

ハイアベイラビリティのセキュアファイアウォール脅威対策における障害ユニットの交換

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[はじめる前に](#)

[障害のあるユニットの特定](#)

[障害のあるユニットをバックアップと交換する](#)

[バックアップを取らない故障したユニットの交換](#)

[関連情報](#)

はじめに

このドキュメントでは、ハイアベイラビリティ(HA)設定の一部である、障害のあるセキュアファイアウォール脅威対策(SFR)モジュールを交換する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco Secure Firewall Management Center(FMC)
- Cisco Firepower eXtensibleオペレーティングシステム(FXOS)
- Cisco Secure Firewall Threat Defense(FTD)

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Firepower 4110はFXOS v2.12(0.498)を実行
- Cisco Secure Firewall v7.2.5を実行する論理デバイス
- Secure Firewall Management Center 2600がv7.4を実行
- Secure Copy Protocol(SCP)の知識

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明





この手順はアプライアンスでサポートされています。

- Cisco Secure Firewall 1000シリーズアプライアンス
- Cisco Secure Firewall 2100シリーズアプライアンス
- Cisco Secure Firewall 3100シリーズアプライアンス
- Cisco Secure Firewall 4100シリーズアプライアンス
- Cisco Secure Firewall 4200シリーズアプライアンス
- Cisco Secure Firewall 9300アプライアンス
- VMware向けCisco Secure Firewall Threat Defense

はじめる前に

このドキュメントでは、新しいユニットが同じFXOSおよびFTDバージョンで設定されている必要があります。

障害のあるユニットの特定

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	↔	⋮

このシナリオでは、セカンダリユニット(FTD-02)は障害状態です。

障害のあるユニットをバックアップと交換する

この手順を使用して、プライマリユニットまたはセカンダリユニットを交換できます。このガイドでは、交換しようとしている故障したユニットのバックアップがあることを前提としています。

ステップ 1 : FMCからバックアップファイルをダウンロードします。System > Tools > Restore > Device Backupsの順に移動し、正しいバックアップを選択します。Downloadをクリックします。

The screenshot shows the FMC interface with the following details:

- Page Title: Firewall Management Center
- Breadcrumbs: System / Tools / Backup/Restore / Backup Management
- Navigation: Overview, Analysis, Policies, Devices, Objects, Integration, Deploy
- Buttons: Firewall Management Backup, Managed Device Backup, Upload Backup
- Section: Firewall Management Backups
- Table Headers: System Information, Date Created, File Name, VDB Version, Location, Size (MB), Configurations, Events, TID
- Storage Location: /var/sf/backup/ (Disk Usage: 8%)
- Section: Device Backups
- Table Headers: System Information, Date Created, File Name, VDB Version, Location, Size (MB), Configurations, Events, TID
- Table Data:

System Information	Date Created	File Name	VDB Version	Location	Size (MB)	Configurations	Events	TID
<input checked="" type="checkbox"/> 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
<input type="checkbox"/> 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
- Buttons: Download, Delete, Move

ステップ 2 : 新しいFTDの/var/sf/backup/ディレクトリにFTDバックアップをアップロードします。

2.1 test-pc (SCPクライアント) から、/var/tmp/ディレクトリにあるFTDにバックアップファイルをアップロードします。

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

2.2 FTD CLIエキスパートモードから、バックアップファイルを/var/tmp/から/var/sf/backup/に移動します。

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

ステップ 3 : clishモードで次のコマンドを適用して、FTD-02バックアップを復元します。

```
>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
```

