ハイアベイラビリティでのSecure Firewall Device Managerの設定

内容

概要

このドキュメントでは、セキュアファイアウォールデバイスでSecure Firewall Device Manager(FDM)ハイアベイラビリティ(HA)を設定および確認する方法について説明します。

前提条件

要件

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。

- Cisco Secure Firewall 2100セキュリティアプライアンスX 2
- FDMバージョン7.0.5（ビルド72）の実行

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。

タスク 1.条件の確認

タスク要件：

両方のFDMアプライアンスがノートの要件を満たし、HAユニットとして構成できることを確認します。

ソリューション：

ステップ 1：SSHを使用してアプライアンスの管理IPに接続し、モジュールハードウェアを確認します。

show versionコマンドを使用して、プライマリデバイスのハードウェアとソフトウェアのバージョンを確認します。

```
> show version
-------------------[ FPR2130-1 ]--------------------
Model : Cisco Firepower 2130 Threat Defense (77) Version 7.0.5 (Build 72)
UUID : 6197946e-2747-11ee-9b20-ead7c72f2631
VDB version : 338
----------------------------------------------------
```

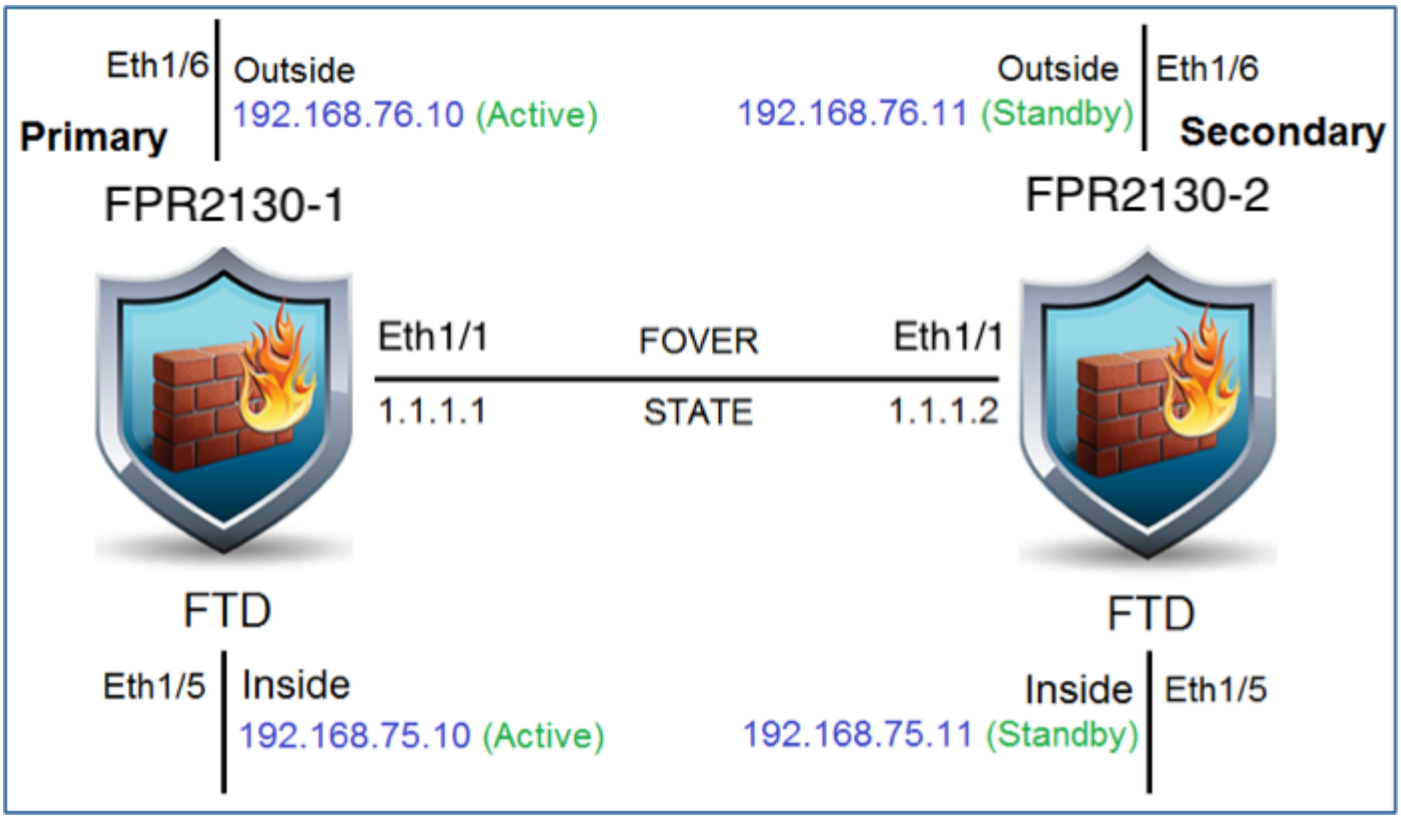
セカンダリデバイスのハードウェアとソフトウェアのバージョンを確認します。

```
> show version
-------------------[ FPR2130-2 ]--------------------
Model : Cisco Firepower 2130 Threat Defense (77) Version 7.0.5 (Build 72)
UUID : 6ba86648-2749-11ee-b7c9-c9e434a6c9ab
VDB version : 338
----------------------------------------------------
```

タスク 2.ハイアベイラビリティでのSecure Firewall Device Managerの設定

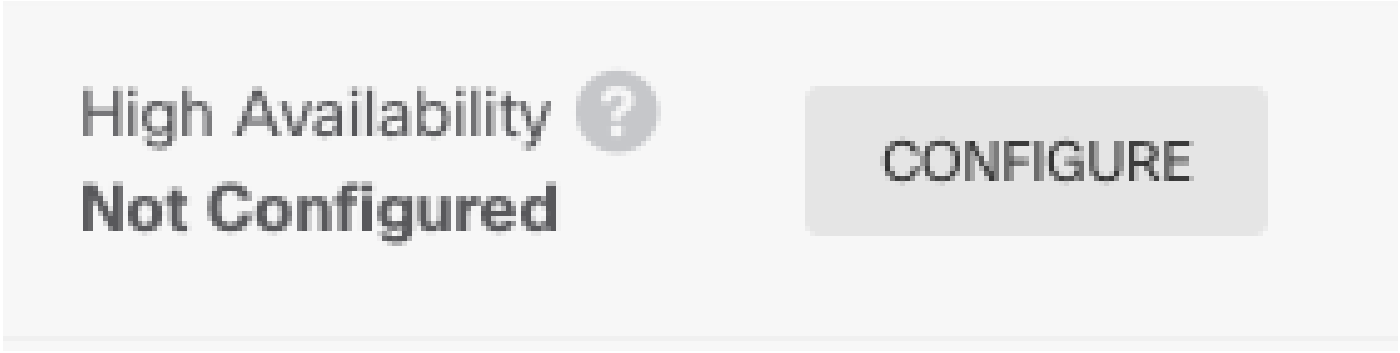
ネットワーク図

次の図に従って、アクティブ/スタンバイのハイアベイラビリティ(HA)を設定します。

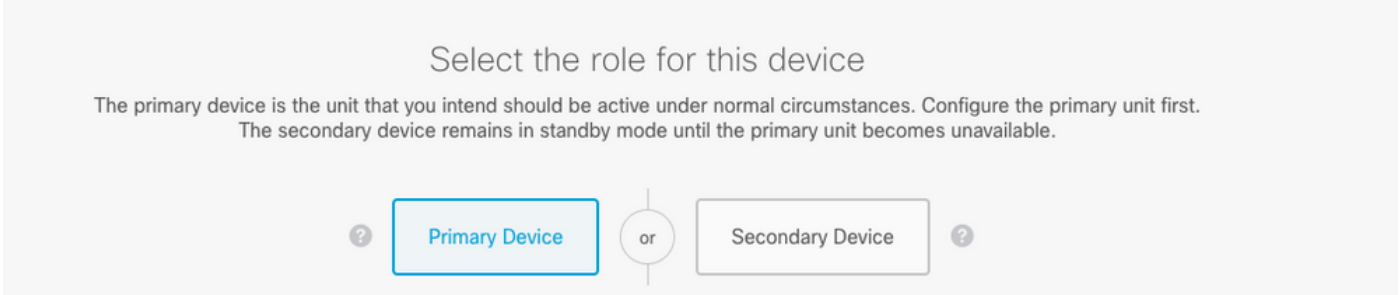


プライマリユニットのSecure Firewall Device Managerでハイアベイラビリティを有効にする

ステップ 1：FDMフェールオーバーを設定するには、Deviceに移動し、High Availabilityグループの横にあるConfigureをクリックします。



