

고가용성의 보안 방화벽 디바이스 관리자 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[작업 1. 조건 확인](#)

[작업 2. 고가용성의 보안 방화벽 디바이스 관리자 구성](#)

[네트워크 다이어그램](#)

[기본 유닛의 Secure Firewall Device Manager에서 고가용성 활성화](#)

[보조 유닛의 Secure Firewall Device Manager에서 고가용성 활성화](#)

[인터페이스 컨피그레이션 완료](#)

[작업 3. FDM 고가용성 확인](#)

[작업 4. 장애 조치 역할 전환](#)

[작업 5. 고가용성 일시 중단 또는 재개](#)

[작업 6. 고가용성 보장](#)

[관련 정보](#)

소개

이 문서에서는 보안 방화벽 디바이스에서 FDM(Secure Firewall Device Manager) HA(High Availability)를 구성하고 확인하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 2xCisco Secure Firewall 2100 Security Appliance
- FDM 버전 7.0.5 실행(빌드 72)

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

작업 1. 조건 확인

작업 요구 사항:

두 FDM 어플라이언스가 메모 요구 사항을 충족하며 HA 단위로 구성할 수 있는지 확인합니다.

해결책:

1단계. SSH를 사용하여 어플라이언스 관리 IP에 연결하고 모듈 하드웨어를 확인합니다.

기본 디바이스 하드웨어 및 소프트웨어 버전에 대해 show version 명령을 사용하여 확인합니다.

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

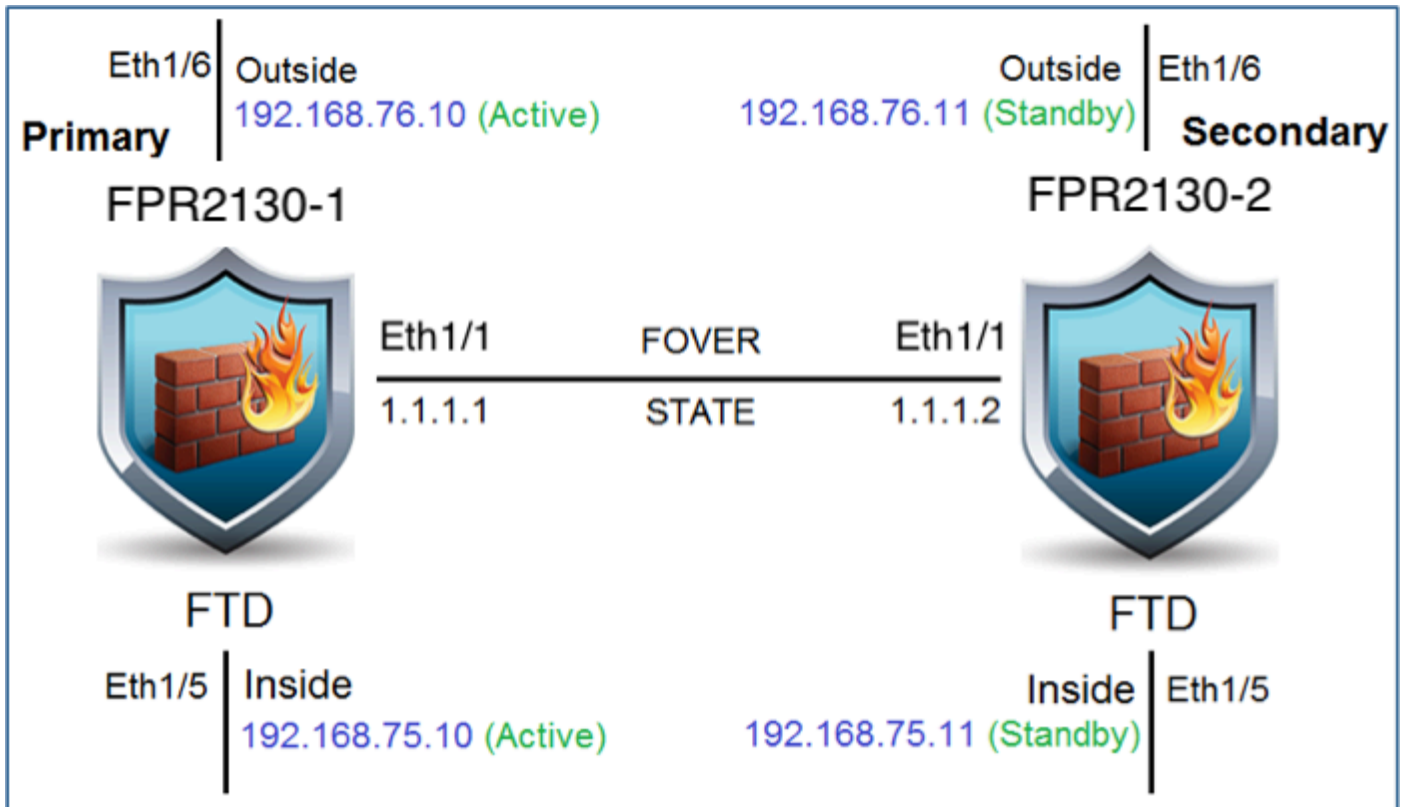
보조 디바이스 하드웨어 및 소프트웨어 버전을 확인합니다.

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

작업 2. 고가용성의 보안 방화벽 디바이스 관리자 구성

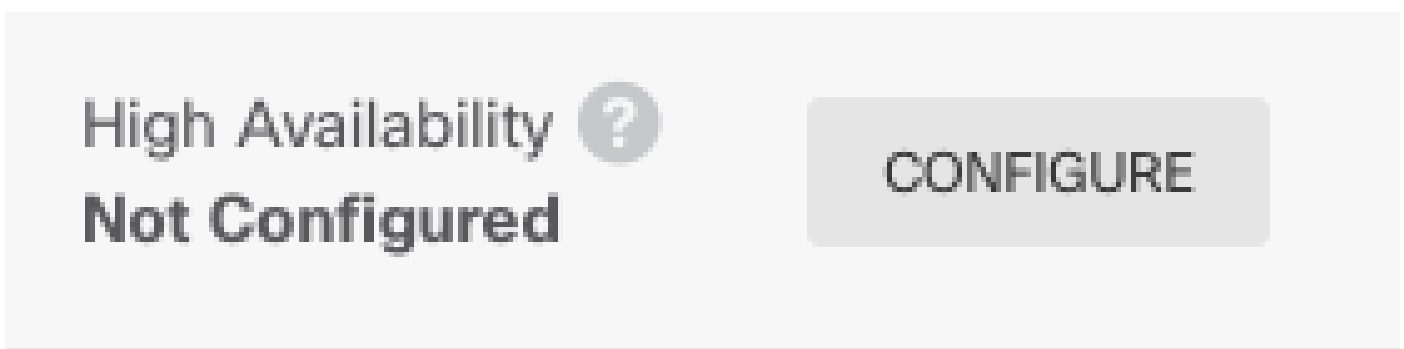
네트워크 다이어그램

이 다이어그램에 따라 액티브/스탠바이 HA(High Availability)를 구성합니다.