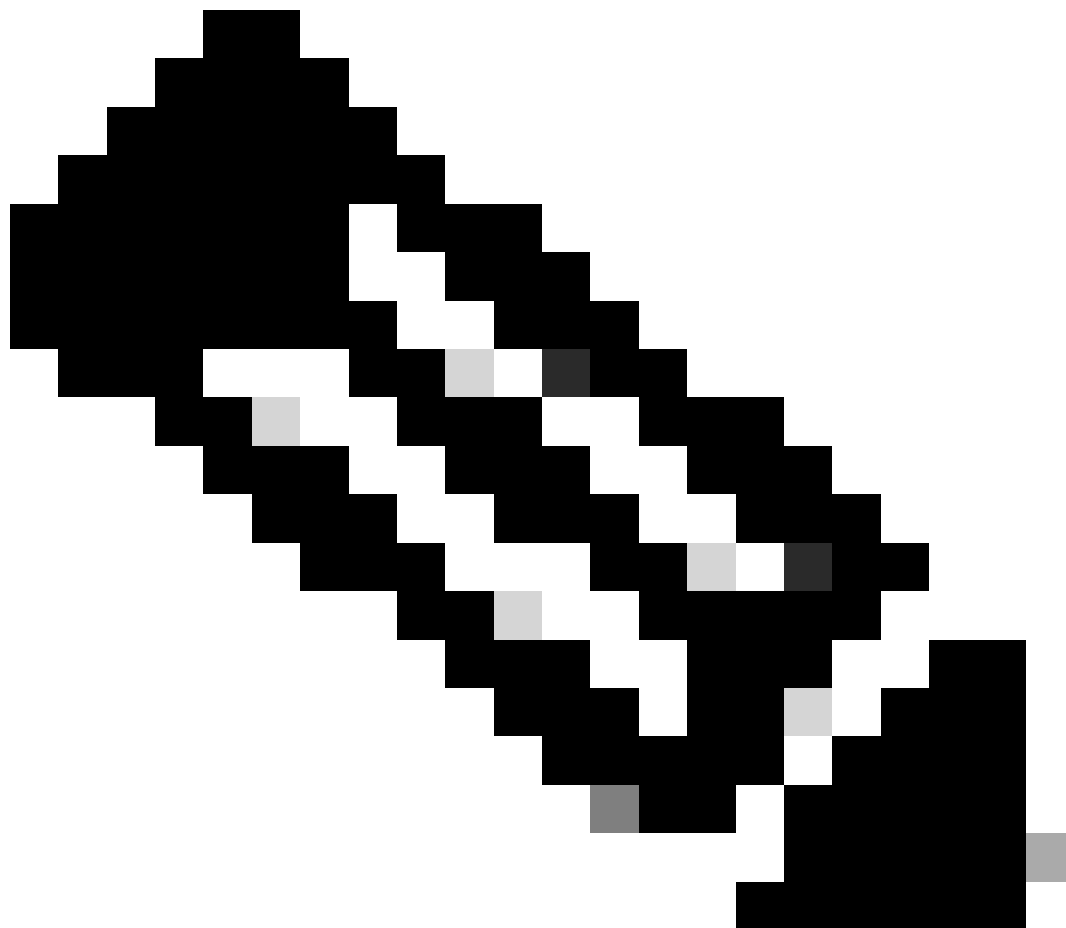
```
Added table rna_vuln with table_id 22
```

```
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：復元が完了すると、デバイスによってCLIからログアウトされ、リブートして、自動的にFMCに接続されます。この時点で、デバイスは古く表示されます。

ステップ 4： HA同期を再開します。FTD CLIから、`configure high-availability resume`と入力します。

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

FTDハイアベイラビリティの設定が完了しました。

Device Name	Role	Model	Version	Security Module	License	Configuration
FTD-01(Primary, Active)	Snort 3	Firepower 4110 with FTD	7.2.5	FPR4110-02:443 Security Module - 1	Essentials	Base-ACP
FTD-02(Secondary, Standby)	Snort 3	Firepower 4110 with FTD	7.2.5	FPR4110-02:443 Security Module - 1	Essentials	Base-ACP

