# Konfigurieren des sicheren Firewall-Gerätemanagers mit hoher Verfügbarkeit

## Inhalt



## Einleitung

In diesem Dokument wird beschrieben, wie Sie Secure Firewall Device Manager (FDM) High Availability (HA) auf sicheren Firewall-Geräten konfigurieren und überprüfen.

## Voraussetzungen

### Anforderungen

### Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- 2 Cisco Secure Firewall 2100 Security Appliances
- Ausführung von FDM Version 7.0.5 (Build 72)

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

## Aufgabe 1: Überprüfen der Bedingungen

Voraussetzung für diese Aufgabe:

Überprüfen Sie, ob beide FDM-Appliances die Notizanforderungen erfüllen und als HA-Einheiten konfiguriert werden können.

Lösung:

Schritt 1: Stellen Sie über SSH eine Verbindung zur Management-IP der Appliance her, und überprüfen Sie die Modulhardware.

Überprüfen Sie mit dem **Befehl show version** die primäre Hardware- und Softwareversion des Geräts:

```
> 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
----------------------------------------------------
```

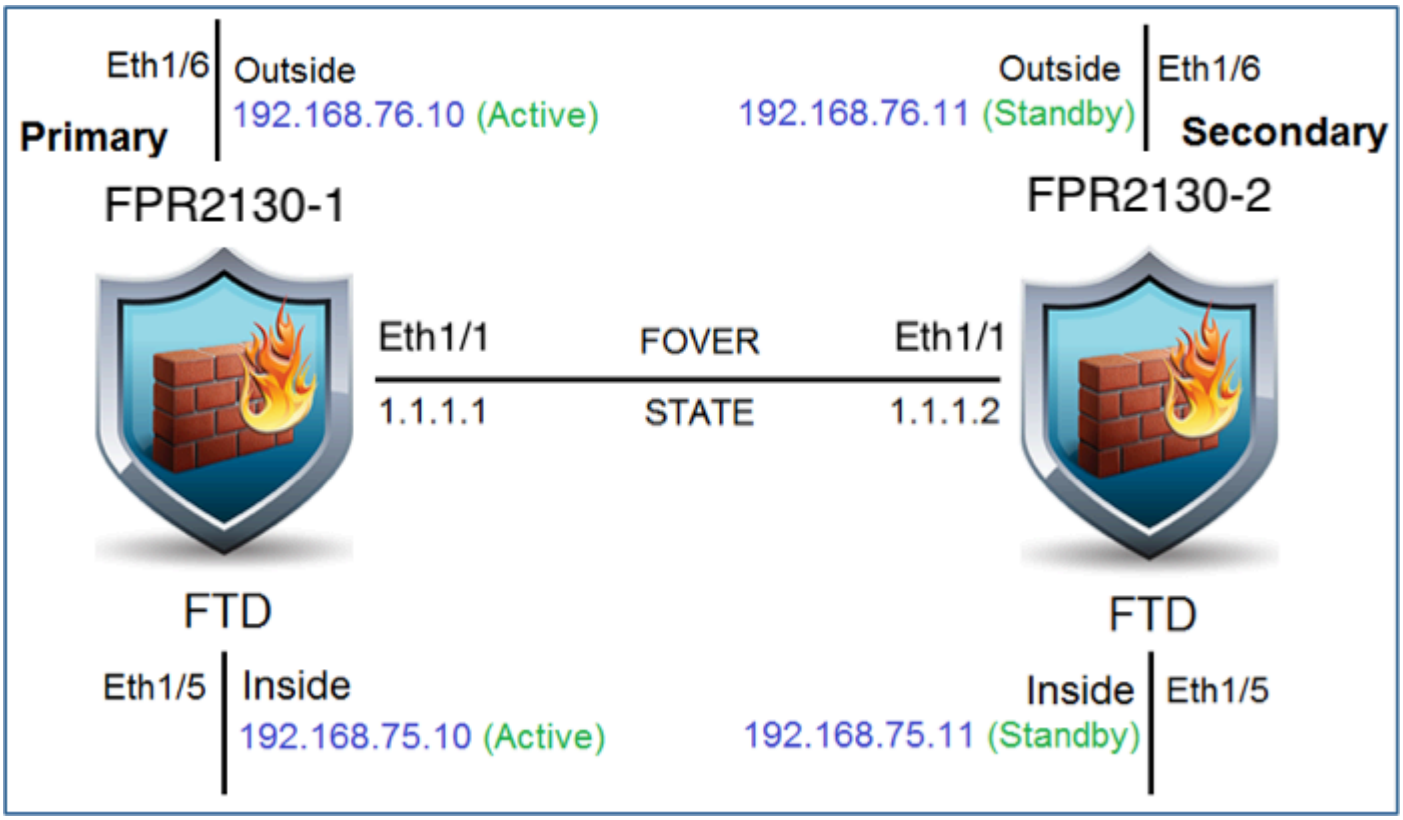
Überprüfen Sie die Hardware- und Softwareversion des sekundären Geräts:

```
> 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
----------------------------------------------------
```

# Aufgabe 2: Konfigurieren des sicheren Firewall-Gerätemanagers mit hoher Verfügbarkeit

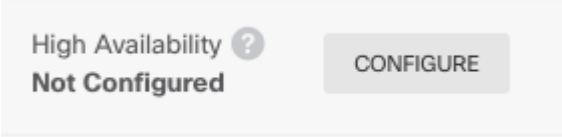
## Netzwerkdiagramm

Konfigurieren Sie Aktiv/Standby-Hochverfügbarkeit (HA) gemäß diesem Diagramm:

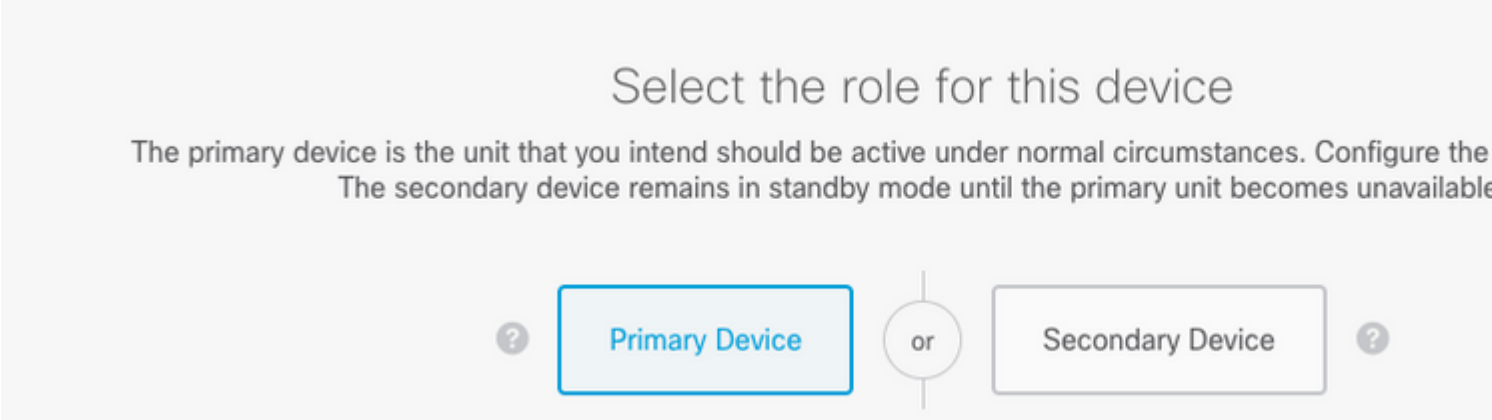



## Aktivieren der hohen Verfügbarkeit im Secure Firewall Device Manager der primären Einheit

Schritt 1: Um FDM-Failover zu konfigurieren, navigieren Sie zu **Device (Gerät)**, und klicken Sie neben der Gruppe **High Availability (Hohe Verfügbarkeit)** auf **Configure** (**Konfigurieren**):