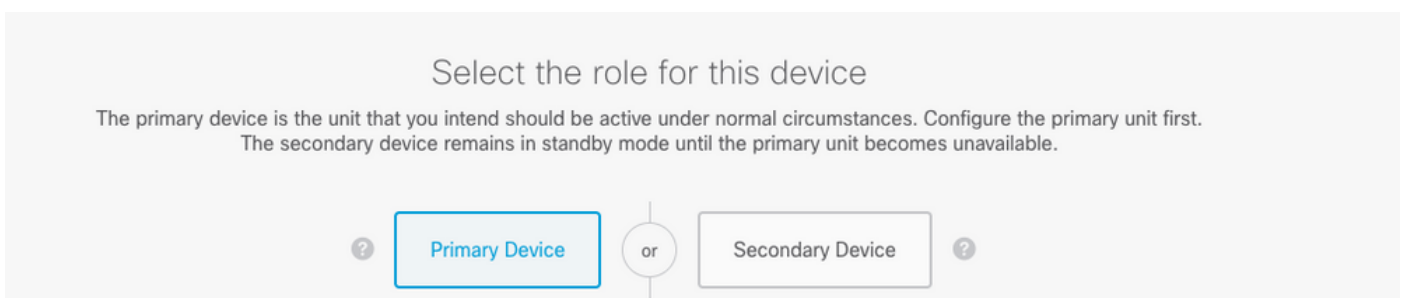


기본 유닛의 Secure Firewall Device Manager에서 고가용성 활성화

1단계. FDM 장애 조치를 구성하려면 Device(디바이스)로 이동하고 High Availability 그룹 옆의 Configure(구성)를 클릭합니다.



2단계. High Availability(고가용성) 페이지에서 Primary Device(기본 디바이스) 상자를 클릭합니다.



경고: 올바른 유닛을 기본 유닛으로 선택해야 합니다. 선택한 기본 유닛의 모든 컨피그레이션이 선택한 보조 FTD 유닛에 복제됩니다. 복제의 결과로 보조 유닛의 현재 컨피그레이션을 교

체할 수 있습니다.

3단계. 장애 조치 링크 및 상태 링크 설정을 구성합니다.

이 예에서 상태 링크는 장애 조치 링크와 동일한 설정을 갖습니다.

FAILOVER LINK	STATEFUL FAILOVER LINK <input checked="" type="checkbox"/> Use the same interface as the Failover Link
Interface unnamed (Ethernet1/1) ▾	Interface unnamed (Ethernet1/1) ▾
Type <input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6	Type <input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6
Primary IP 1.1.1.1 <small>e.g. 192.168.10.1</small>	Primary IP 1.1.1.1 <small>e.g. 192.168.11.1</small>
Secondary IP 1.1.1.2 <small>e.g. 192.168.10.2</small>	Secondary IP 1.1.1.2 <small>e.g. 192.168.11.2</small>
Netmask 255.255.255.252 <small>e.g. 255.255.255.0 or 24</small>	Netmask 255.255.255.252 <small>e.g. 255.255.255.0 or 24</small>
IPSec Encryption Key (optional) <small>For security purposes, the encryption key will not be included in the configuration copied to the clipboard when you activate HA. You will need to manually enter the key when you configure HA on the peer device.</small>	IMPORTANT <small>If you configure an IPsec encryption key with inconsistent settings for export controlled features, both devices will become active after you activate HA. Learn More</small>

4단계. HA 활성화를 클릭합니다.

5단계. 확인 메시지에서 HA 컨피그레이션을 클립보드에 복사하여 보조 유닛에 붙여넣습니다.

You have successfully deployed the HA configuration on the primary device.



What's next?

I need to configure Peer Device

I configured both devices



Copy the HA configuration to the clipboard.

✓ Copied [Click here to copy again](#)



Paste it on the secondary device.

Log into the secondary device and open the HA configuration page.



You are done!

The devices should communicate and establish a high availability pair automatically.

GOT IT

시스템은 즉시 컨피그레이션을 디바이스에 구축합니다. 배포 작업을 시작할 필요가 없습니다. 컨피그레이션이 저장되었고 구축이 진행 중이라는 메시지가 표시되지 않으면 페이지 맨 위로 스크롤하여 오류 메시지를 확인합니다.

구성이 클립보드에도 복사됩니다. 복사본을 사용하여 보조 유닛을 신속하게 구성할 수 있습니다. 보안을 강화하기 위해 암호화 키는 클립보드 복사본에 포함되지 않습니다.

이 시점에서 High Availability(고가용성) 페이지에 있어야 하며 디바이스 상태는 "Negotiating(협상 중)"이어야 합니다. 피어를 구성하기 전이라도 상태가 Active로 전환되어야 합니다. 이 경우 피어를 구성할 때까지 Failed로 표시되어야 합니다.

High Availability

Primary Device: **Active**



Peer: **Failed**

보조 유닛의 Secure Firewall Device Manager에서 고가용성 활성화

액티브/스탠바이 고가용성을 위해 기본 디바이스를 구성한 후에 보조 디바이스를 구성해야 합니다. 해당 디바이스에서 FDM에 로그인하고 이 절차를 실행합니다.

1단계. FDM 장애 조치를 구성하려면 Device(디바이스)로 이동하고 High Availability 그룹 옆의 Configure(구성)를 클릭합니다.

High Availability 
Not Configured

CONFIGURE

2단계. High Availability(고가용성) 페이지에서 Secondary Device(보조 디바이스) 상자를 클릭합니다.

Device Summary

High Availability

How High Availability Works

Select the role for this device

The primary device is the unit that you intend should be active under normal circumstances. Configure the primary unit first.
The secondary device remains in standby mode until the primary unit becomes unavailable.