ステップ 2：High Availabilityページで、Primary Deviceボックスをクリックします。

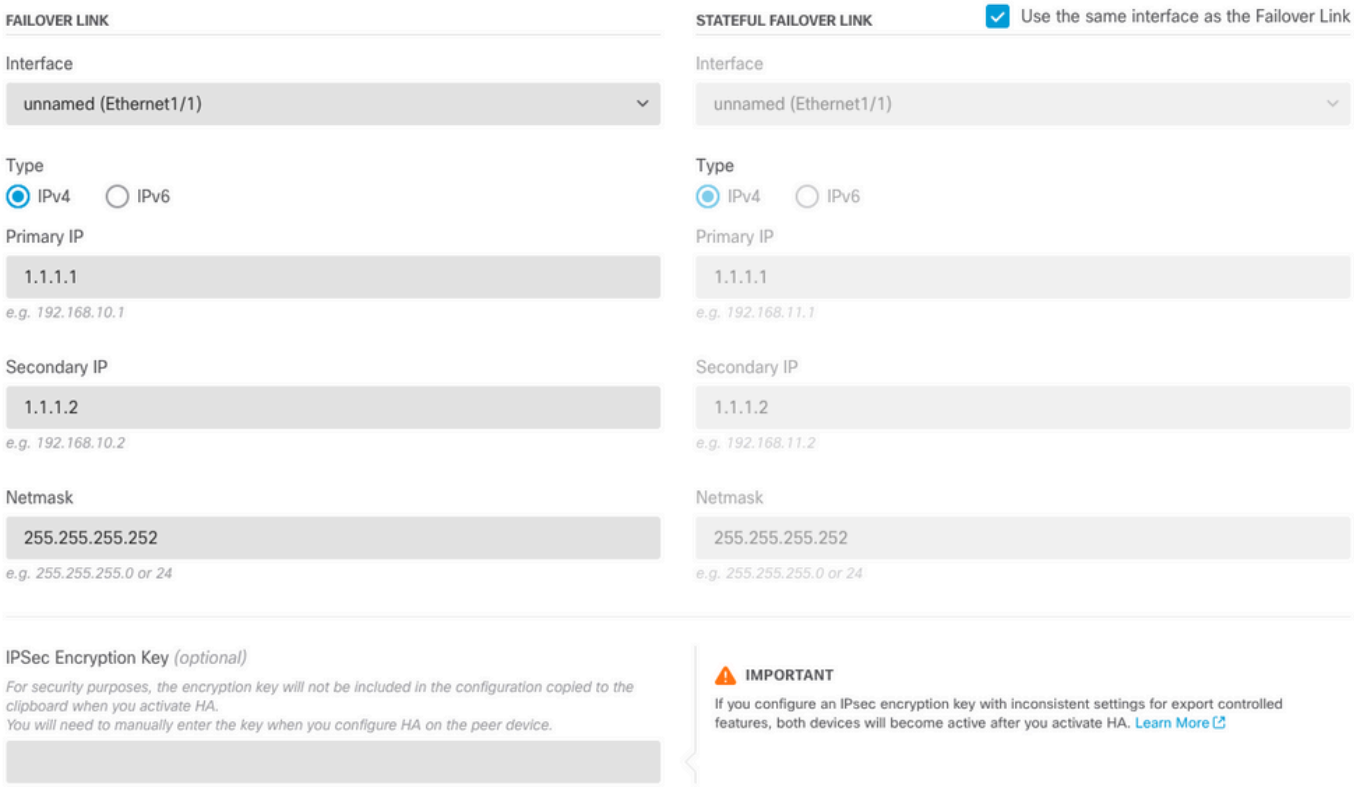


警告:プライマリユニットとして正しいユニットを選択してください。選択したプライマリ

ユニットのすべての設定が、選択したセカンダリFTDユニットに複製されます。複製の結果、セカンダリユニットの現在の設定は置き換えられます。

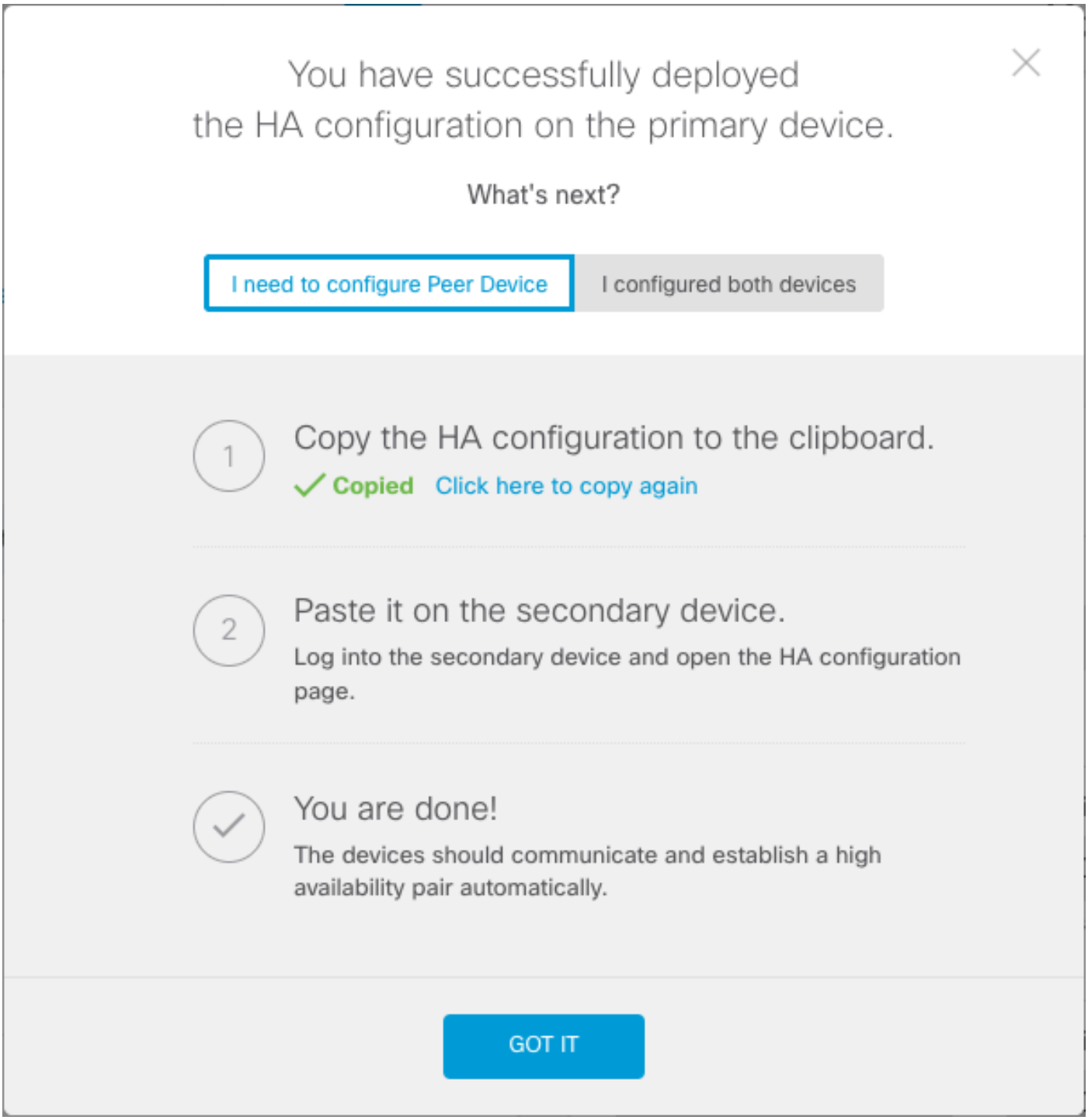
ステップ 3：フェールオーバーリンクとステートリンクの設定を行います。

この例では、ステートリンクはフェールオーバーリンクと同じ設定になっています。



ステップ 4：Activate HAをクリックします。

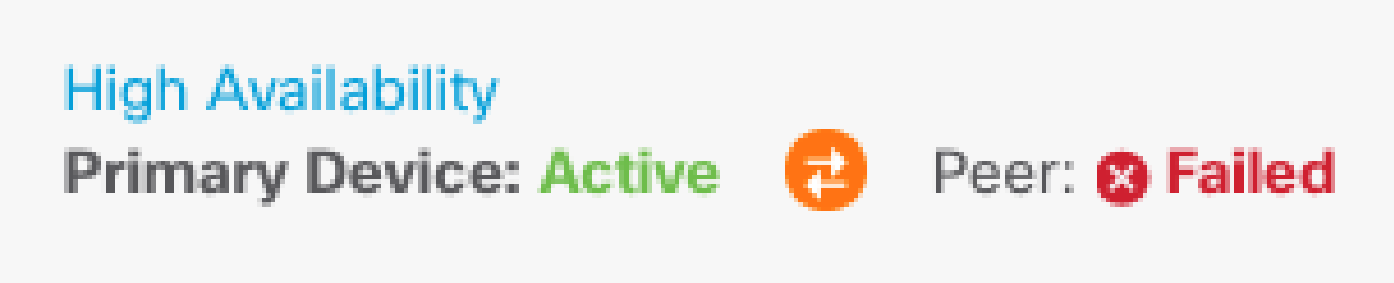
ステップ 5：HA設定を確認メッセージのクリップボードにコピーして、セカンダリユニットに貼り付けます。



システムは即座に設定をデバイスに展開します。導入ジョブを開始する必要はありません。設定が保存され、展開が進行中であることを示すメッセージが表示されない場合は、ページの上部までスクロールしてエラーメッセージを確認します。

設定もクリップボードにコピーされます。コピーを使用して、セカンダリユニットをすばやく設定できます。セキュリティを強化するため、クリップボードのコピーには暗号化キーは含まれません。

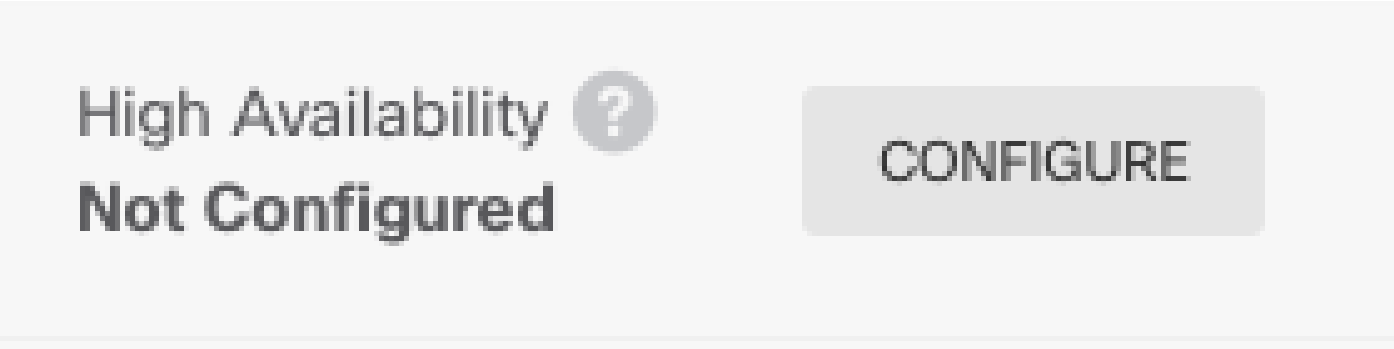
この時点で、High Availabilityページに移動していて、デバイスのステータスが「Negotiating」になっている必要があります。 ピアを設定する前でも、ステータスはActiveに移行する必要があります。ピアを設定するまでは、Failedとして表示される必要があります。



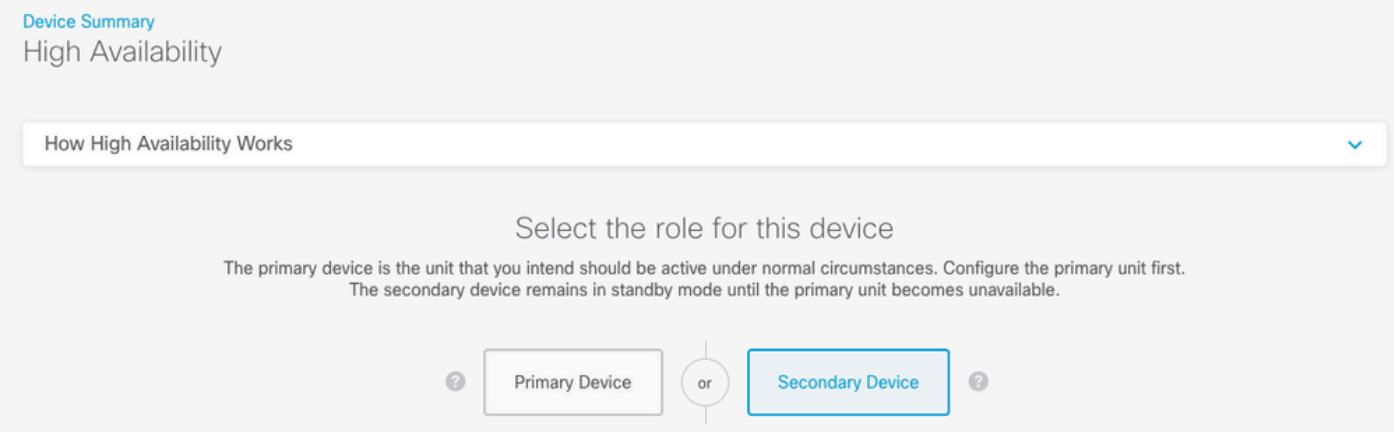
セカンダリユニットのSecure Firewall Device Managerでハイアベイラビリティを有効にする

プライマリデバイスをアクティブ/スタンバイハイアベイラビリティ用に設定した後で、セカンダリデバイスを設定する必要があります。そのデバイスでFDMにログインし、この手順を実行します。

ステップ 1：FDMフェールオーバーを設定するには、Deviceに移動し、High Availabilityグループの横にあるConfigureをクリックします。



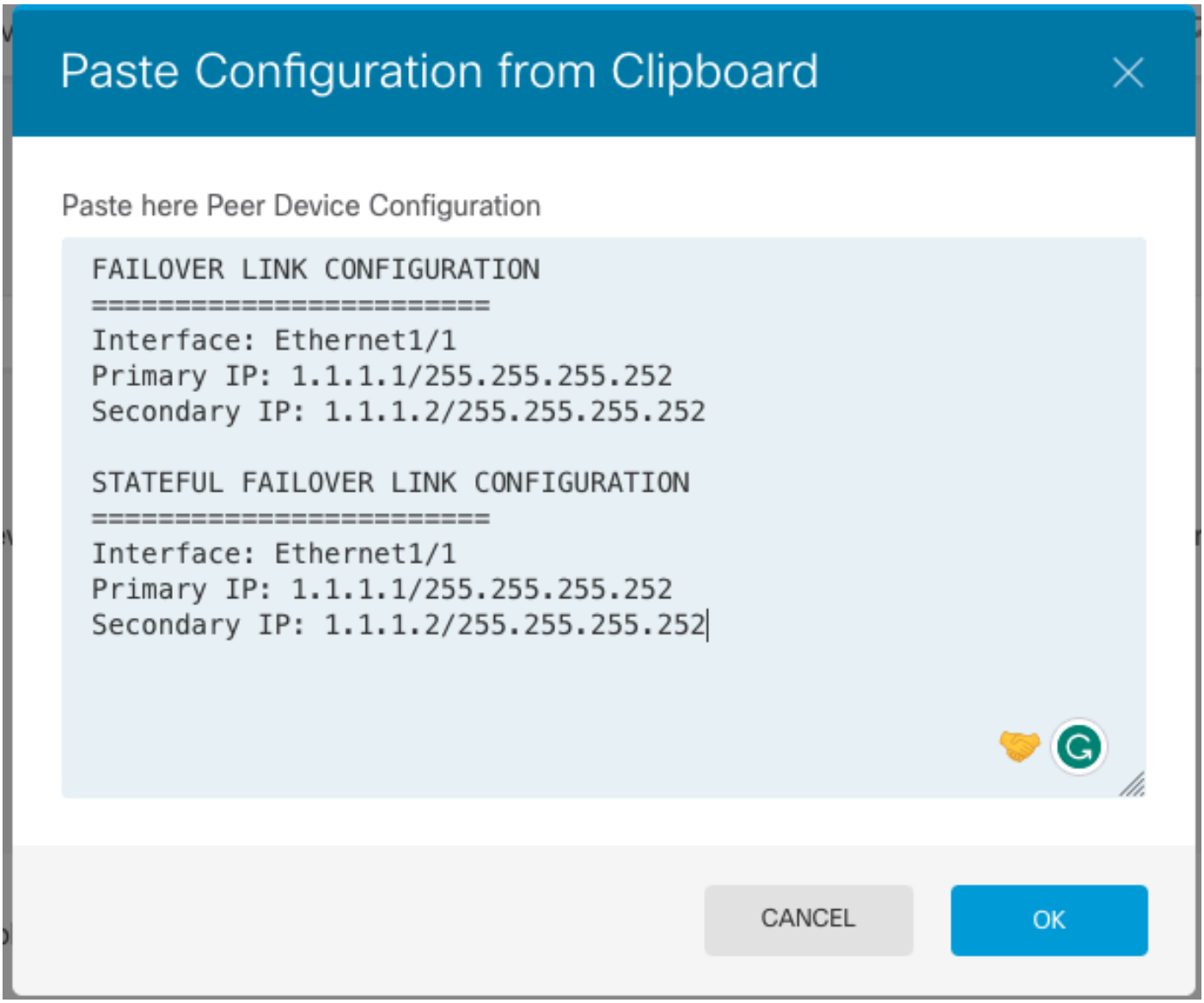
ステップ 2：[ハイアベイラビリティ]ページで、[セカンダリデバイス]ボックスをクリックします。



