA nested traceback with url-filtering policy during failover
CSCud57759	DAP: debug dap trace not fully shown after +1000 lines
CSCud62661	STI Flash write failure corrupts large files
CSCud65506	ASA5585: Traceback in Thread Name:DATAPATH when accessing webvpn urls
CSCud67282	data-path: ASA-SM: 8.5.1 traceback in Thread Name: SSH
CSCud69251	traceback in ospf_get_authtype
CSCud69535	OSPF routes were missing on the Active Firewall after the failover
CSCud70273	ASA may generate Traceback while running packet-tracer
CSCud77352	Upgrade ASA causes traceback with assert during spinlock
CSCud81304	TRACEBACK, DATAPATH-8-2268, Multicast
CSCud84454	ASA in HA lose shared license post upgrade to 9.x
CSCud89974	flash in ASA5505 got corrupted
CSCud90534	ASA traceback with Checkheaps thread
CSCue02226	ASA 9.1.1 - WCCPv2 return packets are dropped
CSCue03220	Anyconnect mtu config at ASA not taking effect at client
CSCue04309	TCP connection to multicast MAC - unicast MAC S/ACK builds new TCP conn
CSCue05458	16k blocks near exhaustion - process emweb/https (webvpn)
CSCue11669	ASA 5505 not Forming EIGRP neighborship after failover
CSCue15533	ASA:Crash while deleting trustpoint
CSCue18975	ASA: Assertion traceback in DATAPATH thread after upgrade
CSCue25524	Webvpn: Javascript based applications not working
CSCue31622	Secondary Flows Lookup Denial of Service Vulnerability
CSCue32221	LU allocate xlate failed (for NAT with service port)
CSCue34342	ASA may crash due to watchdog timer while getting mapped address
CSCue35150	ASA in multicontext mode provides incorrect SNMP status of failover
CSCue35343	Memory leak of 1024B blocks in webvpn failover code
CSCue49077	ASA: OSPF fails to install route into asp table after a LSA update
CSCue54264	WebVPN: outside PC enabled webvpn to management-access inside interface
CSCue55461	ESMTP drops due to MIME filename length >255
CSCue59676	ASA shared port-channel subinterfaces and multicontext traffic failure
CSCue62470	mrib entries mayy not be seen upon failover initiated by auto-update
CSCue62691	ASASM Traceback when issue 'show asp table interface' command
CSCue63881	ASA SSHv2 Denial of Service Vulnerability

Table 14 Resolved Bugs in ASA Version 9.1(2) (continued)

Bug	Description
CSCue67446	The ASA hardware accelerator encountered an error (Bad checksum)
CSCue73708	Group enumeration still possible on ASA
CSCue77969	Character encoding not visible on webvpn portal pages.
CSCue82544	ASA5585 8.4.2 Traceback in Thread Name aaa while accessing Uauth pointer
CSCue88560	ASA Traceback in Thread Name : CERT API
CSCue99041	Smart Call Home sends Environmental message every 5 seconds for 5500-X
CSCuf02988	ASA: Page fault traceback in aaa_shim_thread
CSCuf06633	ASA crash in Thread Name: UserFromCert
CSCuf07810	DTLS drops tunnel on a crypto reset
CSCuf11285	ASA 9.x cut-through proxy ACL incorrectly evaluated
CSCuf16850	split-dns cli warning msg incorrect after client increasing the limit
CSCuf27811	ASA: Pending DHCP relay requests not flushed from binding table
CSCuf34123	ASA 8.3+ l2l tunnel-group name with a leading zero is changed to 0.0.0.0
CSCuf34754	Framed-IP-Address not sent with AC IKEv2 and INTERIM-ACCOUNTING-UPDATE
CSCuf47114	ASA 9.x: DNS inspection corrupts PTR query before forwarding packet
CSCuf52468	ASA Digital Certificate Authentication Bypass Vulnerability
CSCuf57102	FIPS: Continuous RNG test reporting a length failure
CSCuf58624	snmp engineID abnormal for asa version 8.4.5 after secondary asa reload
CSCuf65912	IKEv2: VPN filter ACL lookup failure causing stale SAs and crash
CSCuf77065	Arsenal: Single Core Saleen Admin Driver Fix Revert Bug
CSCuf77294	ASA traceback with Thread Name: DATAPATH-3-1041
CSCuf77606	ASA-SM crash in Thread Name: accept/http
CSCuf89220	ASA IDFW : Unable to handle contacts in DC user groups
CSCug03975	ASA 9.1(1) Reboot while applying regex dns
CSCug14707	ASA 8.4.4.1 Keeps rebooting when FIPS is enabled: FIPS Self-Test failure
CSCug19491	ASA drops some CX/CSC inspected HTTP packets due to PAWS violation
CSCug22787	Change of behavior in Prefill username from certificate SER extraction
CSCug30086	ASA traceback on thread Session Manager
CSCug59177	Page fault on ssh thread

Resolved Bugs in Version 9.1(1)

There are no resolved bugs in Version 9.1(1).

End-User License Agreement

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

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

Related Documentation

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

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

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation*.

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the What's New in Cisco Product Documentation RSS feed. The RSS feeds are a free service.

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

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.