更换安全防火墙中的故障设备高可用性威胁防御

目录

简介

本文档介绍如何更换作为高可用性(HA)设置一部分的有故障的安全防火墙威胁防御模块。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科安全防火墙管理中心(FMC)
- Cisco Firepower可扩展操作系统(FXOS)
- 思科安全防火墙威胁防御(FTD)

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Firepower 4110运行FXOS v2.12(0.498)
- 逻辑设备运行Cisco Secure Firewall v7.2.5

- 安全防火墙管理中心2600运行v7.4
- 安全复制协议(SCP)知识

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。

背景信息

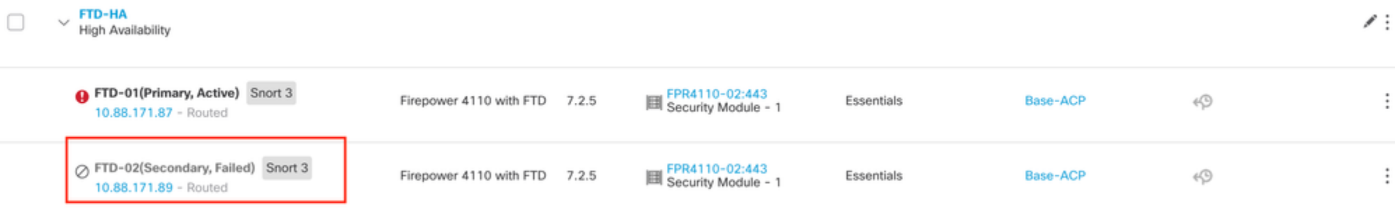
以下设备支持此过程：

- Cisco Secure Firewall 1000系列设备
- 思科安全防火墙2100系列设备
- Cisco Secure Firewall 3100系列设备
- 思科安全防火墙4100系列设备
- Cisco Secure Firewall 4200系列设备
- 思科安全防火墙9300设备
- 适用于VMWare的思科安全防火墙威胁防御

开始使用前

本文档要求您使用相同的FXOS和FTD版本配置新设备。

确定故障设备



FTD-HA
High Availability

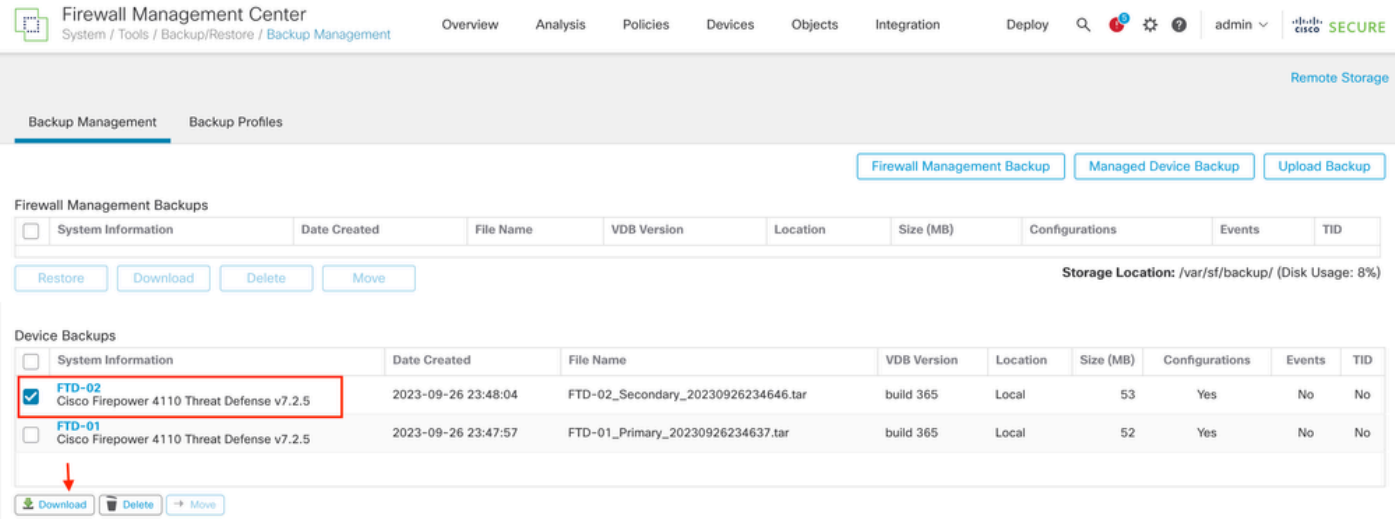
FTD-01(Primary, Active) Snort 3 10.88.171.87 - Routed	Firepower 4110 with FTD	7.2.5	FPR4110-02:443 Security Module - 1	Essentials	Base-ACP	
FTD-02(Secondary, Failed) Snort 3 10.88.171.89 - Routed	Firepower 4110 with FTD	7.2.5	FPR4110-02:443 Security Module - 1	Essentials	Base-ACP	

在这种情况下，辅助设备(FTD-02)处于故障状态。

用备份替换故障设备

您可以使用此过程替换主设备或辅助设备。本指南假设您要更换故障设备的备份。

步骤1.从FMC下载备份文件。导航到System > Tools > Restore > Device Backups，然后选择正确的备份。单击Download:



Firewall Management Backups

	System Information	Date Created	File Name	VDB Version	Location	Size (MB)	Configurations	Events	TID

Storage Location: /var/sf/backup/ (Disk Usage: 8%)