ステップ 3：次のオプションのいずれかを選択します。

- 簡単な方法:Paste from Clipboardボタンをクリックし、設定を貼り付けて、OKをクリックします。これにより、フィールドが適切な値で更新され、確認できます。
- 手動方式：フェールオーバーリンクとステートフルフェールオーバーリンクを直接設定しま

す。プライマリデバイスで入力したセカンダリデバイスとまったく同じ設定を入力します。



ステップ 4：Activate HAをクリックします

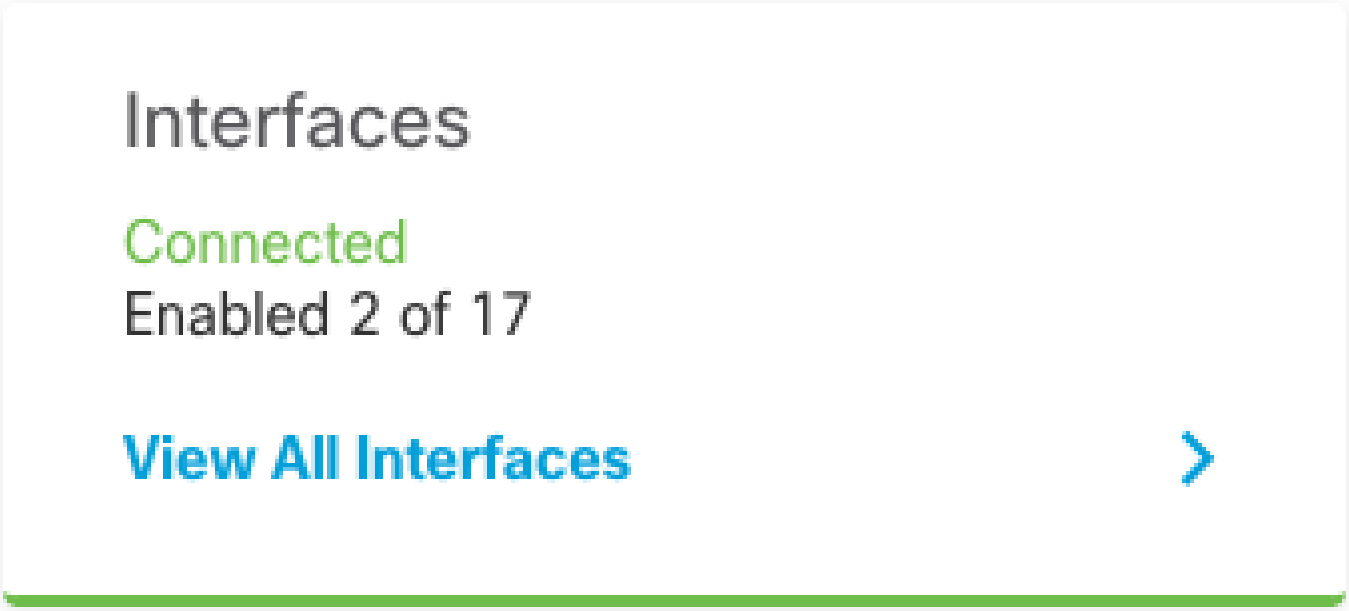
システムは即座に設定をデバイスに展開します。導入ジョブを開始する必要はありません。設定が保存され、展開が進行中であることを示すメッセージが表示されない場合は、ページの上部までスクロールしてエラーメッセージを確認します。

設定が完了すると、HAを設定したというメッセージが表示されます。Got Itをクリックしてメッセージを閉じます。

この時点で、High Availabilityページに移動し、デバイスのステータスに、これがセカンダリデバイスであることが示されている必要があります。プライマリデバイスとの参加が成功した場合、デバイスはプライマリと同期し、最終的にモードはスタンバイで、ピアはアクティブである必要があります。