バックアップを取らない故障したユニットの交換

障害が発生したデバイスのバックアップがない場合は、このガイドに進むことができます。プライマリユニットまたはセカンダリユニットを交換できます。プロセスは、デバイスがプライマリかセカンダリかによって異なります。このガイドで説明するすべての手順は、障害のあるセカンダリユニットの復旧です。障害のあるプライマリユニットを復元する場合は、ステップ5で、既存のセカンダリ/アクティブユニットをプライマリデバイスとして使用し、登録時に交換用デバイスをセカンダリ/スタンバイデバイスとして使用して、ハイアベイラビリティを設定します。

ステップ 1 : Device > Device Managementの順に移動して、ハイアベイラビリティ設定のスクリーンショット (バックアップ) を取得します。正しいFTD HAペアを編集し (鉛筆アイコンをクリック) 、High Availabilityオプションをクリックします。

FTD-HA Save Cancel

Cisco Firepower 4110 Threat Defense

Summary **High Availability** Device Routing Interfaces Inline Sets DHCP VTEP

High Availability Configuration

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

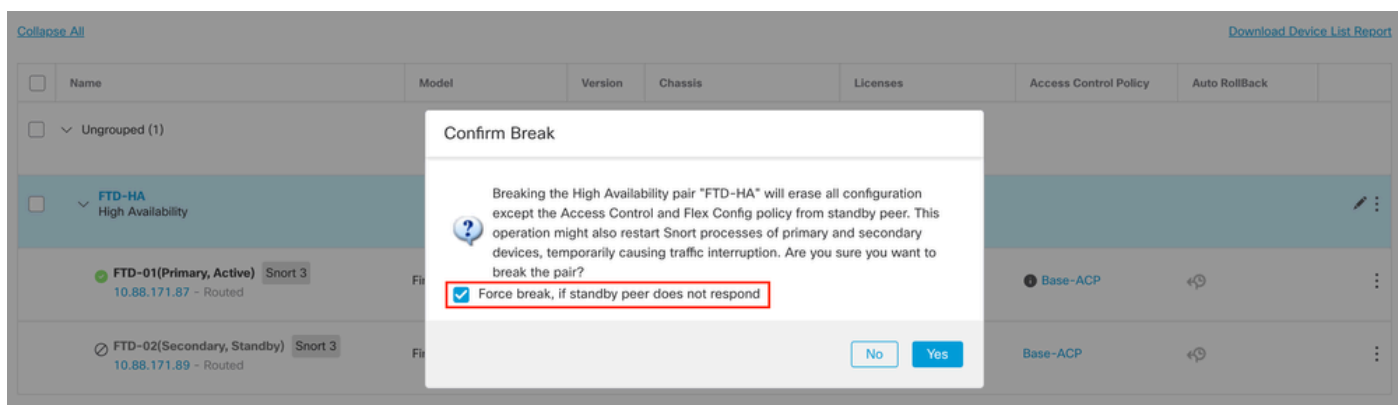
Interface MAC Addresses		
Physical Interface	Active Mac Address	Standby Mac Address
No records to display		

ステップ 2 : HAを切断します。

2.1 Devices > Device Managementの順に選択し、右上隅にある3つのドットメニューをクリックします。Breakオプションをクリックします。



2.2. Force break, if standby peer does not respondオプションを選択します。





注：ユニットが応答しないため、HAを強制的に切断する必要があります。ハイアベイラビリティペアを解除すると、アクティブなデバイスでは展開済みの機能がすべて保持されます。スタンバイデバイスは、フェールオーバーとインターフェイスの設定を失い、スタンドアロンデバイスになります。

ステップ 3：障害のあるFTDを削除します。置き換えるFTDを特定し、3つのドットで構成されるメニューをクリックします。Deleteをクリックします。

<input type="checkbox"/>	Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack	
<input type="checkbox"/>	Ungrouped (2)							