Schritt 2: Klicken Sie auf der Seite für die hohe Verfügbarkeit auf das Feld für das primäre Gerät:



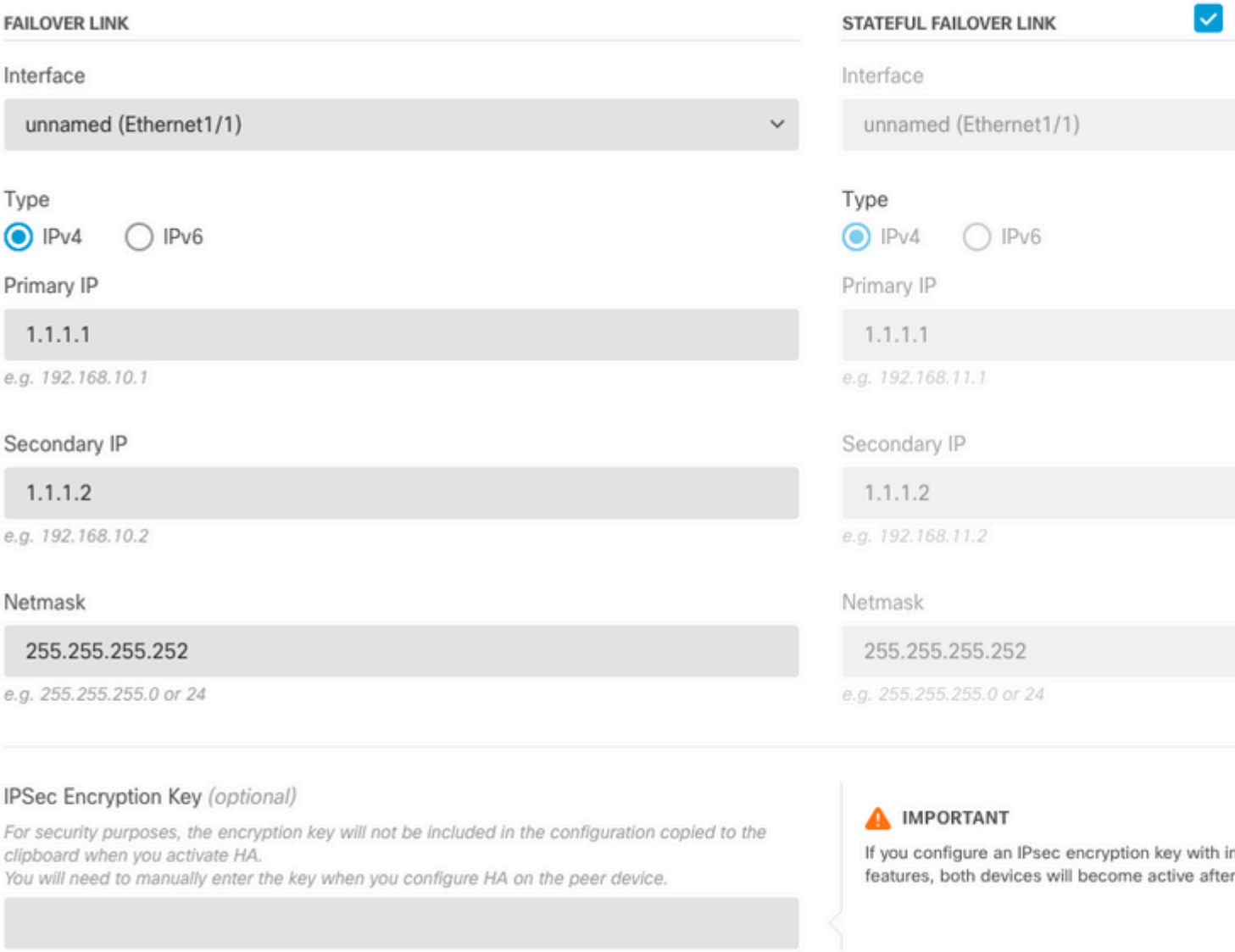

---

**Warnung**: Wählen Sie die richtige Einheit als **primäre** Einheit aus. Alle Konfigurationen auf der ausgewählten primären Einheit werden auf die ausgewählte sekundäre FTD-Einheit repliziert. Durch die Replikation kann die aktuelle Konfiguration auf der sekundären Einheit **ersetzt** werden.

---

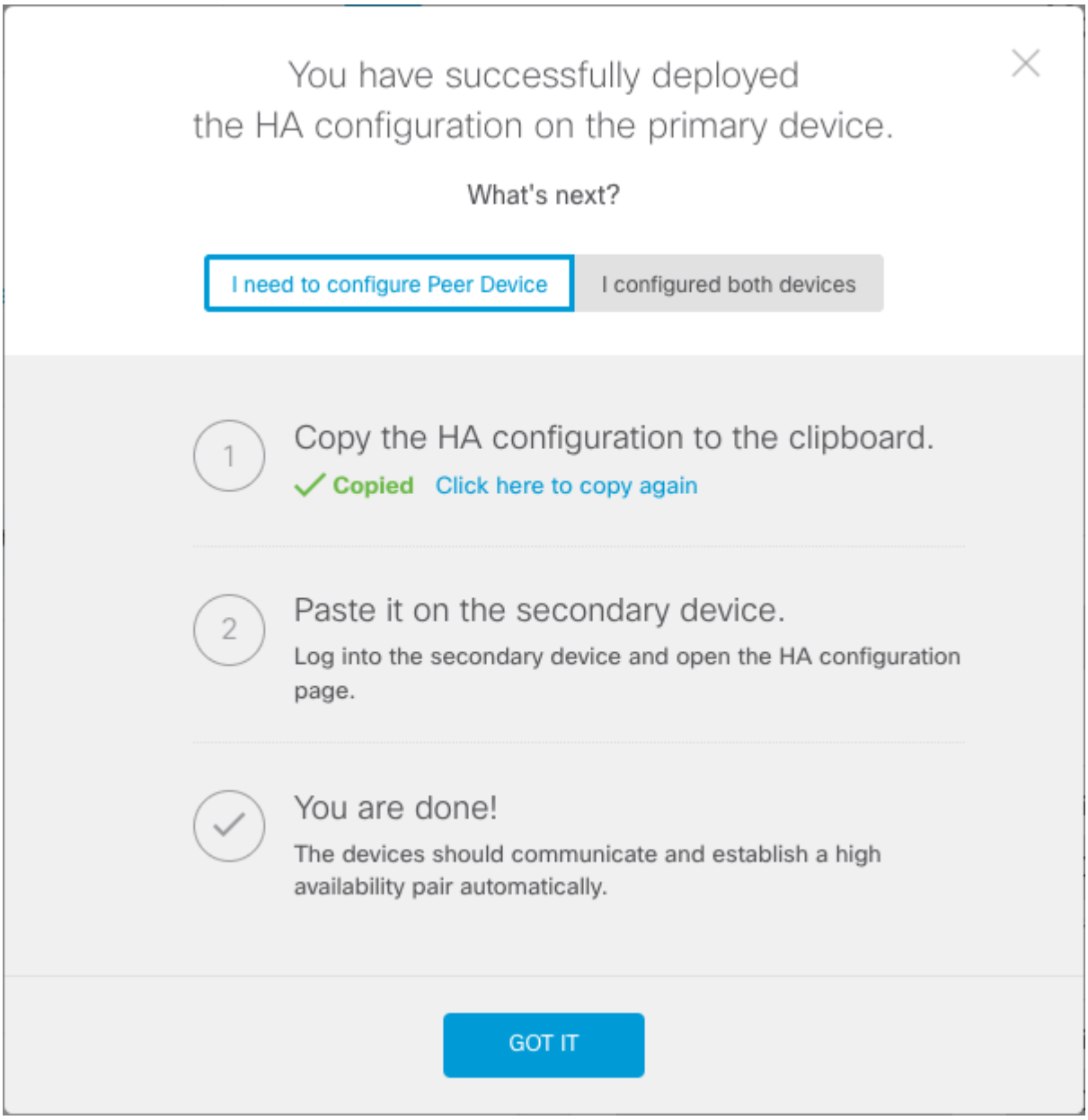
Schritt 3: Konfigurieren Sie die Einstellungen für die Failover-Verbindung und die Statusverbindung:

In diesem Beispiel hat der Status-Link die gleichen Einstellungen wie der Failover-Link.




