

FDM을 사용하여 FTD 고가용성 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[네트워크 토폴로지](#)

[구성](#)

[고가용성을 위한 기본 유닛구성](#)

[고가용성을 위한 보조 유닛구성](#)

[다음을 확인합니다.](#)

소개

이 문서에서는 로컬에서 관리되는 FTD(Secure Firewall Threat Defense)의 액티브/스탠바이 HA(고가용성) 쌍을 설정하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 항목에 대한 지식을 갖추는 것이 좋습니다.

- GUI 및/또는 셸을 통한 Cisco Secure Firewall Threat Defense 초기 컨피그레이션

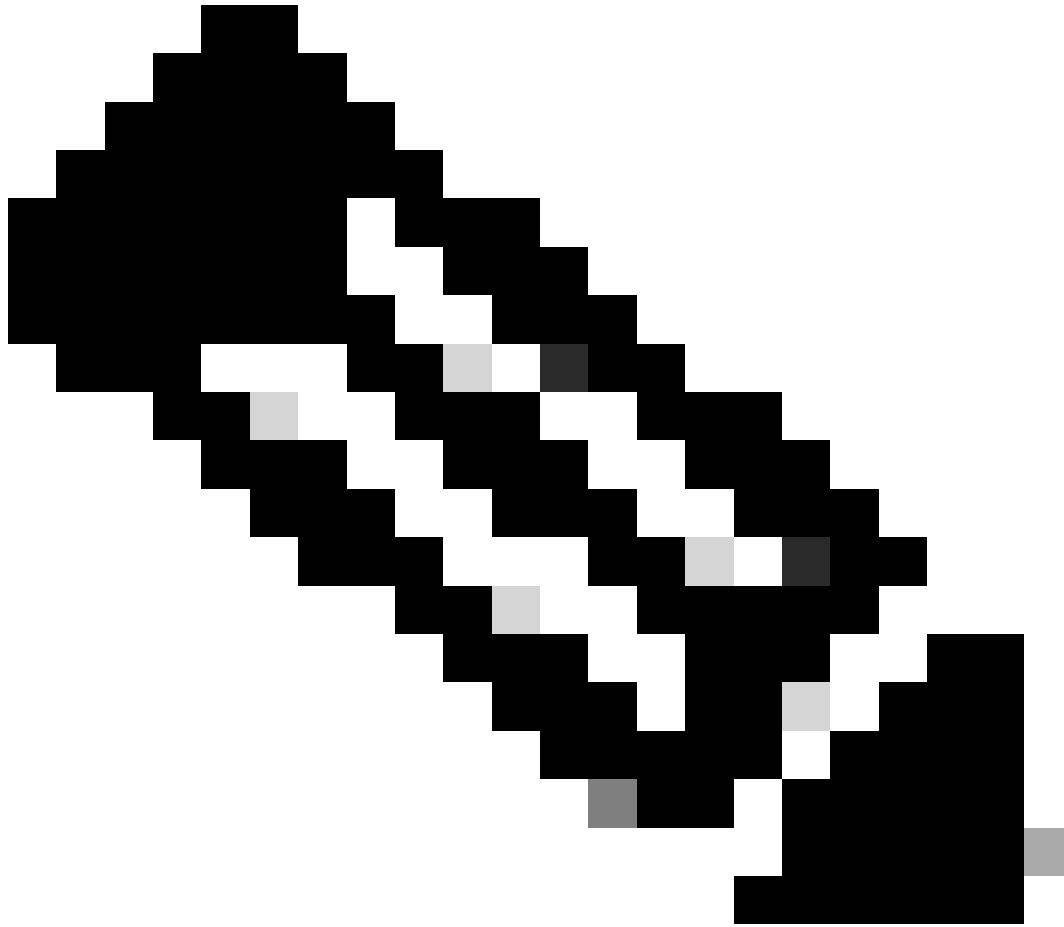
사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

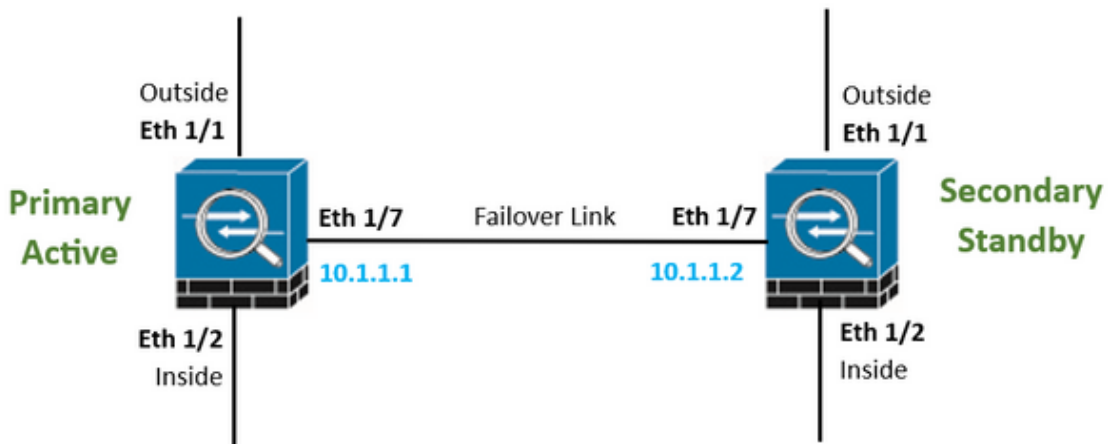
- FDM(Firepower 장치 관리자)에서 로컬로 관리되는 FPR2110 버전 7.2.5