Device Backups

	System Information	Date Created	File Name	VDB Version	Location	Size (MB)	Configurations	Events	TID
☑	FTD-02 Cisco Firepower 4110 Threat Defense v7.2.5	2023-09-26 23:48:04	FTD-02_Secondary_20230926234646.tar	build 365	Local	53	Yes	No	No
□	FTD-01 Cisco Firepower 4110 Threat Defense v7.2.5	2023-09-26 23:47:57	FTD-01_Primary_20230926234637.tar	build 365	Local	52	Yes	No	No

步骤2.将FTD备份上传到新FTD的/var/sf/backup/目录：

2.1从test-pc（SCP客户端）将备份文件上传到/var/tmp/目录下的FTD:

```
@test-pc ~ % scp FTD-02_Secondary_20230926234646.tar cisco@10.88.243.90:/var/tmp/
```

2.2在FTD CLI专家模式下，将备份文件从/var/tmp/移动到/var/sf/backup/:

```
root@firepower:/var/tmp# mv FTD-02_Secondary_20230926234646.tar /var/sf/backup/
```

步骤3.从清洁模式应用下一个命令，恢复FTD-02备份:

```
>restore remote-manager-backup FTD-02_Secondary_20230926234646.tar

Device model from backup :: Cisco Firepower 4110 Threat Defense
This Device Model   :: Cisco Firepower 4110 Threat Defense
***********************************************
Backup Details
***********************************************
Model = Cisco Firepower 4110 Threat Defense
Software Version = 7.2.5
```

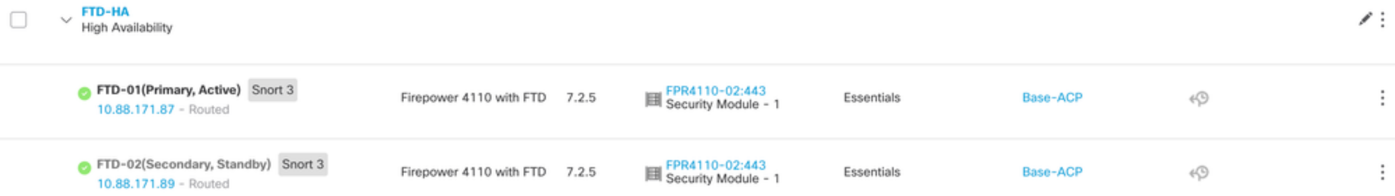
```
Serial = FLM22500791
Hostname = firepower
Device Name = FTD-02_Secondary
IP Address = 10.88.171.89
Role = SECONDARY
VDB Version = 365
SRU Version =
FXOS Version = 2.12(0.498)
Manager IP(s) = 10.88.243.90
Backup Date = 2023-09-26 23:46:46
Backup Filename = FTD-02_Secondary_20230926234646.tar
***********************************************

********************* Caution ****************************
Verify that you are restoring a valid backup file.
Make sure that FTD is installed with same software version and matches versions from backup manifest be
Restore operation will overwrite all configurations on this device with configurations in backup.
If this restoration is being performed on an RMA device then ensure old device is removed from network 
**********************************************************
Are you sure you want to continue (Y/N)Y
Restoring device . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
Added table audit_log with table_id 1
Added table health_alarm_syslog with table_id 2
Added table dce_event with table_id 3
Added table application with table_id 4
Added table rna_scan_results_tableview with table_id 5
Added table rna_event with table_id 6
Added table ioc_state with table_id 7
Added table third_party_vulns with table_id 8
Added table user_ioc_state with table_id 9
Added table rna_client_app with table_id 10
Added table rna_attribute with table_id 11
Added table captured_file with table_id 12
Added table rna_ip_host with table_id 13
Added table flow_chunk with table_id 14
Added table rua_event with table_id 15
Added table wl_dce_event with table_id 16
Added table user_identities with table_id 17
Added table whitelist_violations with table_id 18
Added table remediation_status with table_id 19
Added table syslog_event with table_id 20
Added table rna_service with table_id 21
Added table rna_vuln with table_id 22
Added table SRU_import_log with table_id 23
Added table current_users with table_id 24

Broadcast message from root@firepower (Wed Sep 27 15:50:12 2023):

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

注意：恢复完成后，设备会将您从CLI注销、重新启动并自动连接到FMC。此时，设备即将过期。

第 4 步： 恢复HA同步。在FTD CLI中，输入configure high-availability resume:

```
>configure high-availability resume
```

FTD高可用性配置现已完成：

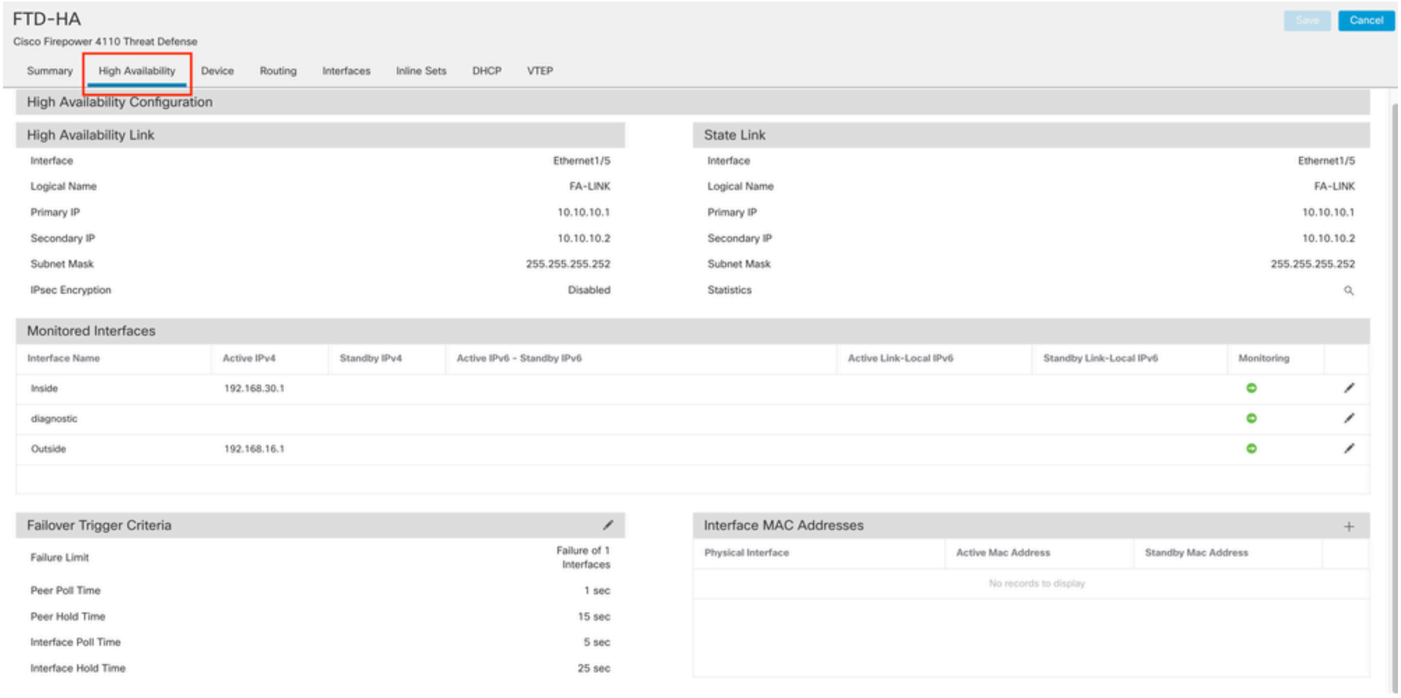


□ FTD-HA High Availability							
FTD-01(Primary, Active) Snort 3 10.88.171.87 - Routed	Firepower 4110 with FTD	7.2.5	FPR4110-02:443 Security Module - 1	Essentials	Base-ACP		⋮
FTD-02(Secondary, Standby) Snort 3 10.88.171.89 - Routed	Firepower 4110 with FTD	7.2.5	FPR4110-02:443 Security Module - 1	Essentials	Base-ACP		⋮

更换故障单元而不备份

如果没有故障设备的备份，您可以继续本指南。您可以替换主设备或辅助设备，此过程取决于设备是主设备还是辅助设备。本指南中介绍的所有步骤都是要恢复有故障的辅助设备。如果要恢复有故障的主设备，请在步骤5中配置高可用性，即在注册期间将现有辅助/主用设备用作主设备，将替换设备用作辅助/备用设备。

步骤1.导航到Device > Device Management，获取高可用性配置的截图（备份）。 编辑正确的FTD HA对（点击铅笔图标），然后点击High Availability选项：



FTD-HA
Cisco Firepower 4110 Threat Defense

High Availability Configuration

High Availability Link

Interface	Ethernet1/5
Logical Name	FA-LINK
Primary IP	10.10.10.1
Secondary IP	10.10.10.2
Subnet Mask	255.255.255.252
IPsec Encryption	Disabled

State Link

Interface	Ethernet1/5
Logical Name	FA-LINK
Primary IP	10.10.10.1
Secondary IP	10.10.10.2
Subnet Mask	255.255.255.252
Statistics	

Monitored Interfaces

Interface Name	Active IPv4	Standby IPv4	Active IPv6 - Standby IPv6	Active Link-Local IPv6	Standby Link-Local IPv6	Monitoring