Primary Device

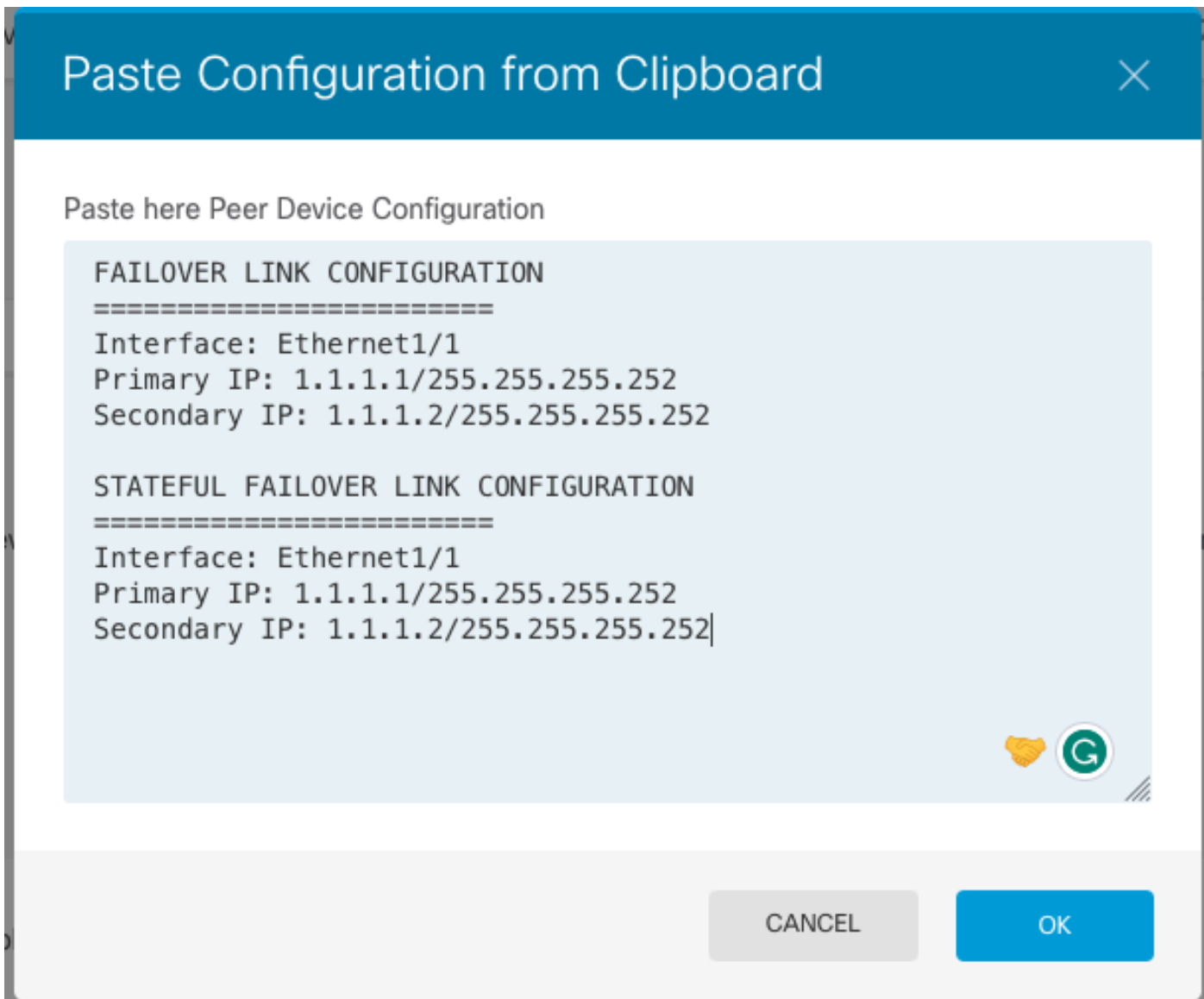
or

Secondary Device



3단계. 다음 옵션 중 하나를 선택합니다.

- Easy method(쉬운 방법) - Paste from Clipboard(클립보드에서 붙여넣기) 버튼을 클릭하고 컨피그레이션에 붙여넣은 다음 OK(확인)를 클릭합니다. 그러면 필드가 적절한 값으로 업데이트 되며, 이 값을 확인할 수 있습니다.
- Manual method(수동 방법) - 장애 조치 및 상태 저장 장애 조치 링크를 직접 구성합니다. 기본 디바이스에서 입력한 것과 동일한 설정을 보조 디바이스에서 입력합니다.

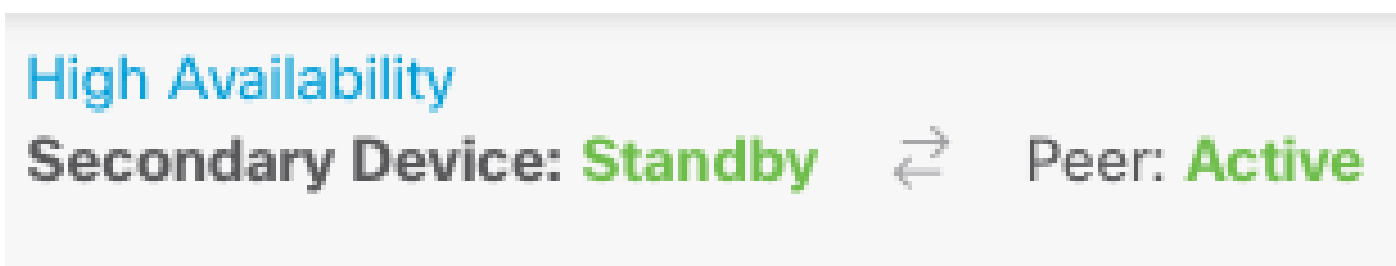


4단계. HA 활성화를 클릭합니다.

시스템은 즉시 컨피그레이션을 디바이스에 구축합니다. 배포 작업을 시작할 필요가 없습니다. 컨피그레이션이 저장되었고 구축이 진행 중이라는 메시지가 표시되지 않으면 페이지 맨 위로 스크롤하여 오류 메시지를 확인합니다.

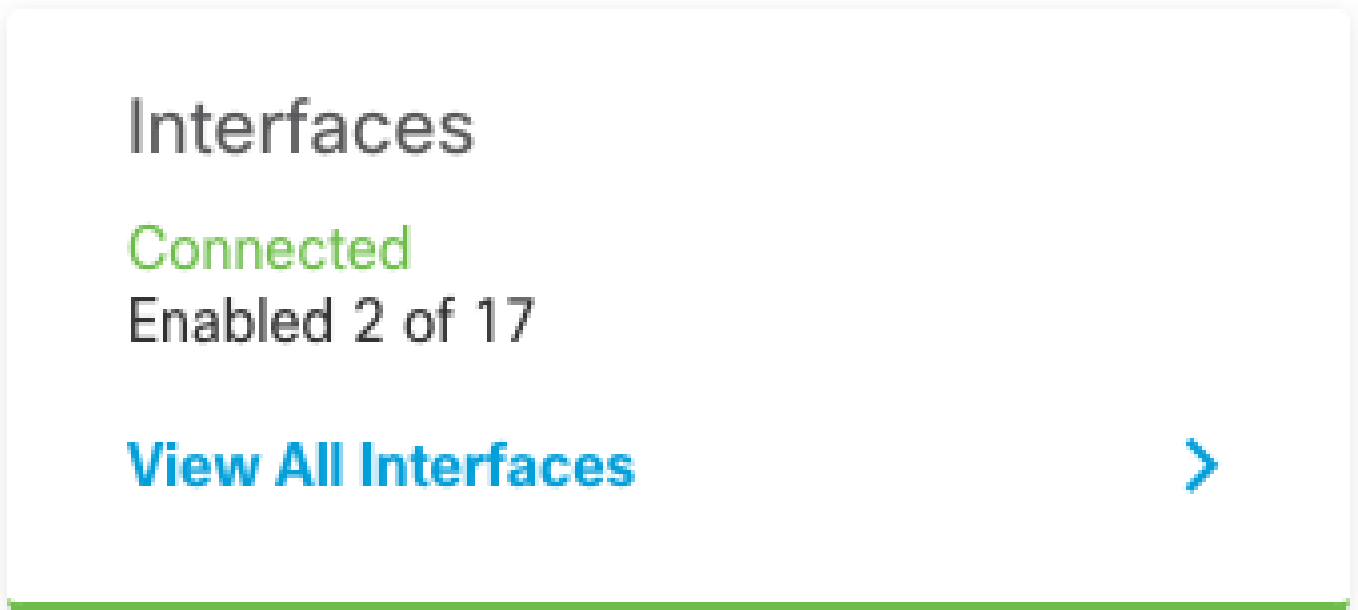
컨피그레이션이 완료되면 HA를 구성했다는 메시지가 표시됩니다. 메시지를 무시하려면 Got It을 클릭합니다.