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.

네트워크 토폴로지



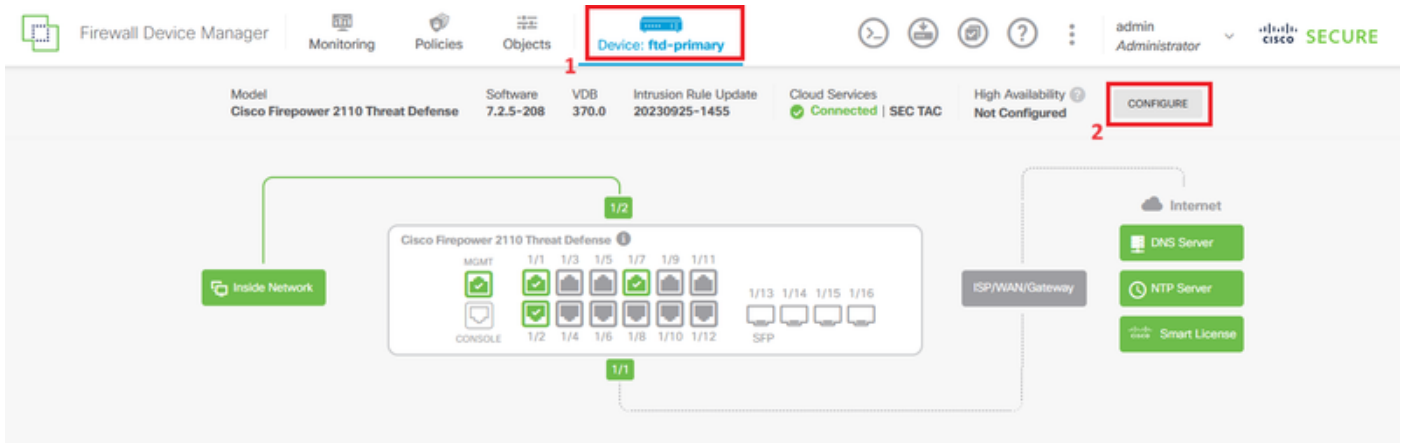
참고: 이 문서에서 설명하는 예는 여러 권장 네트워크 설계 중 하나입니다. 자세한 옵션은 컨피그레이션 가이드 [장애 조치 방지 및 데이터 링크](#)를 참조하십시오.



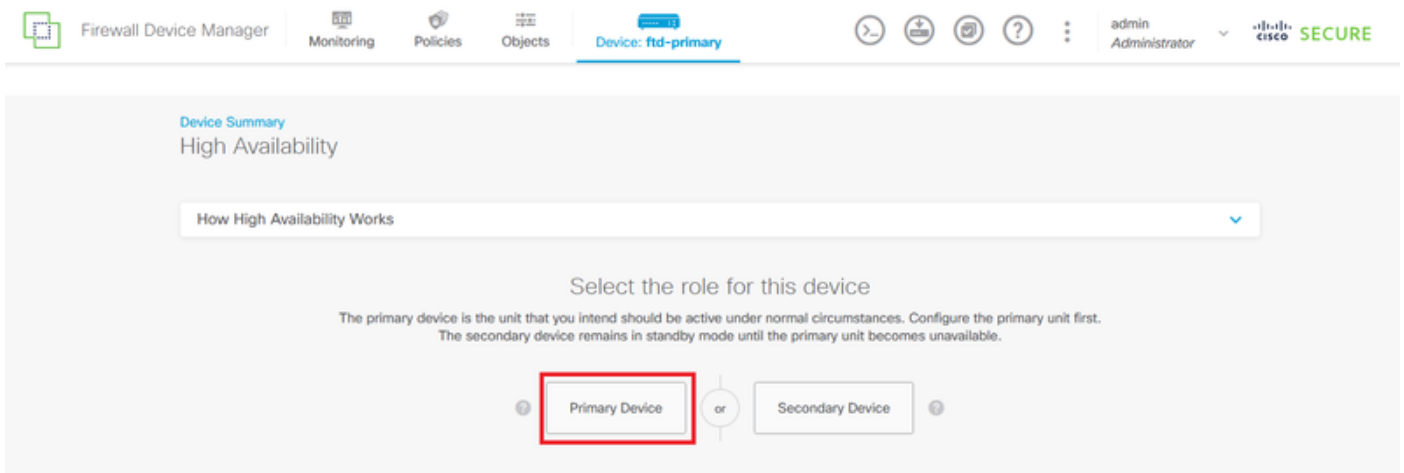
구성

고가용성을 위한 기본 유닛 구성

1단계. Device(디바이스)를 클릭하고 High Availability(고가용성) 상태 옆의 오른쪽 상단 모서리에 있는 Configure(구성) 버튼을 누릅니다.