Inside	192.168.30.1					●
diagnostic						●
Outside	192.168.16.1					●

Failover Trigger Criteria

Failure Limit	Failure of 1 Interfaces
Peer Poll Time	1 sec
Peer Hold Time	15 sec
Interface Poll Time	5 sec
Interface Hold Time	25 sec

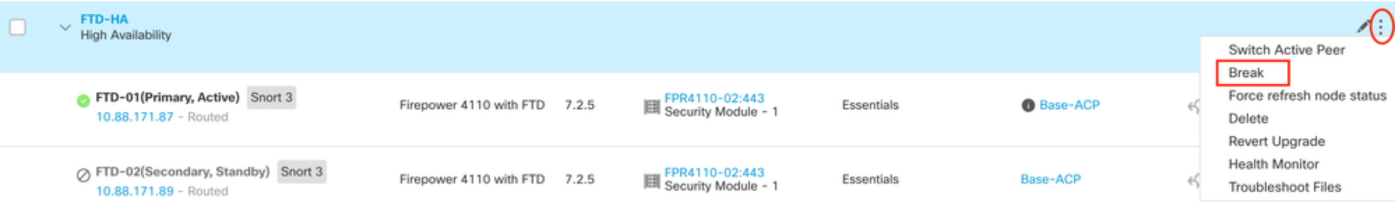
Interface MAC Addresses

Physical Interface	Active Mac Address	Standby Mac Address

No records to display

步骤2.中断HA。

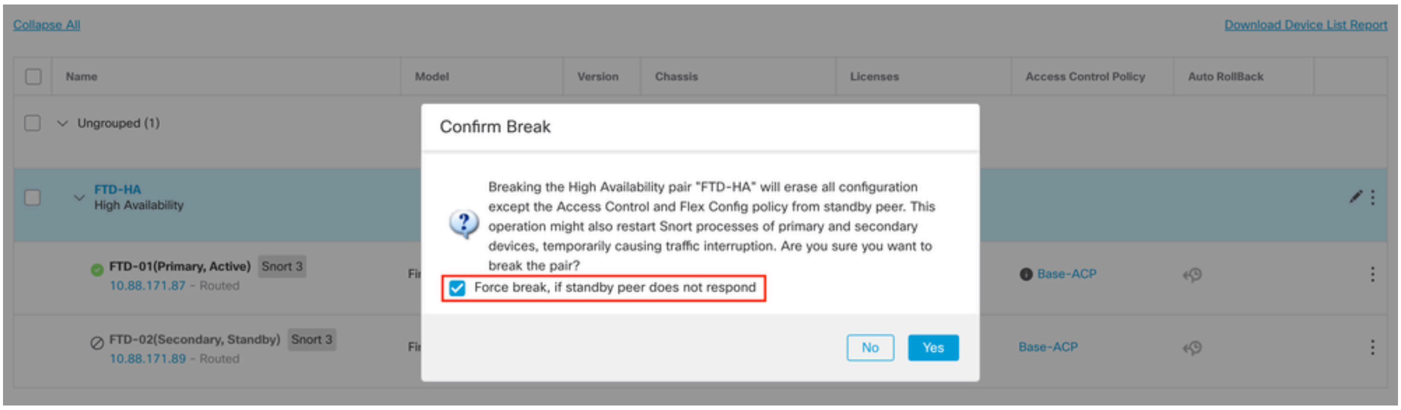
2.1导航到Devices > Device Management，然后单击右上角的三点菜单。然后单击Break选项：



FTD-HA
High Availability

FTD-01(Primary, Active) Snort 3 10.88.171.87 - Routed	Firepower 4110 with FTD	7.2.5	FPR4110-02:443 Security Module - 1	Essentials	Base-ACP
FTD-02(Secondary, Standby) Snort 3 10.88.171.89 - Routed	Firepower 4110 with FTD	7.2.5	FPR4110-02:443 Security Module - 1	Essentials	Base-ACP

2.2.选择Force break， if standby peer does not respond选项：



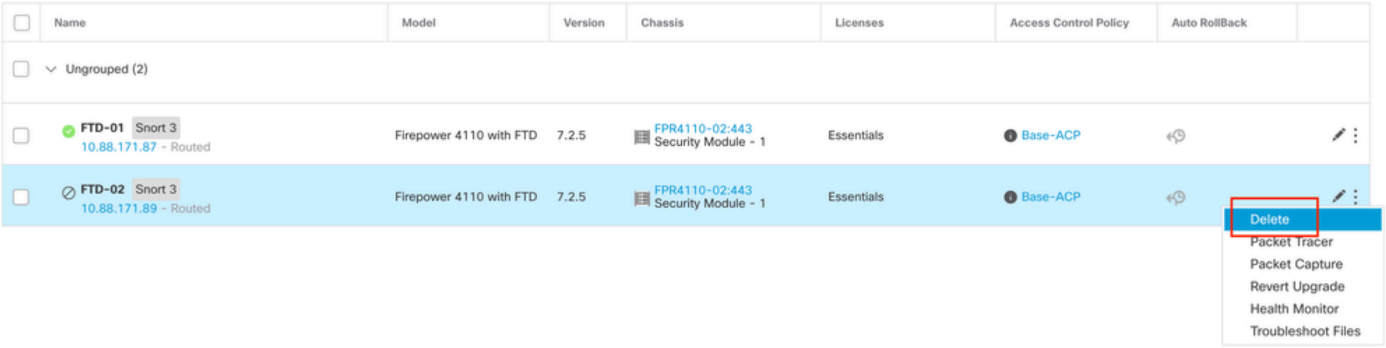
Confirm Break

Breaking the High Availability pair "FTD-HA" will erase all configuration except the Access Control and Flex Config policy from standby peer. This operation might also restart Snort processes of primary and secondary devices, temporarily causing traffic interruption. Are you sure you want to break the pair?

