Understand the Steps and Impact of FTD High Availability Upgrade Procedure

Contents

Issue

A firewall administrator needs to understand the recommended upgrade procedure for Firewall Threat Defense (FTD) devices configured in a High Availability (HA) pair and managed by Cisco Firewall Management Center (FMC). The specific questions include what is the recommended process for software upgrades on these units, whether the upgrades can be performed "on the fly" without downtime, and what impact to expect during the upgrade process.

Environment

- FTD running version 7.4. Other software versions can be also affected.
- FTD configured in High Availability (HA) pair mode.
- FMC 7.4 managing the FTD HA. Other software versions can be also affected.

Resolution

The upgrade procedure for FTD in HA configuration uses a specific sequence to minimize downtime and maintain system integrity.

Recommended Upgrade Order

Step 1. Upgrade the FMC first

Cisco guidance requires that the FMC must run the same or newer version than the devices it manages. You cannot upgrade an FTD device past the FMC to a newer maintenance or major version.

Step 2. Upgrade the FTD HA pair from FMC

When upgrading an FTD HA pair managed by FMC, the FMC upgrades one peer at a time (Standby first, then Active) and a failover occurs as part of the process.

Downtime and Traffic Impact Expectations

- You must plan a maintenance window. Cisco notes upgrades can include interruptions to traffic flow and inspection, and devices can stop passing traffic during upgrade or if an upgrade fails.
- With an HA pair, the goal is to minimize impact, but you need to expect at least one failover event and possible brief interruption (for example, routing adjacency or VPN renegotiation depending on your environment).
- Avoid policy and configuration changes during the upgrade (no deployments or changes until both HA members are fully upgraded and stable).

Pre-Upgrade Health Checks for FTD HA

Before starting the upgrade, confirm FTD HA is stable and both units agree on Active and Standby Ready states:

<#root>

device#

show failover state

```
               State          Last Failure Reason      Date/Time
This host  -   Primary
```

Active

```
None
Other host -   Secondary
```

Standby Ready

```
  Comm Failure             16:10:34 UTC Apr 13 2026

====Configuration State===
```

```
        Sync Skipped
====Communication State===
        Mac set
```

Cause

This is a procedural inquiry regarding best practices for upgrading FMC and FTD systems in HA configuration. The question addresses the need to understand proper upgrade sequencing, downtime expectations, and impact mitigation strategies for critical firewall infrastructure.

Related Content

- Secure Firewall Management Center Upgrade Planning
- Upgrade FTD HA Managed by FMC
- Management Center Compatibility Guide
- Threat Defense Compatibility Guide
- Cisco Technical Support & Downloads