Release Notes for the Cisco Secure Firewall ASA Series, 9.19(x)

First Published: 2022-11-29

Last Modified: 2023-11-01

Release Notes for the Cisco Secure Firewall ASA Series, 9.19(x)

This document contains release information for ASA software Version 9.19(x).

Important Notes

- **No support in ASA 9.19(1) and later for the Firepower 4110, 4120, 4140, 4150, and Security Modules SM-24, SM-36, and SM-44 for the Firepower 9300**—ASA 9.18(x) is the last supported version.

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 Secure Firewall 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 9.19(1)

Released: November 29, 2022

Feature	Description
Platform Features	
Secure Firewall 3105	We introduced the ASA for the Secure Firewall 3105.
ASA virtual Auto Scale solution with Azure Gateway Load Balancer	You can now deploy the ASA virtual Auto Scale Solution with Gateway Load Balancer on Microsoft Azure. See the Interfaces features for more information.
Firewall Features	
Network service groups support	You can now define a maximum of 1024 network service groups.
High Availability and Scalability Features	
Removal of biased language	Commands, command output, and syslog messages that contained the terms "Master" and "Slave" have been changed to "Control" and "Data." New/Modified commands: **cluster control-node**, **enable as-data-node**, **prompt**, **show cluster history**, **show cluster info**
ASA virtual Amazon Web Services (AWS) clustering	The ASA virtual supports Individual interface clustering for up to 16 nodes on AWS. You can use clustering with or without the AWS Gateway Load Balancer.
Routing Features	
BGP graceful restart support for IPv6	We added BGP graceful restart support for IPv6 address family. New/Modified commands: Existing command, extended to support for IPv6 family:**ha-mode graceful-restart**
Interface Features	
ASA virtual support for IPv6	ASAv to support IPv6 network protocol on Private and Public Cloud platforms. Users can now: • Enable and configure an IPv6 management address via day0 configuration. • Assign IPv6 addresses using DHCP and static methods.
Paired proxy VXLAN for the ASA virtual for the Azure Gateway Load Balancer	You can configure a paired proxy mode VXLAN interface for the ASA virtual in Azure for use with the Azure Gateway Load Balancer (GWLB). The ASA virtual defines an external interface and an internal interface on a single NIC by utilizing VXLAN segments in a paired proxy. New/Modified commands: **external-port, external-segment-id, internal-port, internal-segment-id, proxy paired**

Feature	Description
Default Forward Error Correction (FEC) on Secure Firewall 3100 fixed ports changed to cl108-rs from cl74-fc for 25 GB+ SR, CSR, and LR transceivers	When you set the FEC to Auto on the Secure Firewall 3100 fixed ports, the default type is now set to cl108-rs instead of cl74-fc for 25 GB SR, CSR, and LR transceivers. New/Modified commands: **fec**
License Features	
ASA virtual permanent license reservation support for the ASAv5 on KVM and VMware	A new command is available that you can execute to override the default PLR license entitlement and request the Cisco Smart Software Manager (SSM) to issue an ASAv5 PLR license when you are deploying ASAv with 2GB RAM on KVM and VMware. You can modify the same command by adding the <*no*> form to revert the license entitlement from ASAv5 to the default PLR license in correspondence to the RAM configuration.
Administrative, Monitoring, and Troubleshooting Features	
CiscoSSH stack now default	The Cisco SSH stack is now used by default. New/Modified commands: **ssh stack ciscossh**
VPN Features	
VTI loopback interface support	You can now set a loopback interface as the source interface for a VTI. Support has also been added to inherit the IP address from a loopback interface instead of a statically configured IP address. The loopback interface helps to overcome path failures. If an interface goes down, you can access all interfaces through the IP address assigned to the loopback interface. New/Modified commands: **tunnel source interface**, **ip unnumbered**, **ipv6 unnumbered**
Dynamic Virtual Tunnel Interface (dynamic VTI) support	The ASA is enhanced with dynamic VTI. A single dynamic VTI can replace several static VTI configurations on the hub. You can add new spokes to a hub without changing the hub configuration. Dynamic VTI supports dynamic (DHCP) spokes. New/Modified commands: **interface virtual-Template, ip unnumbered, ipv6 unnumbered, tunnel protection ipsec policy.**
VTI support for EIGRP and OSPF	EIGRP and OSPFv2/v3 routing is now supported on the Virtual Tunnel Interface. You can now use these routing protocol to share routing information and to route traffic flow through VTI-based VPN tunnel between peers
TLS 1.3 in Remote Access VPN	You can now use TLS 1.3 to encrypt remote access VPN connections. TLS 1.3 adds support for the following ciphers: • TLS_AES_128_GCM_SHA256 • TLS_CHACHA20_POLY1305_SHA256 • TLS_AES_256_GCM_SHA384 This feature requires Cisco Secure Client, Version 5.0.01242 and above. New/Modified commands: **sslserver-version, sslclient-version**.

