Before You Update: Important Notes

Before you update, familiarize yourself with the update process, the system's behavior during the update, compatibility issues, and required pre or post-update configuration changes.

Caution For Firepower 4100/9300 chassis with FTD, do *not* update to FXOS Version 2.3.1.56 if you updated Firepower Threat Defense from Version 6.0.1.x. This can disable FTD and interrupt traffic on your network. For more information, see CSCvh64138 in the Cisco Bug Search Tool.

Caution Do *not* manually reboot, shut down the system, or restart the update until you see the login prompt. The system may appear inactive during prechecks; this is expected. If you encounter issues with the update, contact Cisco TAC.

Note Do not enable common criteria (CC) or UCAPL mode on 8000 series devices running Version 6.2.2. If you do, the device may fail file system integrity checks (FSIC) and become unresponsive. If this happens, you must reimage. We recommend you upgrade to Version 6.2.2.1+ before you enable security certifications compliance.

For more information, see:

When to Update versus Reimage/Redeploy

In most cases, we recommend you upgrade. However, you must reimage physical devices or redeploy virtual appliances in the following cases:

- Switching device implementations—You want to switch your ASA 5500-X series device between ASA with FirePOWER Services and Firepower Threat Defense.
- Switching management methods—You want to switch management of Firepower Threat Defense between a Firepower Management Center and Firepower Device Manager, and the initially installed version on the device was Version 6.0.1.
- Switching virtual hosting environments—You want to recreate a virtual appliance in a new hosting environment. For example, if you are using Firepower Threat Defense Virtual for VMware but want to deploy in AWS, you must deploy a fresh virtual device.
- New platforms—You want to deploy Firepower Threat Defense Virtual for VMware managed by Firepower Device Manager. This environment is newly supported in Version 6.2.2.
- Other—You are unable or disinclined to follow the required update path as described in Update Paths to Version 6.2.2, on page 2.

For details on reimaging/redeploying, see Reimage or Redeploy Version 6.2.2. For details on switching device implementations, management methods, or virtual hosting environments, see Switching Implementation, Management Method, or Hosting.

Update Paths to Version 6.2.2

To update to Version 6.2.2, you must be running the following Firepower versions:

- Firepower Management Center—Version 6.2.0.x or Version 6.2.1
- Firepower 2100 series with Firepower Threat Defense—Version 6.2.1
- All other devices—Version 6.2.0.x

Note Version 6.2.1 is no longer available. We strongly recommend updating Firepower Management Centers or Firepower 2100 Series devices running Version 6.2.1 to Version 6.2.2, and then to a subsequent patch of Version 6.2.2.x to take advantage of resolved defects and vulnerabilities.

If you update from one major update to another, updating may cause or require significant configuration changes that you must address such as more memory or policy configuration. For example, the Version 6.2.0 update eliminates nested correlation rules, and you may need to take action related to this change.

Another example, updating a Firepower Management Center to Version 6.0 may cause traffic outages and system issues if you are are managing devices running X, Y, or earlier. Before you begin the update to Version 6.0, edit the access control policies deployed to those devices, disable the **Retry URL cache miss lookup** option on the Advanced Options section of the Access Control window, then redeploy. To review the release notes for each destination version on your update path, see the Release Notes page.

Firepower Management Center Update Paths

The following table describes update paths for Firepower Management Centers, including Firepower Management Center Virtual:

Firepower Management Center Platform	Update Path
MC750, MC1000, MC1500, MC2000, MC2500, MC3500, MC4000, MC4500 Firepower Management Center Virtual: VMware	Version 5.4.1.1+ > Version 6.0.0 Pre-Installation Package > Version 6.0.0 > Version 6.0.1 Preinstall > Version 6.0.1 > Version 6.1.0 Pre-Installation Package > Version 6.1.0 > Version 6.2.0 > Version 6.2.2 **Note** For Firepower Management Centers running Version 6.2.1, use the following update path: Version 6.2.1 > Version 6.2.2
Firepower Management Center Virtual: AWS	Version 6.0.1 > Version 6.1.0 Pre-Installation Package > Version 6.1.0 > Version 6.2.0 > Version 6.2.2 **Note** For Firepower Management Center Virtual:AWS running running Version 6.2.1, use the following update path: Version 6.2.1 > Version 6.2.2
Firepower Management Center Virtual: KVM	Version 6.1.0 > Version 6.2.0 > Version 6.2.2 **Note** For Firepower Management Center Virtual: KVM running Version 6.2.1, use the following update path: Version 6.2.1 > Version 6.2.2

Firepower Threat Defense Update Paths—With Firepower Management Center

This table describes update paths for Firepower Threat Defense devices managed by a Firepower Management Center.