Schritt 4: Klicken Sie auf HA aktivieren.

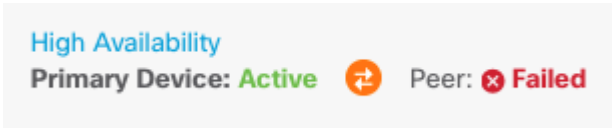
Schritt 5: Kopieren Sie die HA-Konfiguration in die Zwischenablage der Bestätigungsmeldung, um sie in die Sekundäreinheit einzufügen.




Das System stellt die Konfiguration sofort auf dem Gerät bereit. Sie müssen keinen Bereitstellungsauftrag starten. Wenn keine Meldung angezeigt wird, dass Ihre Konfiguration gespeichert wurde und die Bereitstellung ausgeführt wird, scrollen Sie zum Seitenanfang, um die Fehlermeldungen anzuzeigen.

Die Konfiguration wird ebenfalls in die Zwischenablage kopiert. Sie können die Kopie verwenden, um die sekundäre Einheit schnell zu konfigurieren. Um die Sicherheit zu erhöhen, ist der Verschlüsselungsschlüssel nicht in der Zwischenablage enthalten.

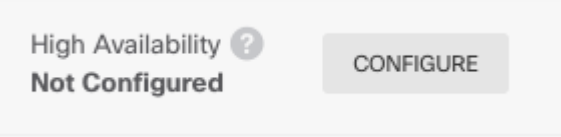
An diesem Punkt müssen Sie sich auf der Seite für Hochverfügbarkeit befinden, und Ihr Gerätestatus muss "Negotiating" lauten. Der Status muss noch vor der Konfiguration des Peers auf "Aktiv" geändert werden. Dieser muss bis zur Konfiguration als "Ausgefallen" angezeigt werden.



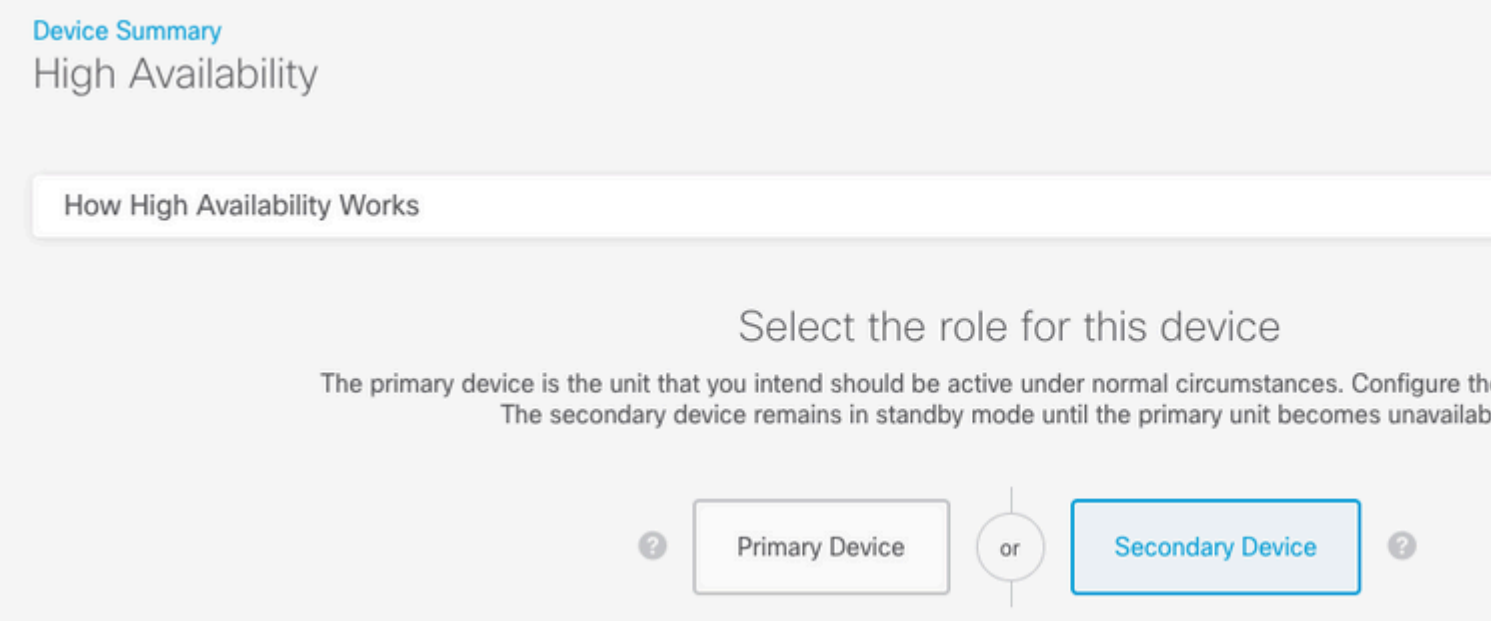

## Aktivieren der hohen Verfügbarkeit im Secure Firewall Device Manager der Sekundäreinheit

Nachdem Sie das primäre Gerät für eine hohe Verfügbarkeit im Aktiv-/Standby-Modus konfiguriert haben, müssen Sie das sekundäre Gerät konfigurieren. Melden Sie sich bei der FDM auf diesem Gerät an, und führen Sie dieses Verfahren aus.

Schritt 1: Um FDM-Failover zu konfigurieren, navigieren Sie zu **Device (Gerät)**, und klicken Sie neben der Gruppe **High Availability (Hohe Verfügbarkeit)** auf **Configure** (**Konfigurieren**):