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

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 9.18 was the final version for the Firepower 4110, 4120, 4140, 4150, and Security Modules SM-24, SM-36, and SM-44 for the Firepower 9300.

ASA 9.16 was the final version for the ASA 5506-X, 5508-X, and 5516-X.

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

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

ASA 9.2 was the final version for the ASA 5505.

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

Current Version	Interim Upgrade Version	Target Version
9.18	—	Any of the following: → **9.19**
9.17	—	Any of the following: → **9.19** → **9.18**
9.16	—	Any of the following: → **9.19** → **9.18** → 9.17
9.15	—	Any of the following: → **9.19** → **9.18** → 9.17 → **9.16**
9.14	—	Any of the following: → **9.19** → **9.18** → 9.17 → **9.16** → 9.15

Current Version	Interim Upgrade Version	Target Version
9.13	—	Any of the following: → **9.19** → **9.18** → 9.17 → **9.16** → 9.15 → 9.14
9.12	—	Any of the following: → **9.19** → **9.18** → 9.17 → **9.16** → 9.15 → 9.14
9.10	—	Any of the following: → **9.19** → **9.18** → 9.17 → **9.16** → 9.15 → 9.14 → 9.12
9.9	—	Any of the following: → **9.19** → **9.18** → 9.17 → **9.16** → 9.15 → 9.14 → 9.12

Current Version	Interim Upgrade Version	Target Version
9.8	—	Any of the following: → **9.19** → **9.18** → 9.17 → **9.16** → 9.15 → 9.14 → 9.12
9.7	—	Any of the following: → **9.19** → **9.18** → 9.17 → **9.16** → 9.15 → 9.14 → 9.12 → 9.8
9.6	—	Any of the following: → **9.19** → **9.18** → 9.17 → **9.16** → 9.15 → 9.14 → 9.12 → 9.8

Current Version	Interim Upgrade Version	Target Version
9.5	—	Any of the following: → **9.19** → **9.18** → 9.17 → **9.16** → 9.15 → 9.14 → 9.12 → 9.8
9.4	—	Any of the following: → **9.19** → **9.18** → 9.17 → **9.16** → 9.15 → 9.14 → 9.12 → 9.8
9.3	—	Any of the following: → **9.19** → **9.18** → 9.17 → **9.16** → 9.15 → 9.14 → 9.12 → 9.8

Current Version	Interim Upgrade Version	Target Version
9.2	—	Any of the following: → **9.19** → **9.18** → 9.17 → **9.16** → 9.15 → 9.14 → 9.12 → 9.8
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 → **9.12** → 9.8 → 9.1(7.4)
9.1(1)	→ 9.1(2)	Any of the following: → 9.14 → **9.12** → 9.8 → 9.1(7.4)
9.0(2), 9.0(3), or 9.0(4)	—	Any of the following: → 9.14 → **9.12** → 9.8 → 9.6 → 9.1(7.4)
9.0(1)	→ 9.0(4)	Any of the following: → 9.14 → **9.12** → 9.8 → 9.1(7.4)

Current Version	Interim Upgrade Version	Target Version
8.6(1)	→ 9.0(4)	Any of the following: → 9.14 → **9.12** → 9.8 → 9.1(7.4)
8.5(1)	→ 9.0(4)	Any of the following: → **9.12** → 9.8 → 9.1(7.4)
8.4(5+)	—	Any of the following: → **9.12** → 9.8 → 9.1(7.4) → 9.0(4)
8.4(1) through 8.4(4)	→ 9.0(4)	→ **9.12** → 9.8 → 9.1(7.4)
8.3	→ 9.0(4)	Any of the following: → **9.12** → 9.8 → 9.1(7.4)
8.2 and earlier	→ 9.0(4)	Any of the following: → **9.12** → 9.8 → 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 9.19(x)