이 시점에서 High Availability(고가용성) 페이지에 있어야 하며 디바이스 상태가 보조 디바이스임을 나타내야 합니다. 기본 디바이스와의 조인에 성공한 경우 디바이스는 기본 디바이스와 동기화되며, 결국 모드는 대기 모드이고 피어는 활성 상태여야 합니다.



인터페이스 컨피그레이션 완료

1단계. FDM 인터페이스를 구성하려면 Device(디바이스)로 이동하고 View All Interfaces(모든 인터페이스 보기)를 클릭합니다.



2단계. 이미지에 표시된 대로 Interfaces 설정을 선택하고 수정합니다.

이더넷 1/5 인터페이스:

Ethernet1/5

Edit Physical Interface



Interface Name

inside

Mode

Routed

Status



Most features work with named interfaces only, although some require unnamed interfaces.

Description

IPv4 Address

IPv6 Address

Advanced

Type

Static

IP Address and Subnet Mask

192.168.75.10

/

255.255.255.0

e.g. 192.168.5.15/17 or 192.168.5.15/255.255.128.0

Standby IP Address and Subnet Mask

192.168.75.11

/

255.255.255.0

e.g. 192.168.5.16

CANCEL

OK

이더넷 1/6 인터페이스

Ethernet1/6 Edit Physical Interface



Interface Name

outside

Mode

Routed

Status



Most features work with named interfaces only, although some require unnamed interfaces.

Description

IPv4 Address

IPv6 Address

Advanced

Type

Static

IP Address and Subnet Mask

192.168.76.10

/

255.255.255.0

e.g. 192.168.5.15/17 or 192.168.5.15/255.255.128.0

Standby IP Address and Subnet Mask

192.168.76.11

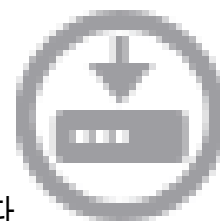
/

255.255.255.0

e.g. 192.168.5.16

CANCEL

OK



3단계. 변경 사항을 구성한 후 Pending Changes(보류 중인 변경 사항)를 클릭합니다
구축할 수 있습니다.

작업 3. FDM 고가용성 확인

작업 요구 사항:

FDM GUI 및 FDM CLI에서 고가용성 설정을 확인합니다.

해결책:

1단계. Device(디바이스)로 이동하여 High Availability(고가용성) 설정을 확인합니다.

The screenshot displays the 'High Availability' configuration page in the FDM GUI. At the top, it shows 'Device Summary' and 'High Availability' status. Below this, there are tabs for 'Primary Device', 'Failover History', and 'Deployment History'. The primary device mode is 'Active' and the peer is 'Standby'. The main configuration area is divided into several sections: 'High Availability Configuration' with a tip to select and configure the peer device; 'GENERAL DEVICE INFORMATION' listing model (Cisco Firepower 2130 Threat Defense), software (7.0.5-72), VDB (338.0), and intrusion rule update (20210503-2107); 'FAILOVER LINK' section with interface (Ethernet1/1), type (IPv4), primary IP/netmask (1.1.1.1/255.255.255.252), and secondary IP/netmask (1.1.1.2/255.255.255.252); 'STATEFUL FAILOVER LINK' which is the same as the failover link; and 'IPSEC ENCRYPTION KEY: NOT CONFIGURED'. On the right, the 'Failover Criteria' section includes 'INTERFACE FAILURE THRESHOLD' (Number of failed interfaces exceeds 1) and 'INTERFACE TIMING CONFIGURATION' (Poll Time: 5000, Hold Time: 25000) and 'PEER TIMING CONFIGURATION' (Poll Time: 1000, Hold Time: 15000). A 'SAVE' button is visible at the bottom of the failover criteria section.

2단계. SSH를 사용하여 FDM 기본 디바이스 CLI에 연결하고 show high-availability config 명령으로 확인합니다.

```
> 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         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

```

3단계. 보조 디바이스에서도 같은 작업을 수행합니다.

4단계. show failover state 명령을 사용하여 현재 상태를 확인합니다.

```
> 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
```

5단계. show running-config failover 및 show running-config 인터페이스를 사용하여 기본 유닛의 컨피그레이션을 확인합니다.

```
> 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
```

작업 4. 장애 조치 역할 전환

작업 요구 사항:

보안 방화벽 디바이스 관리자 그래픽 인터페이스에서 장애 조치 역할을 기본/액티브, 보조/스탠바이에서 기본/스탠바이, 보조/액티브로 전환합니다

해결책:

1단계. Device(디바이스)를 클릭합니다.