Firepower Threat Defense Platform	Update Path
ASA 5506-X, ASAS 5506H-X, ASA 5506W-X, ASA 5508-X, 16-X ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X Firepower Threat Defense Virtual: VMware Firepower Threat Defense Virtual: AWS Firepower 4110, 4120, 4140 Firepower 9300 with SM-24, SM-36, or SM-44 modules	Version 6.0.1 > Version 6.1.0 Pre-Installation Package > Version 6.1.0 > Version 6.2.0 > Version 6.2.2
Firepower Threat Defense Virtual: KVM Firepower 4150	Version 6.1.0 > Version 6.2.0 > Version 6.2.2

Firepower Threat Defense Platform	Update Path
Firepower Threat Defense Virtual: Azure	Version 6.2.0 > Version 6.2.2
Firepower 2110, 2120, 2130, 2140	Version 6.2.2 **Note** For Firepower 2100 Series devices running Version 6.2.1, use the following update path: Version 6.2.1 > Version 6.2.2

Firepower Threat Defense Update Paths—With Firepower Device Manager

This table describes update paths for Firepower Threat Defense devices managed by Firepower Device Manager.

Firepower Threat Defense Platform	Update Path
ASA5506-X, ASA5506H-X, ASA5506W-X, ASA5508-X, ASA5516-X ASA5512-X, ASA5515-X, ASA5525-X, ASA5545-X, ASA5555-X	Version 6.1.0 > Version 6.2.0 > Version 6.2.2
Firepower 2110, 2120, 2130, 2140	Version 6.2.2 **Note** For Firepower 2100 Series devices running Version 6.2.1, use the following update path: Version 6.2.1 > Version 6.2.2
Firepower Threat Defense Virtual: VMware	Version 6.2.2

NGIPS Update Paths—With Firepower Management Center

This table describes update paths for NGIPS devices (including ASA FirePOWER modules) managed by a Firepower Management Center.

NGIPS Platform	Update Path
Firepower 7010, 7020, 7030, 7050, 7110, 7115, 7120, 7125 Firepower 8120, 8130, 8140, 8250, 8260, 8270, 8290, 8350, 8360, 8370, 8390 AMP7150, AMP8050, AMP8150, AMP8350, AMP8360, AMP8370, AMP8390 ASA FirePOWER: ASA5512-X, ASA5515-X, ASA5525-X, ASA5545-X, ASA5555-X ASA FirePOWER: ASA5585-X-SSP-10, ASA5585-X-SSP-20, ASA5585-X-SSP-40, ASA5585-X-SSP-60 NGIPSv: VMware	Version 5.4.0.2 > Version 6.0.0 Pre-Installation Package > Version 6.0.0 > Version 6.0.1 Preinstall > Version 6.0.1 > Version 6.1.0 Pre-Installation Package > Version 6.1.0 > Version 6.2.0 > Version 6.2.2

NGIPS Platform	Update Path
ASA FirePOWER: ASA5506-X, ASA5506H-X, ASA5506W-X, ASA5508-X, ASA5516-X	Version 5.4.1.1 > Version 6.0.0 Pre-Installation Package > Version 6.0.0 > Version 6.0.1 Preinstall > Version 6.0.1 > Version 6.1.0 Pre-Installation Package > Version 6.1.0 > Version 6.2.0 > Version 6.2.2

NGIPS Update Paths—ASA FirePOWER with ASDM

This table describes update paths for ASA FirePOWER modules managed by ASDM.