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

Identifier	Headline
CSCwc58458	AWS C5N-4Xlarge 10g interface just have 4 RX Queues with GENEVE and jumbo frame enabled

Resolved Bugs in Version 9.19(1)

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

Identifier	Headline
CSCvv82681	RTC unstable clock register read causes "watchdog: BUG: soft lockup - CPU#0 stuck" error on console
CSCvw23514	Update FXOS troubleshooting documentation to provide details on isolating potential SSD HW failures
CSCvx54562	High System Overhead memory on FTD
CSCvx99172	M500IT Model Solid State Drives on 4100/9300 may go unresponsive after 3.2 Years in service
CSCvy99348	Shutdown command reboots instead of shutting the FP1k device down.
CSCvz34289	In some cases transition to lightweight proxy doesn't work for Do Not Decrypt flows
CSCvz52785	Management interface flaps every 13mins post upgrade from 9.12 to 9.14.2.15
CSCvz68713	PLR license reservation for ASAv5 is requesting ASAv10
CSCvz69729	Unstable client processes may cause LINA zmqio traceback on FTD
CSCvz90712	9.17/Rare 256 block leak/exhaustion, 1550 block overallocation

Identifier	Headline
CSCvz94217	App-instance startup version is ignored and set to running-version after copy config
CSCwa16257	failover is getting failed in secondary FTD when the loopback interface is configured
CSCwa38996	Big number of repetitive messages in snmpd.log leading to huge log size
CSCwa48169	ASA/FTD traceback and reload on netsnmp_handler_check_cache function
CSCwa52215	Uploading firmware triggers data port-channel to flap
CSCwa55772	FPR 4100 saw an unexpected reload with reason "Reset triggered due to HA policy of Reset"
CSCwa69303	ASA running on SSP platform generate critical error "[FSM:FAILED]: sam:dme:MgmtIfSwMgmtOobIfConfig"
CSCwa76822	Tune throttling flow control on syslog-ng destinations
CSCwa77777	Adding more logs to watchdog infra
CSCwa82850	ASA Failover does not detect context mismatch before declaring joining node as "Standby ready"
CSCwa85297	Multi-instance internal portchannel VLANs may be misprogrammed causing traffic loss
CSCwa90735	FTD/FXOS - ASAconsole.log files fail to rotate causing excessive disk space used in /ngfw
CSCwa96920	ASA/FTD may traceback and reload in process Lina
CSCwa99171	Chassis and application sets the time to Jan 1, 2010 after reboot
CSCwa99932	ASA/FTD stuck after crash and reboot
CSCwb00871	ENH: Reduce latency in log_handler_file to reduce watchdog under scale or stress
CSCwb01633	FXOS misses logs to diagnose root cause of module show-tech file generation failure
CSCwb02689	FXOS should check reference clock stratum instead of NTP server local clock stratum
CSCwb03704	ASA/FTD datapath threads may run into deadlock and generate traceback
CSCwb04000	ASA/FTD: DF bit is being set on packets routed into VTI
CSCwb05148	Cisco ASA Software and FTD Software SNMP Denial of Service Vulnerability
CSCwb18602	crontab -e unable to find editor
CSCwb22359	Portmanager/LACP improvement to avoid false restarts and increase of logging events
CSCwb25809	Single Pass - Traceback due to stale ifc
CSCwb27099	FXOS: Third-party interop between Ciena Waveserver with firepower chassis.

