# Release Notes for the Cisco Secure Firewall ASA, 9.24(x)

**First Published:** 2025-12-03

**Last Modified:** 2026-10-28

## Release Notes for the Cisco Secure Firewall ASA, 9.24(x)

This document contains release information for ASA software version 9.24(x).

## Important Notes

- **MD5 checksum**—Verify the MD5 checksum immediately after downloading the image and before configuring the boot variable, as the MD5 value may change once the variable is set.
- **ASA Virtual cannot be downgraded from 9.24(1)**—After upgrading to 9.24(1), which includes a new Grub bootloader, you cannot downgrade to an earlier version. To upgrade to later versions, you will first have to upgrade to 9.24(1).
- **For ASA Virtual on OCI, Arm instances may experience reduced throughput on legacy hypervisors (especially with SR-IOV enabled)**—See https://docs.oracle.com/en-us/iaas/Content/Compute/known-issues.htm for more information. Contact OCI for support.
- **Removal of ikev1 ipsec-over-tcp support**—For enhanced platform security, IKEv1 ipsec-over-tcp support is being removed. Hence, **crypto ikev1 ipsec-over-tcp**, **show crypto ikev1 ipsec-over-tcp**, **debug ipsec-over-tcp**, and **debug menu ipsec-over-tcp** commands are not supported.
- **During a software upgrade of ASA cluster, the VPN load-balancing cluster does not form if members run different ASA versions.** You must perform one of the following operations:
  - Upgrade all members to the same version. The VPN load-balancing cluster re-forms automatically after all members run the same version. VPN load balancing is unavailable during the mixed-version window.
  - For a hitless upgrade, temporarily remove the cluster keys from all members. Keep the interval without cluster keys as short as possible. Upgrade all members and then reconfigure the cluster keys on all members. VPN load balancing remains available during the upgrade. When you perform this operation, syslog 718089 is logged:

    %ASA-1-718089: VPN LB cluster is running without authentication. Configure *cluster key* to secure the cluster.

## 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 9.24(10)

**Released: September 21, 2026**

| Feature | Description |
|---|---|
| **Firewall Features** | |
| Removed support for HTTP cut through proxy. HTTPS cut through proxy remains available. | You can no longer configure cut-through proxy using the HTTP protocol. You must use the secure HTTPS protocol if you use this feature. Cut-through proxy will always use TLS authentication.<br>The following commands have been removed: **aaa authentication listener http** (note that the **https** version remains available), **aaa authentication secure-http-client**. |
| Simplify Carrier-Grade NAT tracing with predictable port blocks | Introduced deterministic Carrier-Grade NAT (CGNAT), which maps each subscriber to a predefined public IPv4 address and port block instead of assigning ports dynamically for each connection. This helps you reduce NAT logging overhead while making subscriber traceability and troubleshooting easier in large-scale deployments. You configure the feature through the CLI by defining the port block size and assignment algorithm for the NAT policy.<br>New/modified commands:<br>• **nat** (*inside*, *outside*) **source dynamic** *subscriber_object* **pat-pool** *public_pool* **block-allocation deterministic** *block_size* *sequential* \| *inverse* \| *block-to-net*<br>• **show xlate type deterministic** |
| **High Availability and Scalability Features** | |

| Feature | Description |
|---|---|
| Cluster redirect: flow offload support for the Secure Firewall 6100 asymmetric cluster traffic | For asymmetric flows, cluster redirect lets the forwarding node offload flows to hardware. This feature is enabled by default.<br>When traffic for an existing flow is sent to a different node, then that traffic is redirected to the owner node over the cluster control link. Because asymmetric flows can create a lot of traffic on the cluster control link, letting the forwarder offload these flows can improve performance.<br>New/modified commands<br>• **flow-offload cluster-redirect**<br>• **show conn**<br>• **show flow-offload** |
| **Interface Features** | |
| Support for configuring multiple DHCPv6 relay link-addresses per interface | ASA DHCPv6 relay agent can now use multiple configured IPv6 interface addresses as relay link-address values in DHCPv6 RELAY-FORWARD messages. This support provides the flexibility for the DHCPv6 server to choose the appropriate address pool by matching the client's prefix.<br>New/modified commands:<br>• **ipv6 dhcp relay link-address** *ipv6_address*<br>• **show ipv6 dhcprelay interface** |
| **License Features** | |
| Unlimited performance tier (ASAvU) for AWS | ASA Virtual for AWS now supports an unlimited performance tier (ASAvU).<br>Supported vCPU and memory configuration:<br>• 32 vCPU and 64 GB RAM<br>• 64 vCPU and 128 GB RAM |
| **VPN Features** | |

| Feature | Description |
|---|---|
| Distributed site-to-site VPN with inter-site clustering | Distributed VPN support for inter-site clustering enables seamless site-to-site VPN session continuity across geographically dispersed sites. This feature enhances high availability by maintaining both local and remote backups for IKEv2/IPsec traffic during member or site failures.<br>New/modified commands:<br>• **cluster redistribute vpn-sessiondb**<br>• **show cluster vpn-sessiondb**<br>• **vpn-mode**<br>• **show cluster resource usage**<br>• **show vpn-sessiondb**<br>• **show conn detail**<br>• **show crypto ikev2 stats** |
| IPsec flow offload for traffic on the cluster control link on the Secure Firewall 6100 in distributed site-to-site VPN mode | For asymmetric flows in distributed site-to-site VPN mode, IPsec flow offload now lets the flow owner decrypt IPsec traffic in hardware that was forwarded over the cluster control link. This feature is not configurable and is always available when you enable IPsec flow offload.<br>New/modified commands: **show crypto ipsec sa detail** |

## New Features in ASA 9.24(1)

**Released: December 3, 2025**

| Feature | Description |
|---|---|
| **Platform Features** | |
| Secure Firewall 220 | The Secure Firewall 220 is an affordable security appliance for branch offices and remote locations, balancing cost and features. |
| Secure Firewall 6160, 6170 | The Secure Firewall 6160 and 6170 are ultra-high-end firewalls for demanding data center and telecom networks. It has exceptional price-to-performance, modular capability, and high throughput. |
| ASA VirtualGrub bootloader upgraded with UEFI firmware and secure boot. | With the Grub bootloader upgrade from Grub 0.94 to Grub 2.12, we now support UEFI firmware with or without secure boot functionality, along with legacy BIOS mode. Secure boot functionality gives boot-level malware protection. New deployments also use GPT-partitioned images instead of MS-DOS-partitioned disks. If you upgrade, you cannot change to UEFI and secure boot; only new deployments can use the new options.<br>**Note**<br>After upgrading to 9.24, you cannot downgrade to an earlier version. To upgrade to later versions, you must first upgrade to 9.24. |

| Feature | Description |
|---|---|
| ASA Virtual AWS dual-arm clustering | In dual-arm mode, after inspection, the ASA Virtual will NAT and forward outbound traffic from its outside interface directly to the internet via the Internet Gateway. Since outbound traffic is directly forwarded to the internet after inspection without making a round trip through the GWLB and the GWLB endpoint, the number of traffic hops is reduced by 2. This reduction is especially useful in providing a common egress path for a multi-VPC deployment.For dual-arm deployments, only egress traffic is supported. |
| ASA Virtual GCP clustering with autoscale | GCP clustering with autoscale is now supported for ASAv30, ASAv50, and ASAv100. |
| ASA VirtualOCI Ampere A1 ARM compute shape support | New shapes for OCI.<br>**Note**<br>For ASA Virtual on OCI, Arm instances may experience reduced throughput on legacy hypervisors (especially with SR-IOV enabled)—See https://docs.oracle.com/en-us/iaas/Content/Compute/known-issues.htm for more information. Contact OCI for support. |
| ASA VirtualKVM flow offload | Flow offload is now supported on the DPU for KVM. |
| ASA Virtual Nutanix support for AOS 6.8 | Nutanix AOS 6.8 supports VPCs, similar toVPCs in public clouds. |
| ASA Virtual OpenStack support for Caracal | ASA Virtual deployment is supported on the Caracal release of OpenStack. |
| ASA Virtual MANA NIC Support | ASA Virtual supports MANA NIC hardware on Microsoft Azure for the following instances:<br>• Standard_D8s_v5<br>• Standard_D16s_v5 |
| ASA Virtual on VMware ESXi support | ESXi versions 8.0, 9.0, and 9.1 are supported on ASA Virtual 9.24(1) and later versions. |
| **Firewall Features** | |
| Application Visibility and Control for the Secure Firewall 6100 | Application Visibility and Control (AVC) makes it possible for you to write access control rules based on applications rather than just IP addresses and ports. AVC downloads the Vulnerability Database (VDB), which creates network-service objects and groups that you can use in access control rules. The objects define various applications, and the groups define application categories, so you can easily block applications or entire classes of connections without specifying IP address and port.<br>We introduced or modified the following commands: **avc**, **avc download vdb**, **clear avc**, **clear object-group**, **network-service reload**, **show avc**, **show service-policy**. In addition, you can no longer enter the **app-id** command as part of a network-service object definition.<br>Supported platforms: Secure Firewall 6100 |
| **High Availability and Scalability Features** | |

