升级由FDM管理的FTD HA

目录

简介

先决条件

- 要求
- 使用的组件
- 概述

背景信息

配置

- 步骤1.上传升级软件包
- 步骤2.检查就绪性
- 步骤3.在HA中升级FTD
- 步骤4.交换活动对等体（可选）
- 步骤5.最终部署

验证

简介

本文档介绍由Firepower设备管理器管理的高可用性思科安全防火墙威胁防御的升级过程。

先决条件

要求

Cisco 建议您了解以下主题：

- 高可用性(HA)概念和配置
- 思科安全Firepower设备管理器(FDM)配置
- 思科安全防火墙威胁防御(FTD)配置

使用的组件

本文档中的信息基于虚拟思科FTD，版本7.2.8。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

概述

FDM的工作方式是一次升级一个对等体。首先选择Standby（备用），然后选择Active（活动），在活动升级开始之前执行故障切换。

背景信息

升级之前必须从software.cisco.com下载升级软件包。

在CLI清理中，在Active FTD中运行show high-availability configcommand以检查HA的状态。

```
> show high-availability config
Failover On
Failover unit Primary
Failover LAN Interface: failover-link GigabitEthernet0/2 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 3 of 311 maximum
MAC Address Move Notification Interval not set
failover replication http
Version: Ours 9.18(3)53, Mate 9.18(3)53
Serial Number: Ours 9A1QUNFWPK1, Mate 9A45VNEHB5C
Last Failover at: 11:57:26 UTC Oct 8 2024
        This host: Primary - Active
                Active time: 507441 (sec)
                slot 0: ASAv hw/sw rev (/9.18(3)53) status (Up Sys)
                  Interface diagnostic (0.0.0.0): Normal (Waiting)
                  Interface inside (192.168.45.1): Normal (Waiting)
                  Interface outside (192.168.1.10): Normal (Waiting)
                slot 1: snort rev (1.0)  status (up)
                slot 2: diskstatus rev (1.0)  status (up)
        Other host: Secondary - Standby Ready
                Active time: 8 (sec)
                  Interface diagnostic (0.0.0.0): Normal (Waiting)
                  Interface inside (0.0.0.0): Normal (Waiting)
```

```
    Interface outside (0.0.0.0): Normal (Waiting)

  slot 1: snort rev (1.0)  status (up)

  slot 2: diskstatus rev (1.0)  status (up)
```

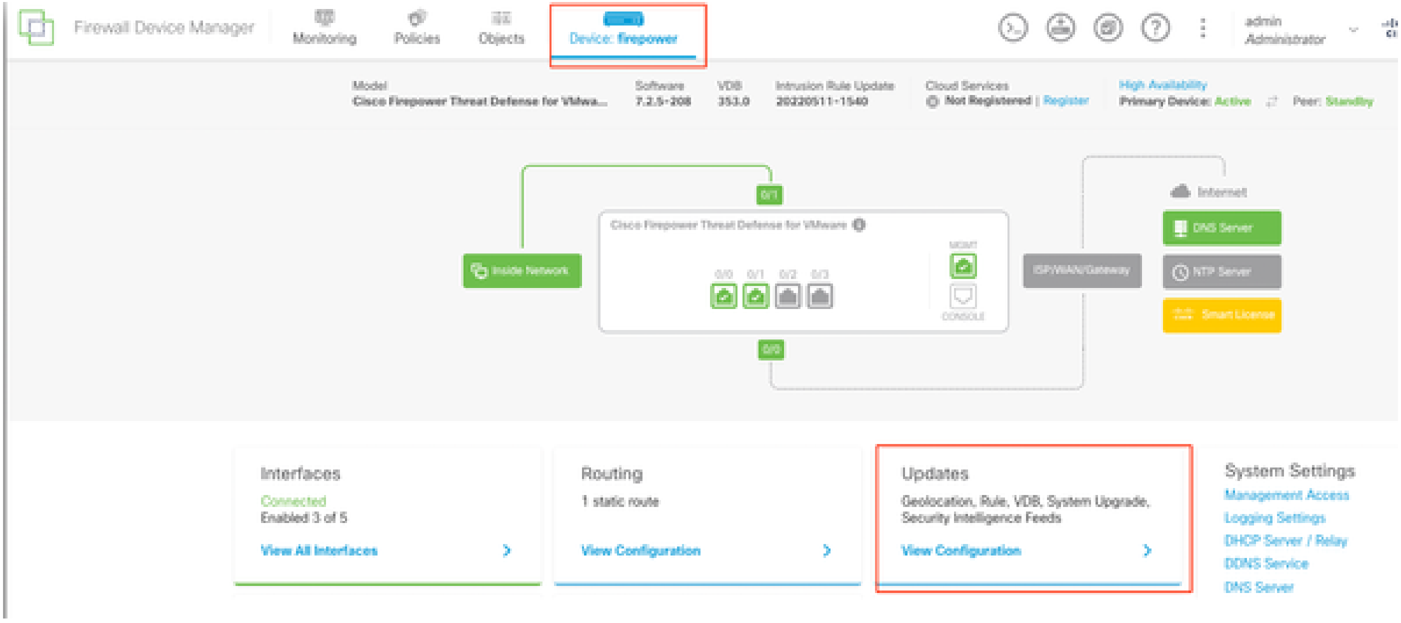
如果未显示错误，则继续升级。

配置

步骤1.上传升级软件包

- 使用GUI将FTD升级包上传到FDM上。

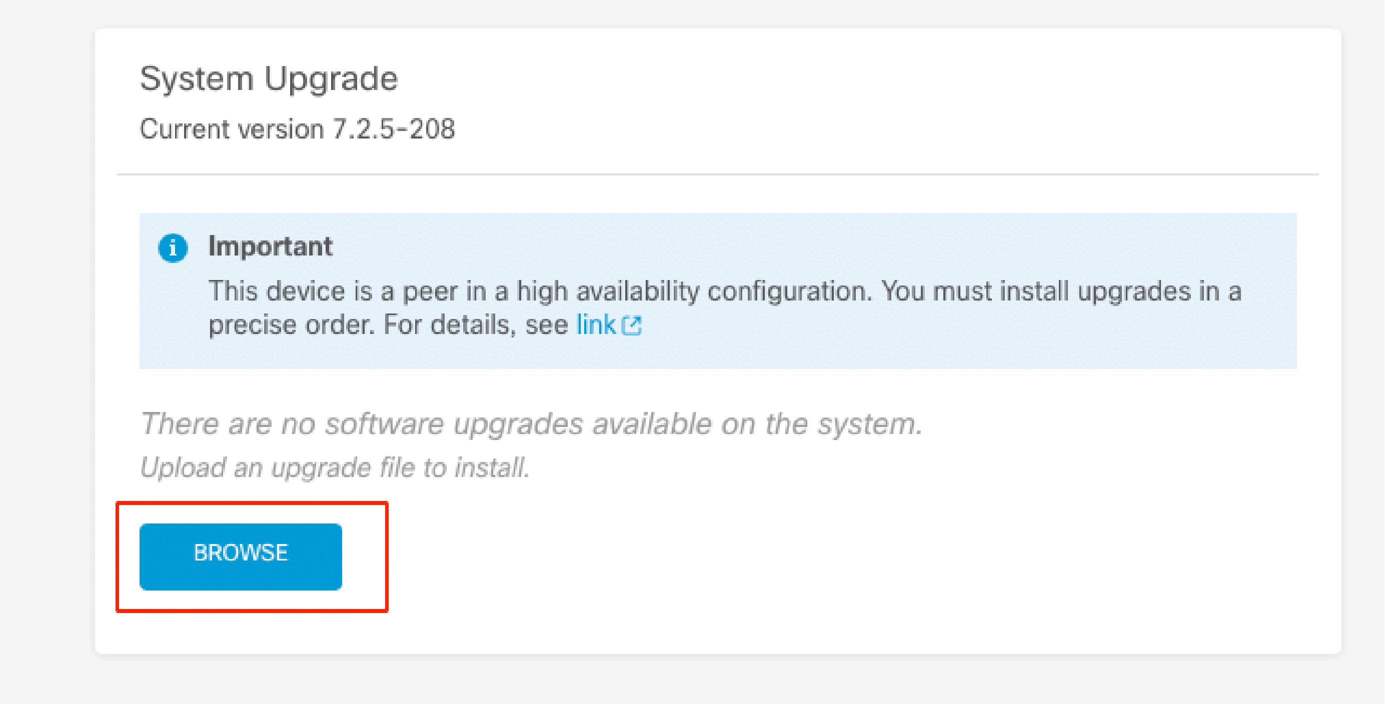
之前必须根据FTD型号和所需版本从思科软件站点下载该软件。导航到Device > Updates > System Upgrade。



更新

- 浏览之前下载的映像，然后选择Upload。

注意：在活动节点和备用节点上传映像。



System Upgrade

Current version 7.2.5-208

Important

This device is a peer in a high availability configuration. You must install upgrades in a precise order. For details, see link

There are no software upgrades available on the system.

