Release Notes for the Cisco ASA Series, 9.17(x)

Release Notes for the Cisco ASA Series, 9.17(x)

This document contains release information for Cisco ASA software Version 9.17(x).

Important Notes

- **ASDM signed-image support in 9.17(1.13)/7.18(1.152) and later**—The ASA now validates whether the ASDM image is a Cisco digitally signed image. If you try to run an older ASDM image with an ASA version with this fix, ASDM will be blocked and the message "%ERROR: Signature not valid for file disk0:/<filename>" will be displayed at the ASA CLI. ASDM release 7.18(1.152) and later are backwards compatible with all ASA versions, even those without this fix. (CSCwb05291, CSCwb05264)
- **No support for the ASA 5506-X, 5506H-X, 5506W-X, ASA 5508-X, and ASA 5516-X in 9.17(1) and later**—ASA 9.16(x) is the last supported version. For the ASA FirePOWER module on the ASA 5508-X and 5516-X, the last supported combination is 9.16/7.0.
- **No support for the ASA FirePOWER module on the ISA 3000 in 9.17(1) and later**—The ISA 3000 continues to be supported in ASA 9.17 and later; however, the last supported combination for the ASA FirePOWER module is 9.16/7.0.
- **No support for Clientless SSL VPN in 9.17(1) and later**—Clientless SSL VPN is no longer supported.
    - **webvpn**—The following subcommands are removed:
        - **apcf**
        - **java-trustpoint**
        - **onscreen-keyboard**
        - **port-forward**
        - **portal-access-rule**
        - **rewrite**
        - **smart-tunnel**
    - **group-policy webvpn**—The following subcommands are removed:
        - **port-forward**
        - **smart-tunnel**
        - **ssl-clientless**

System Requirements

ASDM requires a computer with a CPU with at least 4 cores. Fewer cores can result in high memory usage.

ASA and ASDM Compatibility

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

VPN Compatibility

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

New Features

This section lists new features for each release.

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

New Features in ASA 9.17(1)

Released: December 1, 2021

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

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

Feature	Description
Network-service objects and their use in policy-based routing and access control	You can configure network-service objects and use them in extended access control lists for use in policy-based routing route maps and access control groups. Network-service objects include IP subnet or DNS domain name specifications, and optionally protocol and port specifications, that essentially combine network and service objects. This feature also includes the ability to define trusted DNS servers, to ensure that any DNS domain name resolutions acquire IP addresses from trusted sources. We added or modified the following commands: **access-list extended**, **app-id**, **clear configure object network-service**, **clear configure object-group network-service**, **clear dns ip-cache**, **clear object**, **clear object-group**, **debug network-service**, **description**, **dns trusted-source**, **domain**, **network-service-member**, **network-service reload**, **object-group network-service**, **object network-service**, **policy-route cost**, **set adaptive-interface cost**, **show asp table classify**, **show asp table network-service**, **show dns trusted-source**, **show dns ip-cache**, **show object**, **show object-group**, **show running-config**, **subnet**.
High Availability and Scalability Features	
ASAv30, ASAv50, and ASAv100 clustering for VMware and KVM	ASAv clustering lets you group up to 16 ASAvs together as a single logical device. A cluster provides all the convenience of a single device (management, integration into a network) while achieving the increased throughput and redundancy of multiple devices. ASAv clustering supports Individual Interface mode in routed firewall mode; Spanned EtherChannels are not supported. The ASAv uses a VXLAN virtual interface (VNI) for the cluster control link. New/Modified commands: **cluster-interface vni**, **nve-only cluster**, **peer-group**, **show cluster info**, **show cluster info instance-type**, **show nve 1**
Clearing routes in a high availability group or cluster	In previous releases, the **clear route** command cleared the routing table on the unit only. Now, when operating in a high availability group or cluster, the command is available on the active or control unit only, and clears the routing table on all units in the group or cluster. We changed the **clear route** command.
Interface Features	
Geneve interface support for the ASAv	Geneve encapsulation support was added for the ASAv30, ASAv50, and ASAv100 to support single-arm proxy for the AWS Gateway Load Balancer. New/Modified commands: **debug geneve**, **debug nve**, **debug vxlan**, **encapsulation**, **packet-tracer geneve**, **proxy single-arm**, **show asp drop**, **show capture**, **show interface**, **show nve**
Secure Firewall 3100 auto-negotiation can be enabled or disabled for 1Gigabit and higher interfaces.	Secure Firewall 3100 auto-negotiation can be enabled or disabled for 1Gigabit and higher interfaces. For other model SFP ports, the **no speed nonegotiate** option sets the speed to 1000 Mbps; the new command means you can set auto-negotiation and speed independently. New/Modified commands: **negotiate-auto**
Administrative and Troubleshooting Features	