| Feature | Description |
|---|---|
| No reboot required for changing the VPN mode | When changing the VPN mode between distributed and centralized, a reboot is no longer required. However, you now need to disable clustering on all nodes before changing the mode. |
| Data nodes can join the cluster concurrently | Formerly, the control node only allowed one data node to join the cluster at a time. If the configuration sync takes a long time, data nodes can take a long time to join. Concurrent join is enabled by default. If you have NAT and VPN distributed mode enabled, you cannot use concurrent join.<br>Added/modified commands: **concurrent-join**, **show cluster info concurrent-join incompatible-config** |
| MTU ping test on cluster node join provides more information by trying smaller MTUs | When a node joins the cluster, it checks MTU compatibility by sending a ping to the control node with a packet size matching the cluster control link MTU. If the ping fails, it tries the MTU divided by 2 and keeps dividing by 2 until an MTU ping is successful. The successful ping value is shown in **show cluster info trace** so you can fix the MTU to a working value and try again.<br>Even if the ping fails, the node is allowed to join the cluster. In this case, you need to resolve the MTU mismatch as soon as possible.<br>We recommend increasing the switch MTU size to the recommended value, but if you can't change the switch configuration, a working value for the cluster control link will let you form the cluster.<br>Added/modified commands: **show cluster info trace**, **show cluster history**. |
| Improved cluster control link health check with high CPU | When a cluster node CPU usage is high, the health check will be suspended, and the node will not be marked as unhealthy. You can configure at what CPU use threshold to suspend the health check.<br>Added/modified commands: **cpu-healthcheck-threshold**. |
| Clustering on the Secure Firewall 6100 | You can cluster up to 4 Secure Firewall 6100 nodes in Spanned EtherChannel or Individual interface mode. |
| Block depletion monitoring in clustering | When block depletion occurs, the ASA collects troubleshooting logs and sends out a syslog. For clustering, the node will leave the cluster so that the other nodes can handle the traffic. The ASA can also force a crash and reload to recover from depletion.<br>Added/modified commands: **fault-monitor**, **block-depletion**, **block-depletion recovery-action**, **block-depletion monitor-interval**. |
| Dynamic PAT support for distributed site-to-site VPN mode | Distributed mode now supports dynamic PAT. However, interface PAT is still not supported. |
| SNMP enhancements | This release includes SNMP enhancements to improve the polling experience for ENTITY-MIB and IF-MIB. These improvements are specific to the Secure Firewall 4200 and Secure Firewall 6100 series platforms. |
| **Interface Features** | |

| Feature | Description |
|---|---|
| Recursive DNS Server (RDNSS) and DNS Search List (DNSSL) options to advertise a list of DNS servers and domains to IPv6 clients | You can now configure Recursive DNS Server (RDNSS) and DNS Search List (DNSSL) options to provide DNS servers and domains to SLAAC clients using router advertisements.<br>New/modified commands: **ipv6 nd ra dns-search-list domain**, **ipv6 nd ra dns server**, **show ipv6 nd detail**, **show ipv6 nd ra dns-search-list**, **show ipv6 nd ra dns server**, **show ipv6 nd summary** |
| **Administrative, Monitoring, and Troubleshooting Features** | |
| SSH X.509 certificate authentication | You can now use an X.509v3 certificate to authenticate a user for SSH (RFC 6187).<br>New/Modified commands: **aaa authorization exec ssh-x509**, **ssh authentication method**, **ssh trustpoint sign**, **ssh username-from-certificate**, **validation-usage ssh-client**<br>*Also in 9.20(4), 9.22(3).* |
| AES-256-GCM SSH cipher | The ASA supports the AES-256-GCM cipher for SSH. It is enabled by default for **all** and **high** encryption levels.<br>New/Modified commands: **ssh cipher encryption**<br>*Also in 9.20(4), 9.22(3).* |
| Message-of-the-day (motd) banner shows the failover state and the last failover time | When using failover, if you configure the **banner motd** command, then the banner shows information about the failover state and the last failover time of the unit you are logging into. This information is useful if you are performing actions at the CLI, such as troubleshooting, and a failover occurs between sessions.<br>New or modified commands: **banner motd**<br>*Also in 9.22(3).* |
| Display of UDP's initiator and responder values in connection status output | For UDP traffic flows, the ASA displays the initiator and responder field values in the connection detail status. These field values indicate the direction of communication, which helps in troubleshooting network connectivity issues.<br>New/Modified commands: **show conn detail**<br>*Also in 9.20(1).* |
| Linux kernel crash dump | The Linux kernel crash dump feature lets you debug kernel crash events and find the root cause. This feature is enabled by default.<br>New/Modified commands: **show kernel crash-dump**, **kernel crash-dump**, **crashinfoforce kernel-dump** |
| Root Shell Access Support Using Consent Token on ASA Virtual | ASA Virtual supports a new Consent Token mechanism that allows authorized users to obtain one-time access to the Linux root shell for troubleshooting or diagnostic purposes — without requiring the administrator password.<br>New/Modified commands: **consent-token generate-challenge shell-access**, **consent-token accept-response shell-access** |
| **ASDM Features** | |

| Feature | Description |
|---|---|
| ASDM certificate authentication | ASDM Launcher 1.9(10), which comes with ASDM 7.24, now supports user certificate authentication. Previously, this feature was only supported with Java Web Start (discontinued in 7.18). Because the ASA commands were not deprecated in 9.18, you can configure earlier ASA versions to use certificate authentication when using any ASDM version with ASDM Launcher 1.9(10).<br>New/Modified commands: **http authentication-certificate**, **http username-from-certificate**<br>New/Modified screens:<br>• ASDM Launcher login window. |
| **VPN Features** | |
| SGT over VTI | VTI tunnels now support Cisco TrustSec SGT tags.<br>New/Modified commands: **cts manual**, **propagate sgt**, **policy static sgt** |
| ECMP and BFD fault detection support for VTIs | One or more dynamic VTI interfaces can be part of an Equal-Cost Multi-Path (ECMP) zone. Using zones, traffic towards the spoke can be load-balanced. Bidirectional Forwarding Detection (BFD) link detection is faster, detecting faulty VTI links in few milliseconds or microseconds.<br>New/Modified commands: **bfd template**, **vtemplate-bfd**, **vtemplate-zone-member**, **show zone**, **show conn all**, **show route** |
| Loopback interface support for distributed site-to-site VPN | You can now create site-to-site VPN tunnels using loopback interfaces in distributed site-to-site mode. Unlike outside addresses that are tied to a location network, the loopback interfaces are not. This independence means you can move the address to another cluster and use routing protocols to propagate the new location to the upstream routers. The peer's traffic would then be sent to the new location. |
| IPsec flow offload and DTLS crypto accelerator for the Secure Firewall 6100 | Secure Firewall 6100 supports AES-GCM-128 and AES-GCM-256 ciphers only. |
| IPsec flow offload for the ASA Virtual on KVM | IPsec flow offload is now supported on the DPU for KVM. |

# Upgrade the Software

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

## Upgrade Link

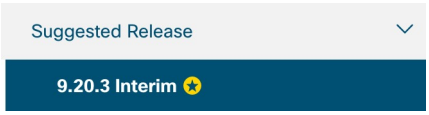
To complete your upgrade, see the ASA upgrade guide.

# Upgrade Path: ASA Appliances

### What Version Should I Upgrade To?

On the Cisco Support & Download site, the suggested release is marked with a gold star. For example:

***Figure 1: Suggested Release***




### View Your Current Version

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.

### Upgrade Guidelines

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.

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

### Upgrade Paths

This table provides upgrade paths for ASA.

**Note** ASA 9.20 was the final version for the Firepower 2100.

ASA 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.

***Table 1: Upgrade Path***

| Current Version | Interim Upgrade Version | Target Version |
|---|---|---|
| 9.23 | — | Any of the following:<br>→ 9.24 |

| Current Version | Interim Upgrade Version | Target Version |
|---|---|---|
| 9.22 | — | Any of the following:<br>→ 9.24<br>→ 9.23 |
| 9.20 | — | Any of the following:<br>→ 9.24<br>→ 9.23<br>→ 9.22 |
| 9.19 | — | Any of the following:<br>→ 9.24<br>→ 9.23<br>→ 9.22<br>→ 9.20 |
| 9.18 | — | Any of the following:<br>→ 9.24<br>→ 9.23<br>→ 9.22<br>→ 9.20<br>→ 9.19 |
| 9.17 | — | Any of the following:<br>→ 9.24<br>→ 9.22<br>→ 9.20<br>→ 9.19<br>→ 9.18 |

| Current Version | Interim Upgrade Version | Target Version |
|---|---|---|
| 9.16 | — | Any of the following:<br>→ 9.24<br>→ 9.23<br>→ 9.22<br>→ 9.20<br>→ 9.19<br>→ 9.18<br>→ 9.17 |
| 9.15 | — | Any of the following:<br>→ 9.24<br>→ 9.23<br>→ 9.22<br>→ 9.20<br>→ 9.19<br>→ 9.18<br>→ 9.17<br>→ 9.16 |
| 9.14 | — | Any of the following:<br>→ 9.24<br>→ 9.23<br>→ 9.22<br>→ 9.20<br>→ 9.19<br>→ 9.18<br>→ 9.17<br>→ 9.16 |