☑ Force break, if standby peer does not respond

注意：由于设备无响应，您需要强制中断HA。当您中断高可用性对时，活动设备将保留已完全部署的功能。备用设备丢失其故障切换和接口配置，成为独立设备。

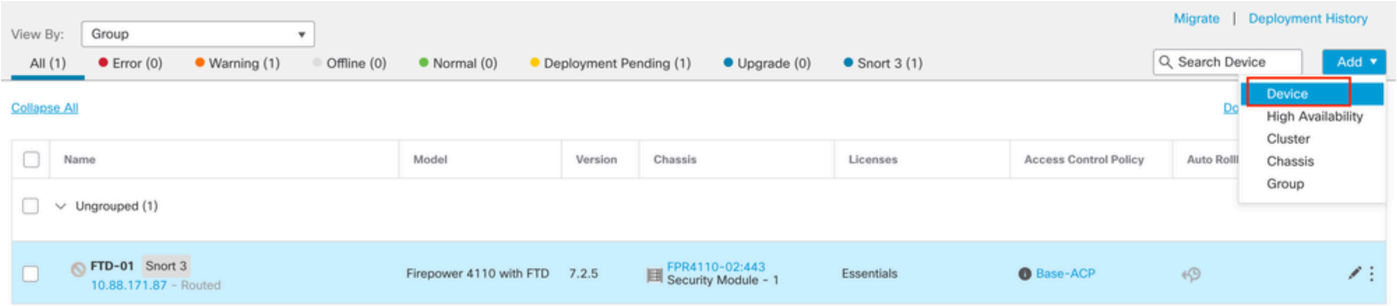
步骤3.删除故障FTD。确定要替换的FTD，然后点击三点菜单。单击Delete:



☐	Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack
☐	Ungrouped (2)						
☐	FTD-01 Snort 3 10.88.171.87 - Routed	Firepower 4110 with FTD	7.2.5	FPR4110-02:443 Security Module - 1	Essentials	Base-ACP	
☐	FTD-02 Snort 3 10.88.171.89 - Routed	Firepower 4110 with FTD	7.2.5	FPR4110-02:443 Security Module - 1	Essentials	Base-ACP	

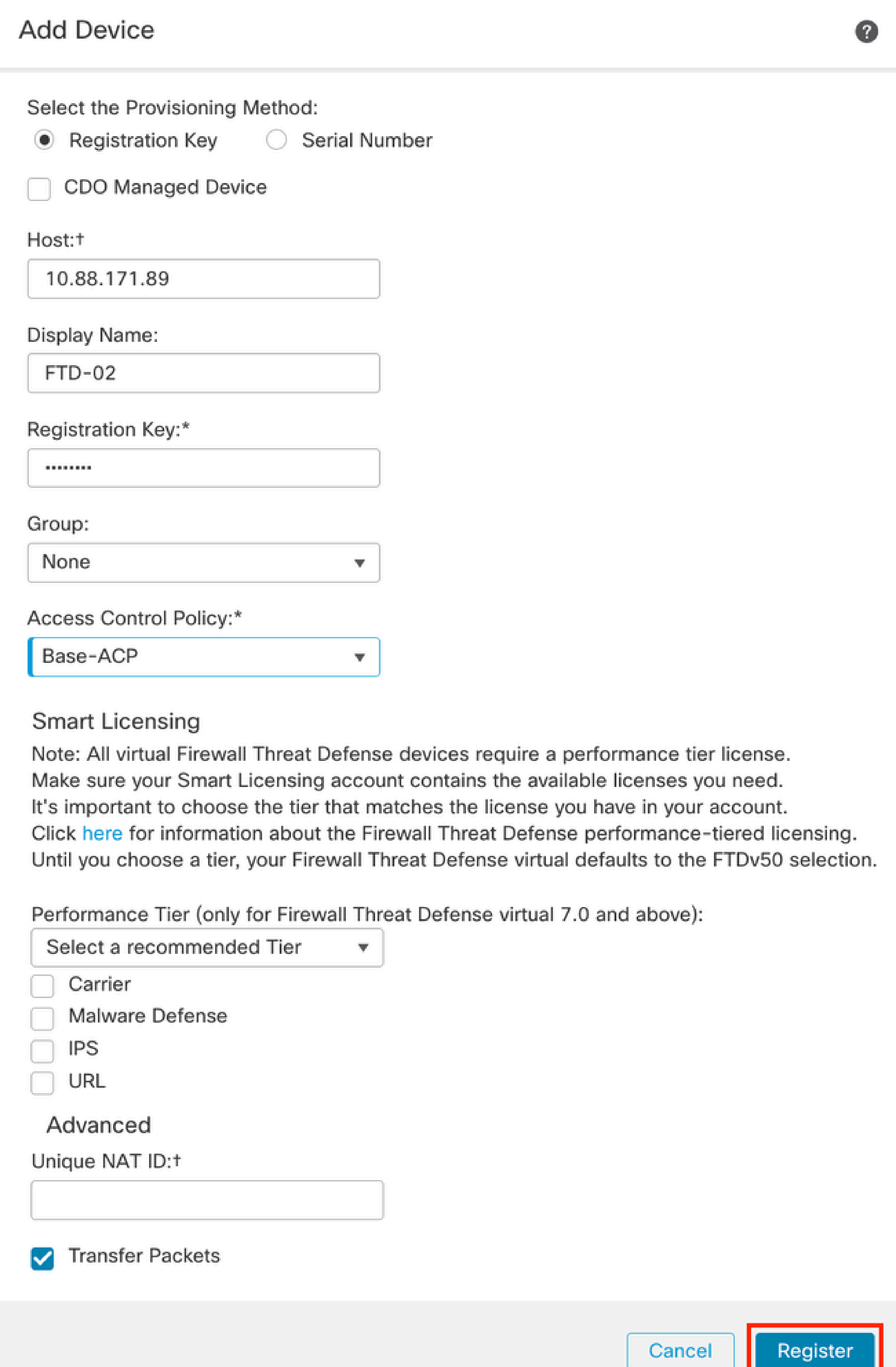
步骤4.添加新的FTD。

4.1.导航到Devices > Device Management > Add，然后单击Device:



☐	Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto Roll
☐	Ungrouped (1)						
☐	FTD-01 Snort 3 10.88.171.87 - Routed	Firepower 4110 with FTD	7.2.5	FPR4110-02:443 Security Module - 1	Essentials	Base-ACP	

4.2.选择“预配方法”(在本例中为Registration Key),配置Host、Display Name、Registration Key。配置访问控制策略并单击Register。



Add Device

Select the Provisioning Method:
● Registration Key ○ Serial Number

□ CDO Managed Device

Host:†
10.88.171.89

Display Name:
FTD-02