Feature	Description
Startup time and tmatch compilation status	The **show version** command now includes information on how long it took to start (boot) up the system. Note that the larger the configuration, the longer it takes to boot up the system. The new **show asp rule-engine** command shows status on tmatch compilation. Tmatch compilation is used for an access list that is used as an access group, the NAT table, and some other items. It is an internal process that can consume CPU resources and impact performance while in progress, if you have very large ACLs and NAT tables. Compilation time depends on the size of the access list, NAT table, and so forth.
Enhancements to **show access-list element-count** output and **show tech-support** content	The output of the **show access-list element-count** has be enhanced to show the following: • When used in the system context in multiple-context mode, the output shows the element count for all access lists across all the contexts. • When used with object-group search enabled, the output includes details about the number of object groups in the element count. In addition, the **show tech-support** output now includes the output **show access-list element-count** and **show asp rule-engine**.
CiscoSSH stack	The ASA uses a proprietary SSH stack for SSH connections. You can now choose to use the CiscoSSH stack instead, which is based on OpenSSH. The default stack continues to be the ASA stack. Cisco SSH supports: • FIPS compliance • Regular updates, including updates from Cisco and the open source community Note that the CiscoSSH stack does not support: • SSH to a different interface over VPN (management-access) • EdDSA key pair • RSA key pair in FIPS mode If you need these features, you should continue to use the ASA SSH stack. There is a small change to SCP functionality with the CiscoSSH stack: to use the ASA **copy** command to copy a file to or from an SCP server, you have to enable SSH access on the ASA for the SCP server subnet/host using the **ssh** command. New/Modified commands: **ssh stack ciscossh**
PCAP support in packet tracer	You can replay a PCAP file in packet tracer tool and obtain the trace results. **pcap** and **force** are two new keywords that is used to support the usage of PCAP in packet tracer. New/Modified commands: **packet-tracer input** and **show packet-tracer**

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

Feature	Description
Multiple SAML trustpoints in IDP configuration	This feature supports adding multiple IDP trustpoints per SAML IDP configuration for applications that support multiple applications for the same Entity ID. New/Modified commands: **saml idp-trustpoint <trustpoint-name>**
AnyConnect Client VPN SAML External Browser	You can now configure VPN SAML External Browser to enable additional authentication choices, such as passwordless authentication, WebAuthN, FIDO2, SSO, U2F, and an improved SAML experience due to the persistence of cookies. When you use SAML as the primary authentication method for a remote access VPN connection profile, you can elect to have the AnyConnect Client use the client's local browser instead of the AnyConnect Client embedded browser to perform the web authentication. This option enables single sign-on (SSO) between your VPN authentication and other corporate logins. Also choose this option if you want to support web authentication methods, such as biometric authentication and Yubikeys, that cannot be performed in the embedded browser. New/Modified commands: **external-browser**
VPN Load balancing with SAML	ASA now supports VPN load balancing with SAML authentication.

Upgrade the Software

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

ASA Upgrade Path

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

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

This table provides upgrade paths for ASA. Some older versions require an intermediate upgrade before you can upgrade to a newer version. Recommended versions are in **bold**.