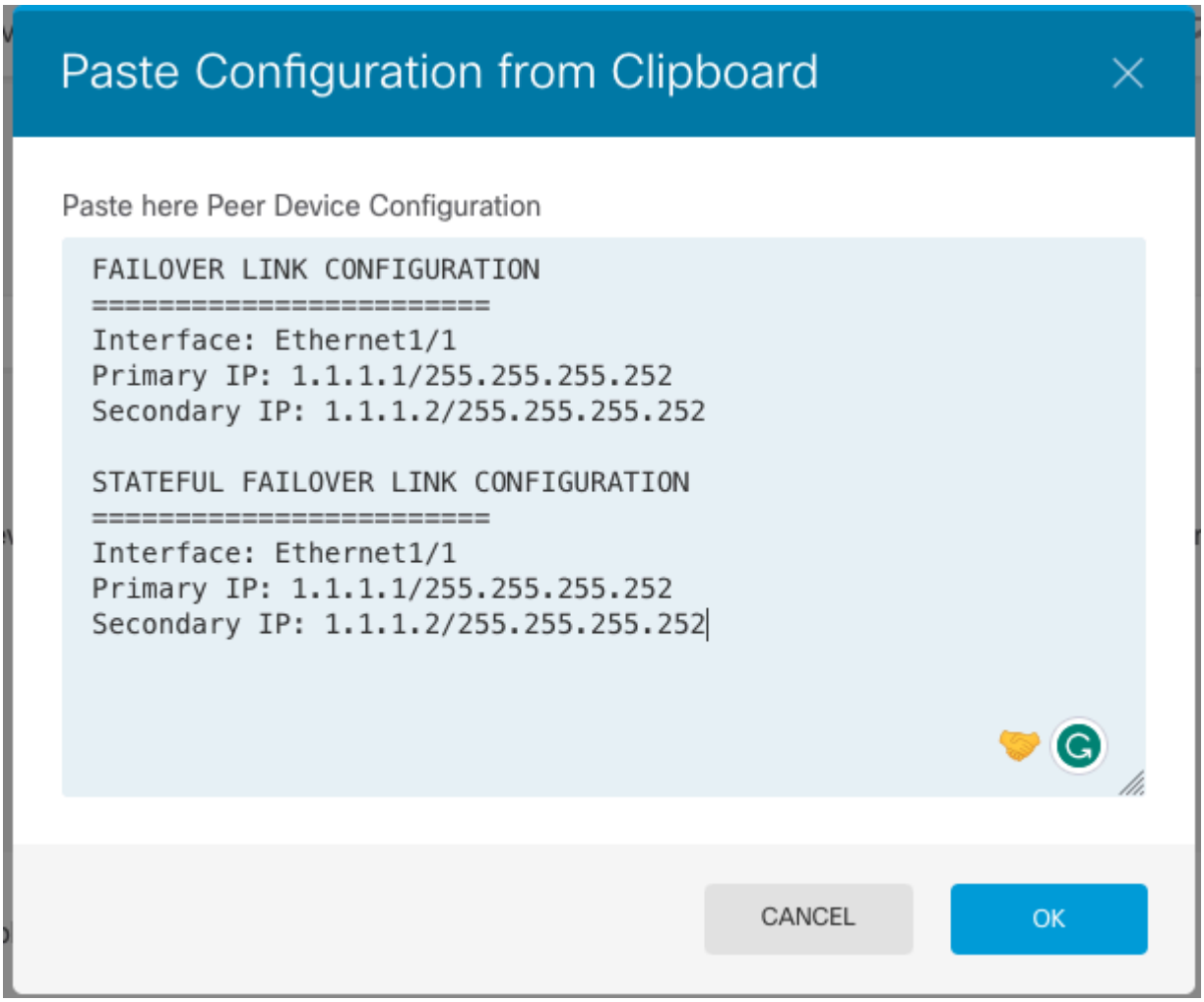



Schritt 2: Klicken Sie auf der Seite für die hohe Verfügbarkeit auf das Kästchen für das sekundäre Gerät:




Schritt 3: Wählen Sie eine der folgenden Optionen aus:

- Einfache Methode - Klicken Sie auf die Schaltfläche Aus Zwischenablage einfügen, fügen Sie die Konfiguration ein, und klicken Sie auf OK. Dadurch werden die Felder mit den entsprechenden Werten aktualisiert, die Sie überprüfen können.
- Manual method (Manuelle Methode): Konfigurieren Sie die Failover- und Stateful Failover-Verbindungen direkt. Geben Sie auf dem sekundären Gerät genau die gleichen Einstellungen ein, die Sie auf dem primären Gerät eingegeben haben.

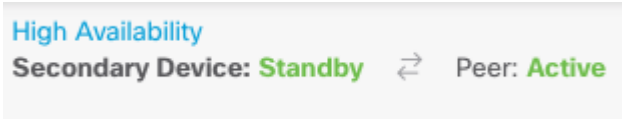



Schritt 4: Klicken Sie auf HA aktivieren

Das System stellt die Konfiguration sofort auf dem Gerät bereit. Sie müssen keinen Bereitstellungsauftrag starten. Wenn keine Meldung angezeigt wird, dass Ihre Konfiguration gespeichert wurde und die Bereitstellung ausgeführt wird, scrollen Sie zum Seitenanfang, um die Fehlermeldungen anzuzeigen.

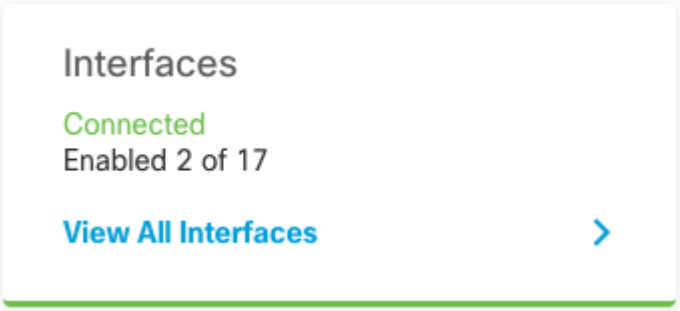
Nach Abschluss der Konfiguration erhalten Sie eine Meldung, wonach Sie HA konfiguriert haben. Klicken Sie auf Got It, um die Nachricht zu verwerfen.

An diesem Punkt müssen Sie sich auf der Seite für Hochverfügbarkeit befinden, und Ihr Gerätestatus muss angeben, dass es sich um das sekundäre Gerät handelt. Wenn die Verbindung mit dem primären Gerät erfolgreich war, wird die Synchronisierung mit dem primären Gerät durchgeführt. Anschließend muss der Standby-Modus und der Peer-Modus "Active" sein.