ASA FirePOWER NGIPS Platform	Update Path
ASA5506-X, ASA5506H-X, ASA5506W-X, ASA5508-X, ASA5516-X	Version 5.4.1.1 > Version 6.0.0 Pre-Installation Package > Version 6.0.0 > Version 6.0.1 Preinstall > Version 6.0.1 > Version 6.1.0 Pre-Installation Package > Version 6.1.0 > Version 6.2.0 > Version 6.2.2
ASA5512-X, ASA5515-X, ASA5525-X, ASA5545-X, ASA5555-X ASA5585-X-SSP-10, ASA5585-X-SSP-20, ASA5585-X-SSP-40, ASA5585-X-SSP-60	Version 6.0.0 > Version 6.0.1 Preinstall > Version 6.0.1 > Version 6.1.0 Pre-Installation Package > Version 6.1.0 > Version 6.2.0 > Version 6.2.2

Update Sequence Guidelines

The following sections describe update sequences for deployments that include appliances that you linked for performance or redundancy:

- Update Sequence for Firepower Management Centers in High Availability, on page 5
- Update Sequence for High Availability Firepower Threat Defense Devices, on page 6
- Update Sequence for Clustered Firepower Threat Defense Devices, on page 7
- Update Sequence for 7000 and 8000 Series Devices in High Availability, on page 7
- Update Sequence for High Availability 7000 and 8000 Series Devices in Inline Deployment, on page 7
- Update Sequence for Stacked 8000 Series Devices, on page 8

Update Sequence for Firepower Management Centers in High Availability

This procedure explains how to upgrade the Firepower software on Firepower Management Centers in a high availability pair.

Do not simultaneously update Firepower Management Centers in a high availaiblity pair. You upgrade peers one at a time. With synchronization paused, first upgrade the standby (or secondary), then the active (or primary). When the standby Firepower Management Center starts prechecks, its status switches from standby to active, so that both peers are active. This temporary state is called *split-brain* and is *not* supported except

during upgrade. Do *not* make or deploy configuration changes while the pair is split-brain; your changes will be lost after you upgrade the Firepower Management Centers and restart synchronization.

Step 1 Pause the synchronization of the active Firepower Management Center of the high availability pair with the High Availability tab of the Integration page (**System > Integration**) as described in the Pausing Communication Between Paired Firepower Management Centers topic of the *Firepower Management Center Configuration Guide*.

Step 2 Update the standby Firepower Management Center in the high availability pair. See the Update Firepower Management Centers for more information.

The Firepower Management Center switches from standby to active so both Firepower Management Centers in the high availability pair are active.

Step 3 Update the other Firepower Management Center within the pair.

Step 4 Click **Make-Me-Active** on the High Availability tab of one of the Firepower Management Center web interfaces.

The Firepower Management Center you do not make active automatically switches to standby mode. Communication between the Firepower Management Center pairs automatically restarts.

Update Sequence for High Availability Firepower Threat Defense Devices

Before you update Firepower Threat Defense, update the operating system on high availability Firepower 4100 series and Firepower 9300 devices to the most recent compatible FXOS version. For more information on FXOS versions, see the Firepower System Compatibility Guide.

Make sure you update FXOS to the most recent compatible FXOS version for the *current* Firepower version, that is, the version you are updating *from*. You may have to update FXOS again after you update Firepower to Version 6.2.2.

⚠

Caution You must always update the FXOS version on the *standby* device of a Firepower Threat Defense high availability pair. Do not update the FXOS version of the active device.

Step 1 Update the FXOS version on the standby Firepower Threat Defense device within the high availability pair. See the Cisco FXOS Release Notes for more information.

Step 2 Click the **Switch Active Peer** icon next the high availability pair on the **Devices** > **Device Management** page to switch failover, so the standby Firepower Threat Defense device is now the active device. The Firepower Threat Defense device that was active is now in standby.

Step 3 Update the FXOS version on the new standby Firepower Threat Defense device.

Step 4 Update the Firepower Threat Defense high availability pair to the most recent Firepower version. See Update Firepower Threat Defense Devices Using the Firepower Management Center for more information.

When you install a Firepower update on Firepower Threat Defense devices in a high availability pair, the devices update one at a time. When the update starts, Firepower first applies it to the standby device, which goes into maintenance mode until any necessary processes restart and the device is processing traffic again. Firepower then updates the active device, which follows the same process.