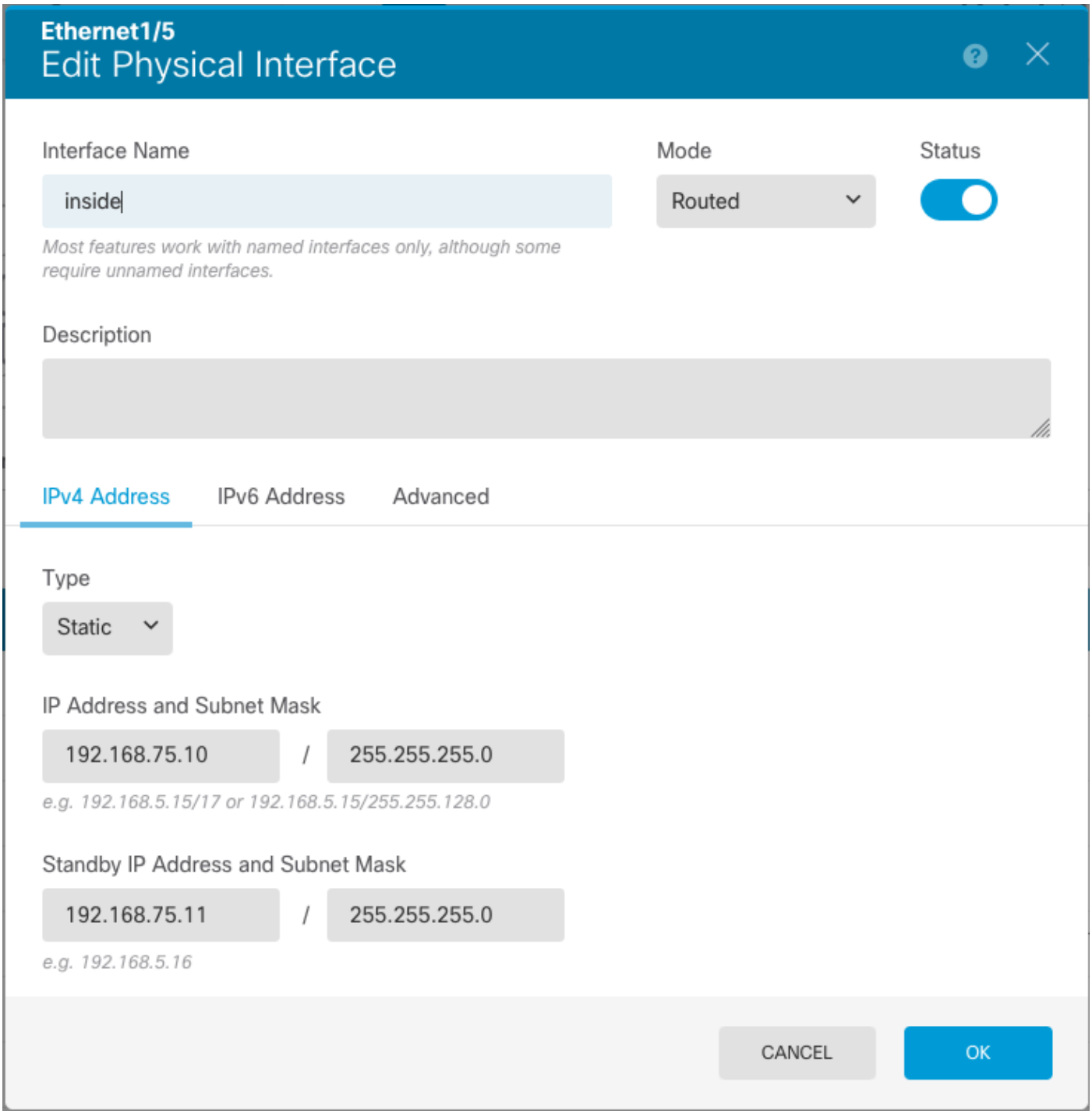
インターフェイスの設定を完了する

ステップ 1：FDMインターフェイスを設定するには、Deviceに移動し、View All Interfacesをクリックします。

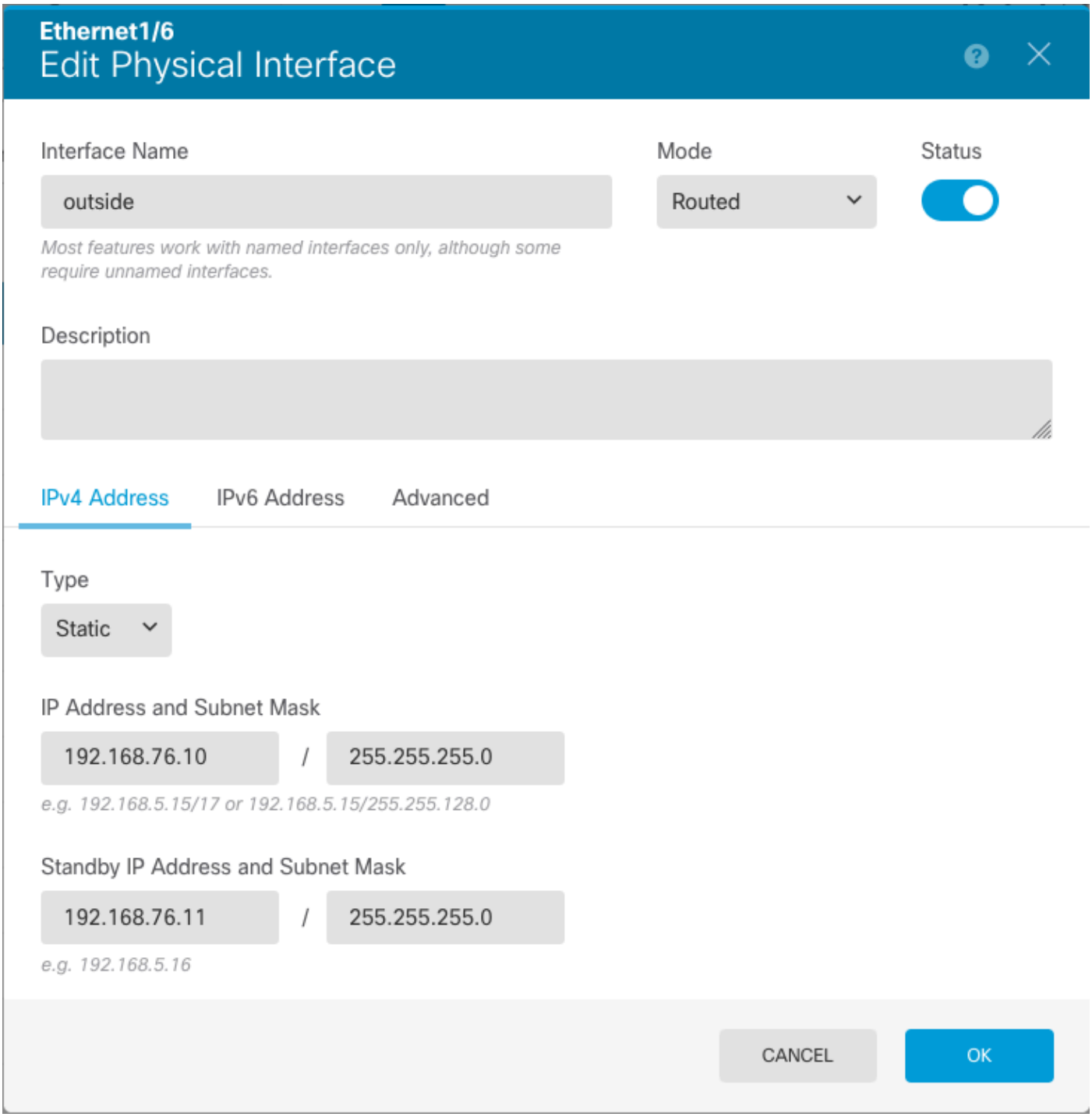


ステップ 2：図に示すように、インターフェイス設定を選択して編集します。

イーサネット1/5インターフェイス：



Ethernet 1/6インターフェイス



ステップ 3：変更を設定したら、Pending Changesをクリックします。今すぐ導入。

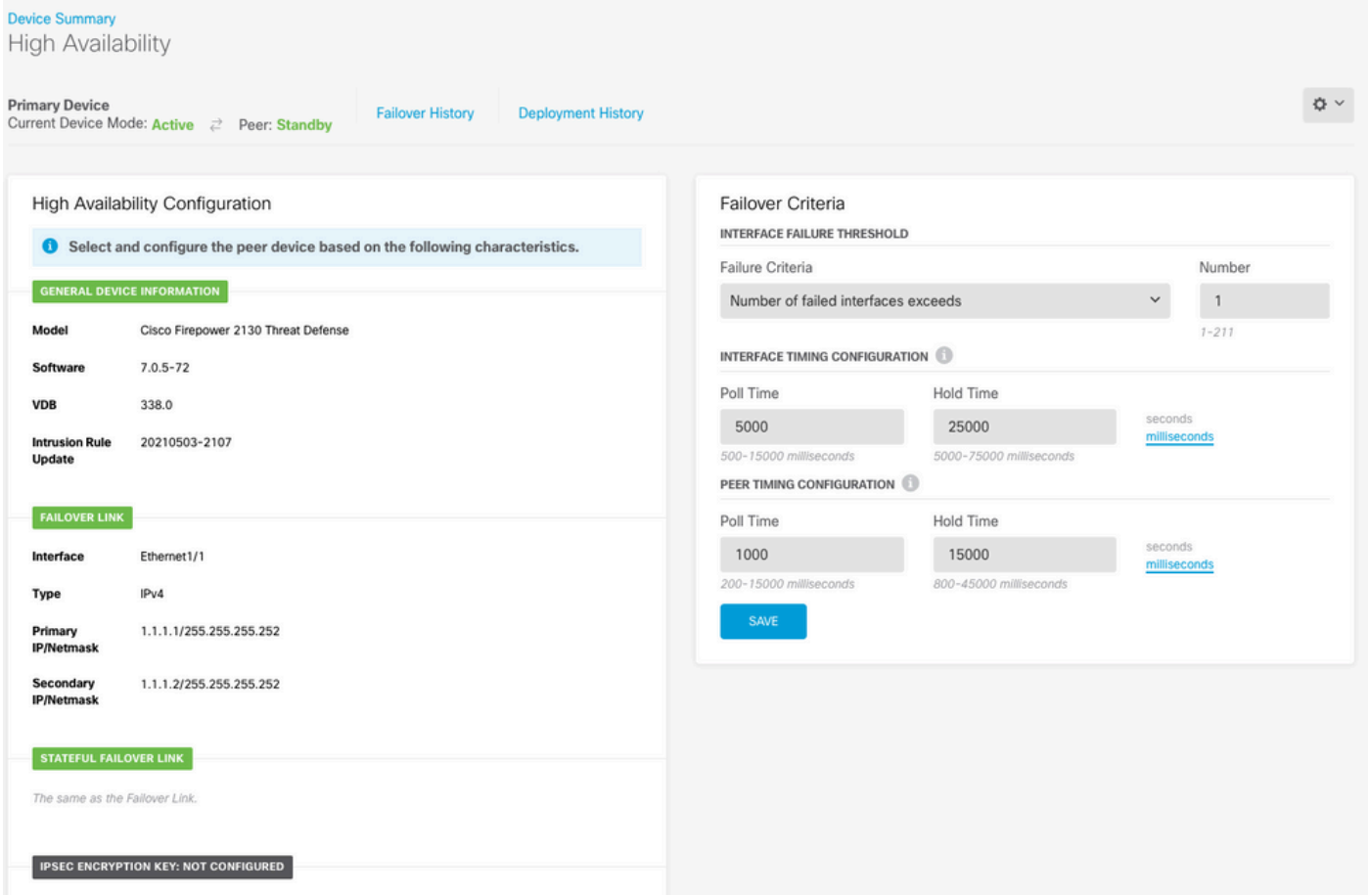
タスク 3.FDMの高可用性の確認

タスク要件：

FDM GUIおよびFDM CLIからハイアベイラビリティ設定を確認します。

ソリューション：

ステップ 1：Deviceに移動し、High Availability設定を確認します。



ステップ 2：SSHを使用してFDMプライマリデバイスのCLIに接続し、show high-availability configコマンドを使用して検証します。

```
> show high-availability config
Failover On
Failover unit Primary
Failover LAN Interface: failover-link Ethernet1/1 (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 4 of 1293 maximum
MAC Address Move Notification Interval not set
failover replication http
Version: Ours 9.16(4)200, Mate 9.16(4)200
Serial Number: Ours JAD231510ZT, Mate JAD2315110V
Last Failover at: 00:01:29 UTC Jul 25 2023
```

```
        This host: Primary - Active
                Active time: 4927 (sec)
                slot 0: FPR-2130 hw/sw rev (1.3/9.16(4)200) status (Up Sys)
                  Interface diagnostic (0.0.0.0): Normal (Waiting)
                  Interface eth2 (0.0.0.0): Link Down (Shutdown)
                  Interface inside (192.168.75.10): No Link (Waiting)
                  Interface outside (192.168.76.10): No Link (Waiting)
                slot 1: snort rev (1.0)  status (up)
                slot 2: diskstatus rev (1.0)  status (up)
        Other host: Secondary - Standby Ready
                Active time: 0 (sec)
                slot 0: FPR-2130 hw/sw rev (1.3/9.16(4)200) status (Up Sys)
                  Interface diagnostic (0.0.0.0): Normal (Waiting)
                  Interface eth2 (0.0.0.0): Link Down (Shutdown)
                  Interface inside (192.168.75.11): No Link (Waiting)
                  Interface outside (192.168.76.11): No Link (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 Ethernet1/1 (up)
        Stateful Obj    xmit       xerr       rcv        rerr
        General         189        0          188        0
        sys cmd         188        0          188        0
        up time         0          0          0          0
        RPC services    0          0          0          0
        TCP conn        0          0          0          0
        UDP conn        0          0          0          0
        ARP tbl         0          0          0          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   0          0          0          0
        Router ID       0          0          0          0
        User-Identity   1          0          0          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
        Rule DB B-Sync  0          0          0          0
        Rule DB P-Sync  0          0          0          0
        Rule DB Delete  0          0          0          0

        Logical Update Queue Information
                        Cur     Max     Total
        Recv Q:         0       10      188
        Xmit Q:         0       11      957
```

ステップ 3：セカンダリデバイスでも同じ操作を行います。

ステップ 4：show failover stateコマンドを使用して、現在の状態を検証します。

```
> show failover state

               State          Last Failure Reason      Date/Time
This host  -   Primary
               Active         None
Other host -   Secondary
               Standby Ready  Comm Failure             00:01:45 UTC Jul 25 2023

====Configuration State===
        Sync Done
====Communication State===
        Mac set
```

ステップ 5：show running-config failoverおよびshow running-config interfaceを使用して、プライマリユニットからの設定を確認します。

```
> show running-config failover
failover
failover lan unit primary
failover lan interface failover-link Ethernet1/1
failover replication http
failover link failover-link Ethernet1/1
failover interface ip failover-link 1.1.1.1 255.255.255.252 standby 1.1.1.2

> show running-config interface
!
interface Ethernet1/1
 description LAN/STATE Failover Interface
 ipv6 enable
!
interface Ethernet1/2
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Ethernet1/3
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Ethernet1/4
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Ethernet1/5
 nameif inside
 security-level 0
 ip address 192.168.75.10 255.255.255.0 standby 192.168.75.11
!
```

```
interface Ethernet1/6
 nameif outside
 security-level 0
 ip address 192.168.76.10 255.255.255.0 standby 192.168.76.11
!
interface Ethernet1/7
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management1/1
 management-only
 nameif diagnostic
 cts manual
  propagate sgt preserve-untag
  policy static sgt disabled trusted
 security-level 0
 no ip address
```

タスク 4.フェールオーバーロールの切り替え

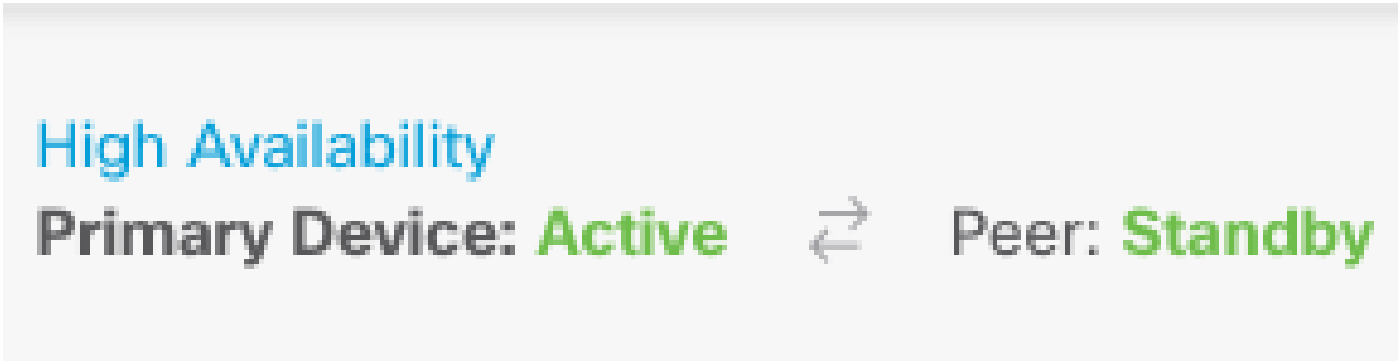
タスク要件：

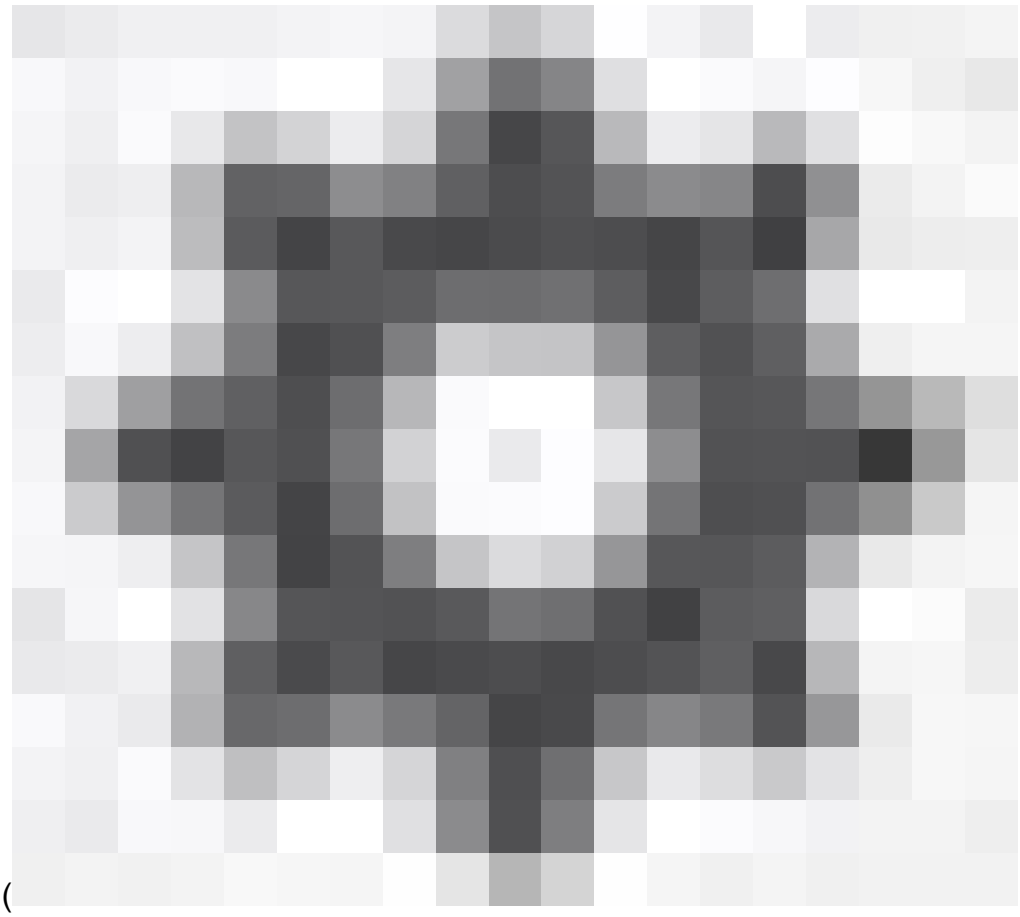
Secure Firewall Device Manager(SDM)のグラフィックインターフェイスで、フェールオーバーのロールをプライマリ/アクティブ、セカンダリ/スタンバイからプライマリ/スタンバイ、セカンダリ/アクティブに切り替えます