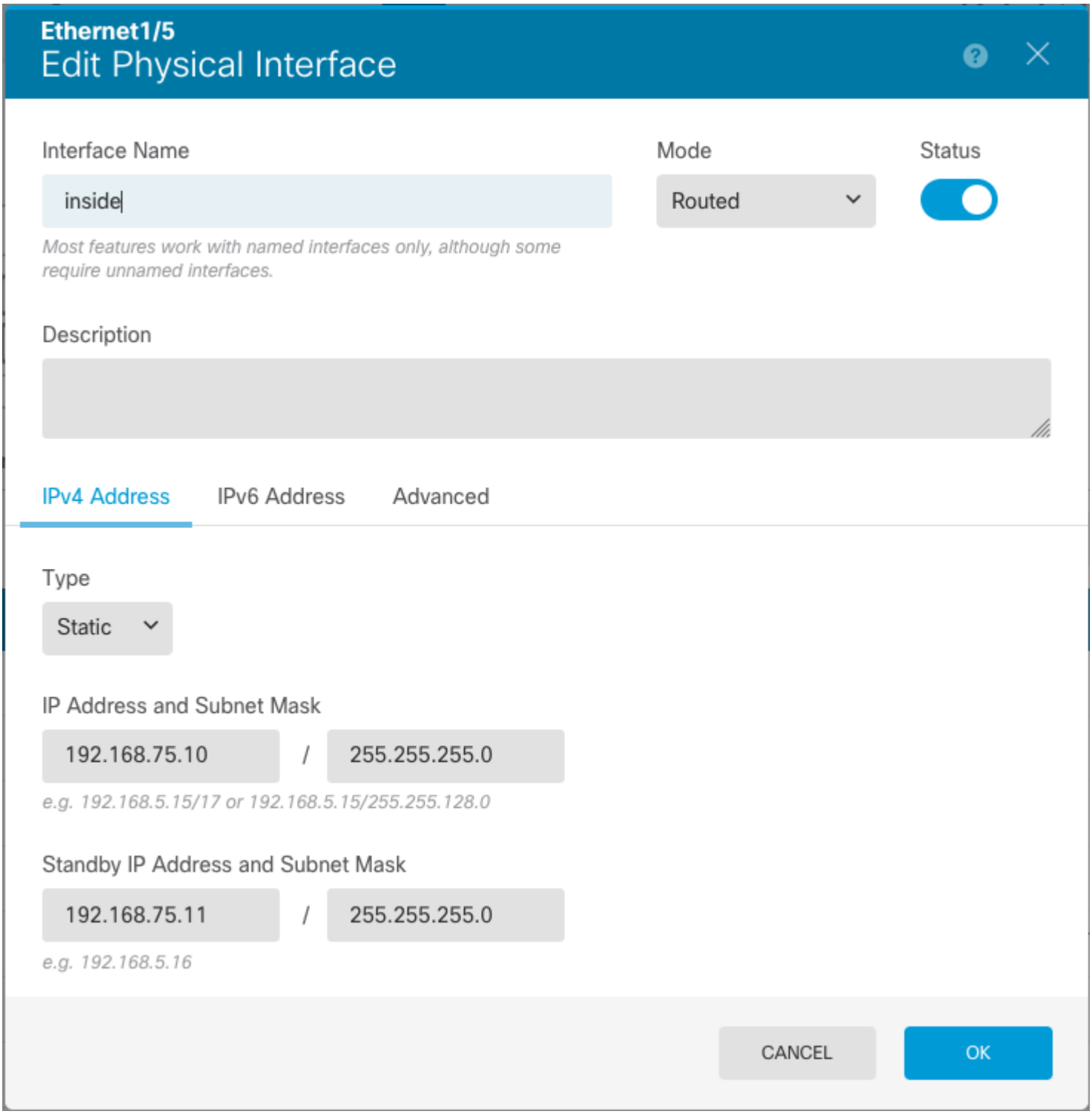

## Abschließen der Schnittstellenkonfiguration

Schritt 1: Um FDM-Schnittstellen zu konfigurieren, navigieren Sie zu **Device (Gerät)**, und klicken Sie auf **View All Interfaces (Alle Schnittstellen anzeigen):**

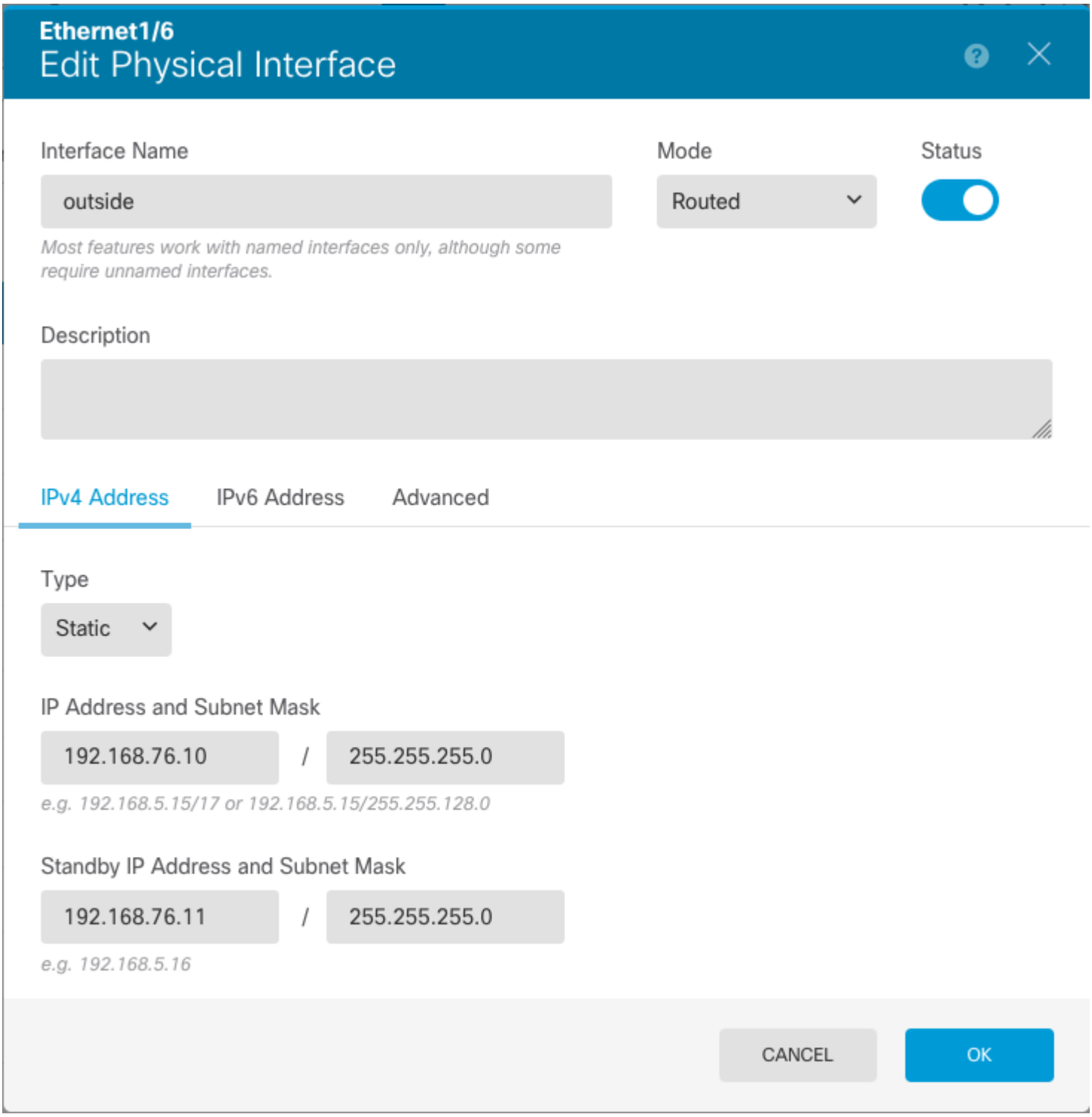



Schritt 2: Wählen und bearbeiten Sie die Schnittstelleneinstellungen wie in den Bildern dargestellt:

Ethernet 1/5-Schnittstelle:




Ethernet 1/6-Schnittstelle




Schritt 3: Nachdem Sie die Änderungen konfiguriert haben, klicken Sie auf **Ausstehende Änderungen** und **Jetzt bereitstellen**.

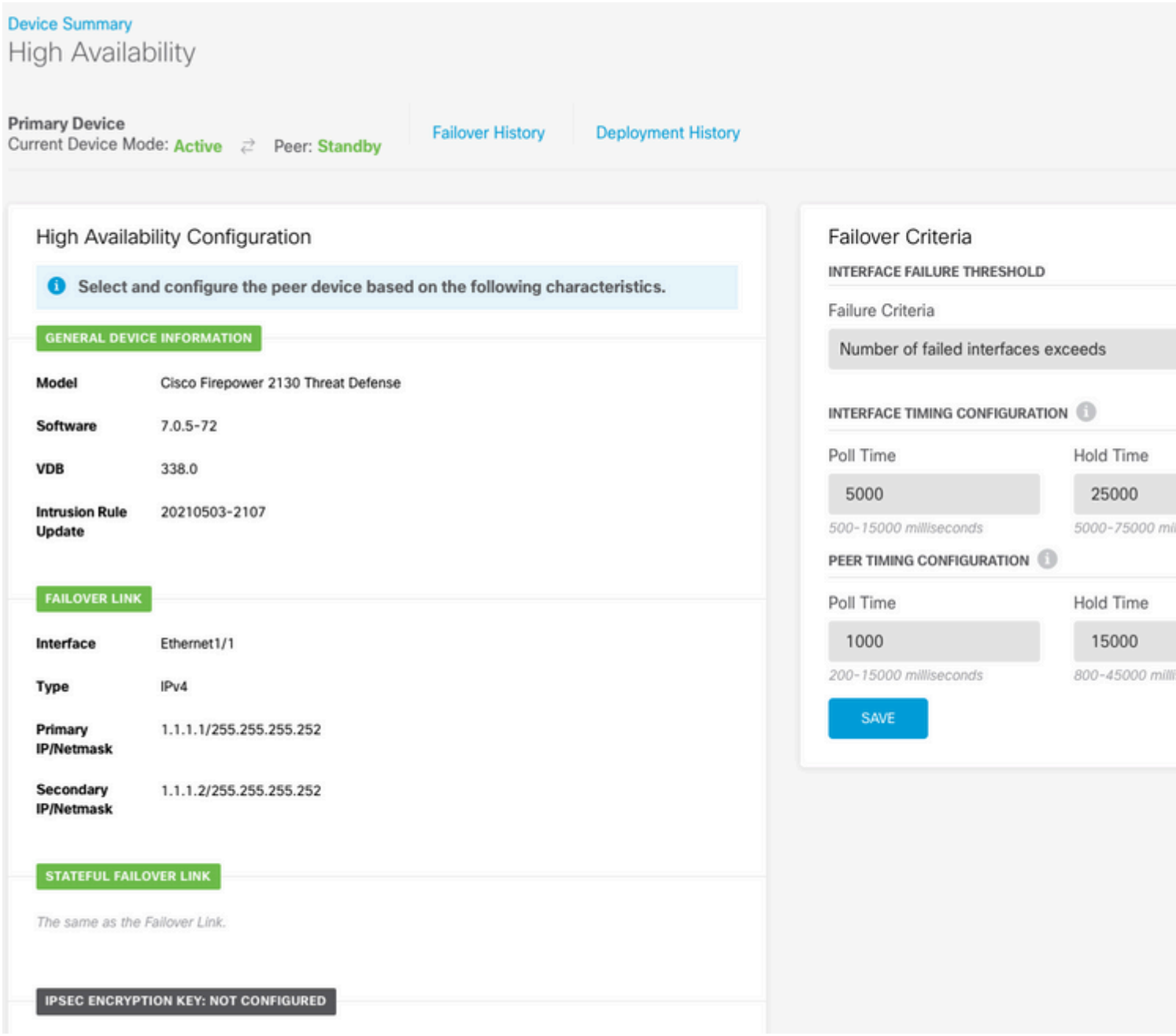
# Aufgabe 3: Überprüfen der hohen FDM-Verfügbarkeit