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



3단계. 장애 조치 링크 속성을 구성합니다.

보조 방화벽에 직접 연결한 인터페이스를 선택하고 기본 및 보조 IP 주소와 서브넷 넷마스크를 설정합니다.

상태 기반 장애 조치 링크에 대해 Use the same interface as the Failover Link 확인란을 선택합니다

IPSec Encryption Key(IPSec 암호화 키) 상자의 선택을 취소하고 Activate HA(HA 활성화)를 클릭하여 변경 사항을 저장합니다.

I have configuration of peer device in clipboard

PASTE FROM CLIPBOARD

FAILOVER LINK

Interface

unnamed (Ethernet1/7)

Type

IPv4 IPv6

Primary IP

10.1.1.1

e.g. 192.168.10.1

Secondary IP

10.1.1.2

e.g. 192.168.10.2

Netmask

255.255.255.252

e.g. 255.255.255.0 or 24

STATEFUL FAILOVER LINK

Use the same interface as the Failover Link

Interface

unnamed (Ethernet1/7)

Type

IPv4 IPv6

Primary IP

10.1.1.1

e.g. 192.168.11.1

Secondary IP

10.1.1.2

e.g. 192.168.11.2

Netmask

255.255.255.252

e.g. 255.255.255.0 or 24

IPSec Encryption Key (optional)

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.

IMPORTANT

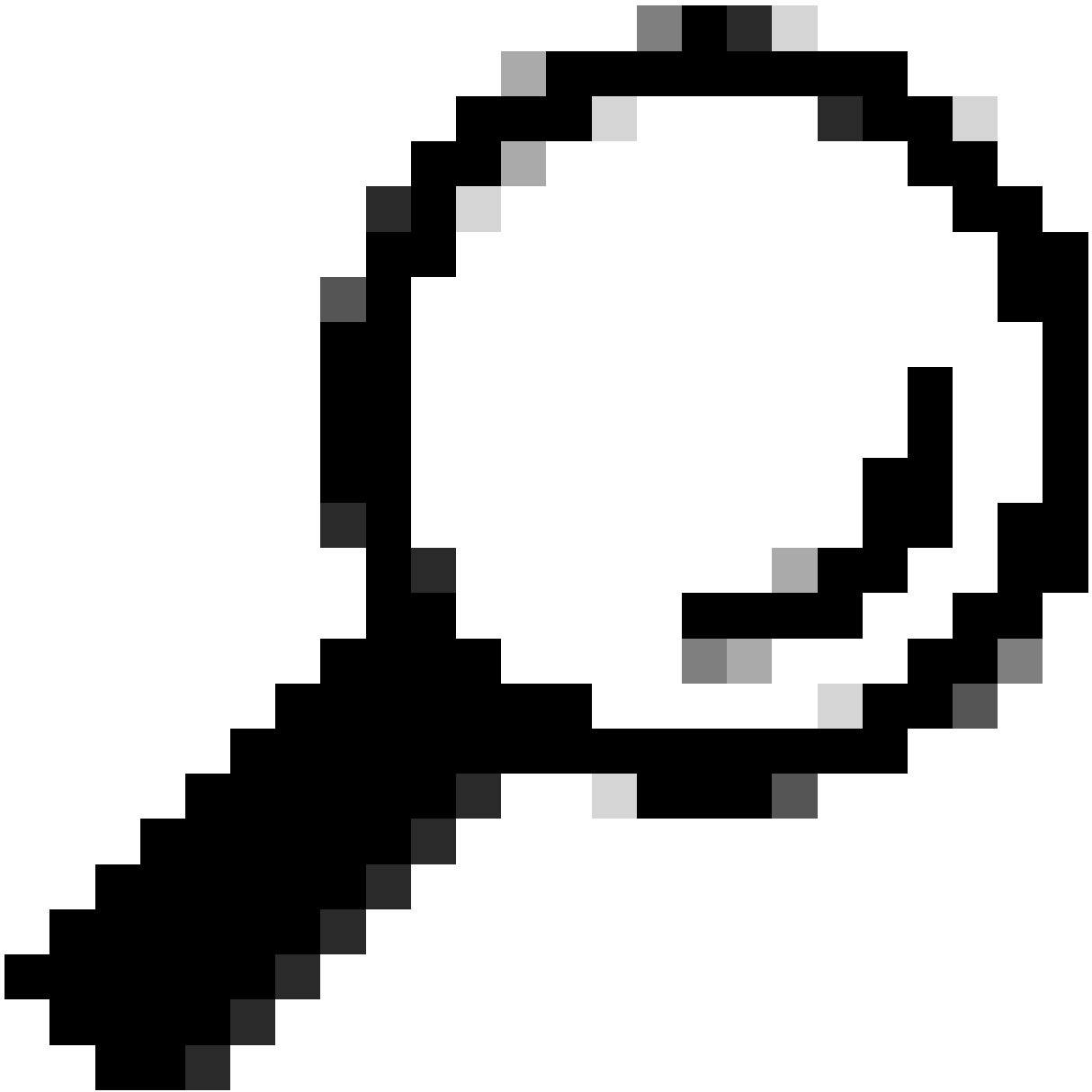
If you configure an IPsec encryption key with inconsistent settings for export controlled features, both devices will become active after you activate HA. [Learn More](#)