| Current Version | Interim Upgrade Version | Target Version |
|---|---|---|
| 9.13 | — | Any of the following:<br>→ 9.24<br>→ 9.23<br>→ 9.22<br>→ 9.20<br>→ 9.19<br>→ 9.18<br>→ 9.17<br>→ 9.16 |
| 9.12 | — | Any of the following:<br>→ 9.24<br>→ 9.23<br>→ 9.22<br>→ 9.20<br>→ 9.19<br>→ 9.18<br>→ 9.17<br>→ 9.16 |
| 9.10 | — | Any of the following:<br>→ 9.24<br>→ 9.23<br>→ 9.22<br>→ 9.20<br>→ 9.19<br>→ 9.18<br>→ 9.17<br>→ 9.16 |

| Current Version | Interim Upgrade Version | Target Version |
|---|---|---|
| 9.9 | — | Any of the following:<br>→ 9.24<br>→ 9.23<br>→ 9.22<br>→ 9.20<br>→ 9.19<br>→ 9.18<br>→ 9.17<br>→ 9.16 |
| 9.8 | — | Any of the following:<br>→ 9.24<br>→ 9.23<br>→ 9.22<br>→ 9.20<br>→ 9.19<br>→ 9.18<br>→ 9.17<br>→ 9.16 |
| 9.7 | — | Any of the following:<br>→ 9.24<br>→ 9.23<br>→ 9.22<br>→ 9.20<br>→ 9.19<br>→ 9.18<br>→ 9.17<br>→ 9.16 |

| Current Version | Interim Upgrade Version | Target Version |
|---|---|---|
| 9.6 | — | Any of the following:<br>→ 9.24<br>→ 9.23<br>→ 9.22<br>→ 9.20<br>→ 9.19<br>→ 9.18<br>→ 9.17<br>→ 9.16 |
| 9.5 | — | Any of the following:<br>→ 9.24<br>→ 9.23<br>→ 9.22<br>→ 9.20<br>→ 9.19<br>→ 9.18<br>→ 9.17<br>→ 9.16 |
| 9.4 | — | Any of the following:<br>→ 9.24<br>→ 9.23<br>→ 9.22<br>→ 9.20<br>→ 9.19<br>→ 9.18<br>→ 9.17<br>→ 9.16 |

| Current Version | Interim Upgrade Version | Target Version |
|---|---|---|
| 9.3 | — | Any of the following:<br>→ 9.24<br>→ 9.23<br>→ 9.22<br>→ 9.20<br>→ 9.19<br>→ 9.18<br>→ 9.17<br>→ 9.16 |
| 9.2 | — | Any of the following:<br>→ 9.24<br>→ 9.23<br>→ 9.22<br>→ 9.20<br>→ 9.19<br>→ 9.18<br>→ 9.17<br>→ 9.16 |

## Upgrade Path: ASA Logical Devices for the Firepower 4100/9300

- FXOS: From FXOS 2.2.2 and later, you can upgrade directly to any higher version. (FXOS 2.0.1–2.2.1 can upgrade as far as 2.8.1. For versions earlier than 2.0.1, you need to upgrade to each intermediate version.) Note that you cannot upgrade FXOS to a version that does not support your current logical device version. You will need to upgrade in steps: upgrade FXOS to the highest version that supports your current logical device; then upgrade your logical device to the highest version supported with that FXOS version. For example, if you want to upgrade from FXOS 2.2/ASA 9.8 to FXOS 2.13/ASA 9.19, you would have to perform the following upgrades:

  1. FXOS 2.2 → FXOS 2.11 (the highest version that supports 9.8)
  2. ASA 9.8 → ASA 9.17 (the highest version supported by 2.11)
  3. FXOS 2.11 → FXOS 2.13
  4. ASA 9.17 → ASA 9.19

- Firewall Threat Defense: Interim upgrades may be required for Firewall Threat Defense, in addition to the FXOS requirements above. For the exact upgrade path, refer to the Firewall Management Center upgrade guide for your version.
- ASA: ASA lets you upgrade directly from your current version to any higher version, noting the FXOS requirements above.

***Table 2: Firepower 4100/9300 Compatibility with ASA and Firewall Threat Defense***

| FXOS Version | Model | ASA Version | Firewall Threat Defense Version |
|---|---|---|---|
| 2.18.10 | Firepower 4112 | **9.24.10** (recommended)<br>9.24.1<br>9.23<br>9.22<br>9.20<br>9.19 | **10.1** (recommended)<br>10.0<br>7.7<br>7.6<br>7.4<br>7.3 |
| | Firepower 4145<br>Firepower 4125<br>Firepower 4115<br>Firepower 9300 SM-56<br>Firepower 9300 SM-48<br>Firepower 9300 SM-40 | **9.24.10** (recommended)<br>9.24.1<br>9.23<br>9.22<br>9.20<br>9.19 | **10.1** (recommended)<br>10.0<br>7.7<br>7.6<br>7.4<br>7.3 |
| 2.18.0 | Firepower 4112 | **9.24.1** (recommended)<br>9.23<br>9.22<br>9.20<br>9.19 | **10.0** (recommended)<br>7.7<br>7.6<br>7.4<br>7.3 |
| | Firepower 4145<br>Firepower 4125<br>Firepower 4115<br>Firepower 9300 SM-56<br>Firepower 9300 SM-48<br>Firepower 9300 SM-40 | **9.24.1** (recommended)<br>9.23<br>9.22<br>9.20<br>9.19 | **10.0** (recommended)<br>7.7<br>7.6<br>7.4<br>7.3 |

| FXOS Version | Model | ASA Version | Firewall Threat Defense Version |
|---|---|---|---|
| 2.17 | Firepower 4112 | **9.23** (recommended)<br>9.22<br>9.20<br>9.19<br>9.18 | **7.7** (recommended)<br>7.6<br>7.4<br>7.3<br>7.2 |
| | Firepower 4145<br>Firepower 4125<br>Firepower 4115 | **9.23** (recommended)<br>9.22<br>9.20<br>9.19<br>9.18 | **7.7** (recommended)<br>7.6<br>7.4<br>7.3<br>7.2 |
| | Firepower 9300 SM-56<br>Firepower 9300 SM-48<br>Firepower 9300 SM-40 | | |
| 2.16 | Firepower 4112 | **9.22** (recommended)<br>9.20<br>9.19<br>9.18<br>9.17 | **7.6** (recommended)<br>7.4<br>7.3<br>7.2<br>7.1 |
| | Firepower 4145<br>Firepower 4125<br>Firepower 4115 | **9.22** (recommended)<br>9.20<br>9.19<br>9.18<br>9.17 | **7.6** (recommended)<br>7.4<br>7.3<br>7.2<br>7.1 |
| | Firepower 9300 SM-56<br>Firepower 9300 SM-48<br>Firepower 9300 SM-40 | | |

| FXOS Version | Model | ASA Version | Firewall Threat Defense Version |
|---|---|---|---|
| 2.14(1) | Firepower 4112 | **9.20** (recommended)<br>9.19<br>9.18<br>9.17<br>9.16<br>9.14 | **7.4** (recommended)<br>7.3<br>7.2<br>7.1<br>7.0<br>6.6 |
| | Firepower 4145<br>Firepower 4125<br>Firepower 4115<br>Firepower 9300 SM-56<br>Firepower 9300 SM-48<br>Firepower 9300 SM-40 | **9.20** (recommended)<br>9.19<br>9.18<br>9.17<br>9.16<br>9.14 | **7.4** (recommended)<br>7.3<br>7.2<br>7.1<br>7.0<br>6.6 |
| 2.13 | Firepower 4112 | **9.19** (recommended)<br>9.18<br>9.17<br>9.16<br>9.14 | **7.3** (recommended)<br>7.2<br>7.1<br>7.0<br>6.6 |
| | Firepower 4145<br>Firepower 4125<br>Firepower 4115<br>Firepower 9300 SM-56<br>Firepower 9300 SM-48<br>Firepower 9300 SM-40 | **9.19** (recommended)<br>9.18<br>9.17<br>9.16<br>9.14 | **7.3** (recommended)<br>7.2<br>7.1<br>7.0<br>6.6 |

| FXOS Version | Model | ASA Version | Firewall Threat Defense Version |
|---|---|---|---|
| 2.12 | Firepower 4112 | **9.18** (recommended)<br>9.17<br>9.16<br>9.14 | **7.2** (recommended)<br>7.1<br>7.0<br>6.6 |
| | Firepower 4145<br>Firepower 4125<br>Firepower 4115 | **9.18** (recommended)<br>9.17<br>9.16<br>9.14<br>9.12 | **7.2** (recommended)<br>7.1<br>7.0<br>6.6<br>6.4 |
| | Firepower 9300 SM-56<br>Firepower 9300 SM-48<br>Firepower 9300 SM-40 | | |
| | Firepower 4150<br>Firepower 4140<br>Firepower 4120<br>Firepower 4110 | **9.18** (recommended)<br>9.17<br>9.16<br>9.14<br>9.12 | **7.2** (recommended)<br>7.1<br>7.0<br>6.6<br>6.4 |
| | Firepower 9300 SM-44<br>Firepower 9300 SM-36<br>Firepower 9300 SM-24 | | |