Voraussetzung für diese Aufgabe:

Überprüfen Sie die Hochverfügbarkeitseinstellungen über die FDM-GUI und die FDM-CLI.

Lösung:

Schritt 1: Navigieren Sie zu **Device (Gerät)**, und überprüfen Sie die **Hochverfügbarkeits**-Einstellungen:




Schritt 2: Stellen Sie mithilfe von SSH eine Verbindung zur CLI des primären FDM-Geräts her, und validieren Sie diese mithilfe des Befehls **show high availability config**:

```
> 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
```

Schritt 3: Wiederholen Sie den Vorgang für das sekundäre Gerät.

Schritt 4: Validieren Sie den aktuellen Status mit dem Befehl **show failover state**:

```
> 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
```

Schritt 5: Überprüfen Sie die Konfiguration der primären Einheit mit dem Failover show running-config und der Schnittstelle show running-config:

```
> 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
```

# Aufgabe 4: Ändern der Failover-Rollen

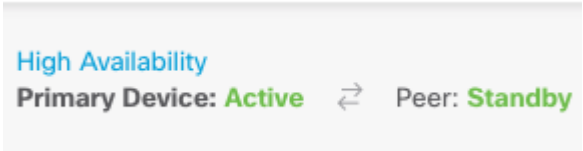
Voraussetzung für diese Aufgabe:

Switching der Failover-Rollen von Primary/Active, Secondary/Standby auf Primary/Standby, Secondary/Active über die grafische Benutzeroberfläche des Secure Firewall Device Manager

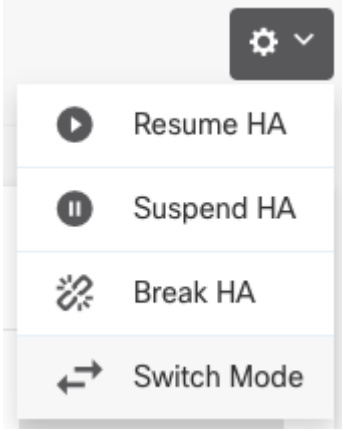
Lösung:

Schritt 1: Auf **Gerät** klicken

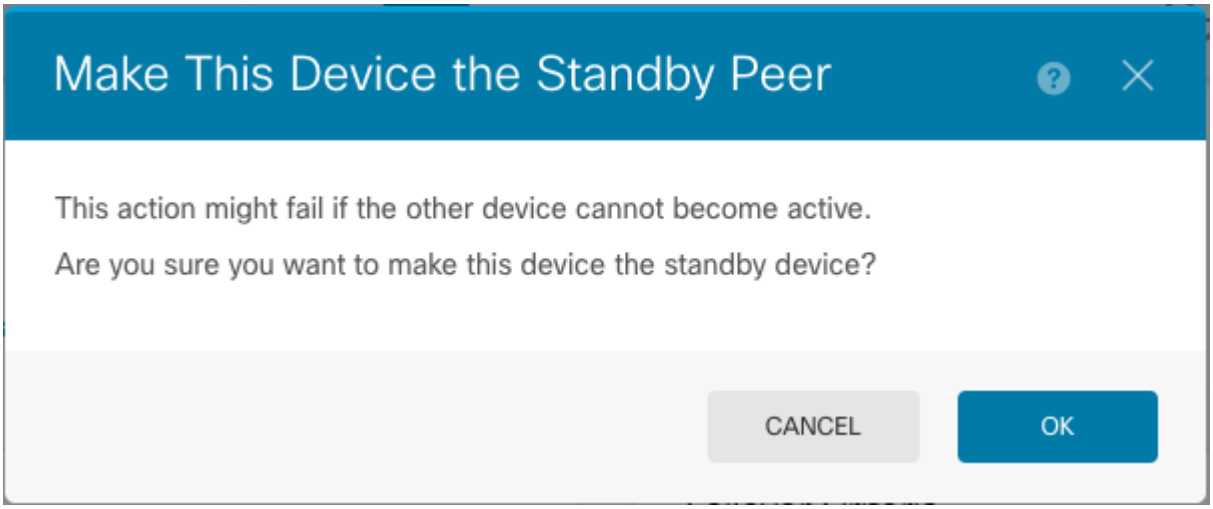

Schritt 2: Klicken Sie auf den Link **Hochverfügbarkeit** rechts in der Geräteübersicht.




Schritt 3: Aus dem Zahnrad-Symbol (), wählen Sie **Switch Mode**.

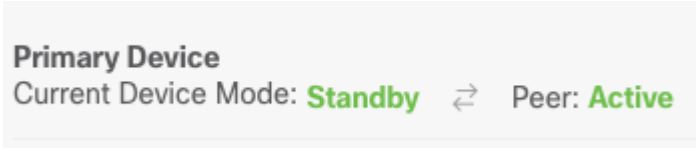



Schritt 4: Lesen Sie die Bestätigungsmeldung, und klicken Sie auf **OK.**




Das System erzwingt einen Failover, sodass das aktive Gerät in den Standby-Modus und das Standby-Gerät in das neue aktive Gerät wechselt.

Schritt 5: Überprüfen Sie das Ergebnis, wie in der Abbildung dargestellt:




Schritt 6: Sie können auch überprüfen, ob der Link "Failover History" (Failoververlauf) verwendet wird und ob das Popup-Fenster der CLI-Konsole die folgenden Ergebnisse anzeigen muss:

```
==========================================================================
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====================================
```

Schritt 7. Erklären Sie nach der Überprüfung die primäre Einheit wieder zur aktiven Einheit.

# Aufgabe 5: Aussetzen oder Wiederaufnehmen der Hochverfügbarkeit

Sie können eine Einheit in einem Paar mit hoher Verfügbarkeit aussetzen. Dies ist nützlich, wenn:

- Beide Geräte befinden sich in einer Aktiv-Aktiv-Situation, und durch die Reparatur der Kommunikation über die Failover-Verbindung wird das Problem nicht behoben.
- Sie möchten eine Fehlerbehebung für ein aktives oder Standby-Gerät durchführen und kein Failover der Geräte während dieser Zeit zulassen.
- Sie möchten Failover verhindern, während Sie ein Software-Upgrade auf dem Standby-Gerät installieren.