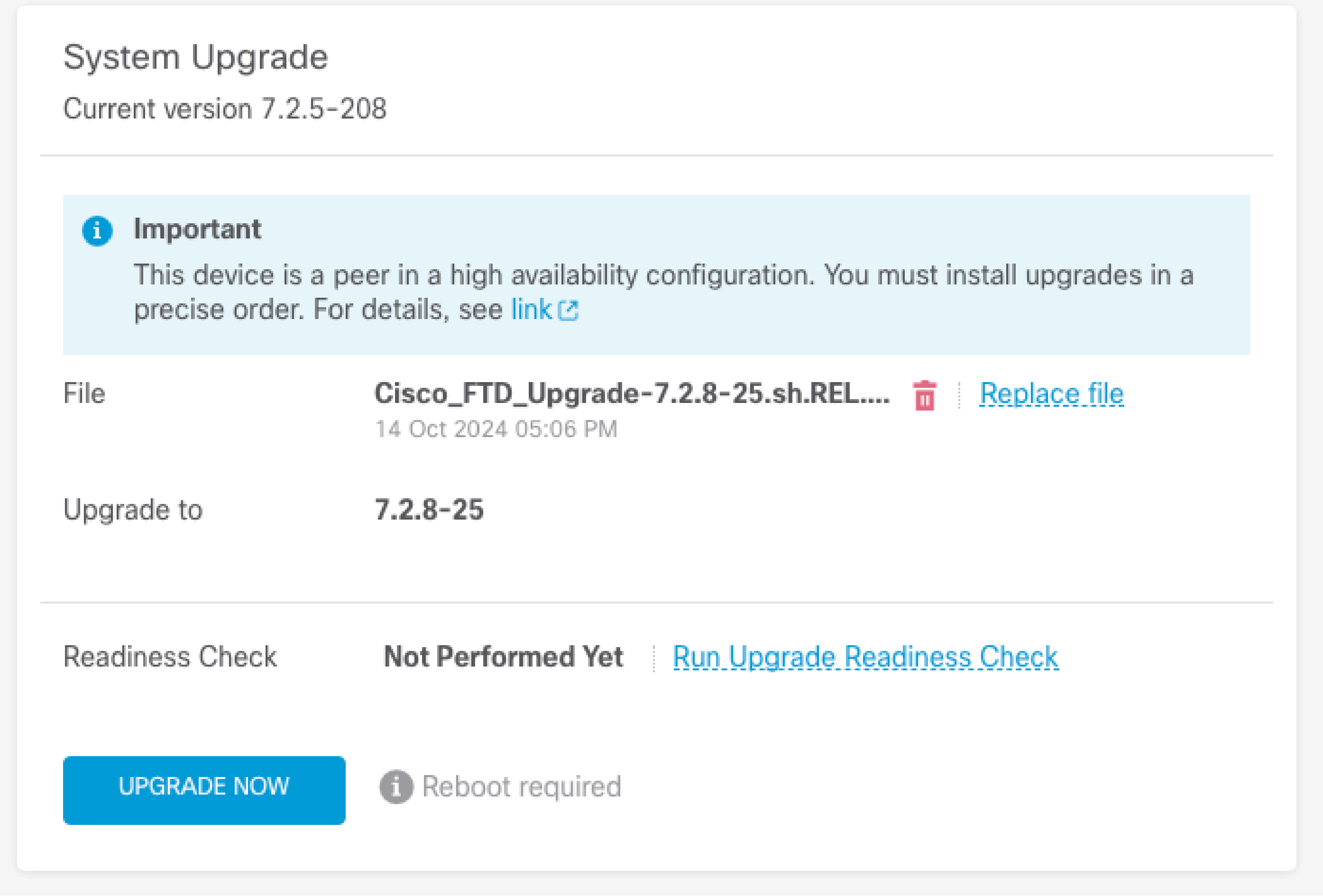
Upload an upgrade file to install.

运行就绪性检查

步骤2.检查就绪性

就绪性检查确认设备是否准备好继续升级。

- 选择Run Upgrade Readiness Check。



System Upgrade

Current version 7.2.5-208

Important

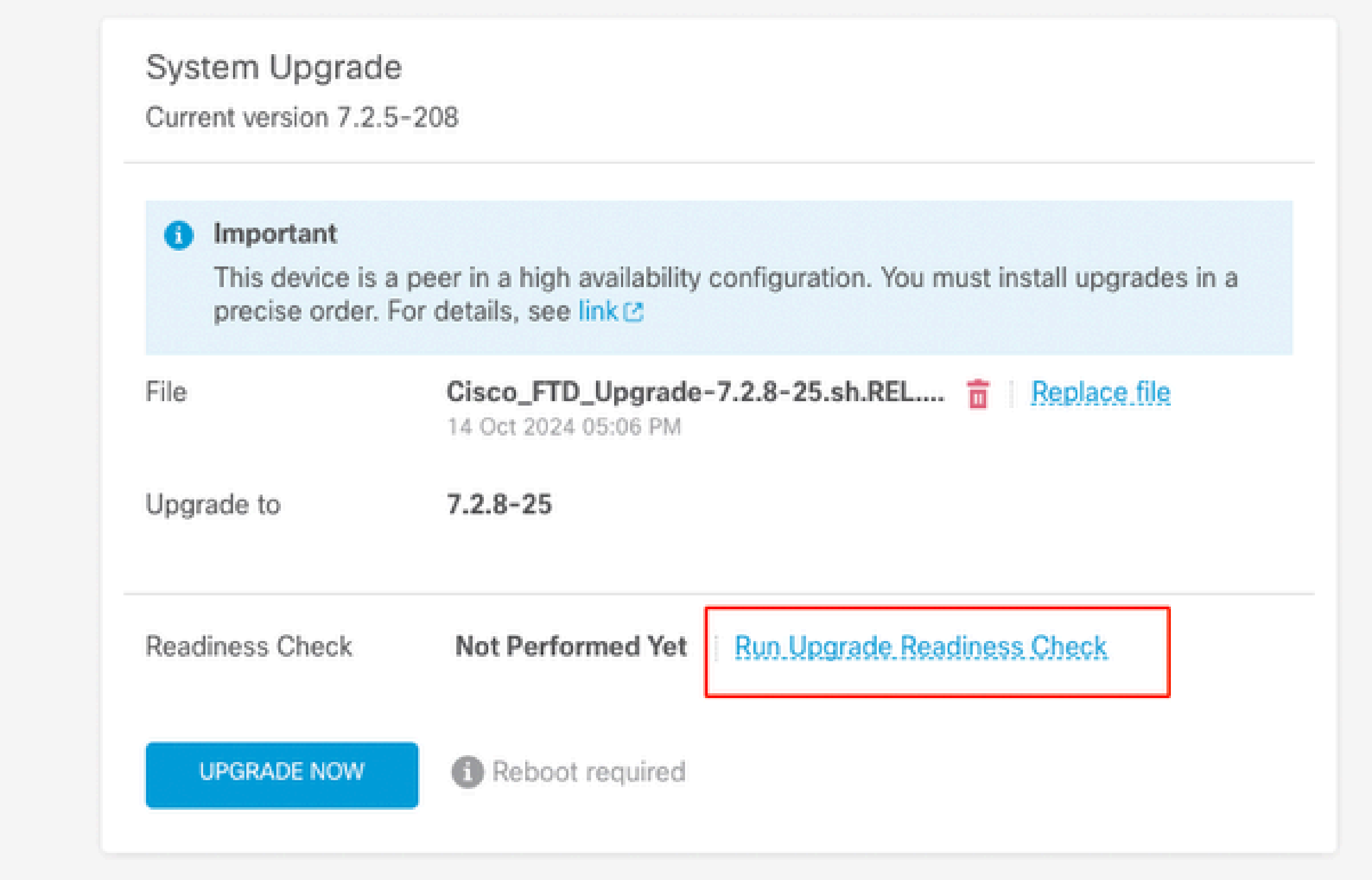
This device is a peer in a high availability configuration. You must install upgrades in a precise order. For details, see link