| FXOS Version | Model | ASA Version | Firewall Threat Defense Version |
|---|---|---|---|
| 2.11 | Firepower 4112 | **9.17** (recommended)<br>9.16<br>9.14 | **7.1** (recommended)<br>7.0<br>6.6 |
| | Firepower 4145<br>Firepower 4125<br>Firepower 4115 | **9.17** (recommended)<br>9.16<br>9.14<br>9.12 | **7.1** (recommended)<br>7.0<br>6.6<br>6.4 |
| | Firepower 9300 SM-56<br>Firepower 9300 SM-48<br>Firepower 9300 SM-40 | | |
| | Firepower 4150<br>Firepower 4140<br>Firepower 4120<br>Firepower 4110 | **9.17** (recommended)<br>9.16<br>9.14<br>9.12<br>9.8 | **7.1** (recommended)<br>7.0<br>6.6<br>6.4 |
| | Firepower 9300 SM-44<br>Firepower 9300 SM-36<br>Firepower 9300 SM-24 | | |
| 2.10<br>**Note** For compatibility with 7.0.2+ and 9.16(3.11)+, you need FXOS 2.10(1.179)+. | Firepower 4112 | **9.16** (recommended)<br>9.14 | **7.0** (recommended)<br>6.6 |
| | Firepower 4145<br>Firepower 4125<br>Firepower 4115 | **9.16** (recommended)<br>9.14<br>9.12 | **7.0** (recommended)<br>6.6<br>6.4 |
| | Firepower 9300 SM-56<br>Firepower 9300 SM-48<br>Firepower 9300 SM-40 | | |
| | Firepower 4150<br>Firepower 4140<br>Firepower 4120<br>Firepower 4110 | **9.16** (recommended)<br>9.14<br>9.12<br>9.8 | **7.0** (recommended)<br>6.6<br>6.4 |
| | Firepower 9300 SM-44<br>Firepower 9300 SM-36<br>Firepower 9300 SM-24 | | |

| FXOS Version | Model | ASA Version | Firewall Threat Defense Version |
|---|---|---|---|
| 2.9 | Firepower 4112 | 9.14 | 6.6 |
| | Firepower 4145<br>Firepower 4125<br>Firepower 4115 | 9.14<br>9.12 | 6.6<br>6.4 |
| | Firepower 9300 SM-56<br>Firepower 9300 SM-48<br>Firepower 9300 SM-40 | | |
| | Firepower 4150<br>Firepower 4140<br>Firepower 4120<br>Firepower 4110 | 9.14<br>9.12<br>9.8 | 6.6<br>6.4 |
| | Firepower 9300 SM-44<br>Firepower 9300 SM-36<br>Firepower 9300 SM-24 | | |
| 2.8 | Firepower 4112 | **9.14** | **6.6**<br>**Note**<br>6.6.1+ requires FXOS 2.8(1.125)+. |
| | Firepower 4145<br>Firepower 4125<br>Firepower 4115 | **9.14** (recommended)<br>9.12<br>**Note**<br>Firepower 9300 SM-56 requires ASA 9.12(2)+ | **6.6** (recommended)<br>**Note**<br>6.6.1+ requires FXOS 2.8(1.125)+.<br>6.4 |
| | Firepower 9300 SM-56<br>Firepower 9300 SM-48<br>Firepower 9300 SM-40 | | |
| | Firepower 4150<br>Firepower 4140<br>Firepower 4120<br>Firepower 4110 | **9.14** (recommended)<br>9.12<br>9.8 | **6.6** (recommended)<br>**Note**<br>6.6.1+ requires FXOS 2.8(1.125)+.<br>6.4<br>6.2.3 |
| | Firepower 9300 SM-44<br>Firepower 9300 SM-36<br>Firepower 9300 SM-24 | | |

| FXOS Version | Model | ASA Version | Firewall Threat Defense Version |
|---|---|---|---|
| 2.6(1.157)<br>**Note** You can now run ASA 9.12+ and FTD 6.4+ on separate modules in the same Firepower 9300 chassis | Firepower 4145<br>Firepower 4125<br>Firepower 4115 | **9.12**<br>**Note** Firepower 9300 SM-56 requires ASA 9.12.2+ | **6.4** |
| | Firepower 9300 SM-56<br>Firepower 9300 SM-48<br>Firepower 9300 SM-40 | | |
| | Firepower 4150<br>Firepower 4140<br>Firepower 4120<br>Firepower 4110 | **9.12** (recommended)<br>9.8 | **6.4** (recommended)<br>6.2.3 |
| | Firepower 9300 SM-44<br>Firepower 9300 SM-36<br>Firepower 9300 SM-24 | | |
| 2.6(1.131) | Firepower 9300 SM-48<br>Firepower 9300 SM-40 | **9.12** | Not supported |
| | Firepower 4150<br>Firepower 4140<br>Firepower 4120<br>Firepower 4110 | **9.12** (recommended)<br>9.8 | |
| | Firepower 9300 SM-44<br>Firepower 9300 SM-36<br>Firepower 9300 SM-24 | | |
| 2.3(1.73) | Firepower 4150<br>Firepower 4140<br>Firepower 4120<br>Firepower 4110 | 9.8<br>**Note** 9.8(2.12)+ is required for flow offload when running FXOS 2.3(1.130)+. | **6.2.3** (recommended)<br>**Note** 6.2.3.16+ requires FXOS 2.3.1.157+ |
| | Firepower 9300 SM-44<br>Firepower 9300 SM-36<br>Firepower 9300 SM-24 | | |

| FXOS Version | Model | ASA Version | Firewall Threat Defense Version |
|---|---|---|---|
| 2.3(1.66)<br>2.3(1.58) | Firepower 4150<br>Firepower 4140<br>Firepower 4120<br>Firepower 4110 | 9.8<br>**Note**<br>9.8(2.12)+ is required for flow offload when running FXOS 2.3(1.130)+. | |
| | Firepower 9300 SM-44<br>Firepower 9300 SM-36<br>Firepower 9300 SM-24 | | |
| 2.2 | Firepower 4150<br>Firepower 4140<br>Firepower 4120<br>Firepower 4110 | **9.8** | Firewall Threat Defense versions are EoL |
| | Firepower 9300 SM-44<br>Firepower 9300 SM-36<br>Firepower 9300 SM-24 | | |

#### Note on Downgrades

Downgrade of FXOS images is not officially supported. The only Cisco-supported method of downgrading an image version of FXOS is to perform a complete re-image of the device.

# 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 9.24(x)

There are no open bugs in this release.

## Resolved Bugs in Version 9.24(10)

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

| Identifier | Headline |
|---|---|
| CSCws03406 | 4200- Block 1550 depletion seen when Snort crashes |
| CSCwt72108 | WA-4215 - Traceback observed due to Block depletion in the 256 1550 and 9344 with UDP traffic |
| CSCwt98497 | routing: FTD DVTI hub leaves stale RIB routes with missing interface after tunnel flap |

## Resolved Bugs in Version 9.24(1)

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

| Identifier | Headline |
|---|---|
| CSCvh98118 | "logging debug-trace persistent" fails for "debug ip ..." related debugs |
| CSCvm76755 | DP-CP arp-in and adj-absent queues need to be separated |
| CSCwa38880 | Order of access-list/ access-group is different in standby unit. Full sync happens during node-join. |
| CSCwb07908 | Standby FTD/ASA sends DNS queries with source IP of 0.0.0.0 |
| CSCwc57341 | Inline pair has incorrect FTW bypass operation mode of 'Phy Bypass' |
| CSCwc82675 | ASA/FTD : High LINA memory observed after configuring multiple AnyConnect packages |
| CSCwd92327 | on 2k platform, external authentication fails for users starting with number |
| CSCwf04460 | The fxos directory disappears after cancelling show tech fprm detail command with Ctr+c is executed. |
| CSCwf25454 | Stale anyconnect entries causing issues with routing |
| CSCwf72285 | DAP: debug dap trace not fully shown after 3000+ lines |
| CSCwh10931 | ASA/FTD traceback and reload when invoking "show webvpn saml idp" CLI command |
| CSCwh41925 | Lina traceback in ZMQ Proxy caused service loss. |
| CSCwh53745 | ASA: unexpected logs for initiating inbound connection for DNS query response |
| CSCwi39206 | 3100/4200: qdma driver watchdog timeout |
| CSCwi95690 | Fault "Adapter 1/x/y is unreachable" due to connectivity failure between supervisor and VIC adapter |
| CSCwk09488 | Incorrect syslog generated on failure to process SGT from ISE during RA authentication |