Der Hauptunterschied zwischen dem Anhalten der HA-Funktion und dem Unterbrechen der HA-Funktion besteht darin, dass bei einem angehaltenen HA-Gerät die Hochverfügbarkeitskonfiguration beibehalten wird. Wenn Sie die hohe Verfügbarkeit unterbrechen, wird die Konfiguration gelöscht. Sie haben also die Möglichkeit, die hohe Verfügbarkeit auf einem außer Betrieb genommenen System wiederherzustellen. Dadurch wird die bestehende Konfiguration aktiviert, und die beiden Geräte funktionieren wieder als Failover-Paar.

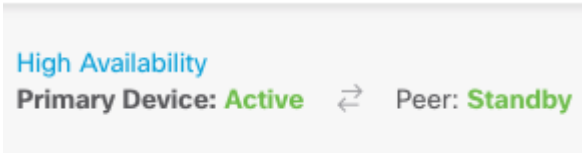
Voraussetzung für diese Aufgabe:

Setzen Sie über die grafische Benutzeroberfläche des Secure Firewall Device Manager die primäre Einheit aus, und setzen Sie die hohe Verfügbarkeit auf derselben Einheit fort.

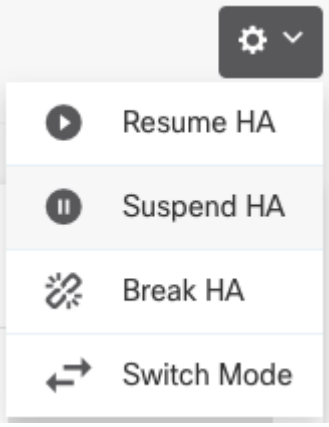
Lösung:

Schritt 1: Klicken Sie auf **Gerät.**

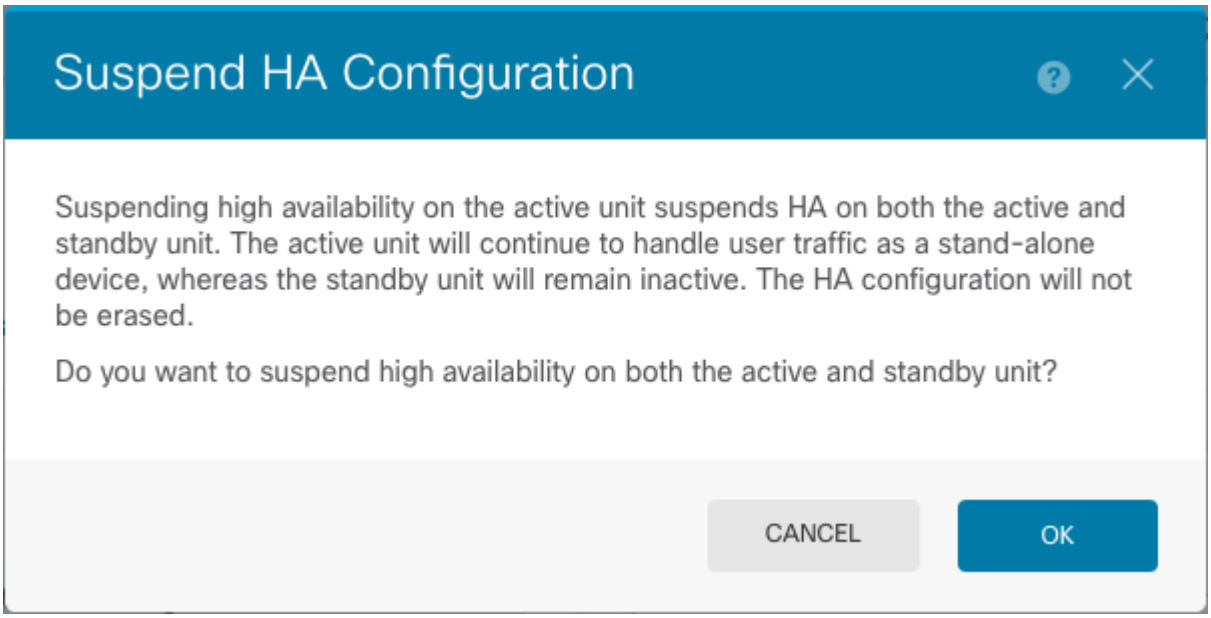

Schritt 2: Klicken Sie auf den Link **Hochverfügbarkeit** rechts in der Geräteübersicht.



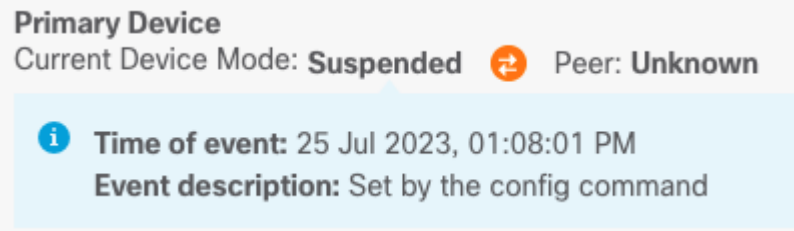

Schritt 3: Aus dem Zahnrad-Symbol (), wählen Sie **HA aussetzen**.



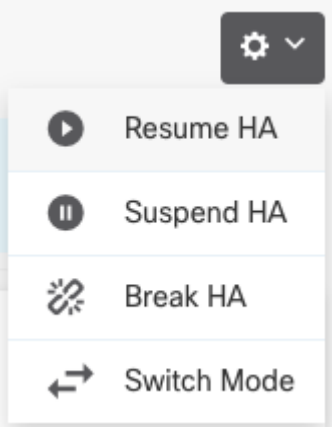

Schritt 4: Lesen Sie die Bestätigungsmeldung, und klicken Sie auf **OK.**



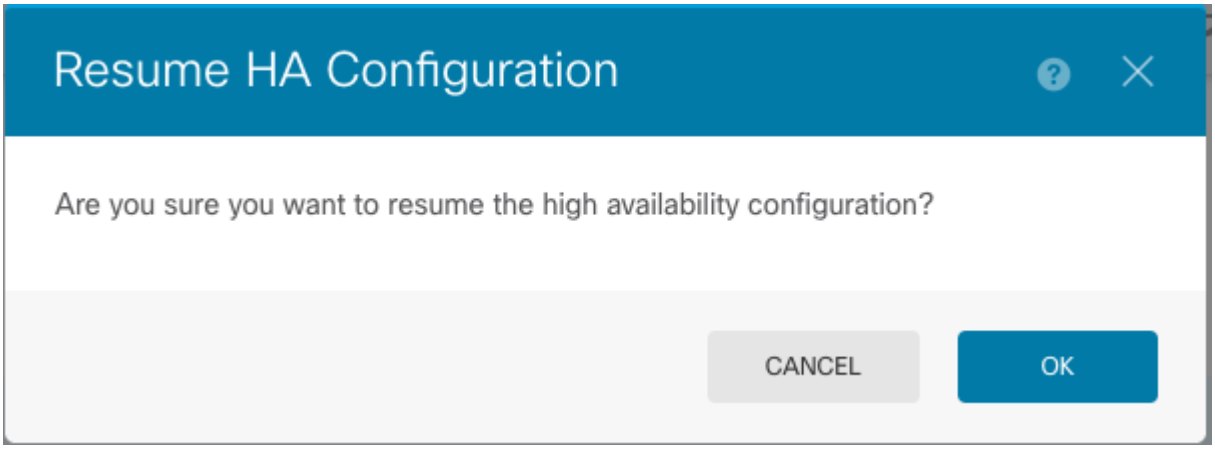

Schritt 5: Überprüfen Sie das Ergebnis, wie in der Abbildung dargestellt:



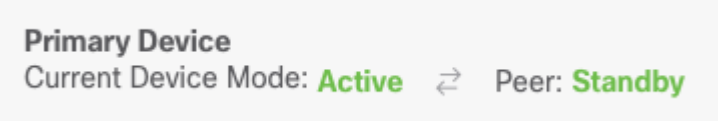

Schritt 6: Um die hohe Verfügbarkeit wieder aufzunehmen, klicken Sie auf das Zahnradsymbol ( ), wählen Sie **Resume HA**.