File: Cisco_FTD_Upgrade-7.2.8-25.sh.REL.... 14 Oct 2024 05:06 PM

Upgrade to: 7.2.8-25

Readiness Check: Not Performed Yet

运行就绪性检查



System Upgrade

Current version 7.2.5-208

Important

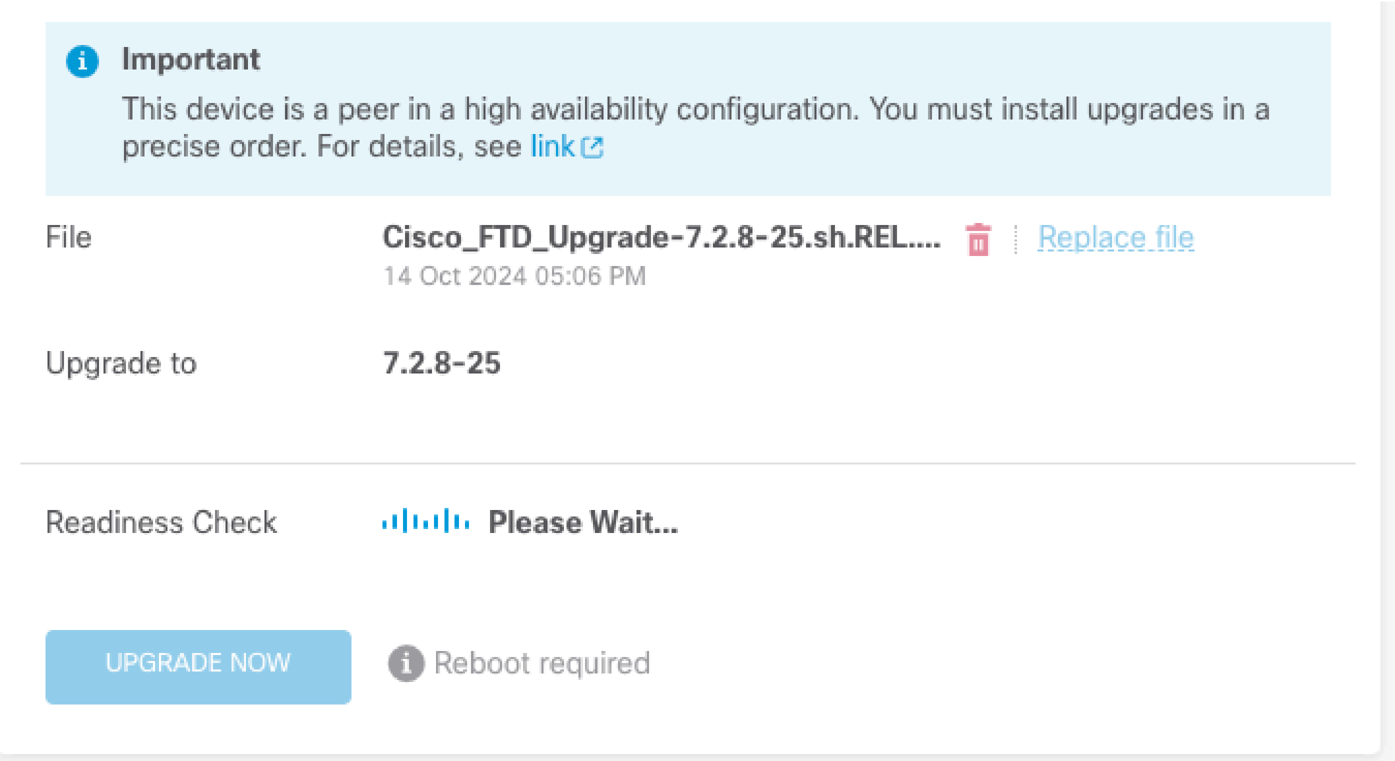
This device is a peer in a high availability configuration. You must install upgrades in a precise order. For details, see link

File: Cisco_FTD_Upgrade-7.2.8-25.sh.REL.... 14 Oct 2024 05:06 PM

Upgrade to: 7.2.8-25

Readiness Check: Not Performed Yet

运行就绪性检查



Important

This device is a peer in a high availability configuration. You must install upgrades in a precise order. For details, see link

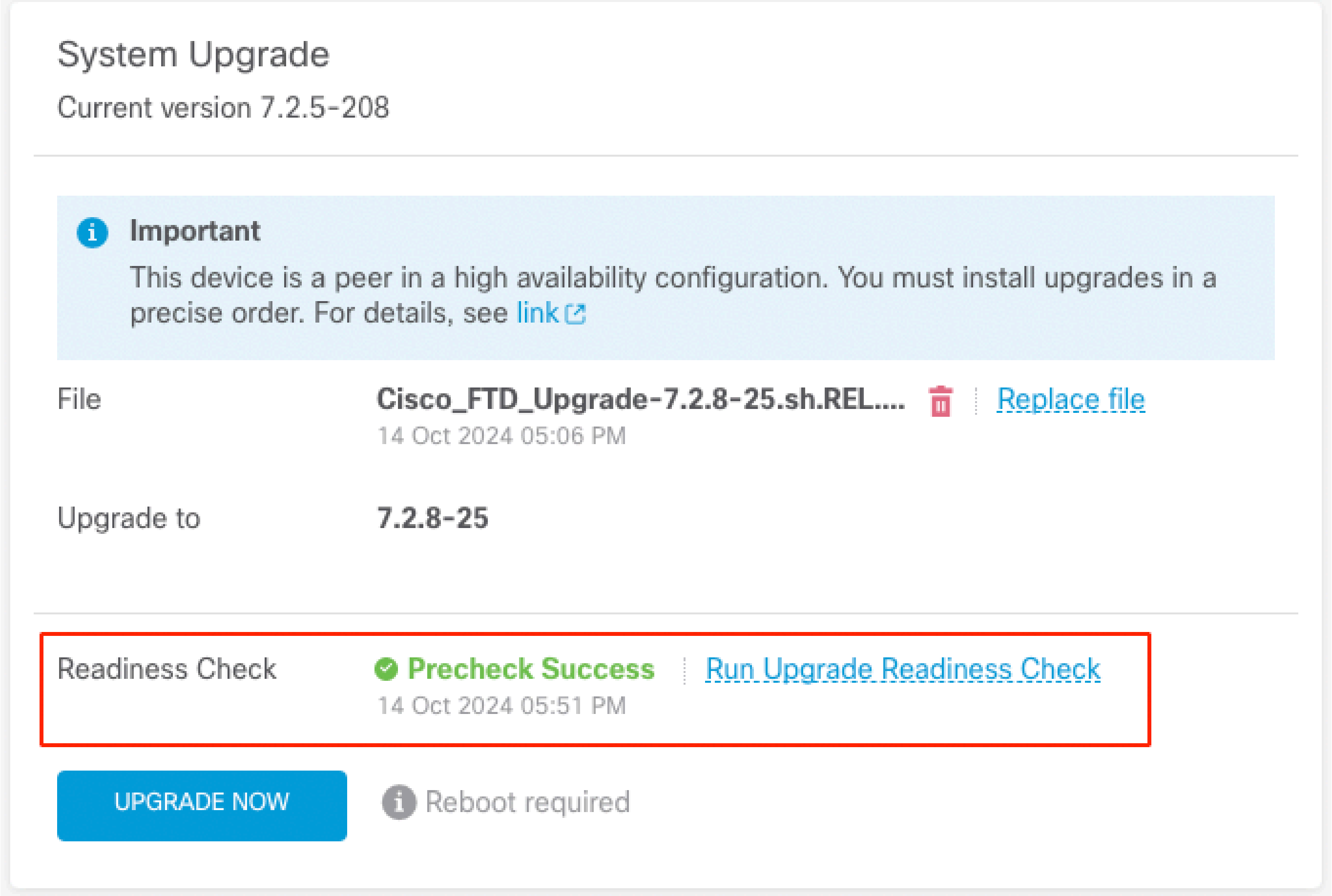
File: Cisco_FTD_Upgrade-7.2.8-25.sh.REL.... 14 Oct 2024 05:06 PM