⚠ Before you activate HA, make sure both devices have the same Smart License and Cloud Region. Otherwise HA will not work.

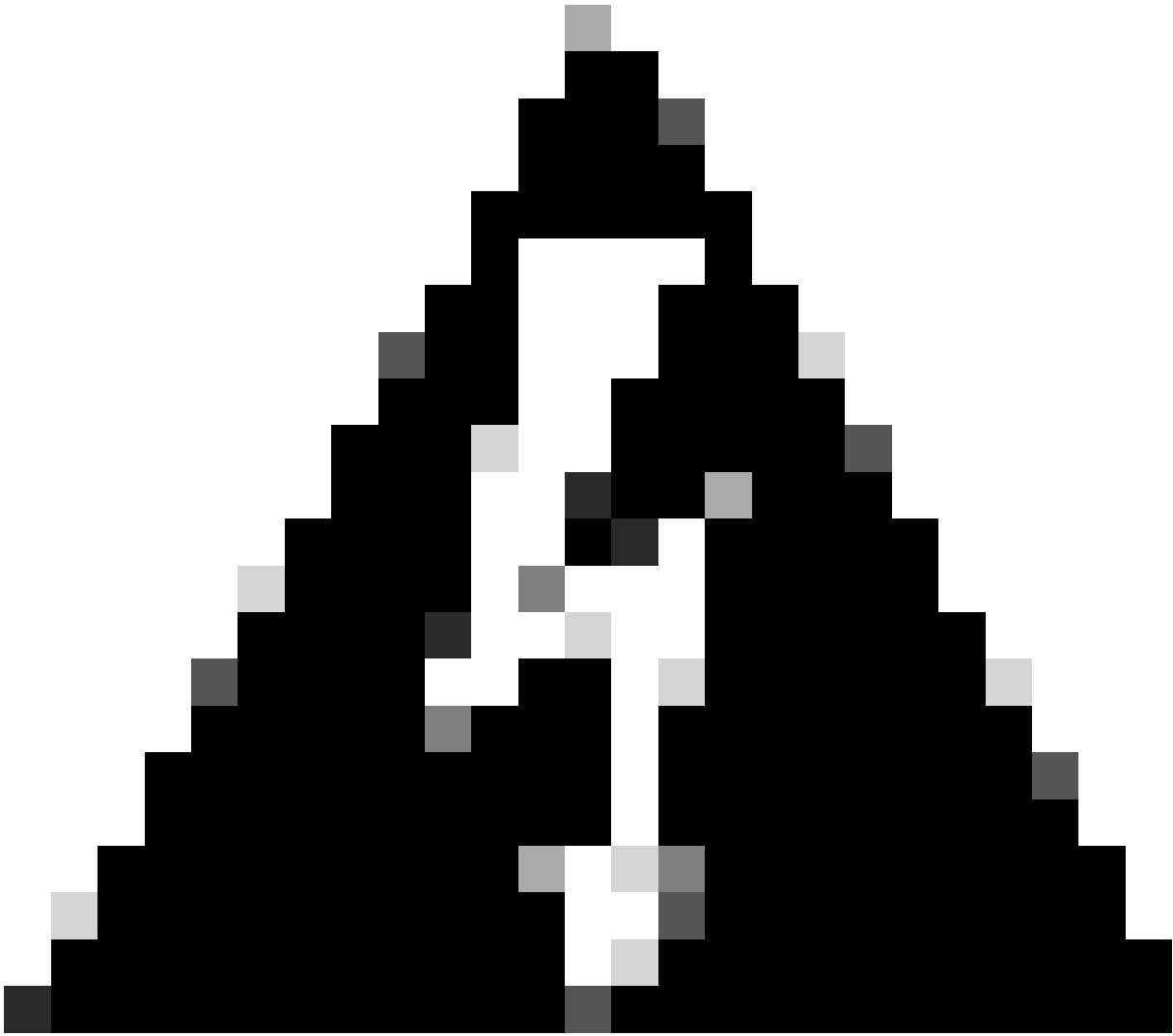
⚠ When you click Activate HA, these settings are automatically deployed to the device. The deployment might restart inspection engines, which can result in the momentary traffic loss. It might take a few minutes for deployment to finish.

i Information is copied to the clipboard when deployment is done. You must allow the browser to access your clipboard for the copy to be successful.