Note Be sure to check the upgrade guidelines for each release between your starting version and your ending version. You may need to change your configuration before upgrading in some cases, or else you could experience an outage.

Note For guidance on security issues on the ASA, and which releases contain fixes for each issue, see the ASA Security Advisories.

Note ASA 9.16(x) was the final version for the ASA 5506-X, 5508-X, and 5516-X.

ASA 9.14(x) was the final version for the ASA 5525-X, 5545-X, and 5555-X.

ASA 9.12(x) was the final version for the ASA 5512-X, 5515-X, 5585-X, and ASASM.

ASA 9.2(x) was the final version for the ASA 5505.

ASA 9.1(x) was the final version for the ASA 5510, 5520, 5540, 5550, and 5580.

Current Version	Interim Upgrade Version	Target Version
9.16(x)	—	Any of the following: → 9.17(x)
9.15(x)	—	Any of the following: → 9.17(x) → **9.16(x)**
9.14(x)	—	Any of the following: → 9.17(x) → **9.16(x)** → 9.15(x)
9.13(x)	—	Any of the following: → 9.17(x) → **9.16(x)** → 9.15(x) → 9.14(x)
9.12(x)	—	Any of the following: → 9.17(x) → **9.16(x)** → 9.15(x) → 9.14(x)

Current Version	Interim Upgrade Version	Target Version
9.10(x)	—	Any of the following: → 9.17(x) → **9.16(x)** → 9.15(x) → 9.14(x) → 9.12(x)
9.9(x)	—	Any of the following: → 9.17(x) → **9.16(x)** → 9.15(x) → 9.14(x) → 9.12(x)
9.8(x)	—	Any of the following: → 9.17(x) → **9.16(x)** → 9.15(x) → 9.14(x) → 9.12(x)
9.7(x)	—	Any of the following: → 9.17(x) → **9.16(x)** → 9.15(x) → 9.14(x) → 9.12(x) → 9.8(x)

Current Version	Interim Upgrade Version	Target Version
9.6(x)	—	Any of the following: → 9.17(x) → **9.16(x)** → 9.15(x) → 9.14(x) → 9.12(x) → 9.8(x)
9.5(x)	—	Any of the following: → 9.17(x) → **9.16(x)** → 9.15(x) → 9.14(x) → 9.12(x) → 9.8(x)
9.4(x)	—	Any of the following: → 9.17(x) → **9.16(x)** → 9.15(x) → 9.14(x) → 9.12(x) → 9.8(x)
9.3(x)	—	Any of the following: → 9.17(x) → **9.16(x)** → 9.15(x) → 9.14(x) → 9.12(x) → 9.8(x)

Current Version	Interim Upgrade Version	Target Version
9.2(x)	—	Any of the following: → 9.17(x) → **9.16(x)** → 9.15(x) → 9.14(x) → 9.12(x) → 9.8(x)
9.1(2), 9.1(3), 9.1(4), 9.1(5), 9.1(6), or 9.1(7.4)	—	Any of the following: → 9.14(x) → **9.12(x)** → 9.8(x) → 9.1(7.4)
9.1(1)	→ 9.1(2)	Any of the following: → 9.14(x) → **9.12(x)** → 9.8(x) → 9.1(7.4)
9.0(2), 9.0(3), or 9.0(4)	—	Any of the following: → 9.14(x) → **9.12(x)** → 9.8(x) → 9.6(x) → 9.1(7.4)
9.0(1)	→ 9.0(4)	Any of the following: → 9.14(x) → **9.12(x)** → 9.8(x) → 9.1(7.4)