<input type="checkbox"/>	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		
<input type="checkbox"/>	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		<ul style="list-style-type: none"> Delete Packet Tracer Packet Capture Revert Upgrade Health Monitor Troubleshoot Files

ステップ 4 : 新しいFTDを追加します。

4.1. Devices > Device Management > Addの順に選択し、Deviceをクリックします。

<input type="checkbox"/>	Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto Roll	
<input type="checkbox"/>	Ungrouped (1)							
<input type="checkbox"/>	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		<ul style="list-style-type: none"> Device High Availability Cluster Chassis Group

4.2.プロビジョニング方式を選択します。この場合は、登録キー、設定ホスト、表示名、および登録キーです。アクセスコントロールポリシーを設定し、Registerをクリックします。

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:†

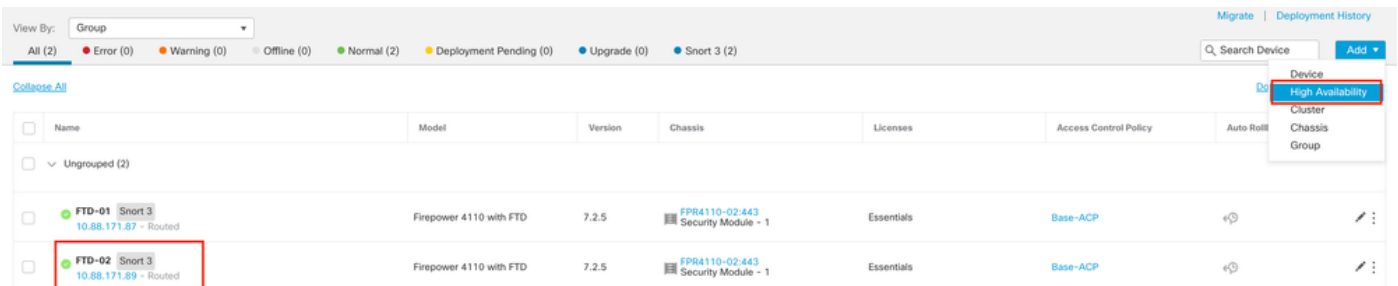
Transfer Packets

Cancel

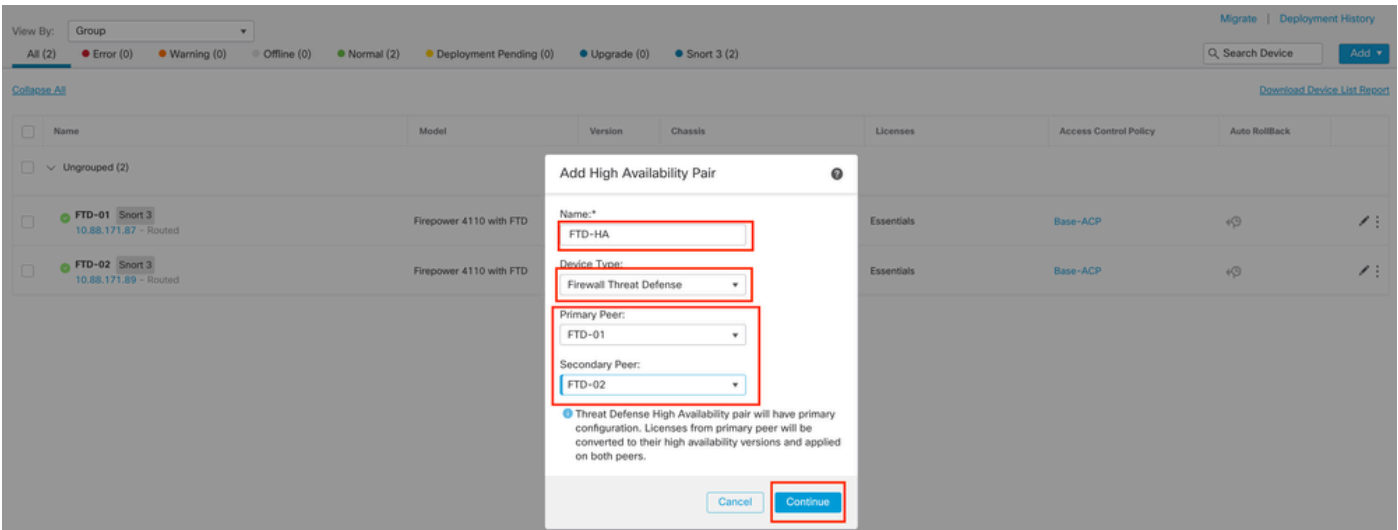
Register

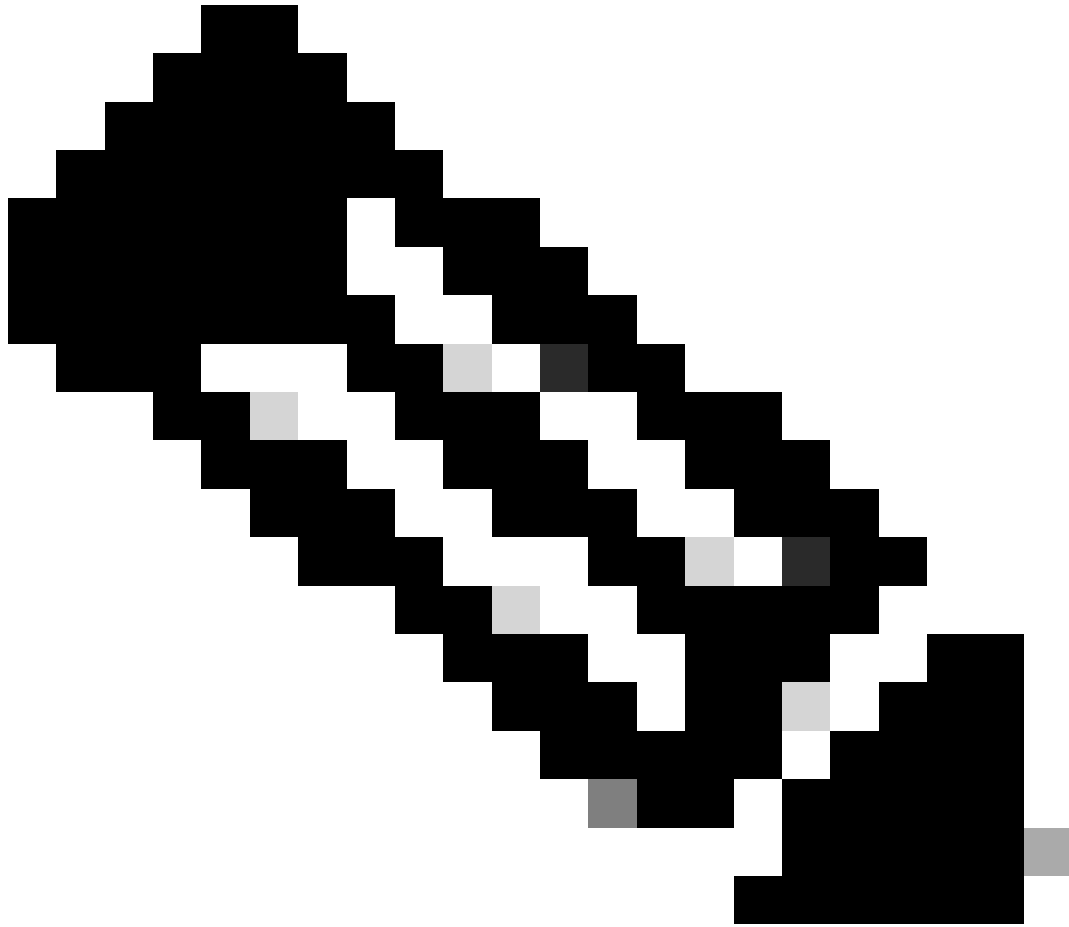
ステップ 5 : HAを作成します。

5.1 Devices > Device Management > Addの順に移動し、High Availabilityオプションをクリックします。



5.2.ハイアベイラビリティペアの追加を設定する。名前、デバイスタイプを設定し、プライマリピアとしてFTD-01を、セカンダリピアとしてFTD-02を選択して、Continueをクリックします。





注：まだ設定が行われているデバイス（この場合はFTD-01）としてプライマリユニット (PU)を選択することを忘れないでください。

5.3. HAの作成を確認し、Yesをクリックします。

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

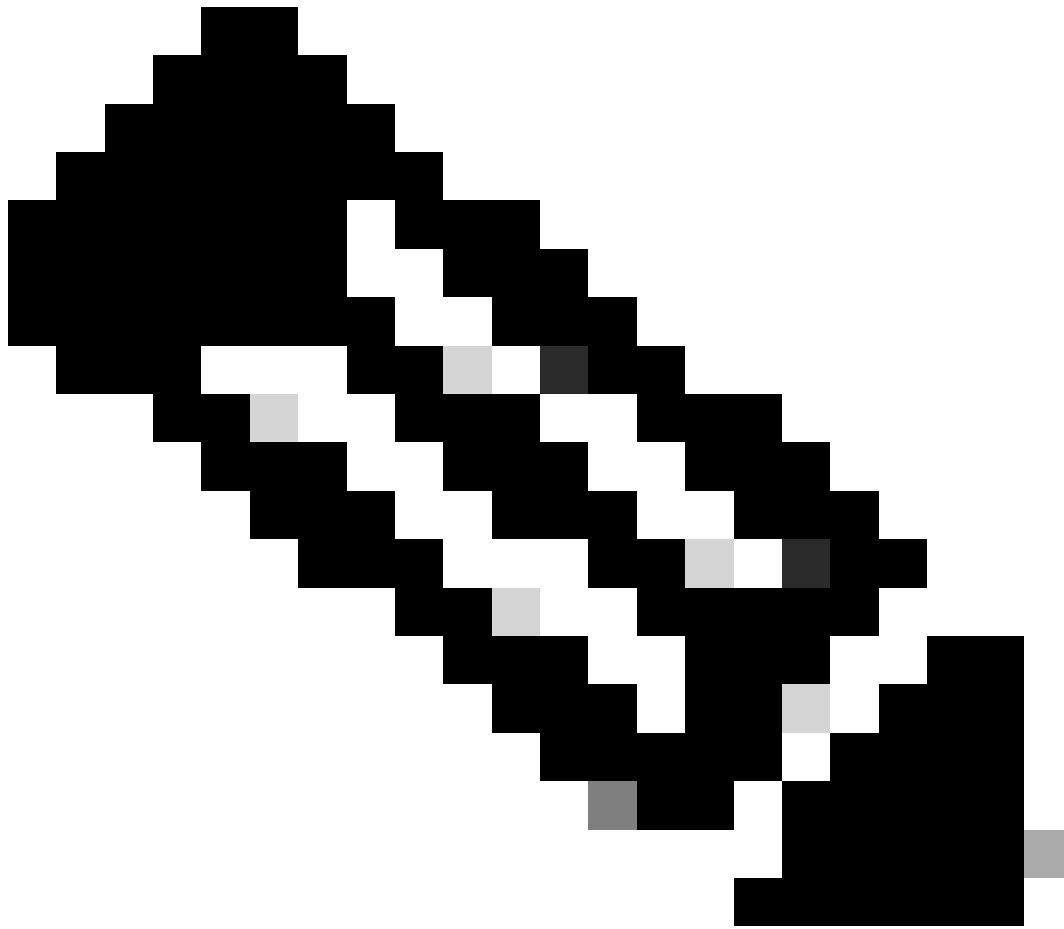