ACTIVATE HA

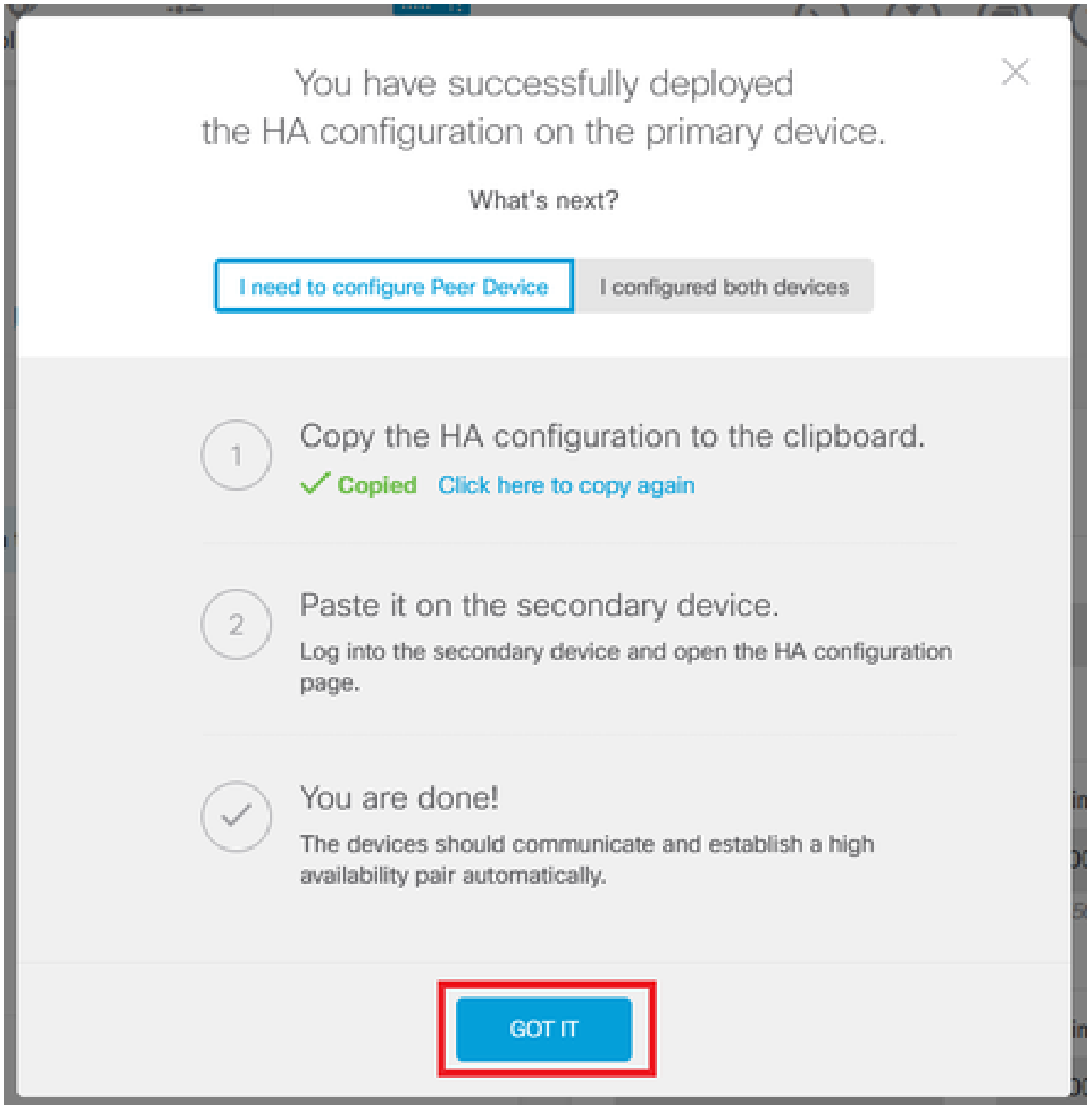


팁: 장애 조치 트래픽 전용 소형 마스크 서브넷을 사용하여 보안 침해 및/또는 네트워크 문제를 최대한 방지하십시오.