ソリューション：

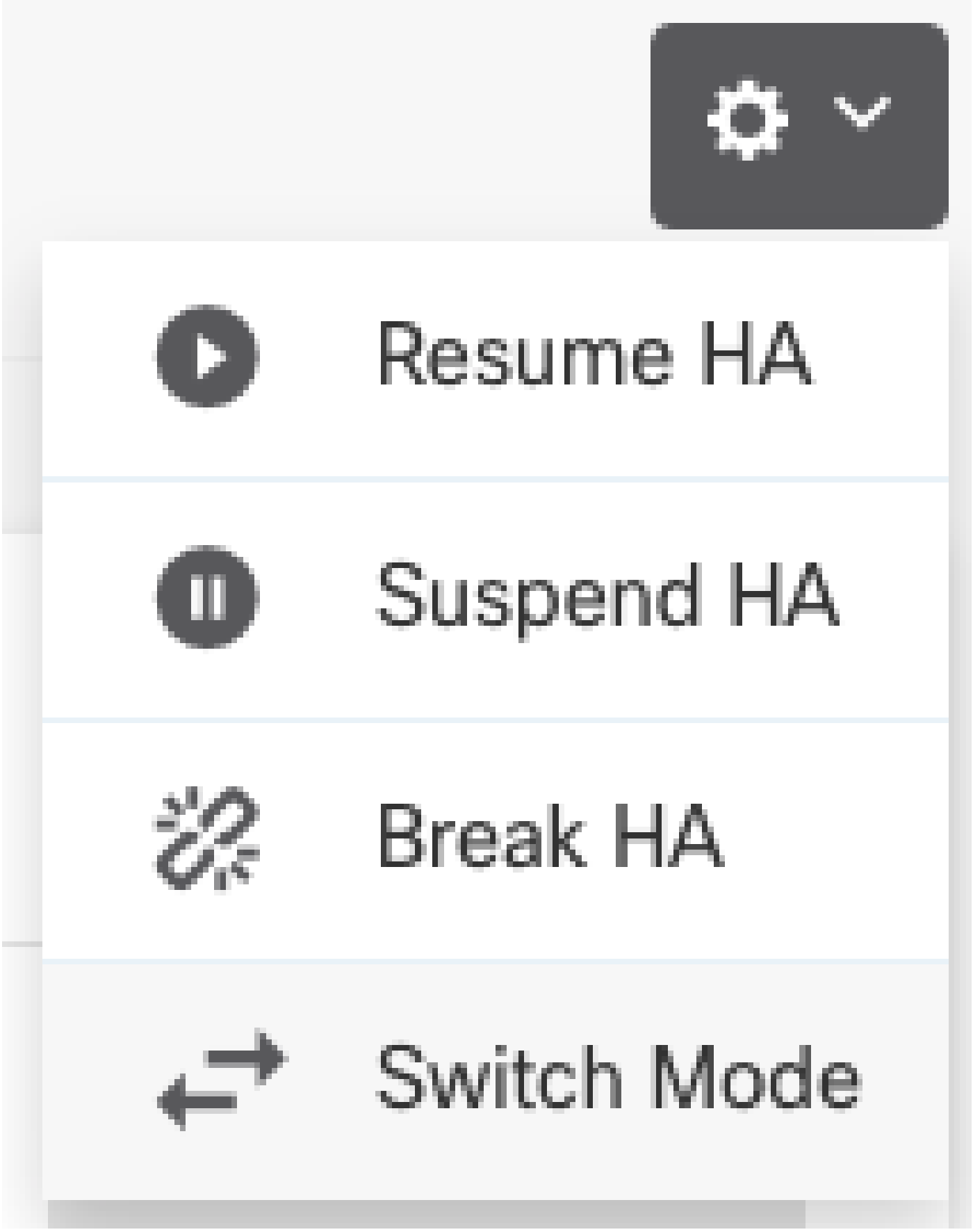
ステップ 1：Deviceをクリックします。

ステップ 2：デバイスサマリーの右側にあるHigh Availabilityリンクをクリックします。

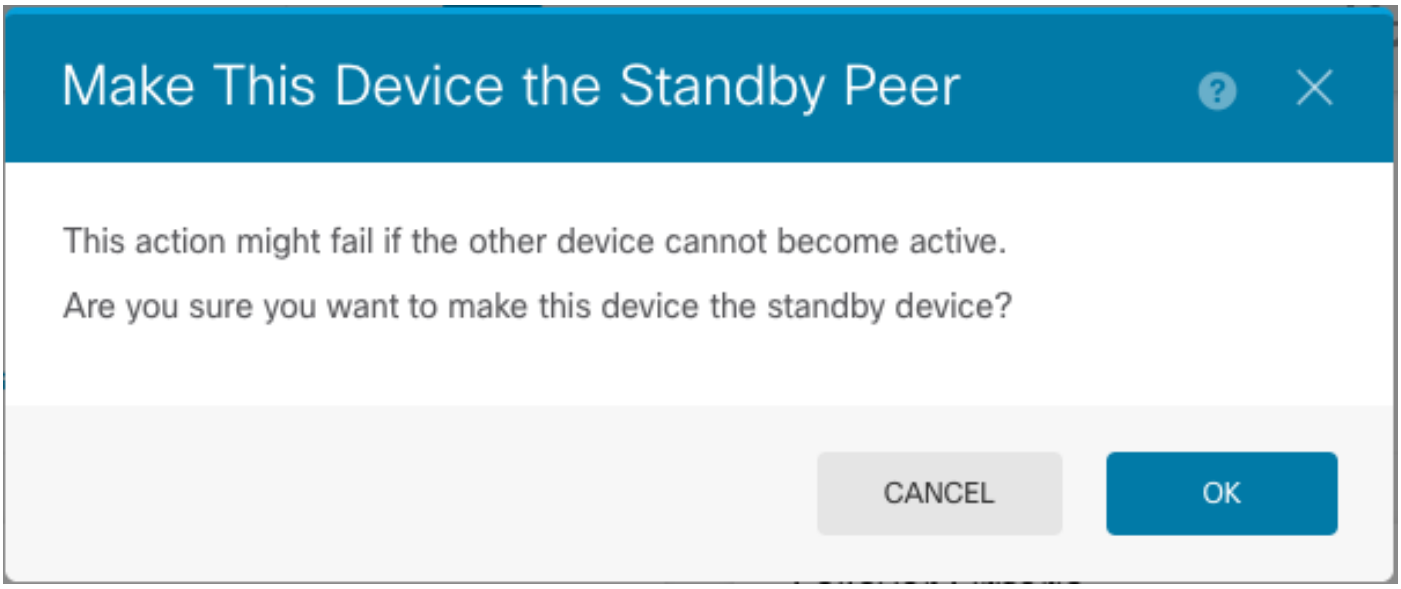




ステップ 3：歯車アイコン(
Switch Modeを選択します。

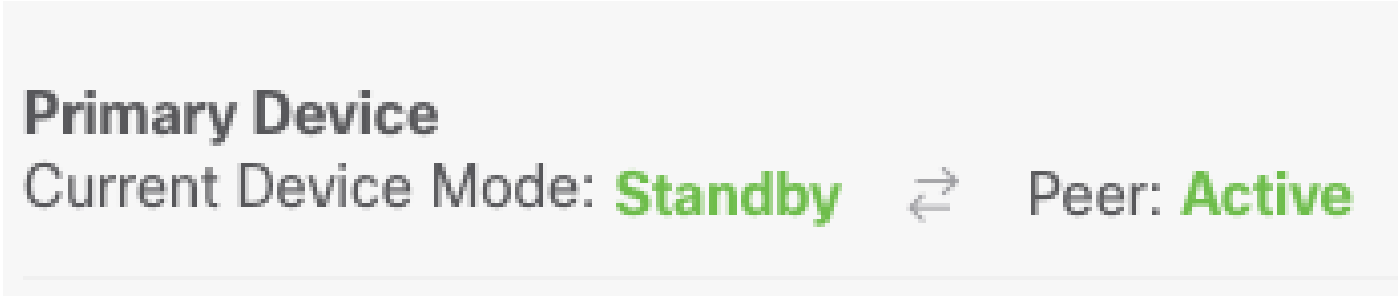


ステップ 4：確認メッセージを読み、OKをクリックします。



システムによってフェールオーバーが強制され、アクティブユニットがスタンバイになり、スタンバイユニットが新しいアクティブユニットになります。

ステップ 5：図に示すように、結果を確認します。



手順 6：フェールオーバー履歴リンクを使用して確認することも可能で、CLIコンソールのポップアップに結果が表示される必要があります。

```
==========================================================================
From State                To State                  Reason
==========================================================================
21:55:37 UTC Jul 20 2023
Not Detected              Disabled                  No Error

00:00:43 UTC Jul 25 2023
Disabled                  Negotiation               Set by the config command

00:01:28 UTC Jul 25 2023
Negotiation               Just Active               No Active unit found

00:01:29 UTC Jul 25 2023
Just Active               Active Drain              No Active unit found

00:01:29 UTC Jul 25 2023
Active Drain              Active Applying Config    No Active unit found

00:01:29 UTC Jul 25 2023
Active Applying Config    Active Config Applied     No Active unit found
```

```
00:01:29 UTC Jul 25 2023
Active Config Applied      Active                    No Active unit found

18:51:40 UTC Jul 25 2023
Active                     Standby Ready             Set by the config command

================================================================================
PEER History Collected at 18:55:08 UTC Jul 25 2023
============================PEER-HISTORY====================================
From State                 To State                  Reason
============================PEER-HISTORY====================================
22:00:18 UTC Jul 24 2023
Not Detected               Disabled                  No Error

00:52:08 UTC Jul 25 2023
Disabled                   Negotiation               Set by the config command

00:52:10 UTC Jul 25 2023
Negotiation                Cold Standby              Detected an Active mate

00:52:11 UTC Jul 25 2023
Cold Standby               App Sync                  Detected an Active mate

00:53:26 UTC Jul 25 2023
App Sync                   Sync Config               Detected an Active mate

01:00:12 UTC Jul 25 2023
Sync Config                Sync File System          Detected an Active mate

01:00:12 UTC Jul 25 2023
Sync File System           Bulk Sync                 Detected an Active mate

01:00:23 UTC Jul 25 2023
Bulk Sync                  Standby Ready             Detected an Active mate

18:45:01 UTC Jul 25 2023
Standby Ready              Just Active               Other unit wants me Active

18:45:02 UTC Jul 25 2023
Just Active                Active Drain              Other unit wants me Active

18:45:02 UTC Jul 25 2023
Active Drain               Active Applying Config    Other unit wants me Active

18:45:02 UTC Jul 25 2023
Active Applying Config     Active Config Applied     Other unit wants me Active

18:45:02 UTC Jul 25 2023
Active Config Applied      Active                    Other unit wants me Active

============================PEER-HISTORY====================================
```

手順 7：確認後、プライマリユニットを再度アクティブにします。

タスク 5.ハイアベイラビリティの一時停止または再開

ハイアベイラビリティペアのユニットは一時停止できます。これは次の場合に役立ちます。

- 両方のユニットがアクティブ – アクティブの状態にあり、フェールオーバーリンクで通信を修正しても問題は解決しません。
- アクティブユニットまたはスタンバイユニットのトラブルシューティングを行い、その間ユニットがフェールオーバーしないようにする必要があります。
- スタンバイデバイスにソフトウェアアップグレードをインストールする際に、フェールオーバーを防止する必要がある。

HAの一時停止とHAの解除の主な違いは、一時停止されたHAデバイスではハイアベイラビリティ設定が維持されることです。HAを解除すると、設定は消去されます。したがって、中断されたシステムでHAを再開するオプションがあります。これにより、既存の設定が有効になり、2つのデバイスが再度フェールオーバーペアとして機能するようになります。