Upgrade to: 7.2.8-25

Readiness Check: Please Wait...

运行就绪性检查

通过导航到System > Upgrade可以检查进度。


System Upgrade

Current version 7.2.5-208

Important

This device is a peer in a high availability configuration. You must install upgrades in a precise order. For details, see link

File: Cisco_FTD_Upgrade-7.2.8-25.sh.REL.... | Replace file

14 Oct 2024 05:06 PM

Upgrade to: 7.2.8-25

Readiness Check: ✓ Precheck Success | Run Upgrade Readiness Check

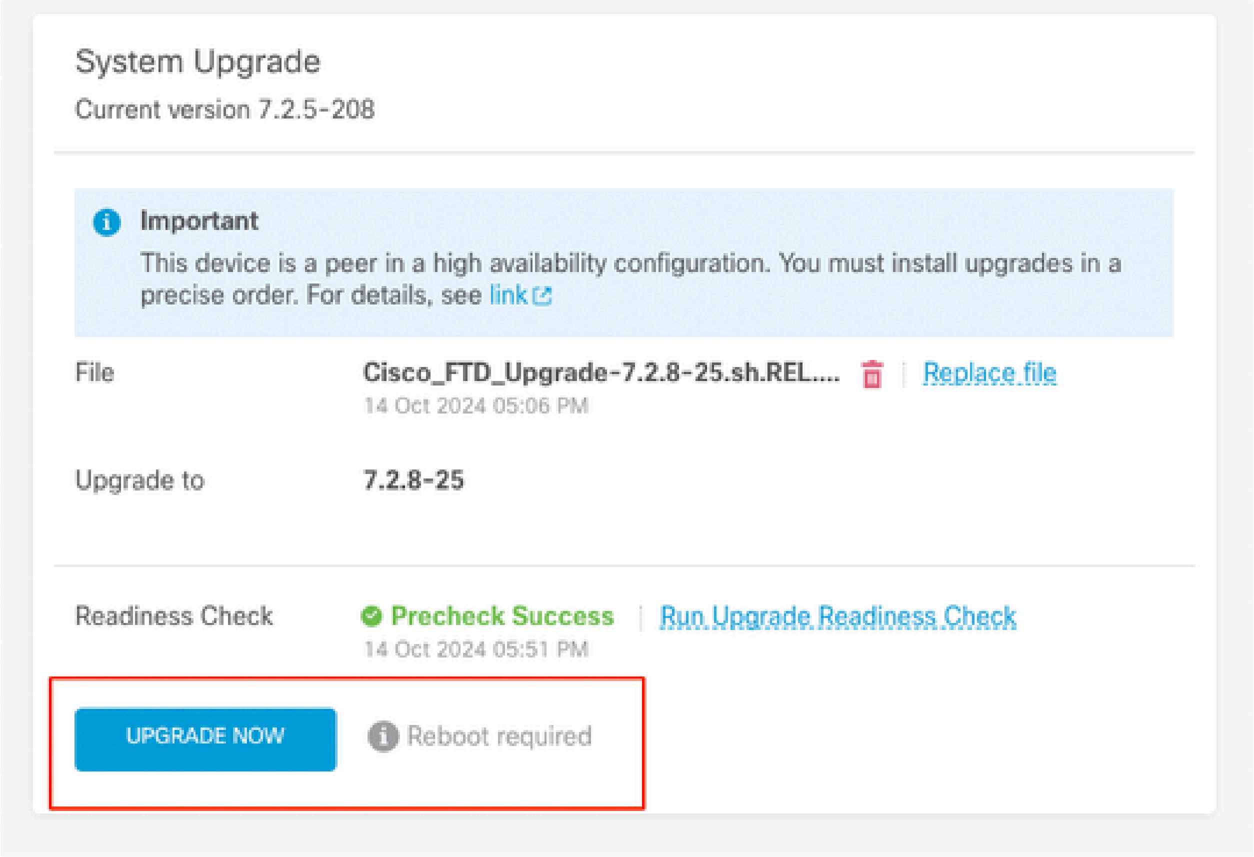
14 Oct 2024 05:51 PM

运行就绪性检查

在两个FTD中均完成就绪性检查且结果为成功时，即可完成升级。

步骤3.在HA中升级FTD

- 选择备用FDM，然后单击立即升级。



System Upgrade

Current version 7.2.5-208

Important

This device is a peer in a high availability configuration. You must install upgrades in a precise order. For details, see link