Device: FPR2130-1

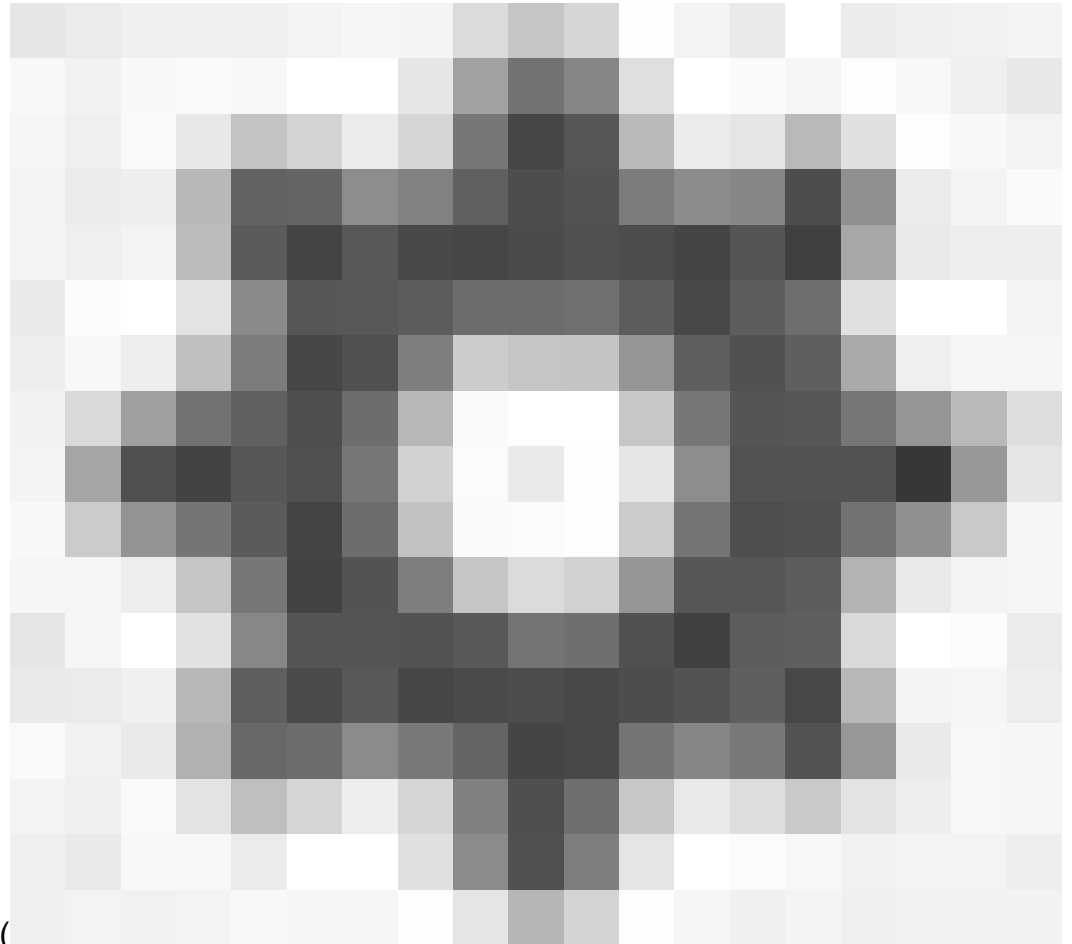
2단계. 장치 요약 오른쪽에 있는 High Availability(고가용성) 링크를 클릭합니다.

High Availability

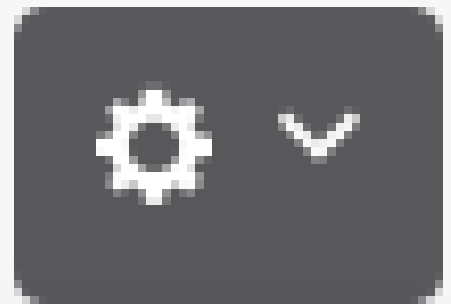
Primary Device: **Active**



Peer: **Standby**



3단계. 톱니바퀴 아이콘(), Switch Mode(스위치 모드)를 선택합니다.



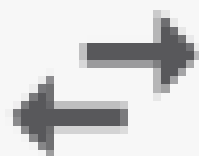
Resume HA



Suspend HA



Break HA



Switch Mode

4단계. 확인 메시지를 읽고 OK(확인)를 클릭합니다.

Make This Device the Standby Peer



This action might fail if the other device cannot become active.

Are you sure you want to make this device the standby device?

CANCEL

OK

시스템은 액티브 유닛이 스탠바이 유닛이 되고 스탠바이 유닛이 새 액티브 유닛이 되도록 장애 조치를 강제로 실행합니다.

5단계. 이미지에 표시된 대로 결과를 확인합니다.

Primary Device

Current Device Mode: **Standby** ↔ Peer: **Active**

6단계. Failover History(장애 조치 기록) 링크를 사용하여 확인할 수도 있으며, CLI Console(CLI 콘솔) 팝업에 결과가 표시되어야 합니다.