Current Version	Interim Upgrade Version	Target Version
8.6(1)	→ 9.0(4)	Any of the following: → 9.14(x) → **9.12(x)** → 9.8(x) → 9.1(7.4)
8.5(1)	→ 9.0(4)	Any of the following: → **9.12(x)** → 9.8(x) → 9.1(7.4)
8.4(5+)	—	Any of the following: → **9.12(x)** → 9.8(x) → 9.1(7.4) → 9.0(4)
8.4(1) through 8.4(4)	→ 9.0(4)	→ **9.12(x)** → 9.8(x) → 9.1(7.4)
8.3(x)	→ 9.0(4)	Any of the following: → **9.12(x)** → 9.8(x) → 9.1(7.4)
8.2(x) and earlier	→ 9.0(4)	Any of the following: → **9.12(x)** → 9.8(x) → 9.1(7.4)

Upgrade Link

To complete your upgrade, see the ASA upgrade guide.

Open and Resolved Bugs

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

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

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

Open Bugs in Version 9.17(x)

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

Caveat ID Number	Description
CSCvz62406	Crash observed on control unit of 6node SSP cluster when pat is configured on s2s traffic (7.0.1-54)
CSCwa08743	ASA/FTD Traceback and reload on 2100 running code 7.0.1
CSCwa19713	Traffic dropped by ASA configured with BVI interfaces due to asp drop type \"no-adjacency\"
CSCwa21054	ASA/FTD may traceback and reload in Thread Name 'DATAPATH-2-14497'
CSCwa29596	FP1010 HA ASA interfaces does not become 'Normal' after failed over, and not able to communicate.

Resolved Bugs in Version 9.17(1)

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

Caveat ID Number	Description
CSCvo77184	VMware ASAv should default to vmxnet3, not e1000
CSCvz00032	Cisco Firepower Threat Defense Software TCP Proxy Denial of Service Vulnerability
CSCvz70595	Traceback observed on ASA while handling SAML handler
CSCwa04461	Cisco ASA Software and FTD Software Remote Access SSL VPN Denial of Service
CSCvu98260	Stale route present on DRP database when HA is nsf enabled in specific scenario.
CSCvx14489	snmpwalk fails on ipv6 interface post a failover

Caveat ID Number	Description
CSCvx16317	Failure accessing FXOS with connect fxos admin from Multi-Context ASA if admin context is changed
CSCvx54562	High System Overhead memory on FTD
CSCvx59252	FXOS is not rotating log files for management interface
CSCvx75683	The 'show cluster info trace' output is overwhelmed by 'tag does not exist' messages
CSCvx76665	Error messages "Updating Interface Status failed" seen on 2100 and 1010
CSCvy03324	ASA: ECMP sVTI support
CSCvy58705	"clear conf all" or "clear conf failover" should clear the failover debugs enabled
CSCvy69453	WM Standby device do not send out coldstart trap after reboot.
CSCvy78525	FTD doesn't TCP ping when VRF's are configured
CSCvy79952	ASA/FTD traceback and reload after downgrade
CSCvy82668	SSH session not being released
CSCvy84336	Add a warning when member interfaces of the port-channel are different between active and standby
CSCvy86817	Cruz CLU filter has the incorrect src/dst IP subnet when a custom CCL IP subnet is set
CSCvy96895	ASA disconnects the VTY session using of Active IP address and Standby MAC address after failed over
CSCvy99217	IKEv2: SA Error code should be translated to human friendly reason
CSCvz14305	IKEv2 RA 3rd party dual stack IPv4 and IPv6 requested - ASA doesn't reply for IKE Auth
CSCvz17046	ASAv crashed when tried to upgrade or reload the 16 node cluster setup
CSCvz25454	ASA: Drop reason is missing from 129 lines of asp-drop capture
CSCvz51258	show tech-support output can be confusing when there crashinfo, need to clean up/make more intuitive
CSCvz67816	IPV6 DNS PTR query getting modified on FTD
CSCvz71064	Deleting The Context From ASA taking Almost 2 Minutes with ikev2 tunnel
CSCvz71596	"Number of interfaces on Active and Standby are not consistent" should trigger warning syslog

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.