No

Yes

Configuration changes from primary peer will be converted to their high availability versions and applied on both peers.

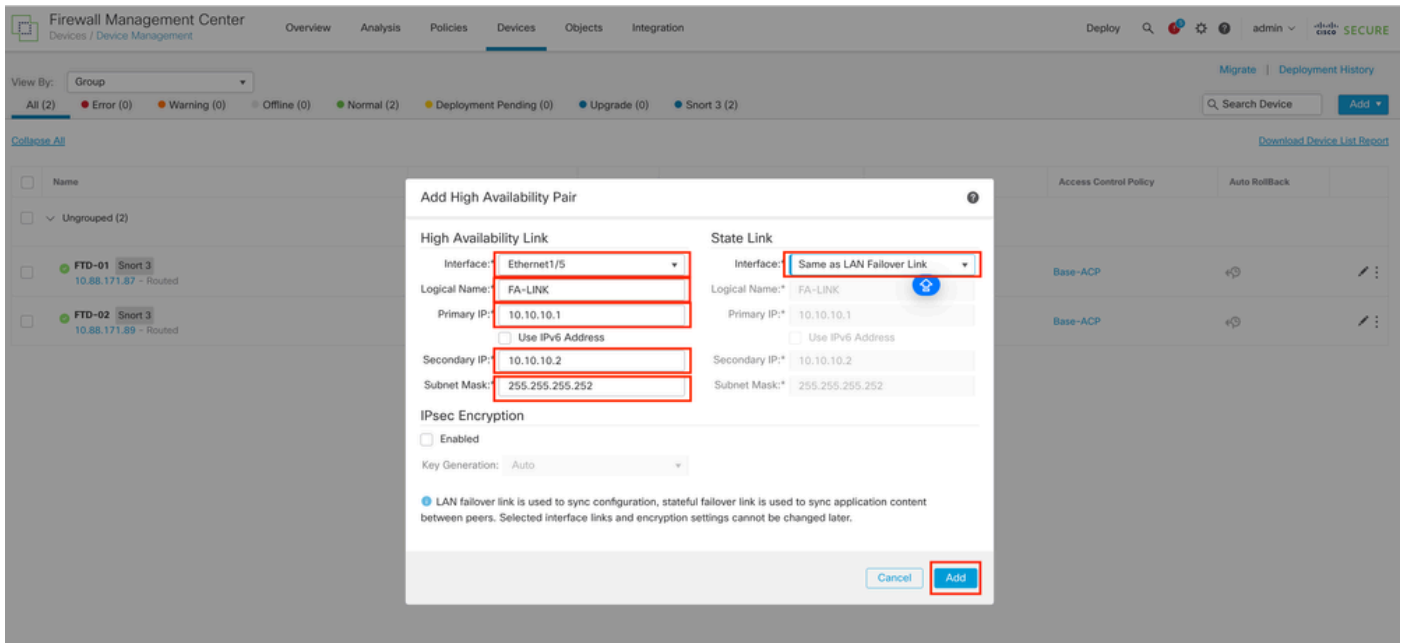
Cancel

Continue



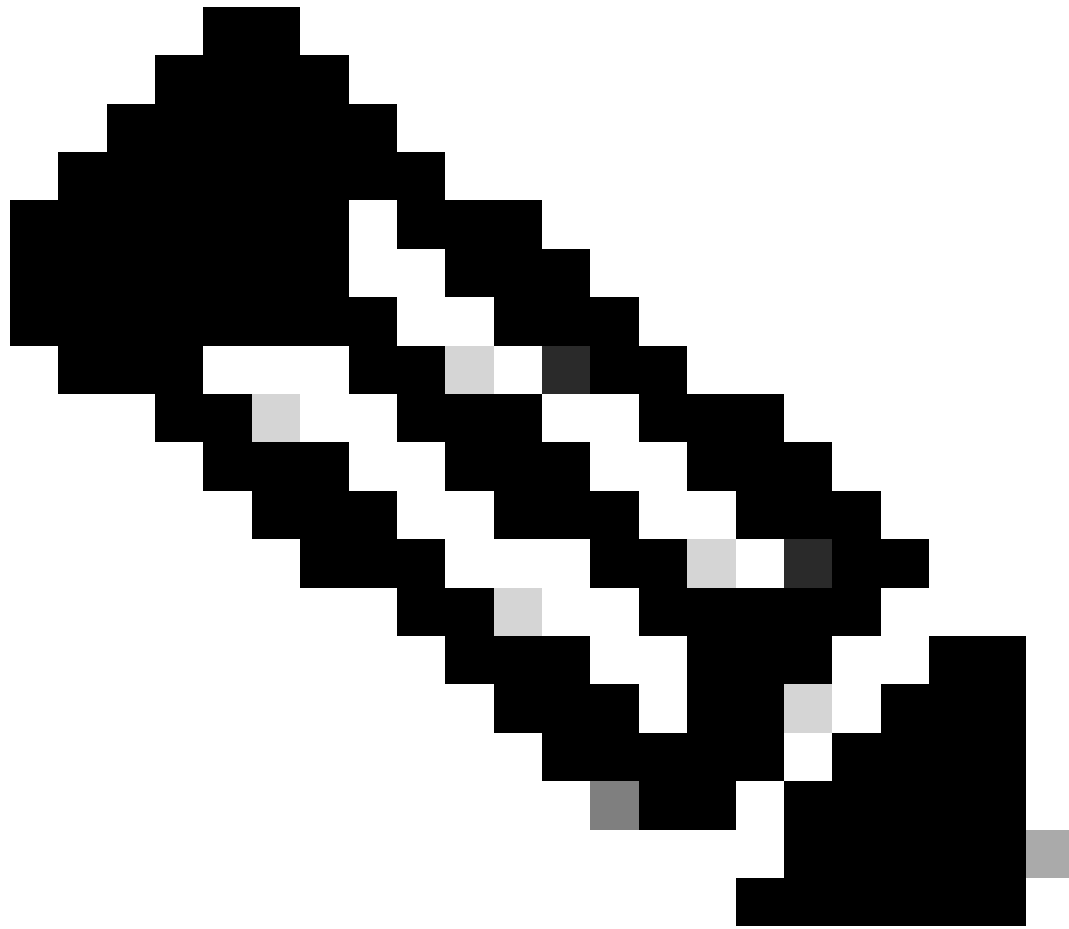
注：ハイアベイラビリティを設定すると、両方のユニットのSnortエンジンが再起動するため、トラフィックが中断される可能性があります。

5.4.ステップ2で取得したハイアベイラビリティパラメータを設定し、Addオプションをクリックします。



6. FTDハイアベイラビリティ(HA)の設定が完了しました。

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：仮想MACアドレスを設定しない場合、プライマリユニットの交換時にトラフィックフローを復元するために、接続されたルータでARPテーブルをクリアする必要があります。詳細については、「[ハイアベイラビリティにおけるMACアドレスおよびIPアドレス](#)」を参照してください。

関連情報

- [シスコのテクニカルサポートとダウンロード](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。