| Identifier | Headline |
|---|---|
| CSCwk33387 | SNMP for mgmt0/diagnostic outgoing traffic is missing |
| CSCwk42676 | Virtual ASA/FTD may traceback and reload in thread PTHREAD |
| CSCwm04866 | debug menu command to prevent 1550 block depletion due to sendinglogs to TCP syslog server |
| CSCwm51747 | SSH access with public key authentication fails after FXOS upgrade |
| CSCwm61345 | FXOS: Directory /var/tmp Triggering FXOS Fault F0182 due to vdc.log (Excessive Logging,Log Rotation) |
| CSCwm74289 | NAT traps have to be rate-limited |
| CSCwm80732 | ASA/FTD - Traceback and reload Due to Race Condition in TCP Proxy |
| CSCwm81280 | Evaluation of ssp for mod_nuova logs authentication tokens |
| CSCwm83088 | Cisco FXOS and UCS Manager Software Stored Cross-Site Scripting Vulnerability |
| CSCwm95189 | Redis is an open source, in-memory database that persists on disk. An |
| CSCwm95191 | In the Linux kernel, the following vulnerability has been resolved: s |
| CSCwm96652 | Cluster assigning wrong nat for unit, traffic not being forwarded properly back to unit |
| CSCwn00475 | Memory Blocks 80 and 9344 leak due to priority-queue |
| CSCwn10661 | FTD running on FPR2k devices, using CMI, has no ARP for 203.0.113.129 |
| CSCwn19190 | Memory fragmentation resulted in huge pages unavailable for lina |
| CSCwn22610 | fs-daemon hap reset with core generation |
| CSCwn24777 | ASA block depletion due to SSL pre auth connections |
| CSCwn27872 | Big chunk of Memory of around 25KB is being allocated on Stack in "eigrp_interface_ioctl" API |
| CSCwn32978 | Traceback and reload in Thread Name Datapath |
| CSCwn35495 | Primary FTD instance MAC address is not updated correctly in FXOS during failover |
| CSCwn36712 | NAT divert for 8305 on standby not updating post failover causing the Primary, standby FTD to show offline on FMC |
| CSCwn39081 | SNMP walk results in ASCII value for IPSEC Peer instead of an IP address. |
| CSCwn40572 | MI: Vlan info is not applied at FXOS level when Virtual MAC is configured |
| CSCwn40702 | ASA traceback and reload in freeb_core_local_internal |
| CSCwn45049 | Coverity System SA warnings 2024-09-09, Coverity Defects 922530 922529 922528 922630 921809 921808 |

| Identifier | Headline |
|---|---|
| CSCwn45510 | S2S VPN tunnel Child SA unsuccessful renegotiation |
| CSCwn47308 | Critical health alerts 'user configuration(FSM.sam.dme.AaaUserEpUpdateUserEp)' on FPR 1100/2100/3100 |
| CSCwn50760 | ASA Traceback after upgrade to 9.20.3.7 |
| CSCwn51845 | Tracebacks observed in a cluster member running ASA 9.20.3.4 |
| CSCwn59032 | FCM GUI became inaccessible after upgrading to ASA 9.18.4.22 \| FPR 2130 Platform Mode |
| CSCwn59379 | Bandwidth information of a port-channel is not getting updated if an interface member goes down. |
| CSCwn60726 | Traceback and reload with Thread Name: vtemplate process |
| CSCwn61041 | Traceback and reload during clear bgp * ipv6 unicast involving watchdog |
| CSCwn63839 | Traceback in thread name Lina on configuring arp permit-nonconnected with BVI |
| CSCwn64025 | ASA: IPv6 EIGRP routes learned from other neighbors are missing in updates after failover |
| CSCwn65415 | ASA: floating-conn not closing UDP conns if conn was created without ARP entry for next hop |
| CSCwn69075 | Cisco Secure Firewall ASA Software and Secure FTD Software OSPF Heap Corruption Vulnerability |
| CSCwn69076 | Cisco Secure Firewall ASA Software and Secure FTD Software OSPF DoS Vulnerability |
| CSCwn69078 | Cisco Secure Firewall ASA Software and Secure FTD Software OSPF DoS Vulnerability |
| CSCwn69079 | Cisco Secure Firewall ASA Software and Secure FTD Software OSPF Memory Exhaustion Vulnerability |
| CSCwn69081 | Cisco Secure Firewall ASA Software and Secure FTD Software OSPF DoS Vulnerability |
| CSCwn69488 | ASA/FTD - Traceback and Reload in Threadname IP RIB Update |
| CSCwn71596 | Intf Link down (Init, mac-link-down) seen - EtherChannel Membership in Down/Down/Down state after unplug/replug of the cable |
| CSCwn71946 | show blocks old core local can lead to unexpected reload. |
| CSCwn73351 | Asia/Bangkok timezone option not listed in ASA running on firepower1k |
| CSCwn73399 | Cisco Secure Firewall Adaptive Security Appliance, and Secure Firewall Threat Defense Software IKEv2 Denial of Service Vulnerability |

| Identifier | Headline |
|---|---|
| CSCwn75667 | Banner motd does not display when configured |
| CSCwn76079 | SSH works in admin context but doesn't work in any user context after changing ssh key-exchange |
| CSCwn79553 | Unreachable LDAP/AD referrals may cause delays or timeouts in external authentication on FTD |
| CSCwn80419 | Need the SVC Rx/Tx queue as a configurable option |
| CSCwn80765 | ISA3000 with ASA Refuses SSH Access If CiscoSSH is Enabled |
| CSCwn81118 | RTSP packets getting stuck in transmit queue leading to 9k blocks exhaustion. |
| CSCwn81784 | Choosing clause 91 FEC via the FMC sets fec 544 instead of fec 528 on QSFP-100G-CU3M |
| CSCwn81995 | Traceback and Reload caused by Memory corruption with SNMP inspection enabled |
| CSCwn84557 | Lina traceback and reload due to "spin_lock_fair_mode_enqueue" |
| CSCwn86002 | core corruption still seen with switching to quick core feature |
| CSCwn87513 | ASA clock is out of sync 2 hours when timezone is configured to Europe/Dublin which is GMT. |
| CSCwn90327 | FP1150 ASA/FTD - Traceback and reload triggered by watchdog timer |
| CSCwn90900 | High ASA/FTD memory usage due to polling of RA VPN related SNMP OIDs |
| CSCwn90958 | Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense Software Authenticated Command Injection Vulnerability |
| CSCwn91612 | Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense Software Authenticated Command Injection Vulnerability |
| CSCwn91996 | WM-DT-7.7.0-40:: Observed switch config failed and switch Mac error on device console |
| CSCwn92248 | FPR2100 & FPR1100: Port-channel interfaces flap with LACP |
| CSCwn92894 | Occasionally, 'show chunkstat top-usage' output does not show all entries |
| CSCwn93319 | ASA/FTD may traceback and reload in Thread Name "DATAPATH" |
| CSCwn93411 | FXOS reset and reload due to snmpd service failure |
| CSCwn95939 | Generate syslog if received CRL is older than cached CRL |
| CSCwn95945 | Generate syslog if received CRL signature validation fails |
| CSCwn96929 | ASA: Traceback and Reload Under Thread Name SSH |
| CSCwn96963 | FTD generates syslog 430002 as VPN Routing without VPN hairpin |

| Identifier | Headline |
|---|---|
| CSCwn97630 | FTD reboot and traceback in DATAPATH due to IPv6 packet processing |
| CSCwn98402 | Debuggability: FP2100 port-channel interfaces flap after upgrade |
| CSCwo00102 | Snort3 trimming packets with invalid sequence number due to bad window size information received |
| CSCwo00225 | VNI source MTU is not IPv6 aware after upgrade if configured prior to upgrade |
| CSCwo00332 | Firepower wiping SSL trustpoint config after reloading. |
| CSCwo00444 | Nitrox Engine (Crypto Accelerator) problem affecting crypto hardware offload on FPR3100/4200 platforms |
| CSCwo00702 | Community lists should not throw an error until the last item in the list is being deleted |
| CSCwo00880 | Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense Software VPN Web Server Denial of Service Vulnerability |
| CSCwo01785 | Memory leak in RAVPN |
| CSCwo05712 | Serviceability Enhancement - Make FXOS disk errors more descriptive |
| CSCwo05801 | SNMP walk on FXOS 2.14.1.167 causing warning loop |
| CSCwo08042 | ASAv reloaded unexpectedly with traceback on Unicorn Proxy Thread |
| CSCwo08306 | Command authorization fallback to Local only works for users with privilege 15. |
| CSCwo08724 | Active HA unit goes into failed state before peer unit gets into a ready state during snort failure |
| CSCwo09060 | SSL trustpoint with 4096 bit RSA keys not allowed by ASA if renewed via CLI |
| CSCwo09195 | Traceback and reload during the deployment after disabling FQDNs. |
| CSCwo09439 | ASA/FTD may traceback and reload in Thread Name 'DATAPATH-3-4280' |
| CSCwo09618 | Enabling debugs with EEM fails |
| CSCwo09921 | The whois lookup command for the FMC GUI does not properly handle errors |
| CSCwo13550 | Dispatch queue drops have no snapshot or tuple view for dropped flows |
| CSCwo15021 | Cisco Secure Firewall Adaptive Security Appliance, and Secure Firewall Threat Defense Software IKEv2 Denial of Service Vulnerability |
| CSCwo15022 | Cisco Secure Firewall Adaptive Security Appliance, and Secure Firewall Threat Defense Software IKEv2 Denial of Service Vulnerability |
| CSCwo15023 | Cisco Secure Firewall Adaptive Security Appliance, and Secure Firewall Threat Defense Software IKEv2 Denial of Service Vulnerability |