Registration Key:*
••••••••

Group:
None ▾

Access Control Policy:*
Base-ACP ▾

Smart Licensing

Note: All virtual Firewall Threat Defense devices require a performance tier license.
Make sure your Smart Licensing account contains the available licenses you need.
It's important to choose the tier that matches the license you have in your account.
Click here for information about the Firewall Threat Defense performance-tiered licensing.
Until you choose a tier, your Firewall Threat Defense virtual defaults to the FTDv50 selection.

Performance Tier (only for Firewall Threat Defense virtual 7.0 and above):
Select a recommended Tier ▾

□ Carrier
□ Malware Defense
□ IPS
□ URL

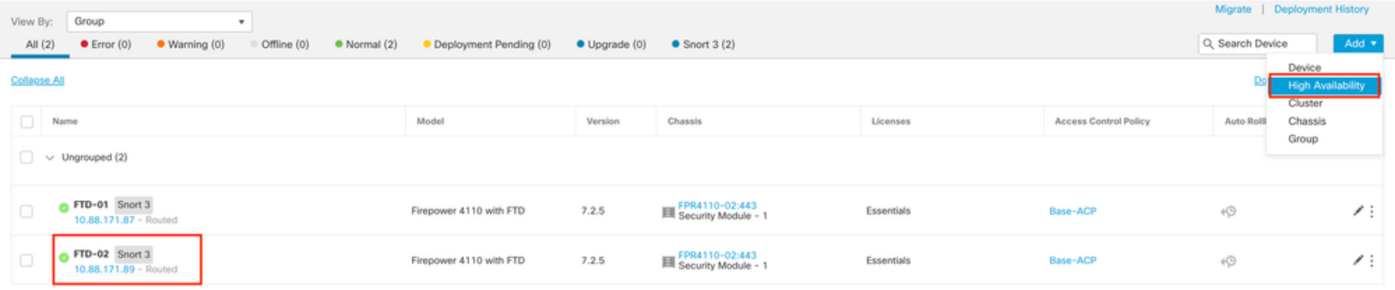
Advanced

Unique NAT ID:†

☑ Transfer Packets

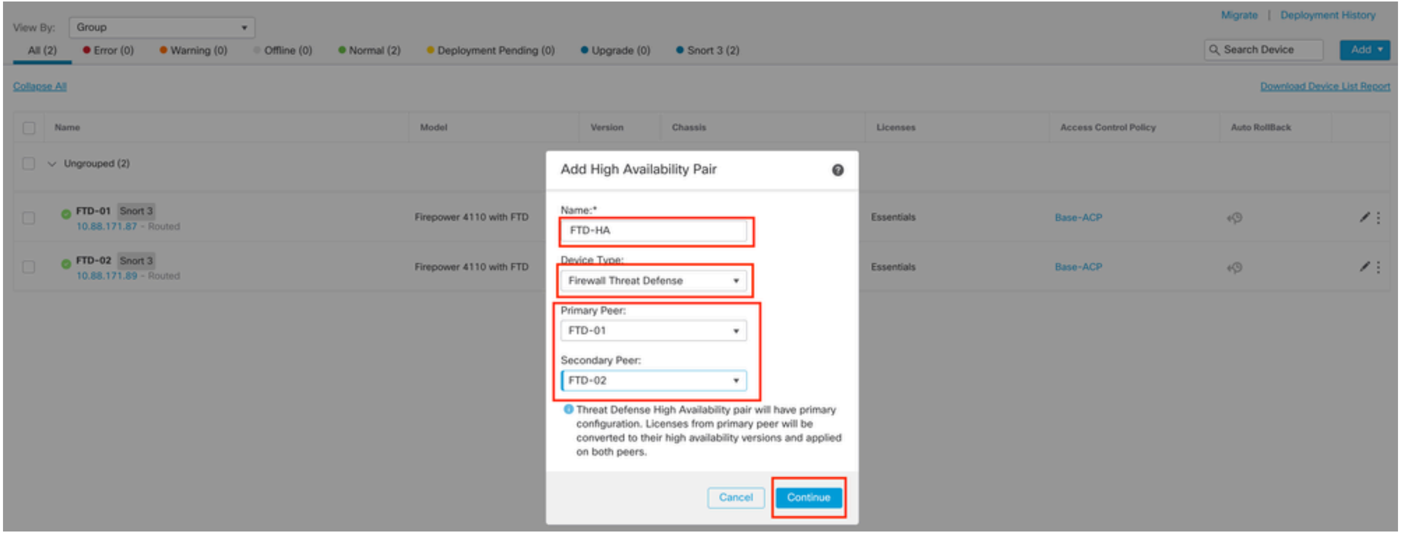
步骤5.创建高可用性。

5.1导航到Devices > Device Management > Add，然后单击High Availability选项。


Migrate | Deployment History
View By: Group
All (2) Error (0) Warning (0) Offline (0) Normal (2) Deployment Pending (0) Upgrade (0) Snort 3 (2)
Search Device
Add
Collapse All
Device
High Availability
Cluster
Chassis
Group

Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack
Ungrouped (2)						