Update Sequence for Clustered Firepower Threat Defense Devices

When you update Firepower 4100 or Firepower 9300 clusters running Firepower Threat Defense, the system updates the security modules one at a time—first the secondary security modules, then the primary security module. Modules operate in maintenance mode while they are updated.

During the primary security module update, although traffic inspection and handling continues normally, the system stops logging events. Event logging resumes after the full update is completed.

Caution Updating FXOS reboots the device, which can affect traffic in a clustered environment until at least one module comes online. In an intra-chassis cluster, traffic drops if the cluster does not use an optional hardware bypass (fail-to-wire) module or if bypass is disabled. Traffic passes without inspection if bypass is enabled. In an inter-chassis cluster, traffic drops during the reboot if chassis reboots overlap before at least one module comes online; traffic is unaffected if there is no reboot overlap.

For more information, see the Firepower Threat Defense Cluster for the FXOS Chassis chapter of the *Firepower Management Center Configuration Guide* and the About Clustering on the FXOS Chassis chapter of the *Cisco FXOS Firepower Chassis Manager Configuration Guide*.

Events for traffic processed during the logging downtime appear with out-of-sync timestamps after the update is completed. However, if the logging downtime was significant, the system may prune the oldest events before they can be logged.

Update Sequence for 7000 and 8000 Series Devices in High Availability

Note Use the Firepower Management Center to update 7000 or 8000 Series devices in a high availability pair. You cannot update using the devices' web interface.

When you install an update on 7000 and 8000 Series devices in a high availability pair, the system updates the devices one at a time. When the update starts, the system first applies it to the standby device, which goes into maintenance mode until any necessary processes restart and the device is processing traffic again. The system then updates the active device, which follows the same process.

Update Sequence for High Availability 7000 and 8000 Series Devices in Inline Deployment

When you install an update on 7000 Series or 8000 Series devices in high availability configured for inline deployment, the system performs the update on the devices one at a time. The system first applies it to the primary device, which goes into maintenance mode until any necessary processes restart and the device is processing traffic again. While the primary device updates in maintenance mode, the secondary device temporarily becomes primary and does not drop traffic. When the primary device update completes, the primary device moves from maintenance mode to primary mode and the system updates the secondary device.

Update Sequence for Stacked 8000 Series Devices

When you install an update on 8000 Series stacked devices, Firepower updates the stacked devices simultaneously. Each device resumes normal operation when the update is completed. Note the following scenarios:

- If the primary device completes the update before all of the secondary devices, the stack operates in a limited, mixed-version state until all devices have completed the update.
- If the primary device completes the update after all of the secondary devices, the stack resumes normal operation when the update is completed on the active device.

Pre-Update Readiness Checks

Caution Do *not* reboot or shut down an appliance during the readiness check. If your appliance fails the readiness check, correct the issues and run the readiness check again. If the readiness check exposes issues that you cannot resolve, do not begin the upgrade. Instead, contact Cisco TAC.

- Checks Firepower software readiness only—The readiness check does not assess preparedness for intrusion rule, VDB, or GeoDB updates.
- Version 6.1+ required—The readiness check was introduced in Version 6.1. A readiness check on the upgrade *to* Version 6.1 may not return accurate results.
- Web interface vs shell—You can use the Firepower Management Center web interface to perform the readiness check on itself and its standalone managed devices only. For clustered devices, stacked devices, and devices in high availability pairs, run the readiness check from each device's shell.
- Time requirements—The time required to run the readiness check varies depending on your appliance model and database size. You may find it expedient to forgo readiness checks if your deployment is large (for example, if your Firepower Management Center manages more than 100 devices).

Run a Readiness Check through the Shell

For clustered devices, stacked devices, and devices in high availability pairs, you *must* use the shell.

Before you begin

- Download the upgrade package for the appliance whose readiness you want to check. Readiness checks are included in upgrade packages.
- Deploy configurations to managed devices whose configurations are out of date. Otherwise, the readiness check may fail.

Step 1 Log into the shell as a user with administrator privileges.