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=====

```

7단계. 확인 후 기본 유닛을 다시 액티브 상태로 설정합니다.

작업 5. 고가용성 일시 중단 또는 재개

고가용성 쌍에서 유닛을 일시 중단할 수 있습니다. 이 기능은 다음과 같은 경우에 유용합니다.

- 두 유닛 모두 액티브-액티브 상황이며 장애 조치 링크에서 통신을 수정해도 문제가 해결되지 않습니다.
- 액티브 또는 스탠바이 유닛의 문제를 해결하고 해당 시간 동안 유닛의 장애 조치를 원치 않을 수 있습니다.
- 스탠바이 디바이스에 소프트웨어 업그레이드를 설치하는 동안 장애 조치를 방지하려는 경우

HA 일시 중단과 HA 중단 사이의 주요 차이점은 일시 중단된 HA 디바이스에서 고가용성 컨피그레이션이 유지된다는 점입니다. HA를 중단하면 컨피그레이션이 지워집니다. 따라서 중단된 시스템에서 HA를 재개할 수 있는 옵션이 있습니다. 그러면 기존 컨피그레이션이 활성화되고 두 디바이스가 장애 조치 쌍으로 다시 작동합니다.

작업 요구 사항:

Secure Firewall Device Manager 그래픽 인터페이스에서 기본 유닛을 일시 중지하고 동일한 유닛에서 고가용성을 다시 시작합니다.

해결책:

1단계. Device를 클릭합니다.



Device: FPR2130-1

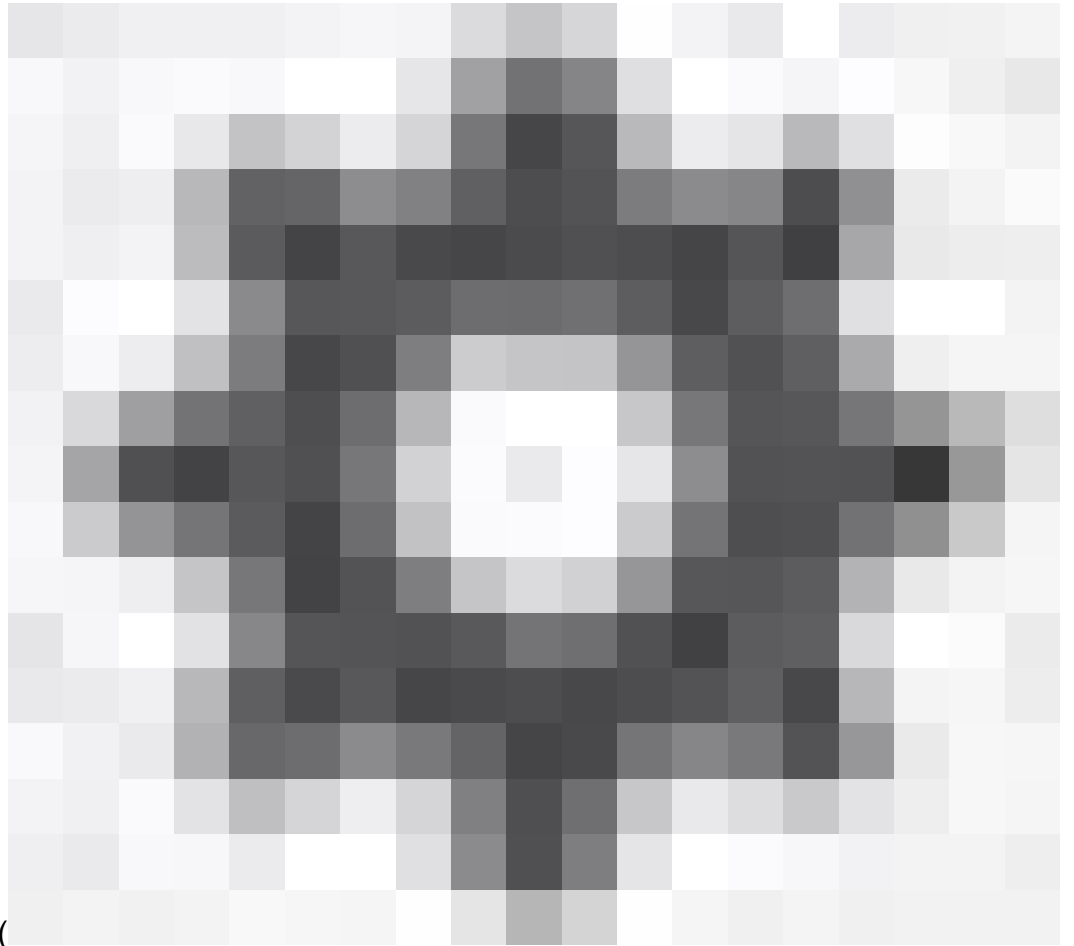
2단계. 장치 요약 오른쪽에 있는 High Availability(고가용성) 링크를 클릭합니다.

High Availability

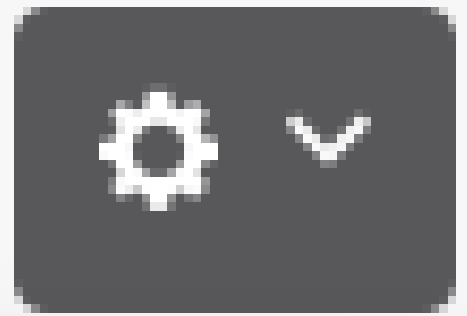
Primary Device: **Active**



Peer: **Standby**



3단계. 톱니바퀴 아이콘(
) Suspend HA(HA 일시 중단)를 선택합니다.



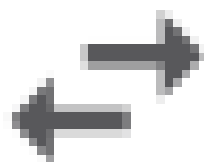
Resume HA



Suspend HA



Break HA



Switch Mode

4단계. 확인 메시지를 읽고 OK(확인)를 클릭합니다.

Suspend HA Configuration



Suspending high availability on the active unit suspends HA on both the active and standby unit. The active unit will continue to handle user traffic as a stand-alone device, whereas the standby unit will remain inactive. The HA configuration will not be erased.