| Identifier | Headline |
|---|---|
| CSCwo15024 | Cisco Secure Firewall Adaptive Security Appliance, and Secure Firewall Threat Defense Software IKEv2 Denial of Service Vulnerability |
| CSCwo15026 | Cisco Secure Firewall Adaptive Security Appliance, and Secure Firewall Threat Defense Software IKEv2 Denial of Service Vulnerability |
| CSCwo15027 | Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense Software Remote Access SSL VPN Denial of Service Vulnerability |
| CSCwo15715 | IKEv2 Rekeys fail due to fragmentation during the IKE Rekey |
| CSCwo16488 | FXOS allows booting and starting an image installation using a Patch image |
| CSCwo18838 | ASA/FTD may traceback and reload in Thread Name 'lina_exec_startup_thread' |
| CSCwo18850 | Cisco Secure Firewall Adaptive Security Appliance, Secure Firewall Threat Defense Software HTTP Server Remote Code Execution Vulnerability |
| CSCwo19762 | Unable to rejoin data node in cluster after re-enabling mac-address auto in multi-context mode |
| CSCwo21767 | Port scan alerts not getting generated for custom configuration |
| CSCwo22091 | FTD sending "0.0.0.0" NAS-IP-Address attribute when authenticating/authorizing using Radius |
| CSCwo24772 | debug packet-condition does not work as expected |
| CSCwo24856 | 9K block depletion causing slowdown of all traffic through firewall |
| CSCwo25236 | Suddenly customer lost SSH access to the ASA |
| CSCwo26258 | Default Route Changes from Management0 to Management1 After Reload or Upgrade on FPR 4200 Series |
| CSCwo27260 | Unit taking ~13 secs to become active |
| CSCwo31094 | Virtual ASA Traceback and Reload Caused by Disk Access Issues with NFS Enabled |
| CSCwo33815 | FMC: Deployment takes longer than expected when removing SNMP hosts from Platform Settings |
| CSCwo35783 | Enhance Debugging for add/update/withdraw of routes with neighbors |
| CSCwo35788 | Serviceability Enhancement - New 'show bgp internal' command for advanced debugging |
| CSCwo35938 | IPv6 Management communication is lost due to a missing management-only multicast route. |
| CSCwo36485 | ASA/FTD traceback and reload in vaccess_nameif_action thread |
| CSCwo40957 | Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense Software IPsec Denial of Service Vulnerability |

| Identifier | Headline |
|---|---|
| CSCwo41250 | Traceback & Reload in thread named: DATAPATH-1-23988 during low memory condition |
| CSCwo42102 | show tech-support fprm detail command is getting stuck for longer duration |
| CSCwo42230 | Memory leak leading to split brain |
| CSCwo42326 | ENH: Include SystemID in "show system detail" in techsupport file |
| CSCwo44732 | ARP is silently dropping packet for an unreachable next hop |
| CSCwo45497 | Counter from IKEV2 stats does not match the number of tunnels in VPN-Sessiondb |
| CSCwo45848 | SecGW: Data node fails to join the cluster with cluster_ccp_make_rpc_call failed to clnt_call error |
| CSCwo46142 | Port-channel member interface flap renders it as an inactive member |
| CSCwo47978 | ASA may traceback and reload in Thread Name 'fover_parse' |
| CSCwo48439 | Traceback & Reload in Thread Name Unicorn Admin Handler |
| CSCwo49425 | Logging recipient-address not overriding the logging mail message severity levels |
| CSCwo49744 | DNS and default gateway are removed on FTD managed through data interface |
| CSCwo49925 | Cisco Secure Firewall ASA Software and Secure FTD Software IKEv2 DoS Vulnerability |
| CSCwo49926 | Cisco Secure Firewall ASA Software and Secure FTD Software IKEv2 DoS Vulnerability |
| CSCwo49928 | Cisco Secure Firewall Adaptive Security Appliance, and Secure Firewall Threat Defense Software IKEv2 Denial of Service Vulnerability |
| CSCwo49932 | Cisco Secure Firewall ASA Software and Secure FTD Software Remote Access SSL VPN Authentication Denial of Service Vulnerability |
| CSCwo49934 | Cisco Secure Firewall ASA Software and Secure FTD Software Remote Access SSL VPN Memory Exhaustion Denial of Service Vulnerability |
| CSCwo50417 | Warwick Avenue: LLDP neighbours are not discovered if MGMT 1/2 interface is down |
| CSCwo54996 | Traffic failure due to 9344 blocks leak |
| CSCwo56698 | Cisco Secure Firewall Threat Defense Software Geolocation Remote Access VPN Bypass Vulnerability |
| CSCwo57740 | '${dsk_a} missing or inoperable. Rebooting Blade.' error does not specify missing or inoperable disk |
| CSCwo58033 | [Cluster] CPU Utilization of 100% when NAT Pool exhaustion happens in a context. |

| Identifier | Headline |
|---|---|
| CSCwo58191 | FTD: Large Delay in packets being inspected by snort |
| CSCwo58260 | Add "built" and "teardown" messages for the GRE \| IPinIP connections to the Lina syslog |
| CSCwo60609 | DNS doctoring not working correctly if the doctoring rule is of type dynamic and has any interface |
| CSCwo61241 | Logical App Stuck in 'Start Failed' Due to checkSystemCPUs Failure |
| CSCwo64788 | FPR9K-SM-56 Cluster - FTD Stuck in an application install loop & error 'pooled address is unknown' |
| CSCwo65060 | FTD HA \| Same MAC for port-channels causing network outage. |
| CSCwo65866 | Network Outage when Primary FTD Instance is Disabled from FCM |
| CSCwo66872 | snmp_logging_thread is utilizing high CPU in control plane |
| CSCwo71052 | FPR1010 Ethernet1/1 trunk port is not passing Vlan traffic after a reload |
| CSCwo71552 | Cisco Secure Firewall ASA Software and Secure FTD Software OSPF DoS Vulnerability |
| CSCwo73885 | Cisco Secure Firewall ASA Software and Secure FTD Software Authenticated Command Injection Vulnerability |
| CSCwo73886 | Cisco Secure Firewall ASA Software and Secure FTD Software Remote Access SSL VPN Unauthenticated Memory Exhaustion Denial of Service Vulnerability |
| CSCwo73888 | Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense Software Lua Code Injection Vulnerability |
| CSCwo73889 | Cisco Secure Firewall ASA Software and Secure FTD Software Remote Access SSL VPN Lua Interpreter Denial of Service Vulnerability |
| CSCwo73891 | Cisco Secure Firewall ASA Software and Secure FTD Software Remote Access SSL VPN Authenticated Memory Exhaustion Denial of Service Vulnerability |
| CSCwo74009 | Cisco FXOS and UCS Manager Software Command Injection Vulnerability |
| CSCwo74496 | BFD flap due to ASA not processing incoming BFD packets after unrelated BFD peers go down |
| CSCwo75483 | SNMP polling to chassis is unsuccessful with FTD Multi-instance in HA used as SNMP agent |
| CSCwo75810 | SNMP configuration is not applied consistently across same FTDs type and version |
| CSCwo76165 | Deployment failure due to rsync |
| CSCwo76436 | 3100 Marvell 4.3.14 CPSS patch for the interface mac stuck issue seen with peer switch reloads |

| Identifier | Headline |
|---|---|
| CSCwo76559 | ASA/FTD traceback and reload with SNMP Notify Thread seen on 3110 |
| CSCwo77665 | Portscan event in FMC displays incorrect source/destination when set to 'low' setting |
| CSCwo78969 | Traceback in thread name DATAPATH when a unit is re-joining the cluster |
| CSCwo79028 | Post-Failover FQDN Resolution Deferred Until Next DNS Poll Interval |
| CSCwo79798 | Cryptochecksum changed after reloading. |
| CSCwo80223 | BFD packets are not dropped for single-hop BFD sessions received via alternate path |
| CSCwo82639 | Local user details not replicated to data nodes in a cluster setup. |
| CSCwo82658 | ASDM: Displays Error of Keypair already exists when adding an identity certificate. |
| CSCwo83389 | Difference in RSA key length at multiple spots in FXOS |
| CSCwo84467 | L3 Clustering where BGP immediately comes up while DATA node is still in bulk sync |
| CSCwo86422 | Unidirectional communication over ccl leading to split-cluster. |
| CSCwo87763 | ASA/FTD: Primary standby unit becomes Active after reload in HA set up |
| CSCwo87938 | backout change preventing enabling clustering in FIPS mode |
| CSCwo88204 | ASA/FTD traceback and reload triggered by the Smart Call Home process in sch_dispatch_to_url. |
| CSCwo88518 | If command replication fails to any nodes in cluster, send kick the node out from cluster to fmc |
| CSCwo89233 | Command replication failure to cluster nodes on command commit noconfirm revert-save after access-list, additional debugs |
| CSCwo91436 | FPR 4125 Multi instance: High Snort and System Core CPU Usage (100%) Triggering FMC Critical Alerts |
| CSCwo91748 | Lina: Traceback in thread name ssh on executing show access-list after ACL deletion |
| CSCwo91965 | ASAv restarts unexpectedly |
| CSCwo92226 | ASA: asacli Processes Not Terminated When SSH Sessions Are Closed |
| CSCwo94260 | FTD: SGT Inline tag stripped from SIP packets |
| CSCwo94274 | FP4100/9300 Fatal error: Incomplete chain observed before watchdogs with reset code 0x0040 |
| CSCwo94483 | LINA stays inactive without reloading after traceback on non-CP thread |
| CSCwo95496 | Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense Software Lua Code Injection Vulnerability |