Step 2 Make sure the upgrade package is on the appliance in the correct place:

- Firepower Threat Defense devices: `/ngfw/var/sf/updates`
- All other Firepower appliances: `/var/sf/updates`

On Firepower Management Centers, you can use the web interface to upload the upgrade package.

If you cannot or do not want to use the Firepower Management Center web interface, use SCP to copy the upgrade package to the appliance. Initiate from the Firepower side.

Step 3 Run this command as the root user:

```
sudo install_update.pl --detach --readiness-check full_path_to_update_package
```

Unless you are running the readiness check from the console, use the `--detach` option to ensure the check does not stop if your user session times out. Otherwise, the readiness check runs as a child process of the user shell. If your connection is terminated, the process is killed, the check is disrupted, and the appliance may be left in an unstable state.

Step 4 (Optional) Monitor the readiness check.

If you use the `--detach` option (or begin another shell session), you can use the `tail` or `tailf` command to display logs, for example:

- Firepower Threat Defense devices: `tail /ngfw/var/log/sf/update_package_name/status.log`
- All other Firepower appliances: `tail /var/log/sf/update_package_name/status.log`

If you use `tailf` to display log entries as they occur, you must cancel (Ctrl+C) to return to the command prompt.

Step 5 When the readiness check completes, access the full readiness check report.

- Firepower Threat Defense devices: `/ngfw/var/log/sf/$rpm_name/upgrade_readiness`
- All other Firepower appliances: `/var/log/sf/$rpm_name/upgrade_readiness`

Run a Readiness Check through the Firepower Management Center Web Interface

You can use the Firepower Management Center web interface to perform readiness checks on itself and its standalone managed devices.

Before you begin

- Readiness checks are included in upgrade packages. Note that upgrade packages from Version 6.2.1+ are *signed*, and terminate in .sh.REL.tar instead of just .sh. Do *not* untar signed upgrade packages before performing either a readiness check or the upgrade itself.
- Redeploy configuration changes to any managed devices. Otherwise, the readiness check may fail.

Step 1 On the Firepower Management Center web interface, choose **System** > **Updates**.

Step 2 Click the Install icon next to the upgrade you want the readiness check to evaluate.

Step 3 Click **Launch Readiness Check**.

Step 4 Monitor the progress of the readiness check in the Message Center.
When the readiness check completes, the system reports success or failure on the Readiness Check Status page.

Step 5 Access the full readiness check report in `/var/log/sf/$rpm_name/upgrade_readiness`.

Pre-Update Configuration and Event Backups

Before you begin the update, we *strongly* recommend that you back up current event and configuration data to an external location. You should also copy any locally stored backups to an external location, because the Firepower Management Center purges locally stored backups from previous updates.

Use the Firepower Management Center to back up event and configuration data for itself and the devices it manages. For more information on the backup and restore feature, see the Firepower Management Center Configuration Guide.

Note Verify that external backups are successful before you begin the update.

Patch or Hotfix for New Dynamic Analysis CA Certificate

Deployments: AMP for Networks (malware detection) deployments where you submit files for dynamic analysis

Upgrading from: A patched/hotfixed system with new CA certificates

Directly to: Version 6.2 through 6.2.3

On June 15, 2018, some Firepower deployments stopped being able to submit files for dynamic analysis. This occurred due to an expired CA certificate that was required for communications with the AMP Threat Grid cloud. In Version 6.1+ deployments, you can obtain a new certificate with a patch or hotfix. For earlier versions, you must upgrade to at least Version 6.1, then patch or hotfix.

If you already patched or hotfixed your deployment, upgrading to a later major version (Version 6.2 through 6.2.3) reverts to the old certificate and disables dynamic analysis. You must patch or hotfix again.

Note If this is your first time installing the patch or hotfix, make sure your firewall allows outbound connections to `fmc.api.threatgrid.com` (replacing `panacea.threatgrid.com`) from both the FMC and its managed devices. Managed devices submit files to the cloud for dynamic analysis; the FMC queries for results.

The following table lists the patches and hotfixes that contain the new certificates, for each major version sequence and platform. Patches and hotfixes are available on the Cisco Support & Download site. For release notes, see Firepower Release Notes.