File: Cisco_FTD_Upgrade-7.2.8-25.sh.REL.... | Replace file

14 Oct 2024 05:06 PM

Upgrade to: 7.2.8-25

Readiness Check: Precheck Success | Run Upgrade Readiness Check

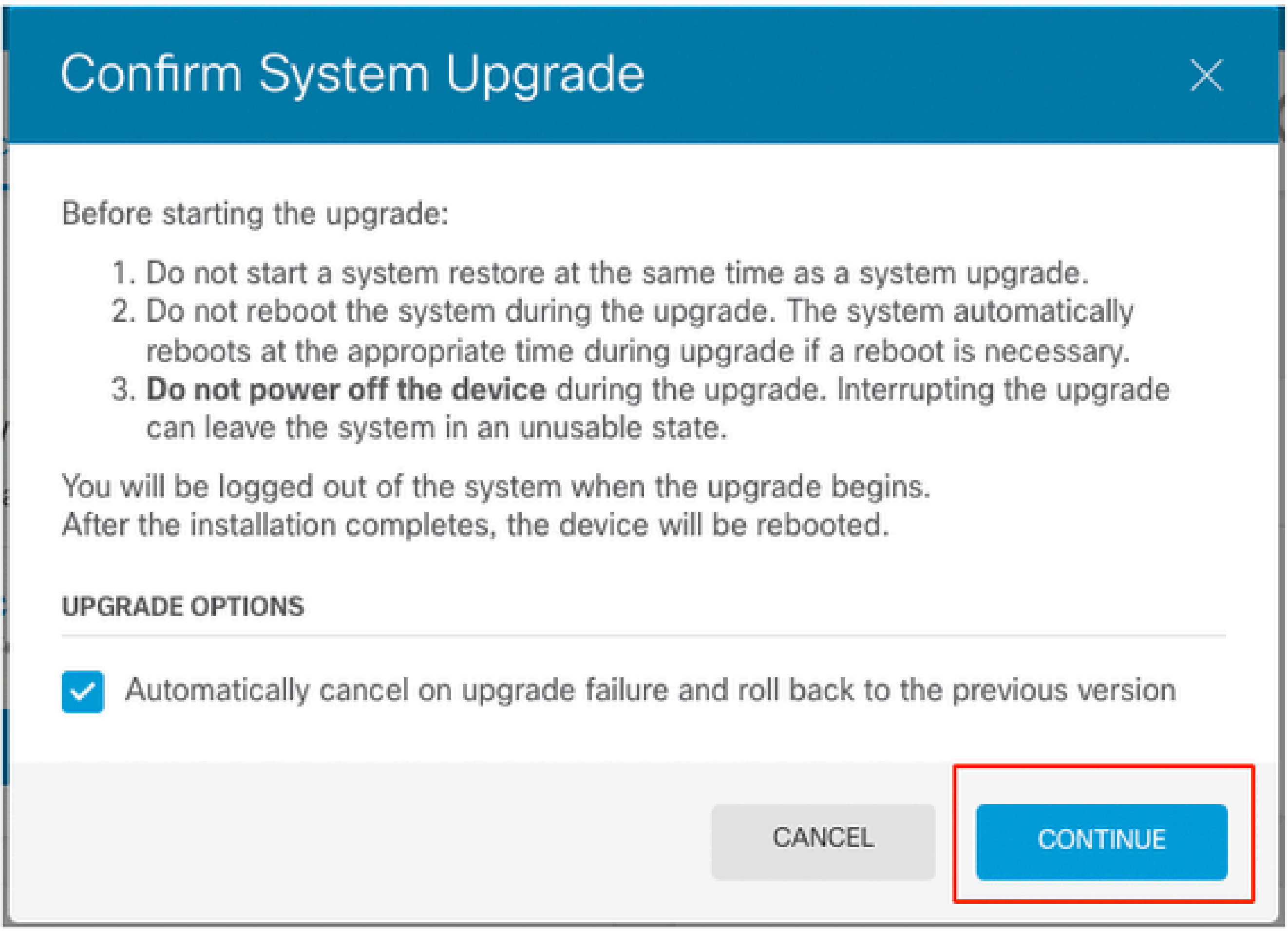
14 Oct 2024 05:51 PM

立即升级

开始升级之前：

1. 请勿在系统升级的同时启动系统还原。
2. 在升级期间不要重新启动系统。如果需要重新启动，系统会在升级期间的适当时间自动重新启动。
3. 在升级过程中请勿关闭设备电源。中断升级可能会使系统不可用。

升级开始时，您将从系统中注销。
安装完成后，设备将重新启动。



Confirm System Upgrade

Before starting the upgrade:

1. Do not start a system restore at the same time as a system upgrade.
2. Do not reboot the system during the upgrade. The system automatically reboots at the appropriate time during upgrade if a reboot is necessary.
3. **Do not power off the device** during the upgrade. Interrupting the upgrade can leave the system in an unusable state.

You will be logged out of the system when the upgrade begins.
After the installation completes, the device will be rebooted.

UPGRADE OPTIONS

☑ Automatically cancel on upgrade failure and roll back to the previous version

继续

注意：每个FTD升级大约需要20分钟。

在CLI上，可以在升级文件夹/ngfw/var/log/sf中检查进度；转到expert modeand enterroot access。

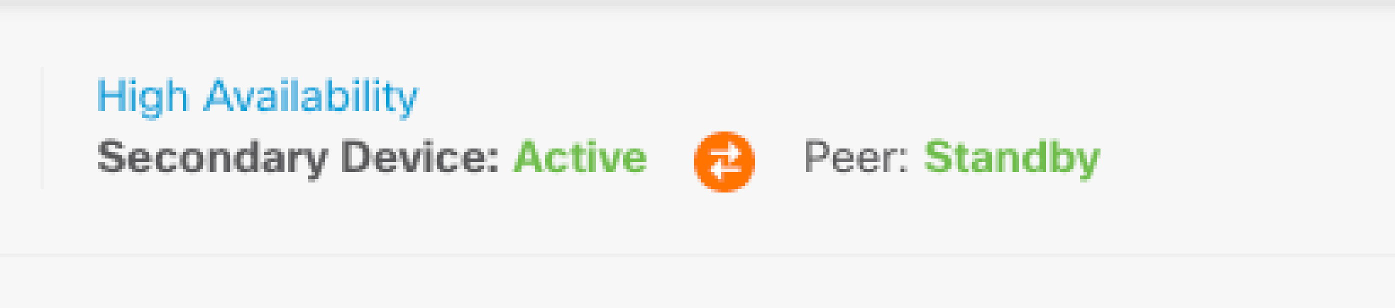
```
> expert

admin@firepower:~$ sudo su

Password:

root@firepower:/home/admin# cd /ngfw/var/log/sf



root@firepower:/ngfw/var/log/sf# ls

Cisco_FTD_Upgrade-7.2.8.
```

```
root@firepower:/ngfw/var/log/sf/Cisco_FTD_Upgrade-7.2.8# ls -lrt



root@firepower:/ngfw/var/log/sf/Cisco_FTD_Upgrade-7.2.8# tail -f status.log

ui: Upgrade in progress: ( 8% done.22 mins to reboot). Preparing to upgrade... (200_pre/011_check_self.

ui: Upgrade in progress: ( 8% done.22 mins to reboot). Preparing to upgrade... (200_pre/015_verify_rpm.

ui: Upgrade in progress: ( 8% done.22 mins to reboot). Preparing to upgrade... (200_pre/100_check_dashb

ui: Upgrade in progress: ( 8% done.22 mins to reboot). Preparing to upgrade... (200_pre/100_get_snort_f

ui: Upgrade in progress: (12% done.21 mins to reboot). Preparing to upgrade... (200_pre/110_setup_upgra

ui: Upgrade in progress: (12% done.21 mins to reboot). Preparing to upgrade... (200_pre/120_generate_au

ui: Upgrade in progress: (12% done.21 mins to reboot). Preparing to upgrade... (200_pre/152_save_etc_sf



ui: Upgrade in progress: (79% done. 5 mins to reboot). Finishing the upgrade... (999_finish/999_zz_inst

ui: Upgrade in progress: (83% done. 4 mins to reboot). Finishing the upgrade... (999_finish/999_zzz_com

ui: Upgrade complete

ui: The system will now reboot.

ui: System will now reboot.



Broadcast message from root@firepower (Mon Oct 14 12:01:26 2024):

System will reboot in 5 seconds due to system upgrade.


Broadcast message from root@firepower (Mon Oct 14 12:01:31 2024):

System will reboot now due to system upgrade.


Broadcast message from root@firepower (Mon Oct 14 12:01:39 2024):

The system is going down for reboot NOW!
```

升级第二台设备。

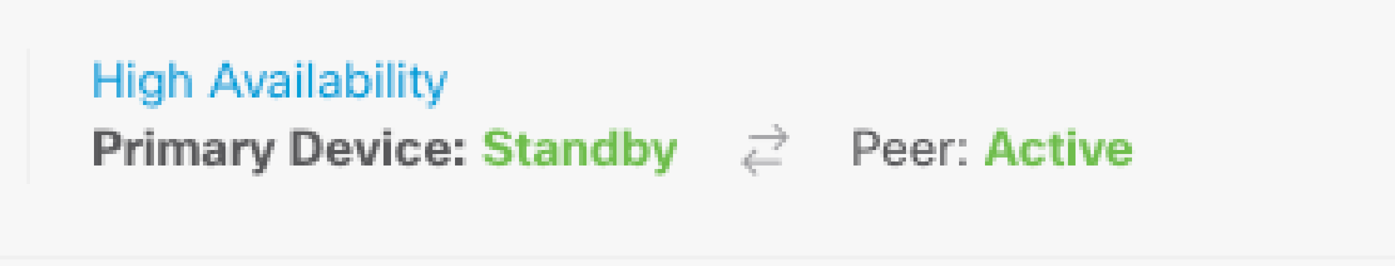
切换角色以使此设备处于活动状态：选择Device> High Availability，然后从gear菜单中选择Switch Mode。等待设备的状态，以便更改为活动状态并确认流量正常流动。然后，注销。