| Identifier | Headline |
|---|---|
| CSCwo97439 | ACL: ASA may show false "OOB Access-list config change detected" warning after AAA authorization command is applied |
| CSCwo99690 | Error Encountered While Disabling the 'Call-Home Reporting Anonymous' Option in Call-Home Configuration |
| CSCwp00977 | FTD Intermittent Syslog Alert: mcelog daemon is not running. Restarting the daemon. |
| CSCwp01015 | ASA/FTD traceback and reload in function mp_percore |
| CSCwp02224 | FPR failover split brain when upgrade primary/standby device's FXOS version |
| CSCwp04235 | ASA traceback and reload |
| CSCwp05866 | Cisco Secure Firewall Adaptive Security Appliance Software Multiple Context Mode SCP Unauthorized File Access Vulnerability |
| CSCwp06882 | high CPU usage after ASA upgrade from 9.20.3.9 to 9.20.3.16 running on Hyper-V |
| CSCwp06890 | SFF_SFP_10G_25G_CSR_S V03 modules from Finisar ports bouncing when connected. |
| CSCwp08772 | ASA: tls-proxy maximum-session command error |
| CSCwp10889 | Packet-tracer displaying incorrect ACL even though traffic action is taken based on the expected ACL. |
| CSCwp10957 | SSL error causing connection to Cisco Smart Software Manager (CSSM) to terminate |
| CSCwp11382 | ASA/FTD: the ssl trust-point command deleted after a reload |
| CSCwp13016 | FTD/ASA SSH: Terminal monitor is not showing logs |
| CSCwp13399 | Collecting "show tech-support fprm" results into core for tar itself |
| CSCwp13540 | Wrong URL incorrectly displayed for file upload with Japanese text in file path for client-less VPN |
| CSCwp14123 | Tmatch memory is mostly consumed by ARP-DP. |
| CSCwp16529 | Negative value displayed for buffer drops when using " show cluster info load-monitor details" |
| CSCwp16739 | ASA crashinfo files not generated on FP4200 devices |
| CSCwp17700 | Syslog format is not properly printed when EMBLEM format is enabled at least in one syslog host |
| CSCwp18885 | FP9300/4100 may traceback & reload due to a "Kernel Panic" |
| CSCwp22214 | Multiple mail drops and enq failures are seen while traffic is going through the box. |
| CSCwp22612 | Policy deploy failing on FTD when trying to remove Umbrella DNS Configuration |

| Identifier | Headline |
|---|---|
| CSCwp22743 | wpk - 1gsx link remains up on wpk but on switch side it shows as not connected |
| CSCwp25033 | An ICMP not reachable storm might cause high CPU on a two units FTD cluster |
| CSCwp26815 | CPU usage by "WebVPN Timer Process" on standby ASA device |
| CSCwp29401 | Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense Software SAML Reflected Cross-Site Scripting Vulnerability |
| CSCwp32469 | Error : Msglyr::ZMQWrapper::registerSender() : Failed to bind ZeroMQ Socket |
| CSCwp33077 | SAML IdP entityID increase from capped 128 character maximum |
| CSCwp33410 | dmesg and kern.log file flooded with Tx Queue=0 logs |
| CSCwp34610 | IKEv2-EAP Authentication Fails with Windows and MacOS Native VPN Clients |
| CSCwp36133 | Clarify the working of Fallthrough to Interface PAT (Destination Interface) as it is not working as expected |
| CSCwp37284 | "CSRF Token Mismatch" error seen when users click logout from Clientless VPN page |
| CSCwp39319 | ASA Memory leak while processing large CRLs. |
| CSCwp60027 | Capture the reason of reboot in FTD logs |
| CSCwp60849 | ASA Core file generated is corrupted |
| CSCwp60896 | ASA Clock reverts to UTC after device reload |
| CSCwp64615 | ASA/FTD: ASP drop capture for 'invalid-ip-length' or 'sp-security-failed' does not work with match criteria |
| CSCwp66721 | Memory leak in SSL crypto causing high Lina memory usage on lower-end devices running FTD 7.7.0 |
| CSCwp67356 | HA state should not transition from ColdStandby to Active |
| CSCwp68059 | Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense Software VPN Web Services Cross-Site Scripting Vulnerability |
| CSCwp83345 | Cluster: Multi-blade chassis not transmitting broadcast traffic outbound to specific vlan |
| CSCwp87708 | FP1140 Critical FXOS fault alerts (F1000413) after upgrade |
| CSCwp89969 | Prolonged delays in firewall restart/reboot completion |
| CSCwp90780 | Restoring .tgz context file causes allocated interfaces to be removed from 'system' configuration |
| CSCwp92390 | FTD - SNMP Walk of FXOS FTD OID Tree Returns Empty or Times Out |

| Identifier | Headline |
|---|---|
| CSCwp93368 | LINA traceback Observed on FTDv Firewalls Deployed in Azure: snp_vxlan_encap_and_send_to_remote_peer |
| CSCwp97402 | WA: Traceback and reload due to lock contention on the tmatch table during deployment with large snmp config |
| CSCwp97862 | If failover IPSEC PSK is 78 characters or greater HA breaks with "Could not set failover ipsec pre-shared-key" |
| CSCwp99130 | FPR42xx - SNMP poll reports incorrect FanTray Status at Down while actually operational |
| CSCwq01516 | Cisco Secure Firewall ASA Software and Secure FTD Software IKEv2 DoS Vulnerability |
| CSCwq01526 | Cisco Secure FTD Software Authenticated DoS Vulnerability |
| CSCwq02055 | Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense Software VPN Web Services Client-Side Request Smuggling Vulnerability |
| CSCwq07441 | Memory Leak observed on FP2110 running ASA due to monitoring interface configured in HA |
| CSCwq07808 | FP3105 Traceback and Reload after changing the speed on Ethernet interface |
| CSCwq11260 | The syslog server called fluentbit can't recognize the fox syslog format and print it |
| CSCwq13032 | 3100/4200: 1G Management interface flapping after upgrade |
| CSCwq15499 | RAVPN Geolocation: Deployment failing by enabling all or specific countries in service access object |
| CSCwq16926 | Traceback and Reload while two processes attempt to free a TD subnet structure |
| CSCwq17612 | Misleading "failover reset" log printed on console when reload triggered by HA. |
| CSCwq18679 | ASA from CSM/CLI - no access-list ACL_name line line_nr remark on last ACL line shows message - "Specified remark does not exist" |
| CSCwq21101 | Invalid host header reveals ASA interface IP address |
| CSCwq21442 | 3RU MI instances offline after baseline/creation |
| CSCwq22206 | VPN lost during a rekey with 'IKEv2 negotiation aborted due to ERROR: Platform errors' |
| CSCwq24081 | Cisco Secure Firewall Adaptive Security Appliance Software SSH Partial Private Key Authentication Bypass Vulnerability |
| CSCwq24140 | Security module reboot triggered by a CIMC reset. |
| CSCwq27217 | ASA: Traceback and reload on threat detection, interfaces unstable after that |
| CSCwq29375 | ASA/FTD - Assert triggered during FP_PUNT replace (aaa account match) |

| Identifier | Headline |
|---|---|
| CSCwq29706 | Traceback and reload after editing SNMP config, with tmatch |
| CSCwq31137 | Firepower 9300 - DNM-2X100G Interfaces not passing traffic post upgrade to FXOS 2.17.0.518 |
| CSCwq31342 | FPR4200 \| FPR3100 Multi Instance Chassis Deployment Failed in DNS configuration |
| CSCwq32051 | Cisco Adaptive Security Appliance and Firepower Threat Defense Software Command Injection Vulnerability |
| CSCwq32085 | FP3100/4200 rebooting after generating crypto_archive with error on console "KC ILK issue detected" |
| CSCwq35960 | OSPF: Lina Traceback and Reload on Both Units in High Availability Setup. |
| CSCwq39942 | CVE-2025-32463: sudo: Sudo before 1.9.17p1 allows local users to obtain |
| CSCwq39943 | CVE-2025-32462: sudo: Before 1.9.17p1, allows users to execute commands on unintended machines. |
| CSCwq40256 | Inbound IPsec packets are dropped by IPsec offload when the crypto map ACL is using specific ports. |
| CSCwq43711 | Idle SSH sessions persist beyond the configured timeout without graceful termination by Fin flag |
| CSCwq46058 | ASA SNMP Response Issue - Responses Sent Only for Odd OIDs, Not for Even |
| CSCwq46143 | SSE-ASAc Recommit the fix got reverted during sync |
| CSCwq46544 | debug menu tls-offload option <> to be provided to resolve slow download speed using curl to download large file with SSL Decrypt Resign Policy |
| CSCwq47622 | Lina Traceback and Reload after enabling 'TLS Server Identity Discovery' |
| CSCwq48842 | FTD: Packets Dropped due to tcp-seq-past-win due to delayed packet through Snort |
| CSCwq50189 | ASAv deploy failed - console stuck at continuous |
| CSCwq50373 | ASA/FTD in HA, snmptranslate process during the boot-up causing High CPU and IPC timeouts, causing split-brain. |
| CSCwq50506 | Cisco Secure Firewall ASA Software and Secure FTD Software IKEv2 DoS Vulnerability |
| CSCwq51981 | FTD packer-tracer showing remark rule id in access-list for a rule not getting hit |
| CSCwq52188 | FTD Traceback while executing 'asp load-balance per-packet' |
| CSCwq52255 | SSH login to FTD management IP address lands in FXOS shell instead of FTD CLISH due to missing /mnt/boot/application/*.def file |
| CSCwq53328 | Multicast and unicast packets do not reach the correct instance for random subinterfaces |