Table 1: Patches and Hotfixes with New CA Certificates

Versions with Old Cert	First Patch with New Cert	Hotfix with New Cert	
6.2.3 through 6.2.3.3	6.2.3.4	Hotfix G	FTD devices
		Hotfix H	FMC, NGIPS devices
6.2.2 through 6.2.2.3	6.2.2.4	Hotfix BN	All platforms
6.2.1	None. You must upgrade.	None. You must upgrade.	
6.2.0 through 6.2.0.5	6.2.0.6	Hotfix BX	FTD devices
		Hotfix BW	FMC, NGIPS devices
6.1.0 through 6.1.0.6	6.1.0.7	Hotfix EM	All platforms
6.0.x	None. You must upgrade.	None. You must upgrade.	

Traffic Flow and Inspection During the Update

When you update your sensing devices, traffic either drops throughout the update or traverses the network without inspection depending on how your devices are configured and deployed: routed or transparent, inline versus passive, bypass mode settings, and so on. We *strongly* recommend performing the update in a maintenance window or at a time when the interruption will have the least impact on your deployment.

Note When you update devices in a high availability pair, the system performs the update one device at a time to avoid traffic interruption.

This section discusses traffic behavior during the followng update stages:

- The update itself, including related reboots
- FXOS updates on clustered Firepower Threat Defense devices
- Configuration deployments after the update

Traffic Behavior During the Update

The following table describes how updates, including related device reboots, affect traffic flow for different deployments. Note that switching, routing, NAT, and VPN are not performed during the update process, regardless of how you configure any inline sets.

Caution Do *not* update to FXOS Version 2.3.1.56 if you are running an instance of Firepower Threat Defense that has been updated from Version 6.0.1.x of the Firepower System. Doing so may disable your Firepower Threat Defense application, which could interrupt traffic on your network. As a workaround, use FXOS Version 2.3.1.58 or later. For more information, see CSCvh64138 in the Cisco Bug Search Tool.

Table 2: Update Traffic Behavior

Device	Deployment	Traffic Behavior
Firepower Threat Defense	inline with optional hardware bypass module; bypass enabled: (**Bypass: Standby** or **Bypass-Force**) or, bypass disabled: (**Bypass: Disabled**)	dropped
Firepower Threat Defense Firepower Threat Defense Virtual	inline with no hardware bypass module; routed, transparent (including EtherChannel, redundant, subinterface)	
	inline in tap mode	egress packet immediately, copy not inspected
	passive	uninterrupted, not inspected

Device	Deployment	Traffic Behavior
7000 and 8000 Series	inline with optional hardware bypass module, bypass enabled (**Bypass Mode: Bypass**)	passed without inspection Note that traffic is interrupted briefly at two points: • At the beginning of the update process as link goes down and up (flaps) and the network card switches into hardware bypass. • After the update finishes as link flaps and the network card switches out of bypass. Inspection resumes after the endpoints reconnect and reestablish link with the device interfaces. The hardware bypass option is *not* supported on nonbypass network modules on Firepower 8000 Series devices, or SFP transceivers on Firepower 7000 Series.
	inline with optional hardware bypass module, bypass disabled (**Bypass Mode: Non-Bypass**)	dropped
7000 and 8000 Series NGIPSv	inline with no hardware bypass module	dropped
	inline in tap mode	egress packet immediately, copy not inspected
	passive	uninterrupted, not inspected
	routed, switched	dropped
ASA FirePOWER	routed or transparent, fail-open (**Permit Traffic**)	passed without inspection (requires the latest supported ASA OS version; otherwise, traffic dropped)
	routed or transparent, fail-close (**Close Traffic**)	dropped

Caution Rebooting the ASA FirePOWER module on an ASA 5585-X, including a reboot that occurs during a module upgrade, causes traffic to drop for up to thirty seconds on the interfaces on the ASA FirePOWER hardware module while the module reboots.

Traffic Behavior When Updating FXOS on Clustered Firepower Threat Defense Devices

Updating FXOS reboots the chassis, which can affect traffic in a clustered environment until at least one module comes online. Whether and how traffic is affected depends on the cluster type:

- **Intra-chassis cluster**—Traffic drops if the cluster does not use an optional hardware bypass (fail-to-wire) module or if bypass is disabled. Traffic passes without inspection if bypass is enabled.
- **Inter-chassis cluster**—Traffic drops during the overlap if multiple chassis reboots overlap before at least one module comes online. Traffic is unaffected if there is no reboot overlap.