경고: 시스템에서 디바이스에 컨피그레이션을 즉시 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 키(설정된 경우)는 클립보드 복사본에 포함되지 않습니다.

4단계. 컨피그레이션이 완료되면 다음 단계를 설명하는 메시지가 표시됩니다. 정보를 읽은 후 [Got It\(가져오기\)](#)을 클릭합니다.

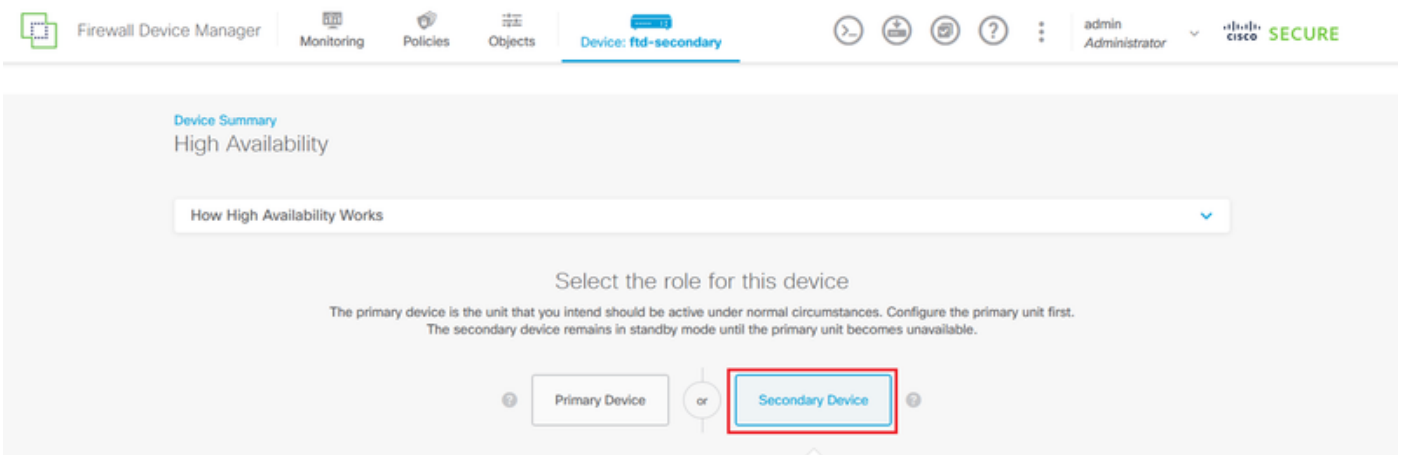


고가용성을 위한 보조 유닛 구성

1단계. Device(디바이스)를 클릭하고 High Availability(고가용성) 상태 옆의 오른쪽 상단 모서리에 있는 Configure(구성) 버튼을 누릅니다.

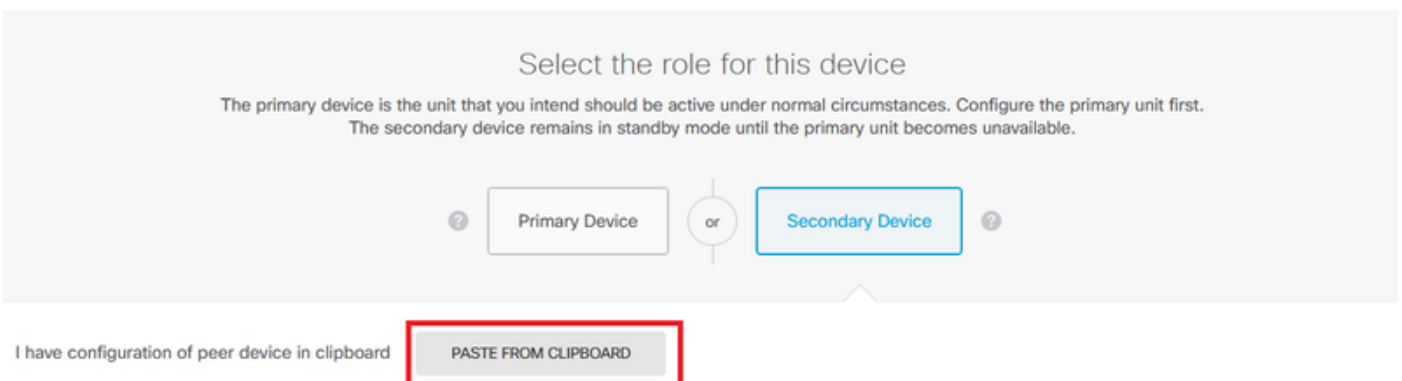


2단계. High Availability(고가용성) 페이지에서 Secondary Device(보조 디바이스) 상자를 클릭합니다.



3단계. 장애 조치 링크 속성을 구성합니다. 기본 FTD를 구성한 후 클립보드에 저장된 설정을 붙여넣거나 수동으로 계속할 수 있습니다.