FTD-01 Snort 3 10.88.171.87 - Routed	Firepower 4110 with FTD	7.2.5	FPR4110-02:443 Security Module - 1	Essentials	Base-ACP	
FTD-02 Snort 3 10.88.171.89 - Routed	Firepower 4110 with FTD	7.2.5	FPR4110-02:443 Security Module - 1	Essentials	Base-ACP	

5.2.配置添加高可用性对。配置Name、Device Type，选择FTD-01作为Primary Peer，选择FTD-02作为Secondary Peer，然后单击Continue。



Add High Availability Pair

Name:* FTD-HA

Device Type: Firewall Threat Defense

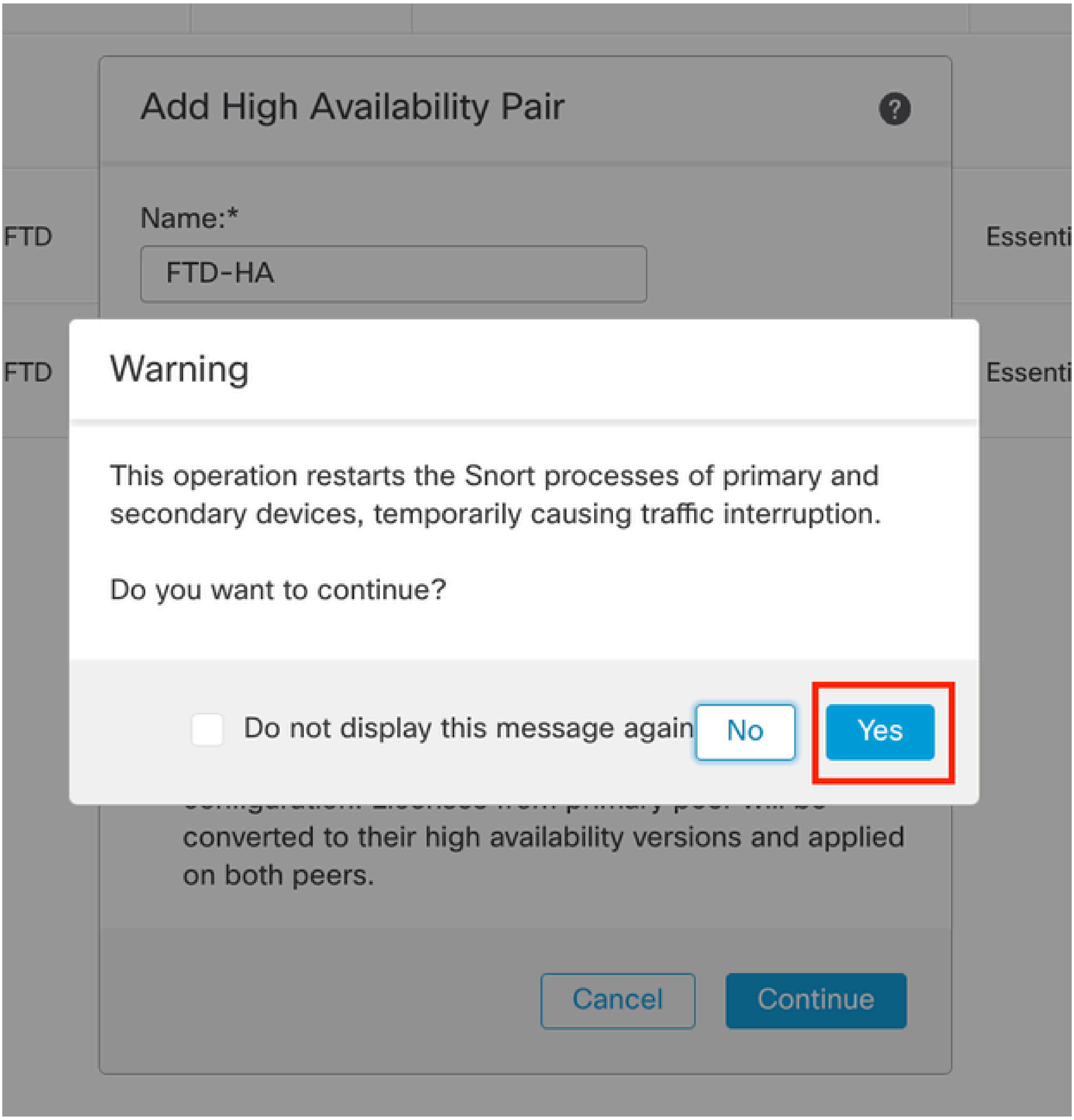
Primary Peer: FTD-01

Secondary Peer: FTD-02

Threat Defense High Availability pair will have primary configuration. Licenses from primary peer will be converted to their high availability versions and applied on both peers.

注意：请记住选择主设备作为仍具有配置的设备，在本例中为FTD-01。

5.3.确认创建高可用性，然后单击Yes。



Add High Availability Pair

Name:*

FTD-HA

Warning

This operation restarts the Snort processes of primary and secondary devices, temporarily causing traffic interruption.

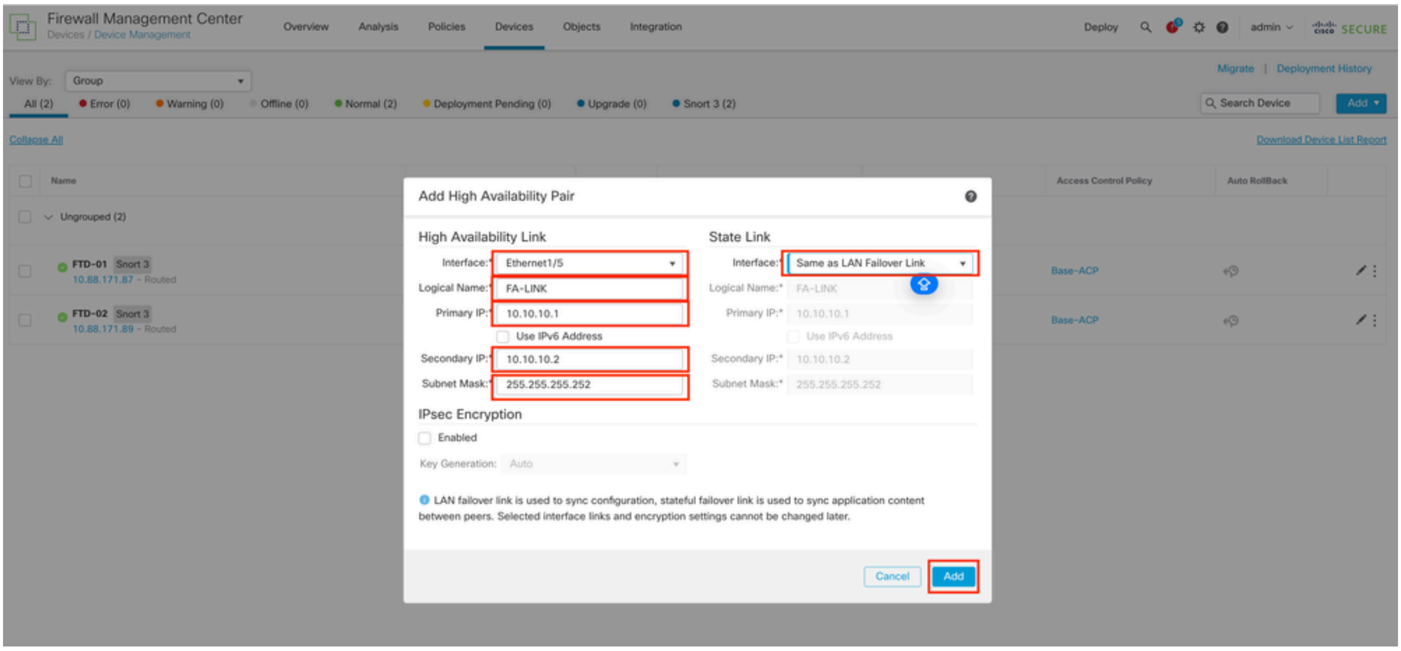
Do you want to continue?

□ Do not display this message again

converted to their high availability versions and applied on both peers.

注意：配置高可用性会重新启动两台设备的snort引擎，这可能会造成流量中断。

5.4.配置步骤2中介绍的高可用性参数，然后单击Add选项：