升级:重复上述步骤以登录新备用设备、上传数据包、升级设备、监控进度并验证成功。



High Availability
Secondary Device: Active ⇄ Peer: Standby

高可用性



High Availability
Primary Device: Standby ⇄ Peer: Active

高可用性

在CLI上，转到LINA（系统支持diagnostic-cli），并使用show failover state命令检查备用FTD上的故障切换状态。

```
> system support diagnostic-cli

Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.

Type help or '?' for a list of available commands.



primary_ha> enable

Password:

primary_ha# show failover state



               State          Last Failure Reason      Date/Time

This host  -   Primary

               Standby Ready  None

Other host -   Secondary
```

```
               Active         None



====Configuration State===

        Sync Skipped - STANDBY

====Communication State===

        Mac set



primary_ha#
```

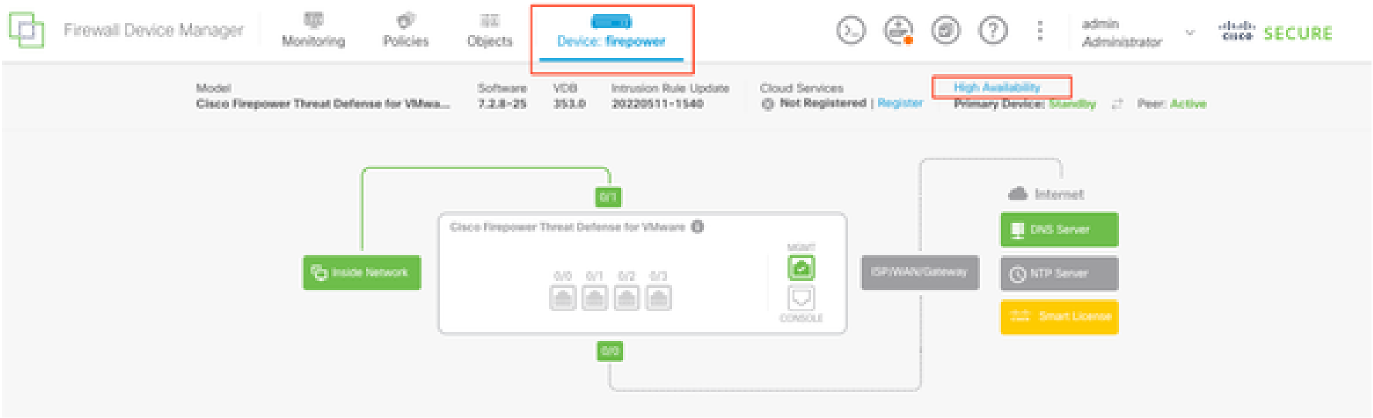
步骤4.交换活动对等体（可选）

注意：如果辅助设备处于活动状态，它不会对操作有任何影响。

将主设备设置为主用设备，将辅助设备设置为备用设备，这是帮助跟踪可能发生的任何故障转移的最佳实践。

在这种情况下，FTD Active现在为Standby，可以使用手动故障切换将其设回Active。

- 导航到设备>高可用性。



Model
Cisco Firepower Threat Defense for VMwa...

Software
7.2.8-25

VDB
353.0

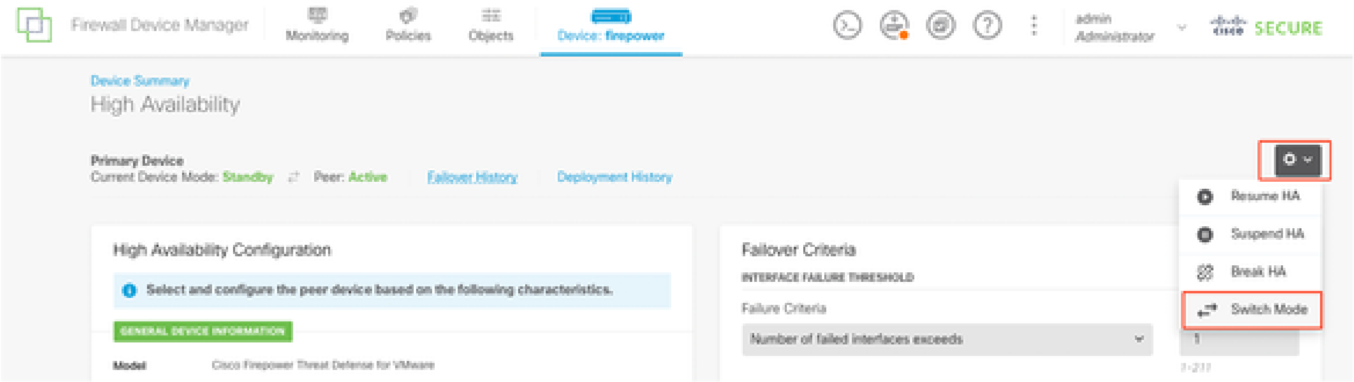
Intrusion Rule Update
20220511-1540

Cloud Services
Not Registered | Register

Primary Device: Standby ⇄ Peer: Active

高可用性

- 选择Switch Mode。



High Availability

Primary Device
Current Device Mode: Standby ⇄ Peer: Active

High Availability Configuration

Select and configure the peer device based on the following characteristics.