3.1단계. 클립보드에서 붙여넣으려면 Paste from Clipboard(클립보드에서 붙여넣기) 버튼을 클릭하고 컨피그레이션에 붙여넣은 다음(Ctrl+v 키를 동시에 누름) OK(확인)를 클릭합니다.



Paste Configuration from Clipboard



Paste here Peer Device Configuration

```
FAILOVER LINK CONFIGURATION
=====
Interface: Ethernet1/7
Primary IP: 10.1.1.1/255.255.255.252
Secondary IP: 10.1.1.2/255.255.255.252

STATEFUL FAILOVER LINK CONFIGURATION
=====
Interface: Ethernet1/7
Primary IP: 10.1.1.1/255.255.255.252
Secondary IP: 10.1.1.2/255.255.255.252
```

CANCEL

OK

3.2단계. 수동으로 진행하려면 보조 방화벽에 직접 연결한 인터페이스를 선택하고 기본 및 보조 IP 주소와 서브넷 넷마스크를 설정합니다. 상태 기반 장애 조치 링크에 대해 Use the same interface as the Failover Link 확인란을 선택합니다.

I have configuration of peer device in clipboard

PASTE FROM CLIPBOARD

FAILOVER LINK

Interface

unnamed (Ethernet1/7)

Type

IPv4 IPv6

Primary IP

10.1.1.1

e.g. 192.168.10.1

Secondary IP

10.1.1.2

e.g. 192.168.10.2

Netmask

255.255.255.252

e.g. 255.255.255.0 or 24

STATEFUL FAILOVER LINK

Use the same interface as the Failover Link

Interface

unnamed (Ethernet1/7)

Type

IPv4 IPv6

Primary IP

10.1.1.1

e.g. 192.168.11.1

Secondary IP

10.1.1.2

e.g. 192.168.11.2

Netmask

255.255.255.252

e.g. 255.255.255.0 or 24

IPSec Encryption Key (optional)

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.

IMPORTANT

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](#)

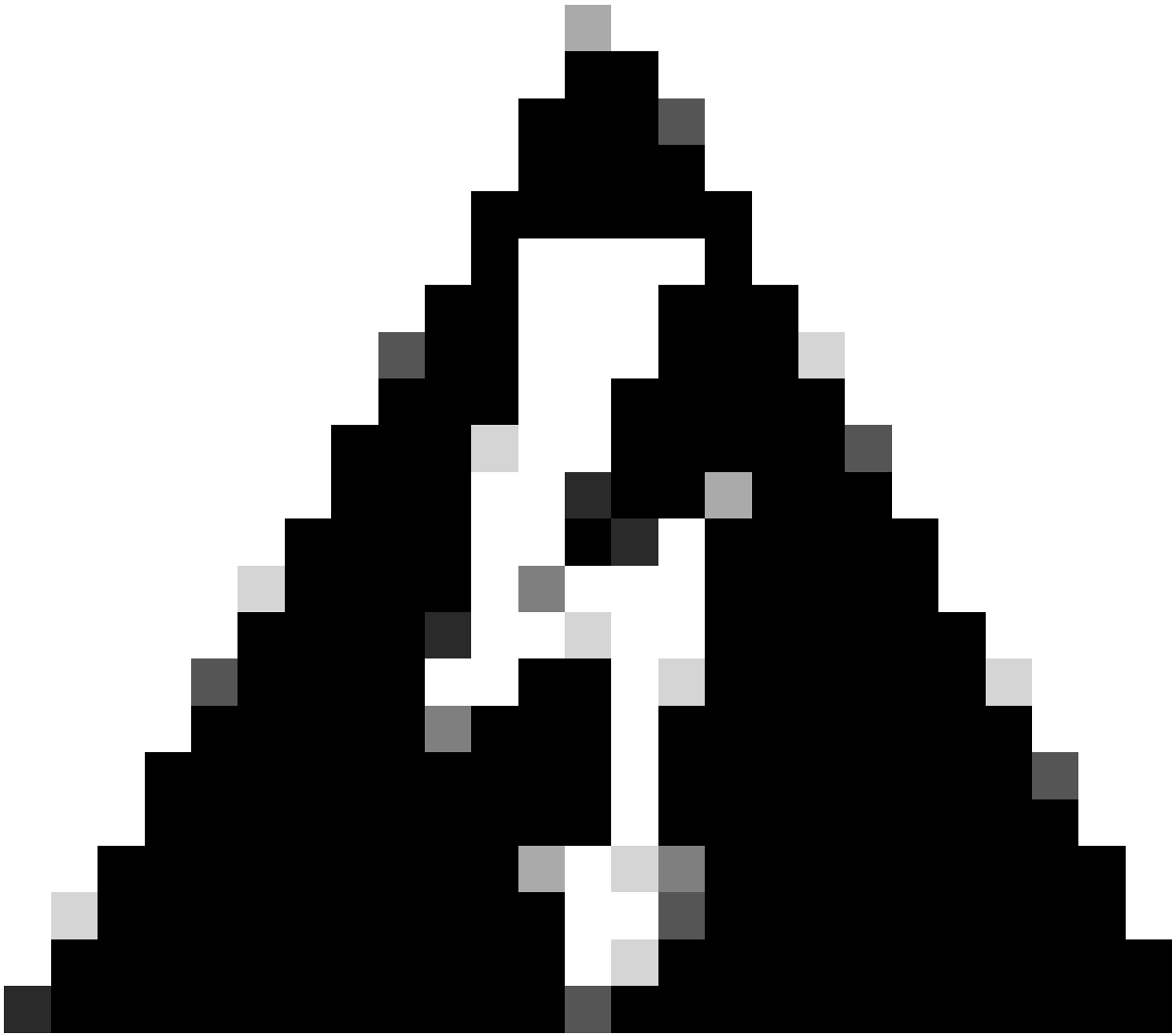
⚠ Before you activate HA, make sure both devices have the same Smart License and Cloud Region. Otherwise HA will not work.