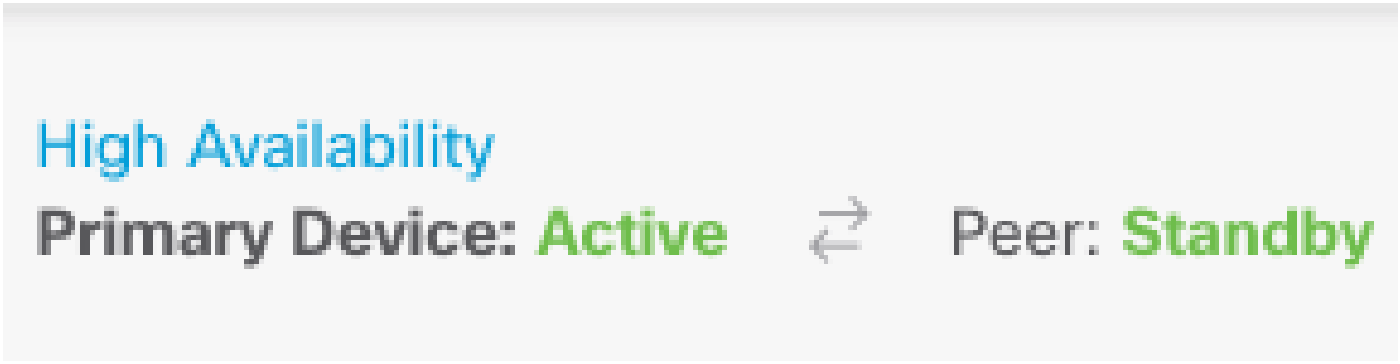
タスク要件：

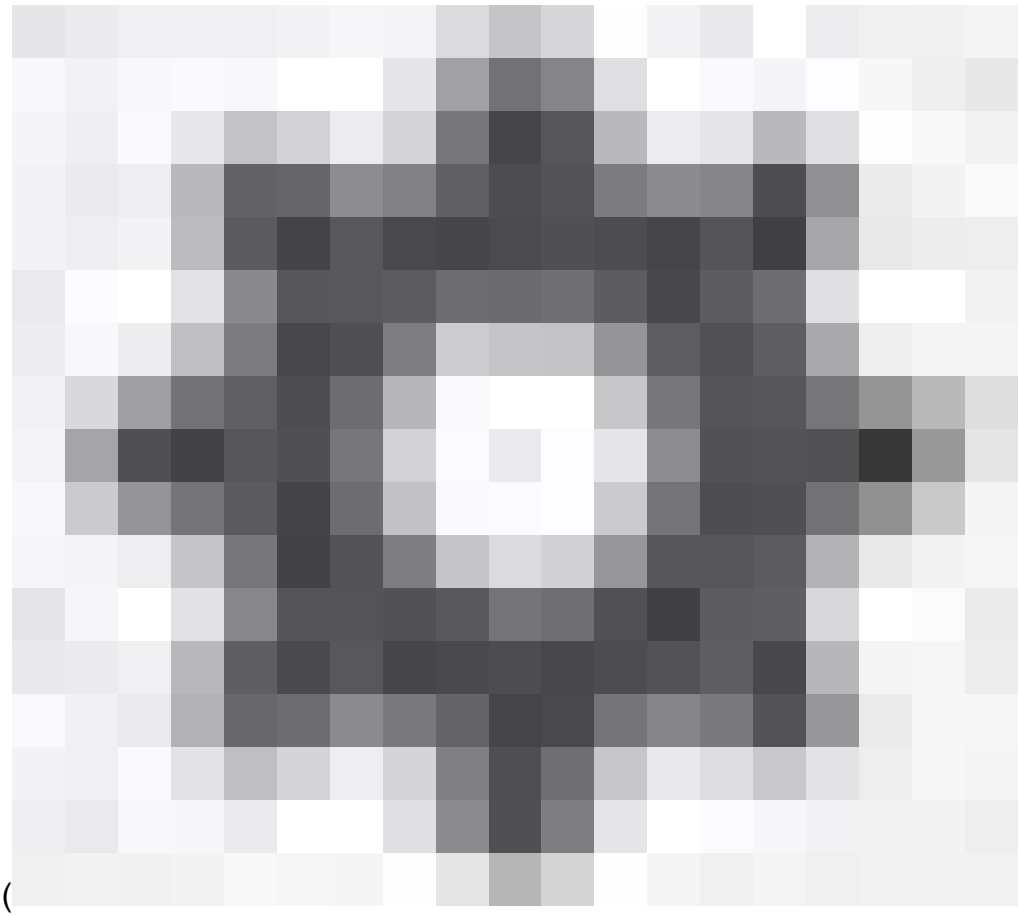
Secure Firewall Device Manager(SDM)グラフィックインターフェイスから、プライマリユニットを一時停止し、同じユニットでハイアベイラビリティを再開します。