Schritt 7. Lesen Sie die Bestätigungsmeldung, und klicken Sie auf **OK.**




Schritt 5: Überprüfen Sie das Ergebnis, wie in der Abbildung dargestellt:




# Aufgabe 6: Hohe Verfügbarkeit

Wenn die beiden Geräte nicht mehr als hochverfügbares Paar betrieben werden sollen, können Sie die HA-Konfiguration unterbrechen. Wenn Sie die hohe Verfügbarkeit unterbrechen, wird jedes Gerät zu einem eigenständigen Gerät. Ihre Konfigurationen müssen sich wie folgt ändern:

- Das aktive Gerät behält die vollständige Konfiguration wie vor der Unterbrechung bei, ohne dass die HA-Konfiguration geändert wurde.
- Auf dem Standby-Gerät wurden zusätzlich zur HA-Konfiguration alle Schnittstellenkonfigurationen entfernt. Alle physischen Schnittstellen sind deaktiviert, Subschnittstellen jedoch nicht. Die Management-Schnittstelle bleibt aktiv, sodass Sie sich beim Gerät anmelden und es neu konfigurieren können.

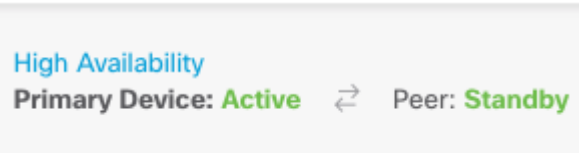
Voraussetzung für diese Aufgabe:

Brechen Sie das Hochverfügbarkeitspaar von der grafischen Benutzeroberfläche des Secure Firewall Device Manager auf.

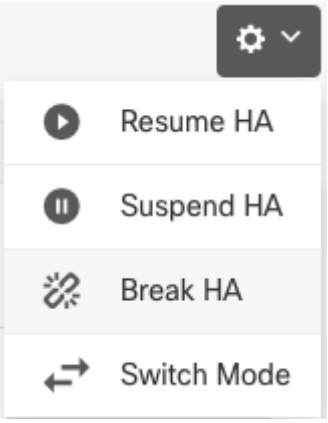
Lösung:

Schritt 1: Klicken Sie auf **Gerät.**


Schritt 2: Klicken Sie auf den Link **Hochverfügbarkeit** rechts in der Geräteübersicht.



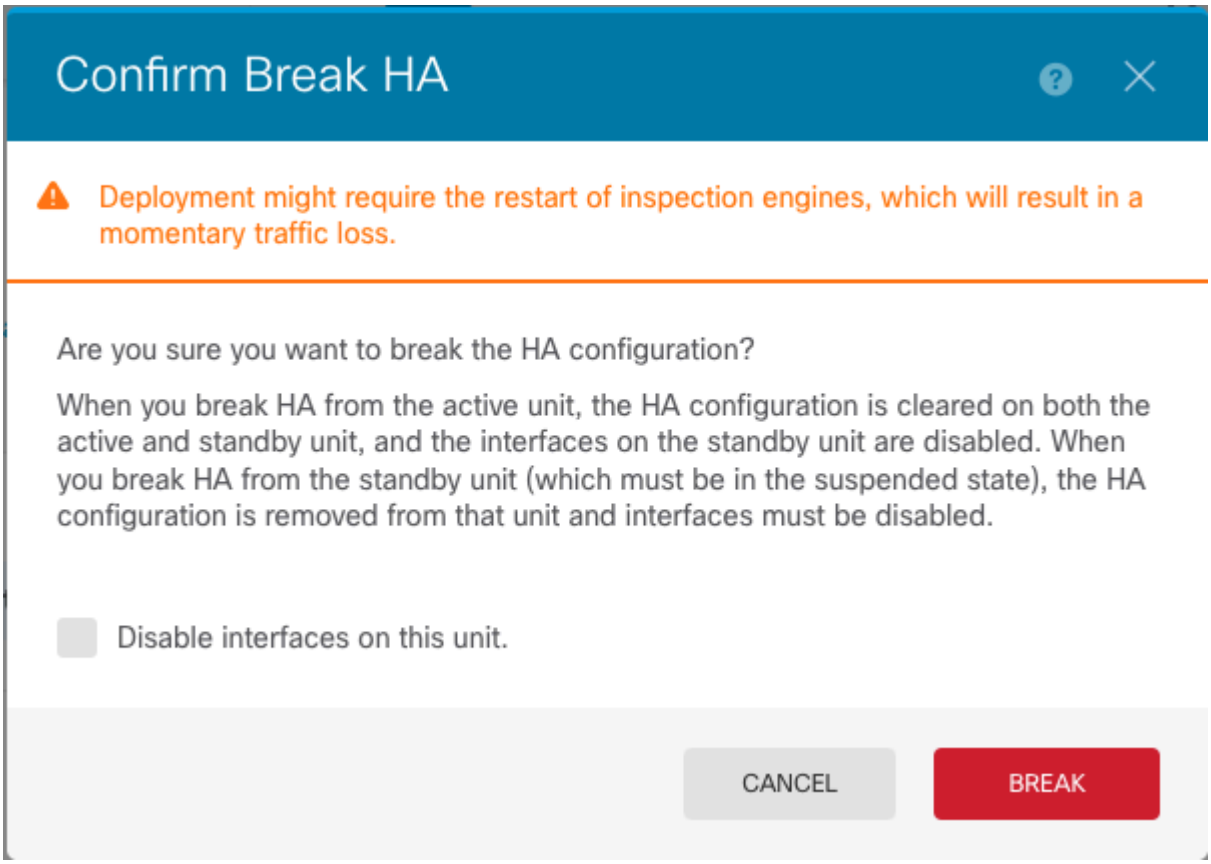

Schritt 3: Aus dem Zahnrad-Symbol (), wählen Sie **Break HA**.



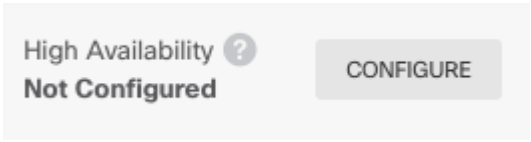

Schritt 4: Lesen Sie die Bestätigungsmeldung, wählen Sie die Option zum Deaktivieren der Schnittstellen aus, und klicken Sie auf **Break (Unterbrechung)**.

Sie müssen die Option zum Deaktivieren der Schnittstellen auswählen, wenn Sie die HA-Funktion des Standby-Geräts unterbrechen.

Das System stellt Ihre Änderungen sofort sowohl auf diesem Gerät als auch auf dem Peer-Gerät bereit (wenn möglich). Es kann einige Minuten dauern, bis die Bereitstellung auf jedem Gerät abgeschlossen ist und jedes Gerät unabhängig wird.




Schritt 5: Überprüfen Sie das Ergebnis, wie in der Abbildung dargestellt:




# Zugehörige Informationen

- Alle Versionen des Cisco Secure Firewall Device Manager-Konfigurationsleitfadens finden Sie hier.

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

- Das Cisco Global Technical Assistance Center (TAC) empfiehlt dringend diesen Leitfaden, um detailliertes praktisches Wissen über die Sicherheitstechnologien der nächsten Generation von Cisco FirePOWER zu erhalten:

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

- Für alle technischen Hinweise zu Konfiguration und Fehlerbehebung, die sich auf die FirePOWER-Technologien beziehen

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

- Technischer Support und Dokumentation für Cisco Systeme

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.