  For example, there would be no reboot overlap, and no dropped traffic, if you complete the FXOS update first on one chassis and then on another. Depending on when each update is initiated, there could be reboot overlap (and dropped traffic) if you update multiple chassis simultaneously.

The following table summarizes this behavior.

Table 3: Traffic Behavior During an FXOS Update of Clustered Firepower Threat Defense Devices

Device Model	Deployment	Traffic Behavior
Firepower 9300	intra-chassis cluster without optional hardware bypass module	dropped
	intra-chassis cluster with optional hardware bypass module, bypass disabled	dropped
	intra-chassis cluster with optional hardware bypass module, bypass enabled	passed without inspection
Firepower 9300 Firepower 4100 Series	inter-chassis cluster with no reboot overlap	unaffected
	inter-chassis cluster with reboot overlap before at least one module comes online	dropped

Traffic Behavior During Configuration Deployment

During the upgrade process, you deploy configurations either twice (standalone devices) or three times (devices managed by the Firepower Management Center). When you deploy, resource demands may result in a small number of packets dropping without inspection. In most cases, the deployment immediately after the upgrade restarts the Snort process. During subsequent deployments, the Snort process restarts only if, before deploying, you modify specific policy or device configurations that always restart the process when deployed.

The following table describes how different devices handle traffic during Snort process restarts.

Table 4: Restart Traffic Effects by Managed Device Model

Device Model	Interface Configuration	Restart Traffic Behavior
Firepower Threat Defense, Firepower Threat Defense Virtual	inline, **Snort Fail Open: Down**: enabled	passed without inspection
	inline, **Snort Fail Open: Down**: disabled	dropped
	routed, transparent (including EtherChannel, redundant, subinterface)	dropped
	inline, tap mode	egress packet immediately, copy bypasses Snort
	passive	uninterrupted, not inspected
7000 and 8000 Series, NGIPSv	inline, **Failsafe** enabled or disabled	passed without inspection A few packets might drop if **Failsafe** is disabled and Snort is busy but not down.
	inline, tap mode	egress packet immediately, copy bypasses Snort
	passive	uninterrupted, not inspected
7000 and 8000 Series	routed, switched, transparent	dropped
ASA FirePOWER	routed or transparent with fail-open (**Permit Traffic**)	passed without inspection
	routed or transparent with fail-close (**Close Traffic**)	dropped

Time and Disk Space Requirements For Version 6.2.2

To upgrade a Firepower appliance, you must have enough free disk space or the upgrade fails. When you use the Firepower Management Center to upgrade a managed device, the Firepower Management Center requires additional disk space in its /Volume partition.

You must also have enough time to perform the upgrade. We provide estimates of upgrade times for each release. Note that depending on your deployment, upgrades may take longer than the provided estimates. For example, lower-memory appliances and appliances under heavy load may take longer to upgrade. These estimates also do not include the time required to complete a readiness check.

Platform	Space on /	Space on /Volume	Space on Manager	Time
FMC	From 6.2.0: 22 MB From 6.2.1: 21 MB	From 6.2.0: 6467 MB From 6.2.1: 6916 MB	—	From 6.2.0: 52 min From 6.2.1: 61 min

Platform	Space on /	Space on /Volume	Space on Manager	Time
FMCv	From 6.2.0: 24 MB From 6.2.1: 24 MB	From 6.2.0: 6987 MB From 6.2.1: 5975 MB	—	Hardware dependent
Firepower 2100 series	5613 MB	5613 MB	925 MB	57 min
Firepower 9300 chassis	4635 MB	4635 MB	743 MB	14 min
FTDv	.92 MB	3586 MB	987 MB	Hardware dependent
ASA 5500-X series with FTD	.16 MB	3683 MB	987 MB	80 min
Firepower 7000/8000 series	18 MB	6745 MB	1300 MB	27 min
ASA FirePOWER	16 MB	7021 MB	1200 MB	131 min
NGIPSv	18 MB	7261 MB	1300 MB	Hardware dependent