Identifier	Headline
CSCwb28123	FTD HA deployment fails with error "Deployment failed due to major version change on device"
CSCwb31551	When inbound packet contains SGT header, FPR2100 cannot distribute properly per 5 tuple
CSCwb40662	ENH: FCM should include option for modifying the interface 'link debounce time'
CSCwb48166	FXOS upgrade to 2.11 is stuck
CSCwb57524	FTD upgrade fails - not enough disk space from old FXOS bundles in distributables partition
CSCwb57615	Configuring pbr access-list with line number failed.
CSCwb57988	The smConLogger traceback is caused by memory leak.
CSCwb58007	CVE-2022-28199: Evaluation for FTDv and ASAv
CSCwb62059	Unable to login to FTD using external authentication after upgrade
CSCwb63827	Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software DoS
CSCwb66382	ASAv - 9344 Block not created automatically after enabling JumboFrames, breaks OSPF MD5
CSCwb70030	MIO: No blade reboot during CATERR if fault severity is non-Severe or CATERR sensor is different
CSCwb73678	/var/tmp partition fullness warning on FXOS
CSCwb74498	Cisco FXOS and NX-OS Software CDP DoS and Arbitrary Code Execution Vulnerability
CSCwb82796	ASA/FTD firewall may traceback and reload when tearing down IKE tunnels
CSCwb83691	ASA/FTD traceback and reload due to the initiated capture from FMC
CSCwb88090	FXOS:after fxos config import new port-channel creation causing existing port-channel flap
CSCwb90074	ASA: Multiple Context Mixed Mode SFR Redirection Validation
CSCwb95787	FPR1010 - No ARP on switchport VLAN interface after portmanager DIED event
CSCwc02133	Cisco FTD Software and Cisco FXOS Software Command Injection Vulnerability
CSCwc08683	The interface's LED remains green blinking when the optical fiber is unplugged on FPR1150
CSCwc10145	FTDv Cluster unit not re-joining cluster with error msg "Failed to open NLP SSL listening socket"

Identifier	Headline
CSCwc12652	Control-Plane ACL Non-Functional After Upgrade to 9.18(1) or 7.2.0-82 Firepower
CSCwc13017	FTD/ASA traceback and reload at at ../inspect/proxy.h:439
CSCwc27846	Observing Crash in QP(multicontext)-99.18(28)9 while HA sync after upgrading and reloading.
CSCwc28806	ASA Traceback and Reload on process name Lina
CSCwc31457	ASA process with cleartext token when not able to encrypt it
CSCwc37061	SNMP: FMC doesn't reply to OID 1.3.6.1.2.1.25.3.3.1.2
CSCwc38361	Cisco FXOS Software Command Injection Vulnerability
CSCwc40352	Lina Netflow sending permited events to Stealthwatch but they are block by snort afterwards
CSCwc44289	FTD - Traceback and reload when performing IPv4 <> IPv6 NAT translations
CSCwc48375	Inbound IPSEC SA stuck inactive - many inbound SPIs for one outbound SPI in "show crypto ipsec sa"
CSCwc50887	FTD - Traceback and reload on NAT IPv4<>IPv6 for UDP flow redirected over CCL link
CSCwc50891	MPLS tagging removed by FTD
CSCwc61106	Unable to configure domain\username under cfg-export-policy in FXOS
CSCwc67687	ASA HA failover triggers HTTP server restart failure and ASDM outage
CSCwc70962	FTD/ASA "Write Standby" enables ECDSA ciphers causing AC SSLv3 handshake failure
CSCwc73209	DOC:The default keying is only used by FCM on FXOS.
CSCwc77519	FPR1120-ASA:Primary takes active role after reloading
CSCwc77680	ASA/FTD may traceback and reload in Thread Name 'DATAPATH-0-4948'
CSCwc77892	CGroups errors in ASA syslog after startup
CSCwc80234	"inspect snmp" config difference between active and standby
CSCwc88897	ASA traceback and reload due to null pointer in Umbrella after modifying DNS inspection policy
CSCwc90091	ASA 9.12(4)47 with user-statistics, will affects the "policy-server xxxx global" visibility.
CSCwc94466	Cisco ASA/FTD Firepower 2100 SSL/TLS Denial of Service Vulnerability
CSCwc99242	ISA3000 LACP channel member SFP port suspended after reload

Identifier	Headline
CSCwd00778	ifAdminStatus output is abnormal via snmp polling
CSCwd03793	FTD Traceback and reload
CSCwd05756	FTD traceback on Lina due to syslog component.
CSCwd22349	ASA: Unable to connect AnyConnect Cert based Auth with "periodic-authentication certificate" enabled
CSCwd31960	Management access over VPN not working when custom NAT is configured
CSCwd40260	Serviceability Enhancement - Unable to parse payload are silently drop by ASA/FTD
CSCwd51757	Unable to get polling results using snmp GET for connection rate OIDâ€™s

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 Secure Firewall ASA Series Documentation.