Do you want to suspend high availability on both the active and standby unit?

CANCEL

OK

5단계. 이미지에 표시된 대로 결과를 확인합니다.

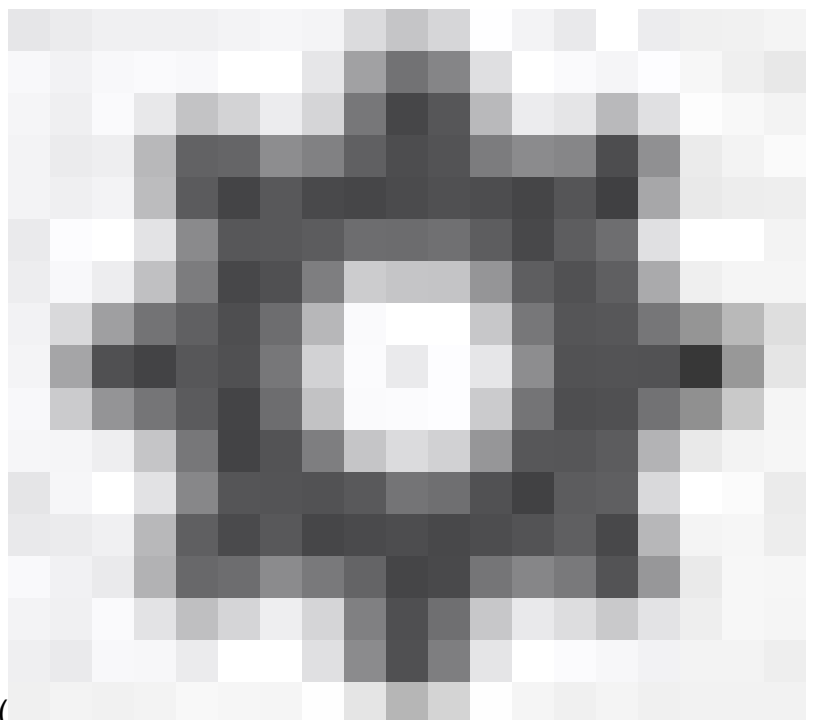
Primary Device


Current Device Mode: **Suspended**  Peer: **Unknown**



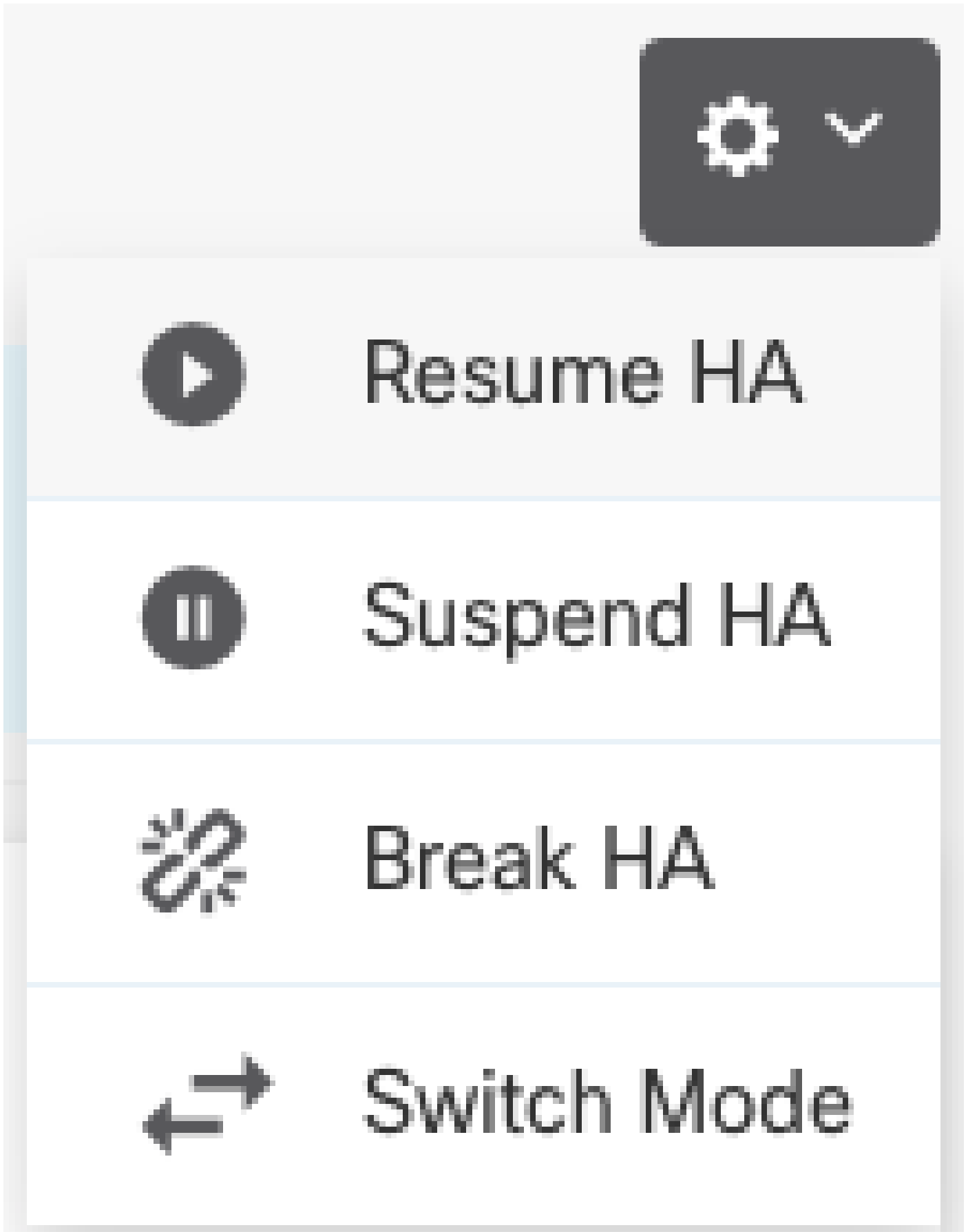
Time of event: 25 Jul 2023, 01:08:01 PM

Event description: Set by the config command

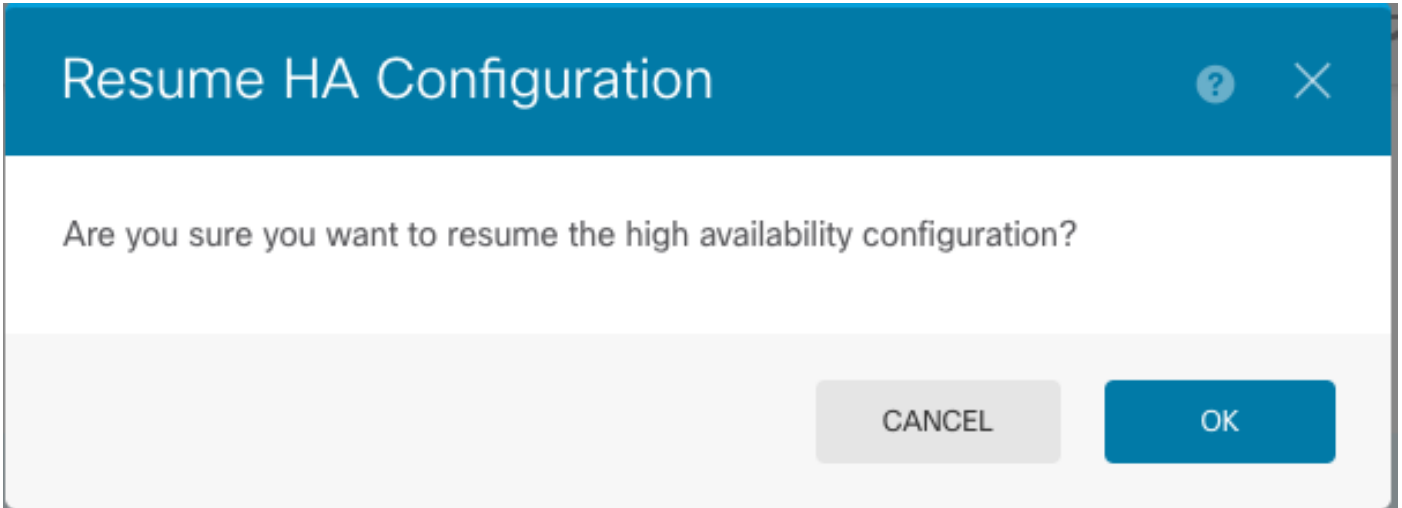


6단계. HA를 재개하려면 톱니바퀴 아이콘()

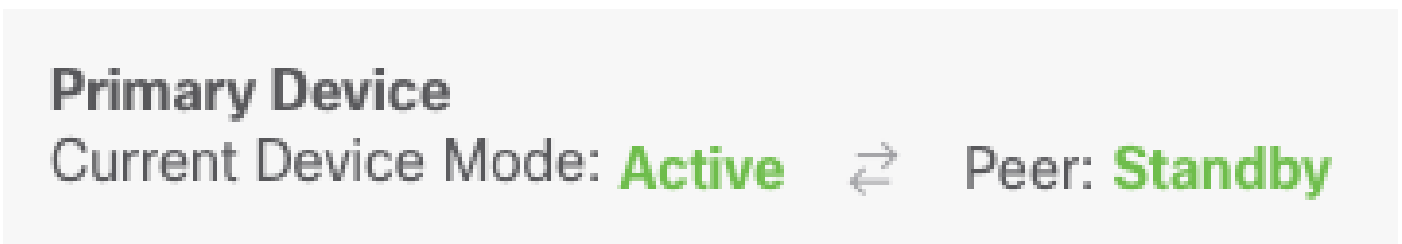
) Resume HA(HA 재개)를 선택합니다.



7단계. 확인 메시지를 읽고 OK(확인)를 클릭합니다.



5단계. 이미지에 표시된 대로 결과를 확인합니다.



작업 6. 고가용성 보장

두 디바이스를 더 이상 고가용성 쌍으로 작동하지 않으려면 HA 컨피그레이션을 중단할 수 있습니다. HA를 중단하면 각 디바이스는 독립형 디바이스가 됩니다. 해당 구성은 다음과 같이 변경해야 합니다.

- 활성 디바이스는 중단 이전의 전체 컨피그레이션을 유지하고 HA 컨피그레이션은 제거합니다.
- 스탠바이 디바이스에는 HA 컨피그레이션 외에도 모든 인터페이스 컨피그레이션이 제거됩니다. 모든 물리적 인터페이스는 비활성화되지만 하위 인터페이스는 비활성화되지 않습니다. 관리 인터페이스는 활성 상태로 유지되므로 디바이스에 로그인하고 다시 구성할 수 있습니다.

작업 요구 사항:

Secure Firewall Device Manager 그래픽 인터페이스에서 고가용성 쌍을 해제합니다.

해결책:

1단계. Device를 클릭합니다.



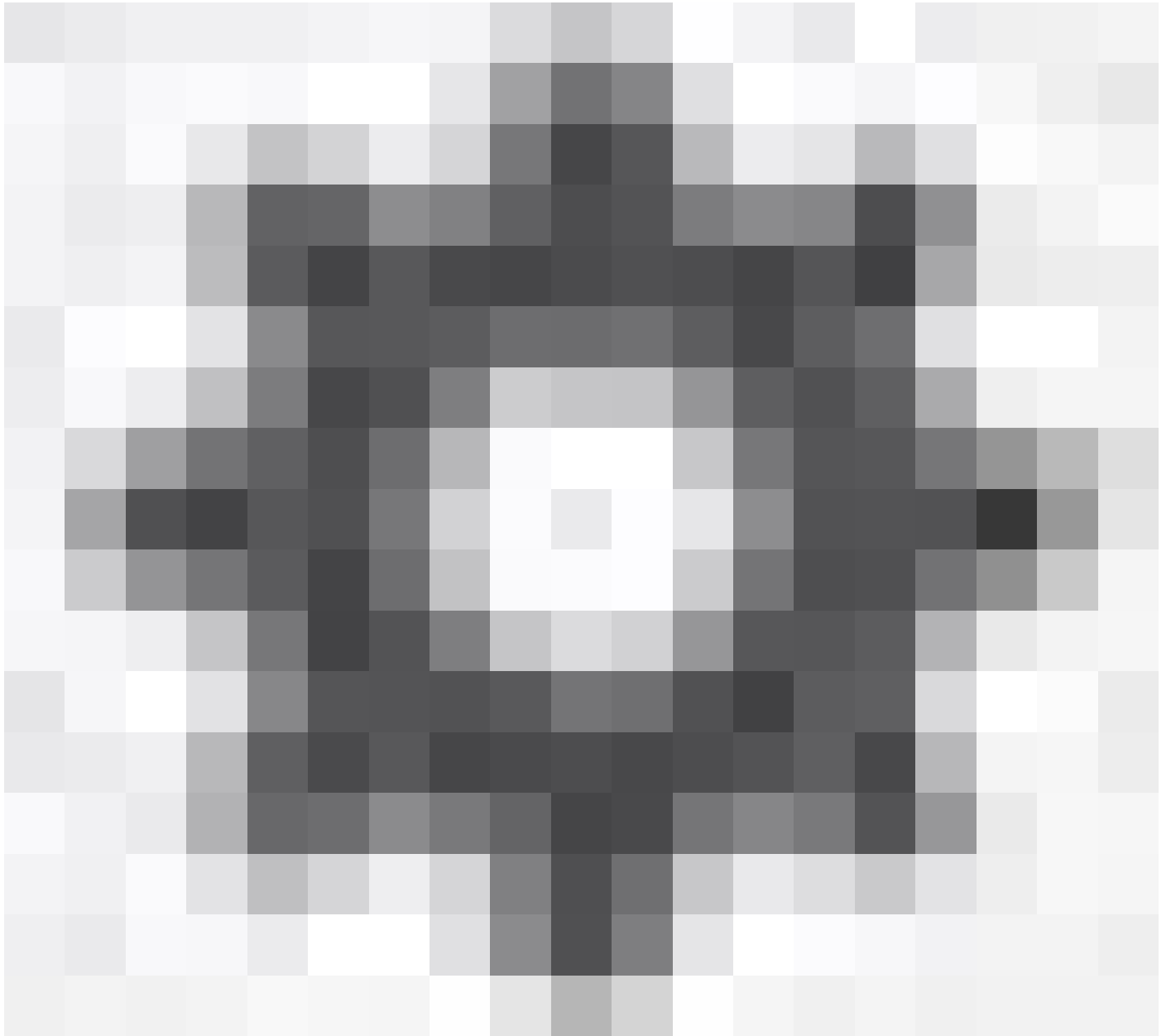
Device: FPR2130-1

2단계. 장치 요약 오른쪽에 있는 High Availability(고가용성) 링크를 클릭합니다.

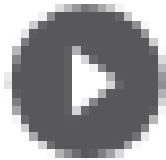
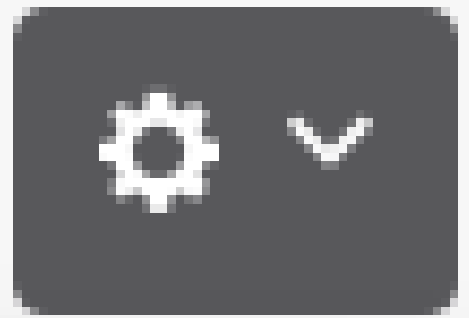
High Availability

Primary Device: **Active** ↔ Peer: **Standby**

3단계. 톱니바퀴 아이콘(



), Break HA(HA 중단)를 선택합니다.



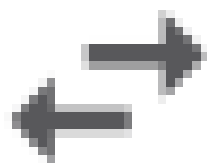
Resume HA



Suspend HA



Break HA



Switch Mode