GENERAL DEVICE INFORMATION

Model Cisco Firepower Threat Defense for VMware

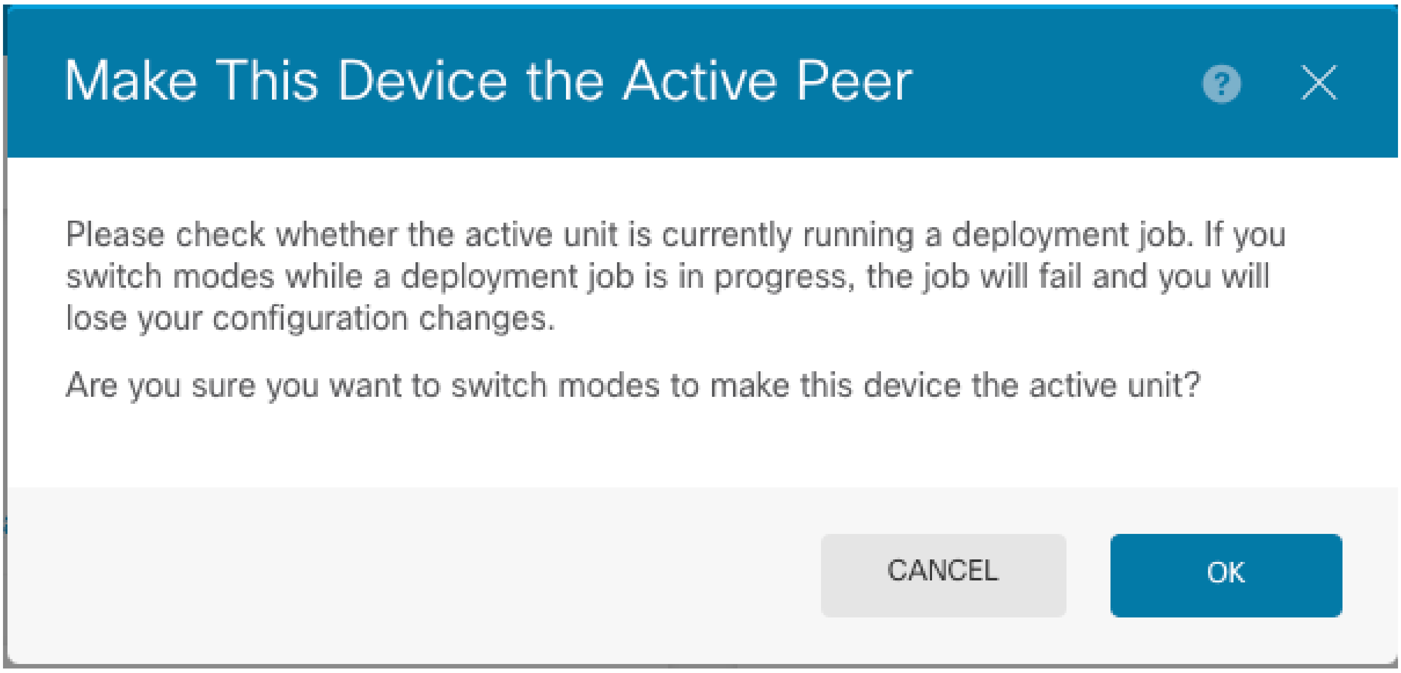
Failover Criteria

INTERFACE FAILURE THRESHOLD

Failure Criteria
Number of failed interfaces exceeds 1
1-211

交换模式

- 选择OK以确认故障切换。



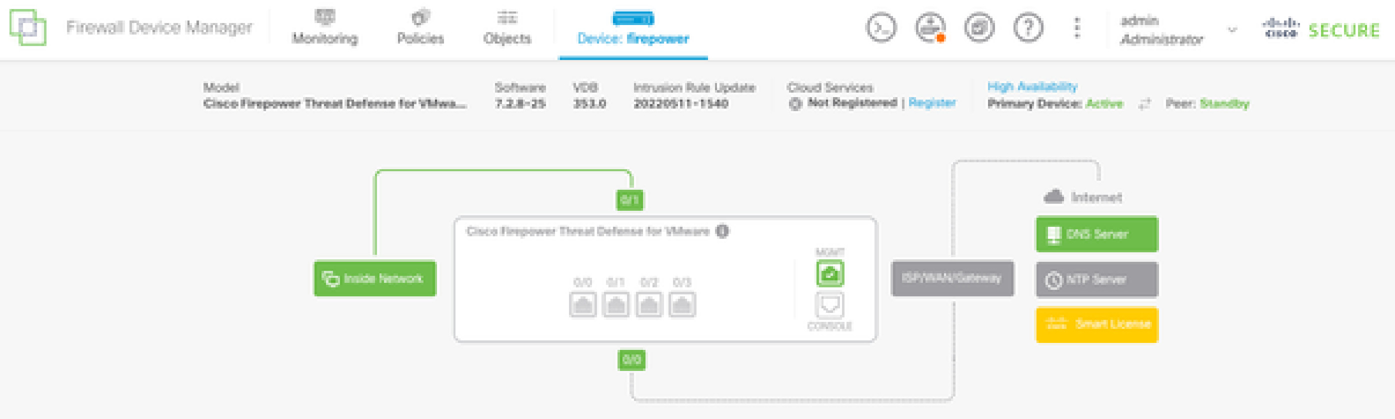
Make This Device the Active Peer

Please check whether the active unit is currently running a deployment job. If you switch modes while a deployment job is in progress, the job will fail and you will lose your configuration changes.

Are you sure you want to switch modes to make this device the active unit?

活动对等体

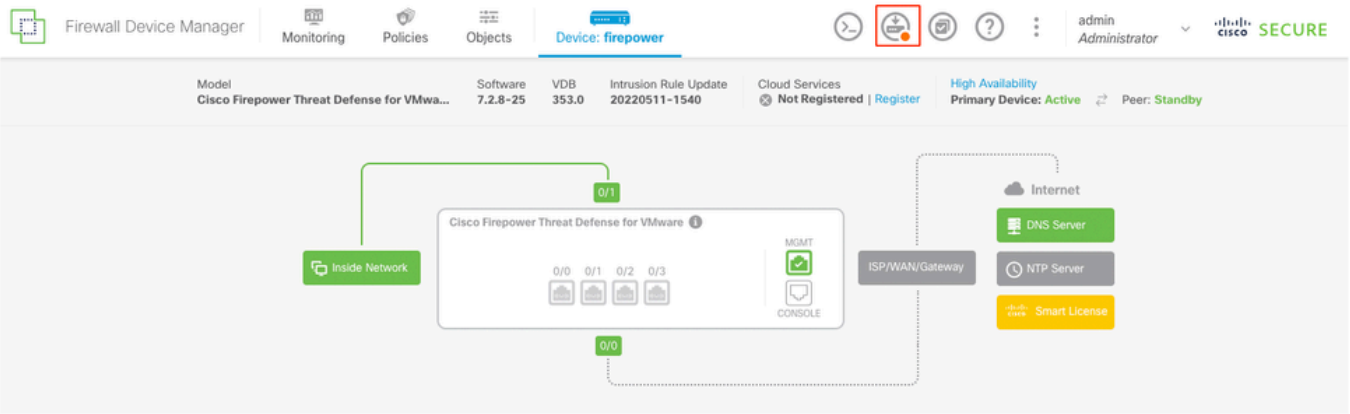
完成升级和故障转移后，验证高可用性状态。

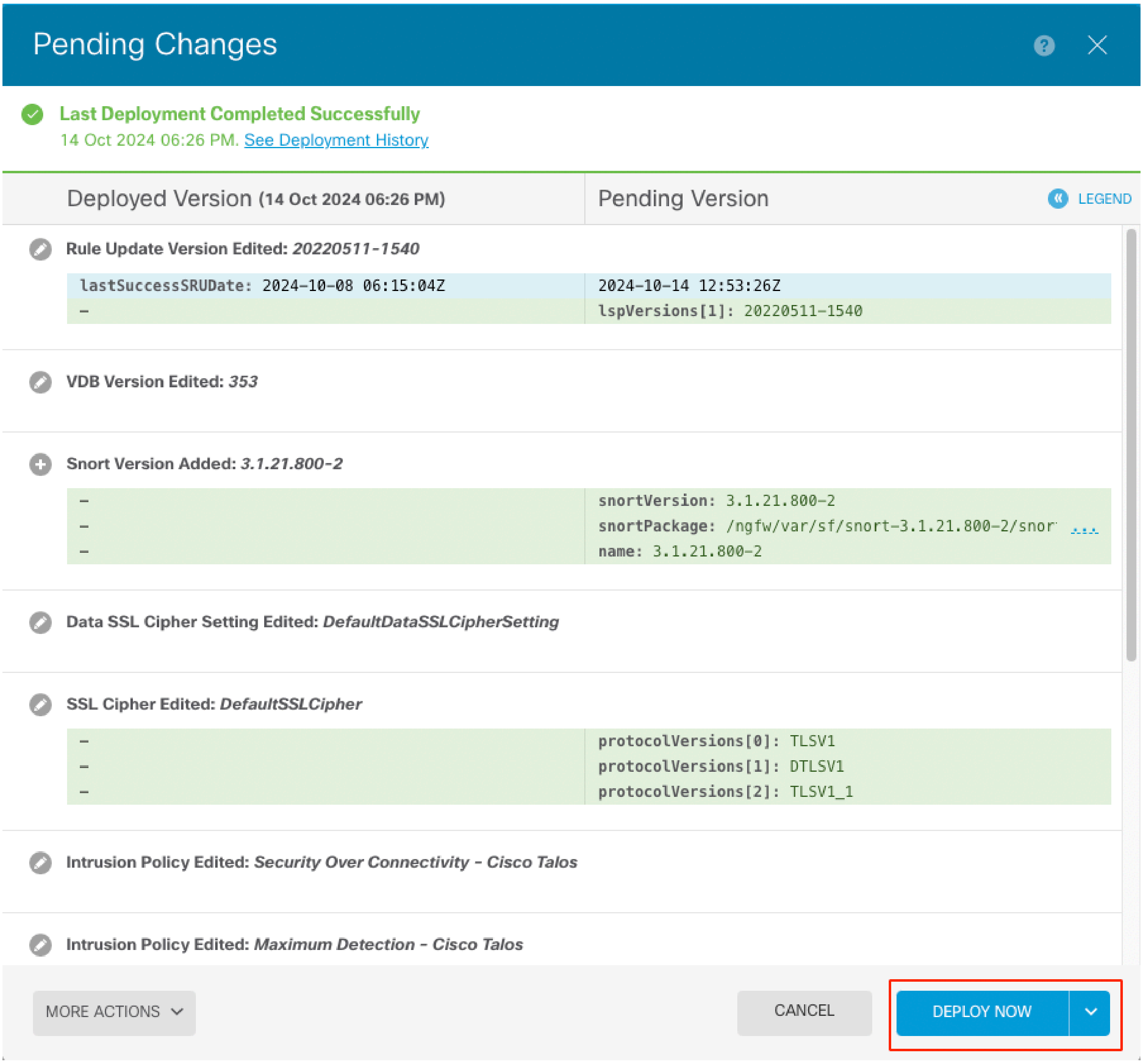


设备

步骤5.最终部署

- 通过点击Deployment选项卡下的DEPLOY NOW将策略部署到设备。




Pending Changes
?
Last Deployment Completed Successfully
14 Oct 2024 06:26 PM. See Deployment History
Deployed Version (14 Oct 2024 06:26 PM)
Pending Version
LEGEND
MORE ACTIONS
CANCEL
DEPLOY NOW