ソリューション：

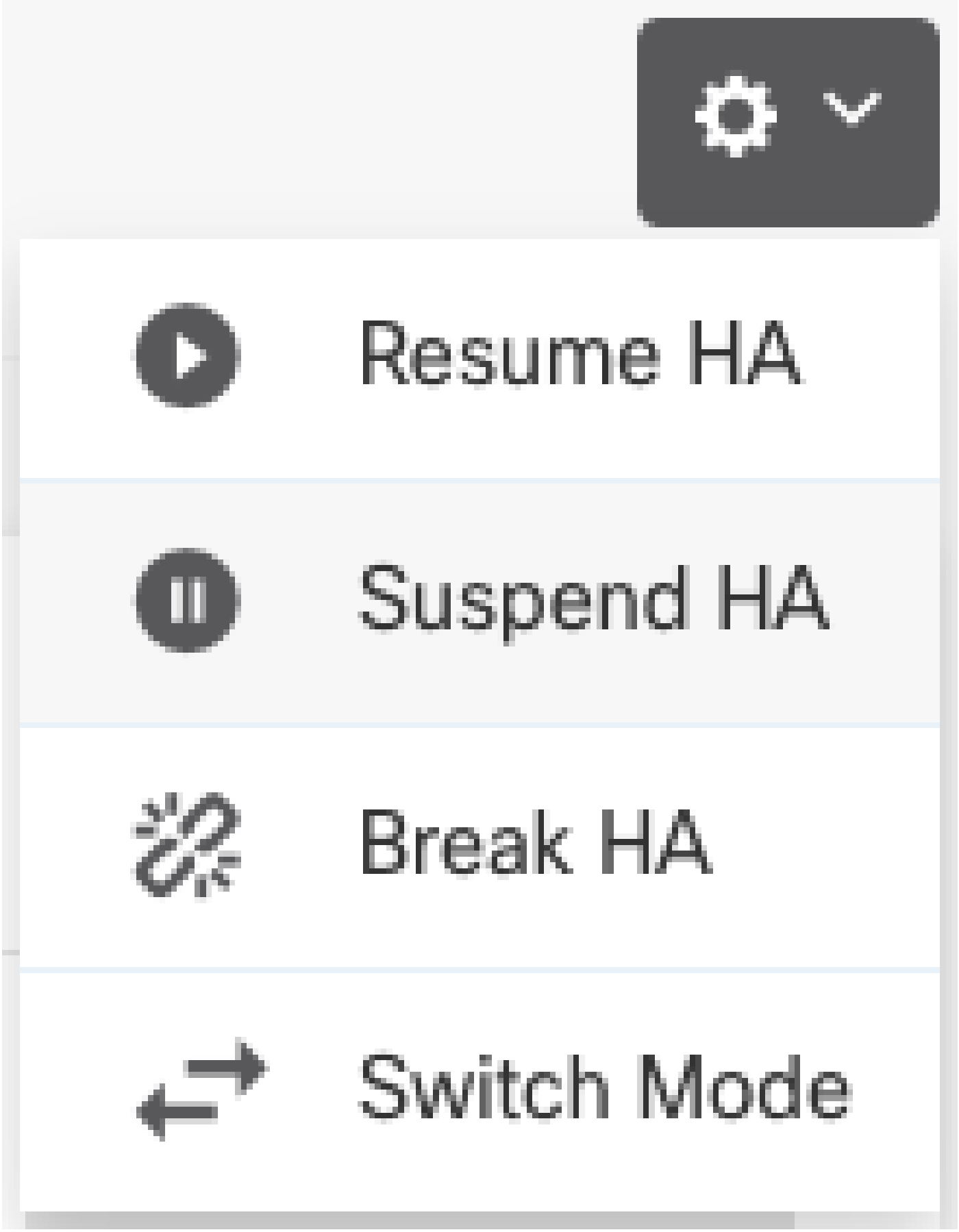
ステップ 1：Deviceをクリックします。

ステップ 2：デバイスサマリーの右側にあるHigh Availabilityリンクをクリックします。

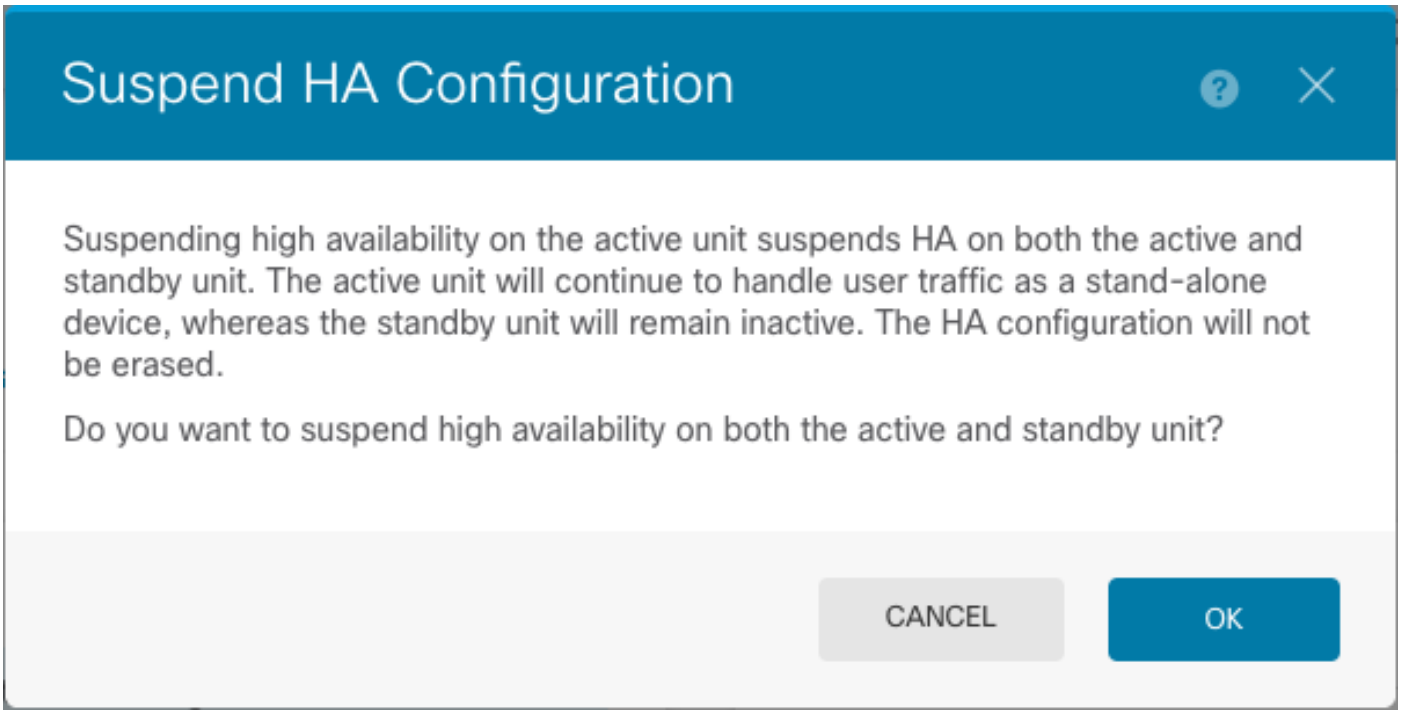




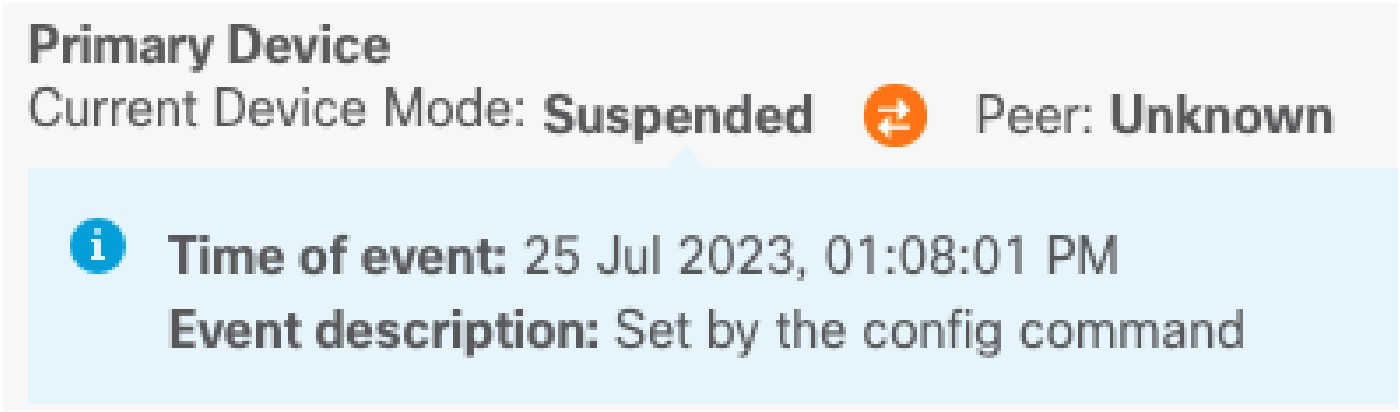
ステップ 3：歯車アイコン(
Suspend HAを選択します。



ステップ 4：確認メッセージを読み、OKをクリックします。

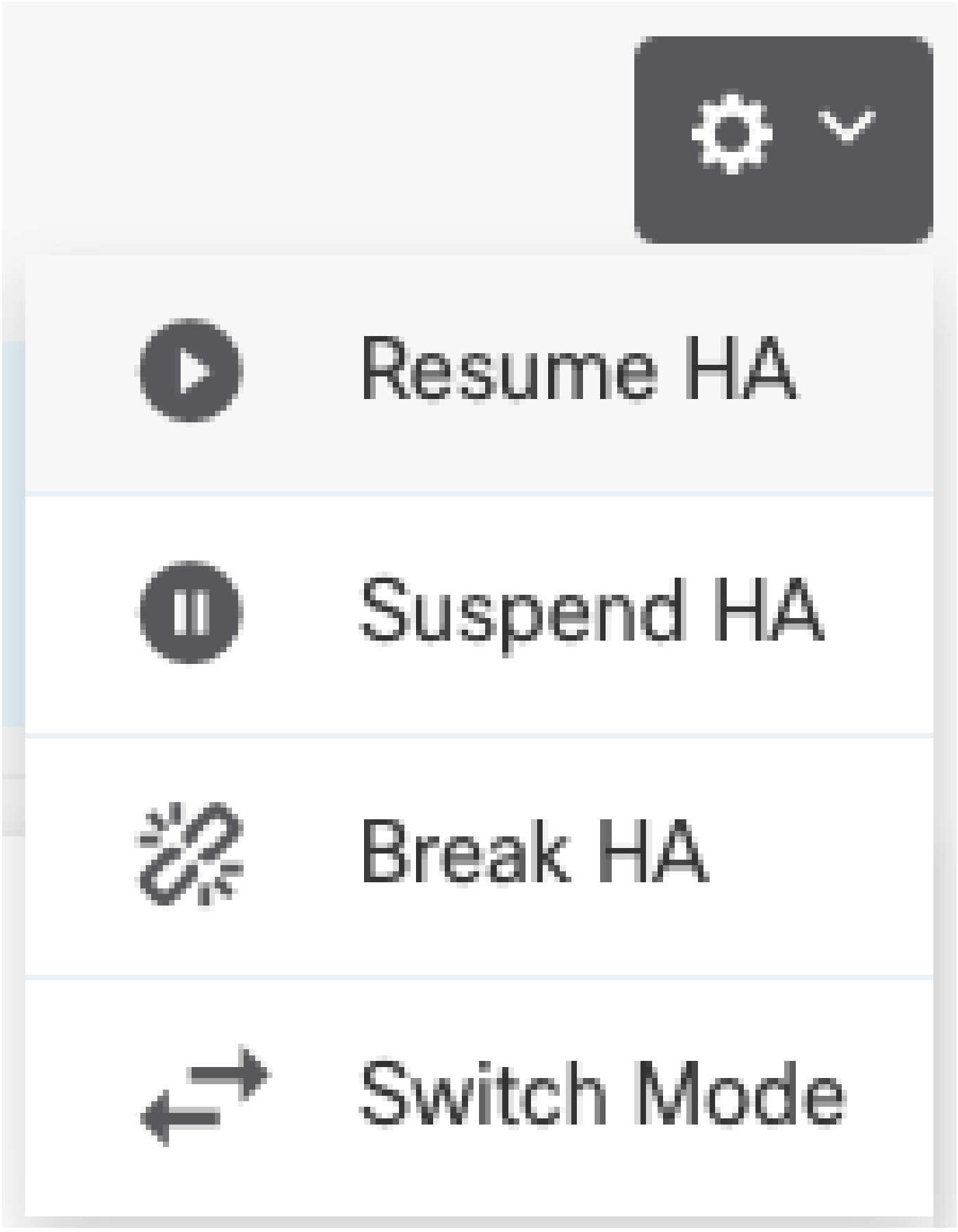


ステップ 5：図に示すように、結果を確認します。

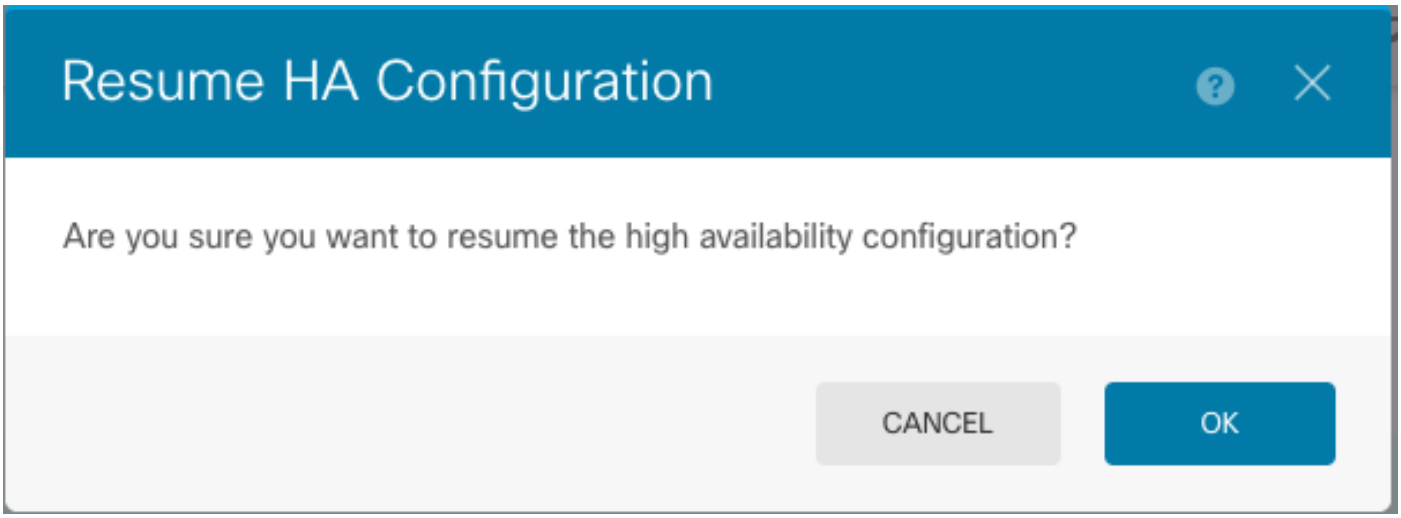


手順 6：HAを再開するには、ギアアイコン(

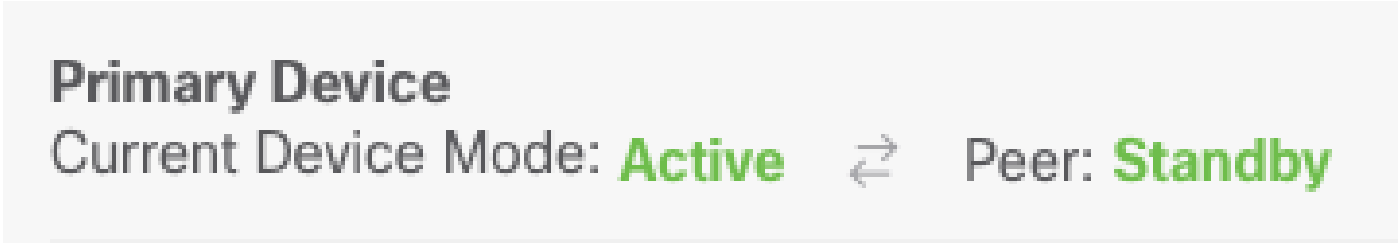
Resume HAを選択します。



手順 7：確認メッセージを読み、OKをクリックします。



ステップ 5：図に示すように、結果を確認します。



タスク 6.画期的なハイアベイラビリティ

2台のデバイスをハイアベイラビリティペアとして動作させたくない場合は、HA設定を解除できます。HAを解除すると、各デバイスがスタンドアロンデバイスになります。設定は次のように変更する必要があります。

- アクティブなデバイスは、HA設定を削除した状態で、休憩の前の完全な設定を保持します。
- スタンバイデバイスでは、HA設定に加えて、すべてのインターフェイス設定が削除されています。サブインターフェイスは無効ではありませんが、すべての物理インターフェイスは無効です。管理インターフェイスはアクティブのままなので、デバイスにログインして再設定できます。

タスク要件：

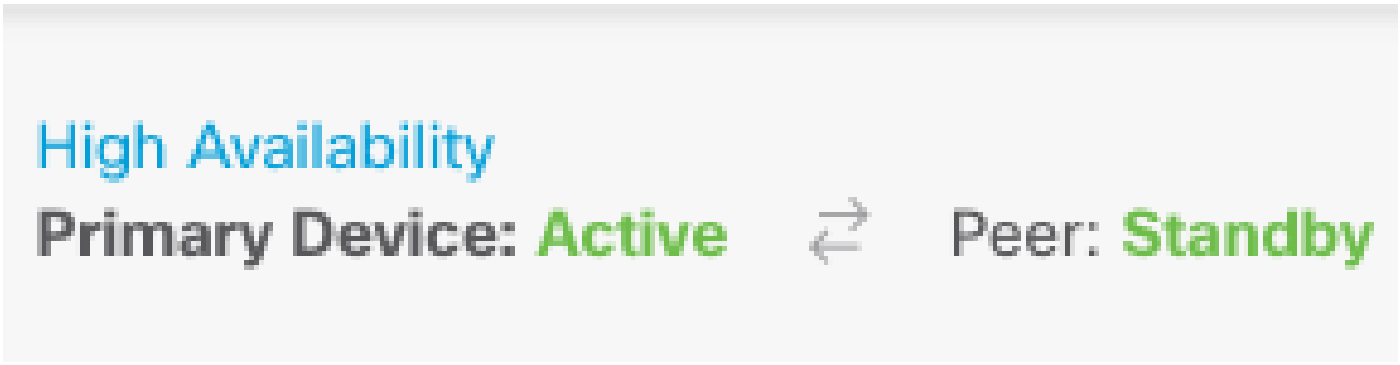
Secure Firewall Device Manager(SDM)グラフィックインターフェイスから、ハイアベイラビリティペアを解除します。