4단계. 확인 메시지를 읽고 인터페이스를 비활성화할 옵션을 선택할지 결정한 후 Break(중단)를 클릭합니다.

스탠바이 유닛에서 HA를 중단하는 경우 인터페이스를 비활성화하는 옵션을 선택해야 합니다.

시스템은 이 디바이스와 피어 디바이스(가능한 경우) 모두에 변경 사항을 즉시 구축합니다. 각 디바이스에서 구축이 완료되고 각 디바이스에서 독립화되는 데 몇 분 정도 걸릴 수 있습니다.

Confirm Break HA ? ×

⚠ Deployment might require the restart of inspection engines, which will result in a momentary traffic loss.

Are you sure you want to break the HA configuration?

When you break HA from the active unit, the HA configuration is cleared on both the active and standby unit, and the interfaces on the standby unit are disabled. When you break HA from the standby unit (which must be in the suspended state), the HA configuration is removed from that unit and interfaces must be disabled.

Disable interfaces on this unit.

CANCEL BREAK

5단계. 이미지에 표시된 것과 같이 결과를 확인합니다:

High Availability ?
Not Configured

CONFIGURE

관련 정보

- 모든 버전의 Cisco Secure Firewall Device Manager 컨피그레이션 가이드는 여기에서 확인할 수 있습니다

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

- Cisco TAC(Global Technical Assistance Center)에서는 Cisco Firepower Next-Generation Security 기술에 대한 심층적인 실무 지식을 얻을 수 있도록 이 시각적 가이드를 적극 권장합니다.

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

- firepower 기술과 관련된 모든 컨피그레이션 및 문제 해결 TechNotes

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

- [기술 지원 및 문서 - Cisco Systems](#)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.