Add High Availability Pair

High Availability Link

- Interface:* Ethernet1/5
- Logical Name:* FA-LINK
- Primary IP:* 10.10.10.1
- □ Use IPv6 Address
- Secondary IP:* 10.10.10.2
- Subnet Mask:* 255.255.255.252

State Link

- Interface:* Same as LAN Failover Link
- Logical Name:* FA-LINK
- Primary IP:* 10.10.10.1
- □ Use IPv6 Address
- Secondary IP:* 10.10.10.2
- Subnet Mask:* 255.255.255.252

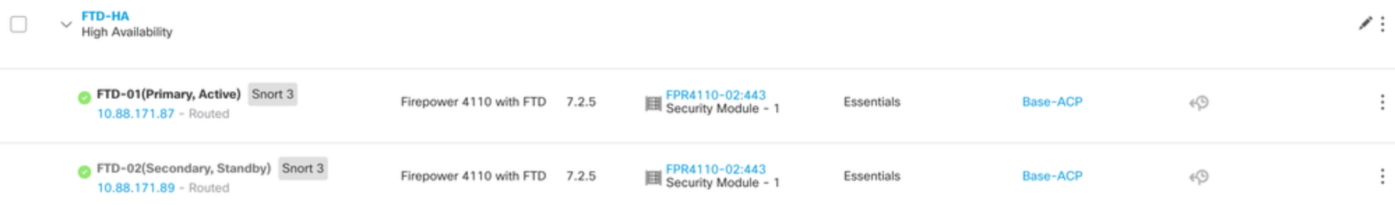
IPsec Encryption

- □ Enabled
- Key Generation: Auto

LAN failover link is used to sync configuration, stateful failover link is used to sync application content between peers. Selected interface links and encryption settings cannot be changed later.

Cancel | Add

6. FTD高可用性配置现已完成：



FTD-HA High Availability						
FTD-01(Primary, Active) Snort 3 10.88.171.87 - Routed	Firepower 4110 with FTD	7.2.5	FPR4110-02:443 Security Module - 1	Essentials	Base-ACP	
FTD-02(Secondary, Standby) Snort 3 10.88.171.89 - Routed	Firepower 4110 with FTD	7.2.5	FPR4110-02:443 Security Module - 1	Essentials	Base-ACP	

注意：如果不配置虚拟MAC地址，您需要清除相连路由器上的ARP表，以便在更换主设备时恢复流量。有关详细信息，请参阅高可用性中的MAC地址和IP地址。

相关信息

- 思科技术支持和下载

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）。