| Identifier | Headline |
|---|---|
| CSCwq54109 | FTD 3130 HA Lina tracebacks at ikev2_bin2hex_str |
| CSCwq55887 | FMC 7.6 NAT Source and IP Not Populating within Unified Event Viewer |
| CSCwq56279 | 7.6 - Firepower 3100 series - Upgrading an HA pair from a version without the fix for CSCwo00444 to 7.6 causes one firewall to go into a traceback/reload loop |
| CSCwq60586 | FTD upgrade failed due to bundle image existence verification failure |
| CSCwq65955 | FPR 4200: HA link arp packets getting dropped, internal uplink linkChange counters incrementing |
| CSCwq70133 | Password Expiry Age does not reset after Password Change |
| CSCwq70773 | show asp rule-engine issues with complete and run time |
| CSCwq72156 | SNMP traps are not sent to one of multiple SNMP servers, in certain conditions |
| CSCwq73656 | Cisco Secure Firewall ASA Software and Secure FTD Software OSPF Memory Corruption Vulnerability |
| CSCwq73994 | ASA : Performance and high CPU usage seen on Hyper-V |
| CSCwq74204 | IKEv1 L2Lvpn fails in phase 2 with "Rejecting IPsec tunnel: no matching crypto map entry" after upgrade |
| CSCwq74738 | RAVPN SSL/IKEV2 AUTH FAILURE: AAA PROCESS MISHANDLING BROKEN FIBER CLASS |
| CSCwq74986 | FTD: Instance stuck in Boot Loop |
| CSCwq75116 | IPv6 function is stalled, link-local address marked [DUPLICATE] and IPv6 traffic stopped after failover due to split-brain |
| CSCwq76130 | Clustering : SNMP traffic drop due to cluster redirect offload |
| CSCwq78991 | Firewall joins a cluster although gets incomplete ACL policy rules during replication |
| CSCwq78991 | Firewall joins a cluster although gets incomplete ACL policy rules during replication |
| CSCwq79815 | Cisco Secure Firewall Adaptive Security Appliance Software and Secure Firewall Threat Defense Software VPN Web Server Unauthorized Access Vulnerability |
| CSCwq79815 | Cisco Secure Firewall Adaptive Security Appliance Software and Secure Firewall Threat Defense Software VPN Web Server Unauthorized Access Vulnerability |
| CSCwq79831 | Cisco Secure Firewall Adaptive Security Appliance Software and Secure Firewall Threat Defense Software VPN Web Server Remote Code Execution Vulnerability |
| CSCwq79831 | Cisco Secure Firewall Adaptive Security Appliance Software and Secure Firewall Threat Defense Software VPN Web Server Remote Code Execution Vulnerability |
| CSCwq81480 | FTD MI: SNMP polling fails to work after the upgrade |

| Identifier | Headline |
|---|---|
| CSCwq82095 | SAML response rejected with message for certain IDPs |
| CSCwq82095 | SAML response rejected with message for certain IDPs |
| CSCwq82225 | Drop counter doesn't increment for embryonic related drops in 'show service policy' |
| CSCwq85028 | Packet Captures show misleading information when blocked due to TCP server unavailable. |
| CSCwq85986 | FP4225: Interface with SFP - 10/25G_LR_S (or CSR_S) is not coming up after reboot of peer side. |
| CSCwq90072 | ASDM Parsing Failure on Two Contexts |
| CSCwq92373 | WA MI: Two apps went to Not Responding state with reason: Error in App Instance ftd. sma reported fault: Instance xxx is disabled due to restart loop. Please consider reinstalling this app-instance. |
| CSCwq92728 | ASA client IP missing from TACACS+ authorization request in SSH |
| CSCwq95241 | Reboots on FP2130 due to missing heimdall PID |
| CSCwq95810 | "no http server basic-auth-client ASDM" allows ASDM connections to ASA. |
| CSCwq96870 | Interfaces are coming up when the Firepower is shutting down |
| CSCwq98101 | Policy deployment fails when inline-set is configured on FTD HA |
| CSCwq98648 | Low RAM allocation on ASAv can trigger unexpected behavior in 'asdm image' command |
| CSCwr01482 | FPR4215 "Not supported" alarm occurred, when insert the SFPs |
| CSCwr04957 | Deployment failure or traffic not matching configured rules after renaming several objects |
| CSCwr05406 | Traceback in HA stby node while snmpwalk on natAddrMapTable |
| CSCwr05837 | SNMP process continuously restarts |
| CSCwr06290 | ASA/FTD: Traceback in thread name CP Processing due to DCERPC inspection |
| CSCwr10732 | Connection blocking active although "logging permit-hostdown' is set |
| CSCwr12965 | Both the units in HA changed the encryption algorithm simultaneously |
| CSCwr13046 | Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense Software VPN Web Services Cross-Site Scripting Vulnerability |
| CSCwr14186 | add context for cmd-invalid-encap asp-drop type in the "show asp drop" command usage |
| CSCwr15697 | Block 80 depletion ssl_decrypt_cb |

| Identifier | Headline |
|---|---|
| CSCwr19123 | FPR HA ESP sequence number discrepancy when standby changes to Active resulting in Anti-replay drops |
| CSCwr21375 | FTD port status not reflecting properly on FMC. |
| CSCwr21683 | Deployment changed performance profile, unable to retrieve running configuration |
| CSCwr22256 | Traceback seen while FQDN list expands more than 200 entries for a resolved ip |
| CSCwr22508 | Device doesn't boot and gets stuck after a successful upgrade |
| CSCwr24999 | FP3140 FTD HA Upgrade Getting Stuck |
| CSCwr26857 | File policy stops working due to SMB tcp conn terminated after 1hr for unknown reason despite not idle |
| CSCwr27095 | Anyconnect users incorrectly get the prompts, based on the previous tunnel-group |
| CSCwr28908 | ASA: Traceback and reload after saving asdm image |
| CSCwr29314 | Show crypto accelerator shows max crypto throughput is 6 Gbps For 3K & 225Mbps for FTDv |
| CSCwr31782 | Secure Client SAML - External Browser May Prompt for a Certificate when using IKEv2-IPsec and Certificate Mapping |
| CSCwr35582 | Continuous logs_archive.asa-interface-idb.log getting generated on ASA |
| CSCwr42577 | ASA/FTD may traceback and reload citing Thread Name 'lina' as the faulting thread. |
| CSCwr42969 | Dynamic Offloaded Flows Interrupted midstream |
| CSCwr43586 | Intermittent drop of self-originated ICMP TTL exceeded messages with reason "Unable to obtain connection lock (connection-lock)" |
| CSCwr48605 | Lina traceback due to the incorrect option being received in the packet. |
| CSCwr49028 | Secure client tunnel group authentication is affected when using SDI protocol |
| CSCwr49171 | Interlaken (ILK) link between the Nitrox and KC2 failure, causing traffic backpressure / traffic outage |
| CSCwr50466 | ASA/FTD: Wrong value shown for X509_STORE_CTX in 'show ssl objects' |
| CSCwr51629 | RTSP Flows are dropped with drop reason "First TCP packet not SYN" |
| CSCwr55089 | ASA/FTD - Traceback and Reload in Threadname DATAPATH |
| CSCwr57552 | Rate limit conn-limit SNMP traps |
| CSCwr59870 | ASAv on Hyper-v encountering boot loop issues when running netvsc driver |
| CSCwr61452 | ASA traceback and reload due to memory corruption in IPsec SA pointers |

| Identifier | Headline |
|---|---|
| CSCwr62800 | High network latency observed on ASAv |
| CSCwr79344 | ASA/FTD traceback and reload in Lina |
| CSCwr84343 | ASA/FTD Traceback and reload in L2 table creation failure |
| CSCwr85470 | FTD silently drops out of order packets |
| CSCws05886 | ASA may traceback during manual failover |

# Cisco General Terms

The Cisco General Terms (including other related terms) govern the use of Cisco software. You can request a physical copy from Cisco Systems, Inc., P.O. Box 641387, San Jose, CA 95164-1387. Non-Cisco software purchased from Cisco is subject to applicable vendor license terms. See also: https://cisco.com/go/generalterms.

# Related Documentation

For additional information on the ASA, see Navigating the Cisco Secure Firewall ASA Series Documentation.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2026 Cisco Systems, Inc. All rights reserved.