Rule Update Version Edited: *20220511-1540*

```
lastSuccessSRUDate: 2024-10-08 06:15:04Z    2024-10-14 12:53:26Z
-                                           lspVersions[1]: 20220511-1540
```

VDB Version Edited: *353*

Snort Version Added: *3.1.21.800-2*

```
-    snortVersion: 3.1.21.800-2
-    snortPackage: /ngfw/var/sf/snort-3.1.21.800-2/snor ...
-    name: 3.1.21.800-2
```

Data SSL Cipher Setting Edited: *DefaultDataSSLCipherSetting*

SSL Cipher Edited: *DefaultSSLCipher*

```
-    protocolVersions[0]: TLSV1
-    protocolVersions[1]: DTLSV1
-    protocolVersions[2]: TLSV1_1
```

Intrusion Policy Edited: *Security Over Connectivity - Cisco Talos*

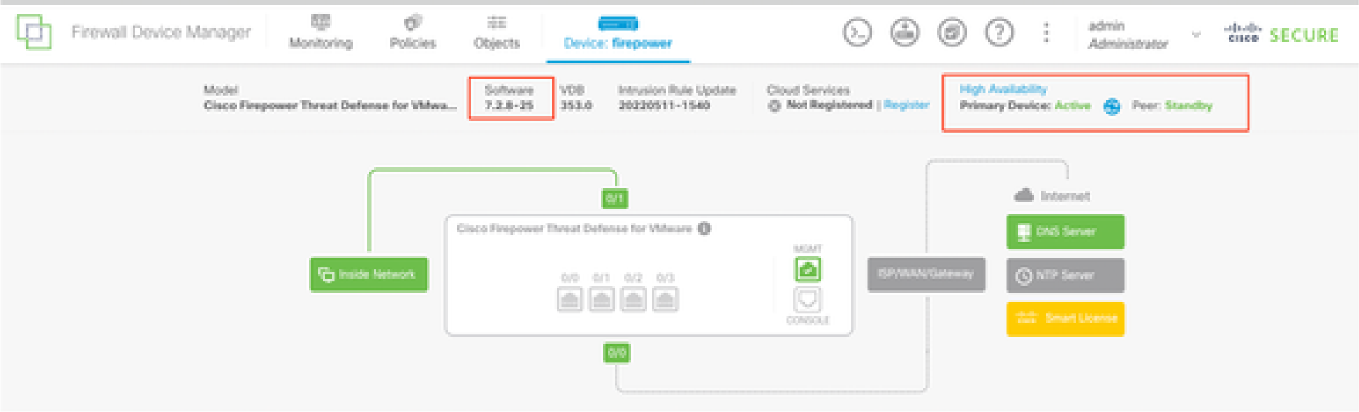
Intrusion Policy Edited: *Maximum Detection - Cisco Talos*

策略部署

验证

要验证HA状态和升级是否完成，您必须确认状态：
首选：主用
辅助：备用就绪

这两个版本都是最近更改的版本（本例中为7.2.8）。



Model
Cisco Firepower Threat Defense for VMwa...
Software
7.2.8-25
VDB
353.0
Intrusion Rule Update
20220511-1540
Cloud Services
Not Registered | Register
High Availability
Primary Device: Active
Peer: Standby

故障转移

- 在CLI清理上，使用命令show failover states和show failoverflow检查故障切换状态，了解更多详细信息。

Cisco Firepower可扩展操作系统(FX-OS)v2.12.1（内部版本73）
适用于VMware v7.2.8的思科Firepower威胁防御（内部版本25）

```
> show failover state

               State          Last Failure Reason      Date/Time
This host  -   Primary
               Active         None
Other host -   Secondary
               Standby Ready  None

====Configuration State===
        Sync Skipped
====Communication State===
        Mac set

> show failover
Failover On
Failover unit Primary
Failover LAN Interface: failover-link GigabitEthernet0/2 (up)
```

```
Reconnect timeout 0:00:00

Unit Poll frequency 1 seconds, holdtime 15 seconds

Interface Poll frequency 5 seconds, holdtime 25 seconds

Interface Policy 1

Monitored Interfaces 3 of 311 maximum

MAC Address Move Notification Interval not set

failover replication http

Version: Ours 9.18(4)210, Mate 9.18(4)210

Serial Number: Ours 9A1QUNFWPK1, Mate 9A45VNEHB5C

Last Failover at: 14:13:56 UTC Oct 15 2024

        This host: Primary - Active

                Active time: 580 (sec)

                slot 0: ASAv hw/sw rev (/9.18(4)210) status (Up Sys)

                  Interface diagnostic (0.0.0.0): Normal (Waiting)

                  Interface inside (192.168.45.1): Normal (Waiting)

                  Interface outside (192.168.1.10): Normal (Waiting)

                slot 1: snort rev (1.0)  status (up)

                slot 2: diskstatus rev (1.0)  status (up)

        Other host: Secondary - Standby Ready

                Active time: 91512 (sec)

                  Interface diagnostic (0.0.0.0): Normal (Waiting)

                  Interface inside (0.0.0.0): Normal (Waiting)

                  Interface outside (0.0.0.0): Normal (Waiting)

                slot 1: snort rev (1.0)  status (up)

                slot 2: diskstatus rev (1.0)  status (up)



Stateful Failover Logical Update Statistics

        Link : failover-link GigabitEthernet0/2 (up)

        Stateful Obj    xmit       xerr       rcv        rerr

        General         11797      0          76877      0
```

```
sys cmd         11574      0          11484      0
up time         0          0          0          0
RPC services    0          0          0          0
TCP conn        0          0          0          0
UDP conn        176        0          60506      0
ARP tbl         45         0          4561       0
Xlate_Timeout   0          0          0          0
IPv6 ND tbl     0          0          0          0
VPN IKEv1 SA    0          0          0          0
VPN IKEv1 P2    0          0          0          0
VPN IKEv2 SA    0          0          0          0
VPN IKEv2 P2    0          0          0          0
VPN CTCP upd    0          0          0          0
VPN SDI upd     0          0          0          0
VPN DHCP upd    0          0          0          0
SIP Session     0          0          0          0
SIP Tx  0          0          0          0
SIP Pinhole     0          0          0          0
Route Session   1          0          0          0
Router ID       0          0          0          0
User-Identity   0          0          30         0
CTS SGTNAME     0          0          0          0
CTS PAC         0          0          0          0
TrustSec-SXP    0          0          0          0
IPv6 Route      0          0          0          0
STS Table       0          0          0          0
Umbrella Device-ID      0          0          0          0
Rule DB B-Sync  0          0          30         0
Rule DB P-Sync  1          0          266        0
Rule DB Delete  0          0          0          0
```

```
        Logical Update Queue Information
                        Cur     Max     Total
        Recv Q:         0       31      123591
        Xmit Q:         0       1       12100
```

如果两个FTD位于同一版本，并且HA状态正常，则升级完成。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。