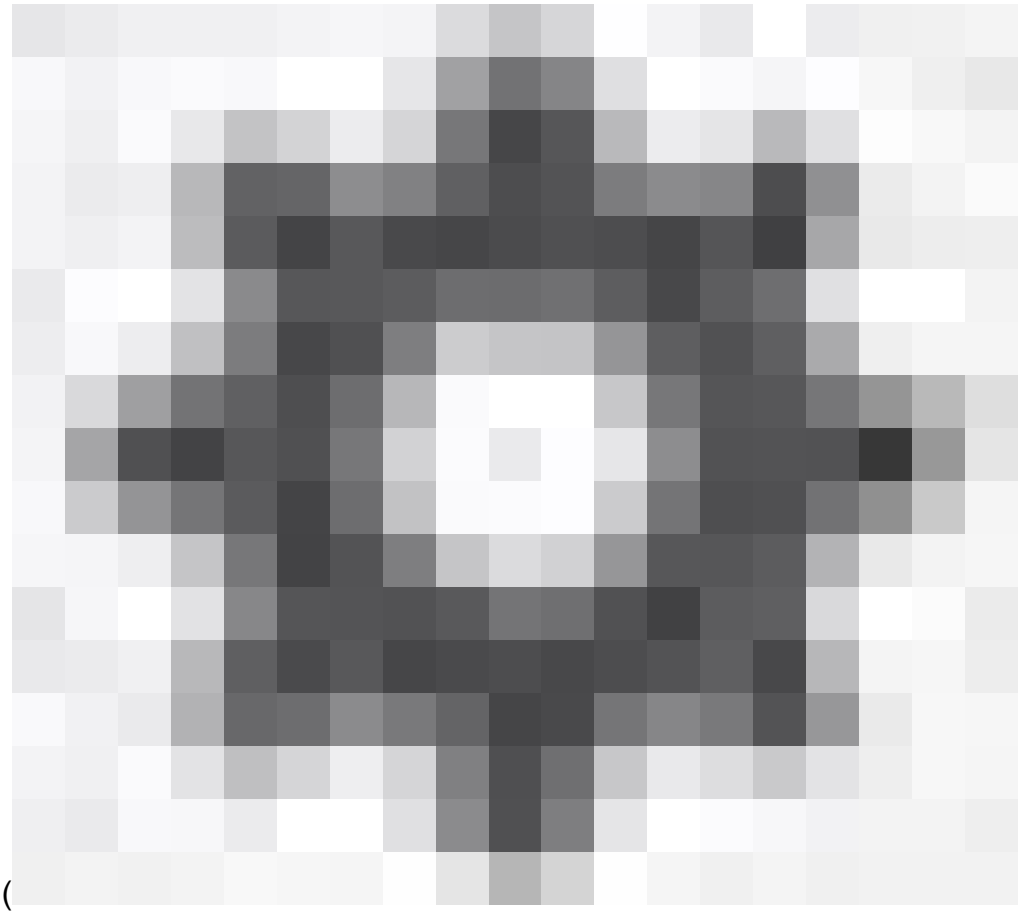
ソリューション：

ステップ 1：Deviceをクリックします。

Device: FPR2130-1

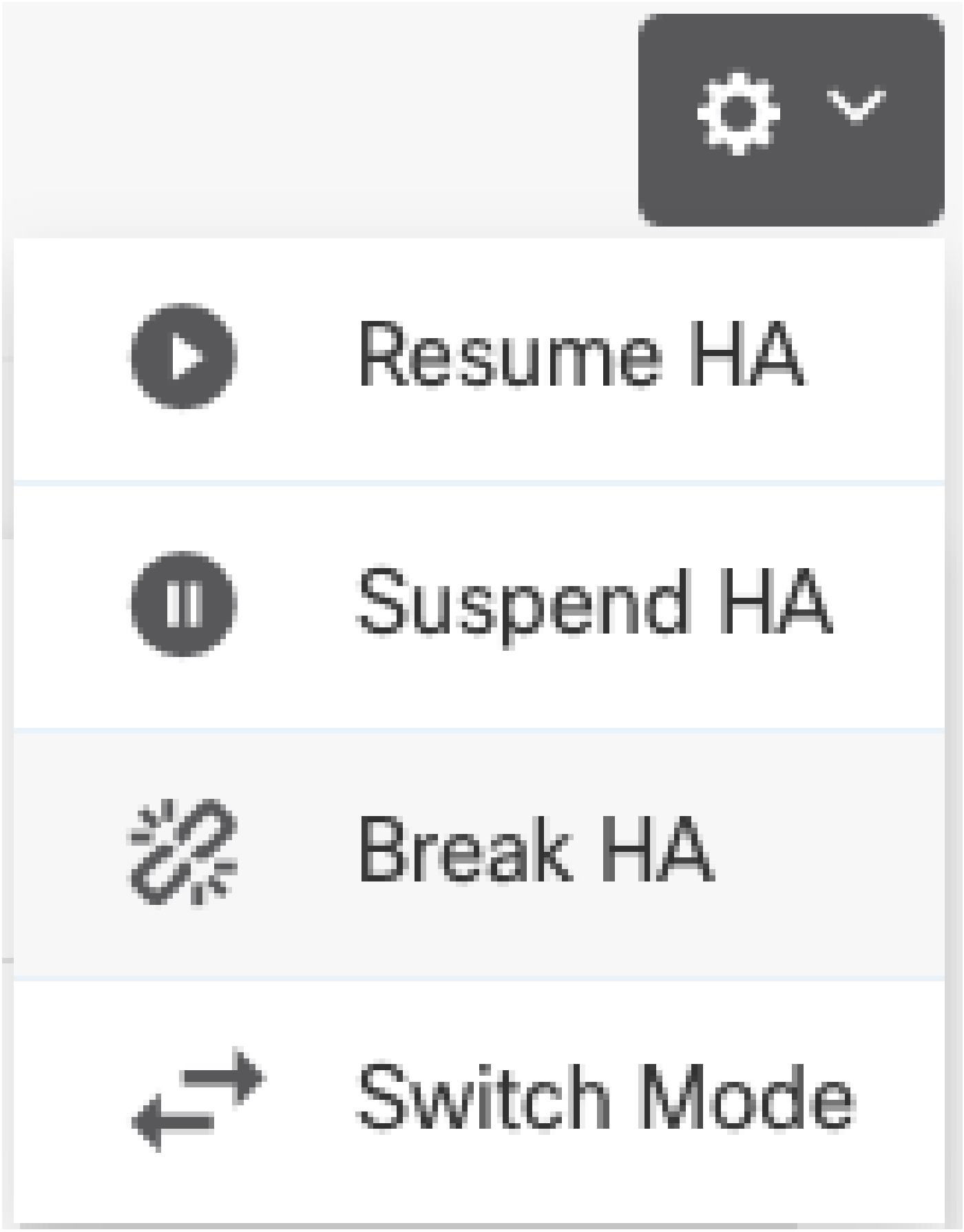
ステップ 2：デバイスサマリーの右側にあるHigh Availabilityリンクをクリックします。





ステップ 3：歯車アイコン(

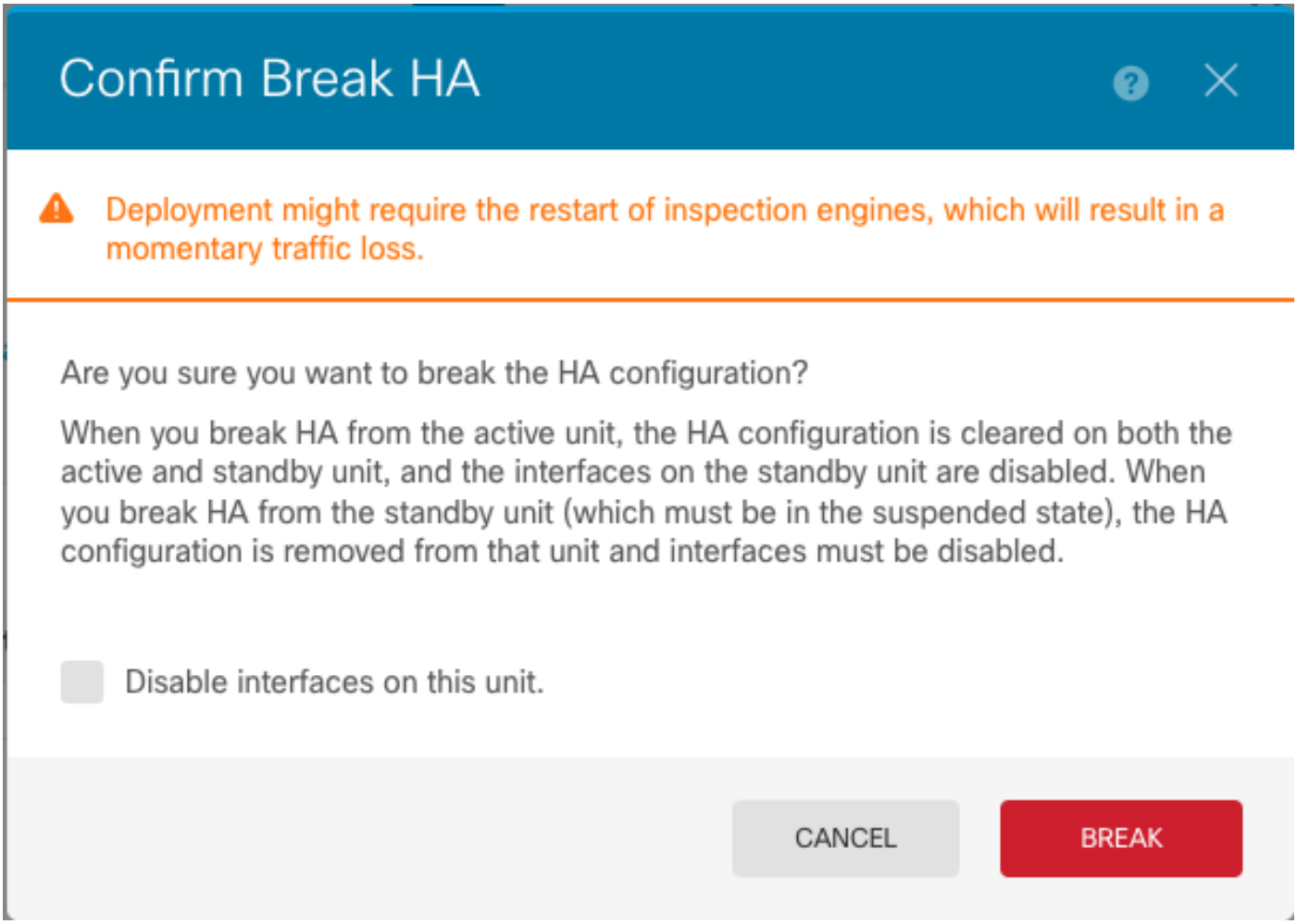
Break HAを選択します。



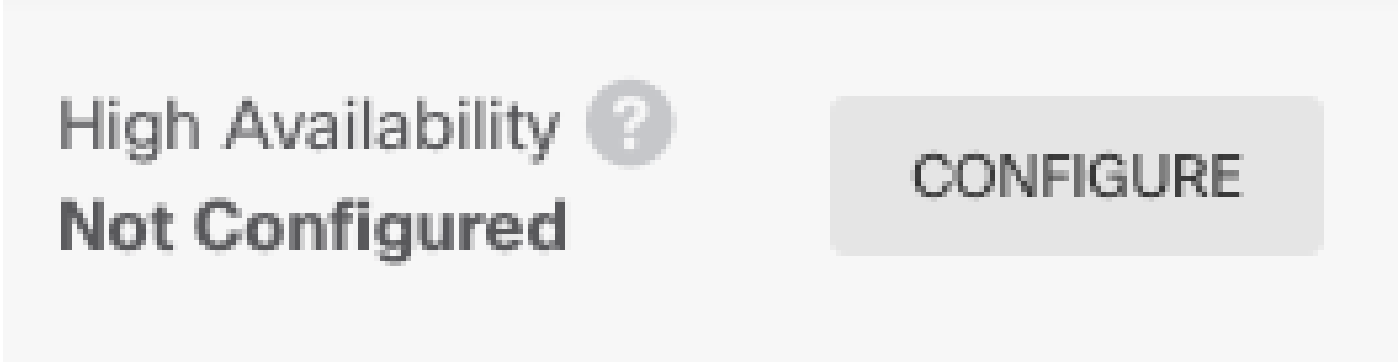
ステップ 4：確認メッセージを読み、インターフェイスを無効にするオプションを選択するかどうかを決定し、Breakをクリックします。

スタンバイユニットからHAを切断する場合は、インターフェイスを無効にするオプションを選択する必要があります。

このデバイスとピアデバイス（可能な場合）の両方に変更が即座に適用されます。導入が各デバイスで完了し、各デバイスが独立するまで数分かかることがあります。



ステップ5：図に示すように結果を確認します。



関連情報

- Cisco Secure Firewall Device Managerコンフィギュレーションガイドのすべてのバージョンは、次のリンクから入手できます

https://www.cisco.com/c/en/us/support/security/firepower-ngfw/products-installation-and-configuration-guides-list.html

- Cisco Global Technical Assistance Center(TAC)では、シスコのFirepowerNext-Generation Security Technologiesに関する詳細な実践知識を得るために、次のビジュアルガイドを強く推奨しています。

https://www.ciscopress.com/store/cisco-firepower-threat-defense-ftd-configuration-and-9781587144806

- firepowerテクノロジーに関連するすべての設定およびトラブルシューティングテクニカルノート

https://www.cisco.com/c/en/us/support/security/defense-center/series.html

- テクニカル サポートとドキュメント - Cisco Systems

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。