⚠ When you click Activate HA, these settings are automatically deployed to the device. The deployment might restart inspection engines, which can result in the momentary traffic loss. It might take a few minutes for deployment to finish.

i Information is copied to the clipboard when deployment is done. You must allow the browser to access your clipboard for the copy to be successful.

ACTIVATE HA

4단계. IPSec Encryption Key(IPSec 암호화 키) 상자의 선택을 취소하고 Activate HA(HA 활성화)를 클릭하여 변경 사항을 저장합니다.



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

5단계. 컨피그레이션이 완료되면 수행해야 할 다음 단계를 설명하는 메시지가 표시됩니다. 정보를 읽은 후 Got It(가져오기)을 클릭합니다.

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



What's next?

I need to configure Peer Device

I configured both devices

1

Copy the HA configuration to the clipboard.

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

2

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.

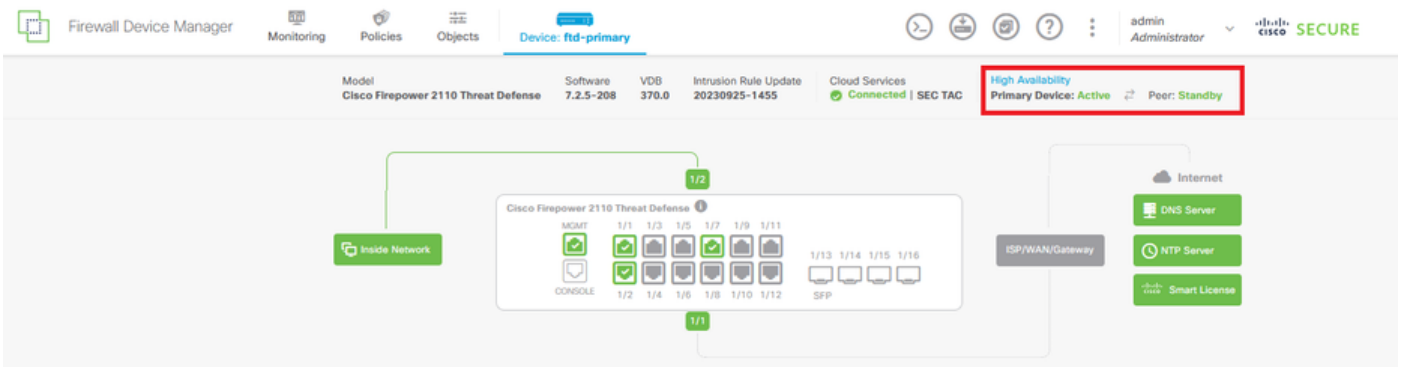
GOT IT

다음을 확인합니다.

- 이 시점에서 디바이스 상태가 대부분 High Availability(고가용성) 페이지의 보조 디바이스임을 나타냅니다. 기본 디바이스와의 조인에 성공하면 디바이스가 기본 디바이스와 동기화를 시작하고, 결국 모드가 Standby(대기)로 변경되고 피어가 Active(활성)로 변경됩니다.



- 기본 FTD는 고가용성 상태도 표시하지만 활성 및 피어: 대기로 표시됩니다.



- 기본 FTD에 대한 SSH 세션을 열고 show running-config failover 명령을 실행하여 컨피그레이션을 확인합니다.

```
> show running-config failover
failover
failover lan unit primary
failover lan interface failover-link Ethernet1/7
failover replication http
failover link failover-link Ethernet1/7
failover interface ip failover-link 10.1.1.1 255.255.255.252 standby 10.1.1.2
```

- show failover state 명령을 사용하여 디바이스의 현재 상태를 확인합니다.

```
> show failover state
```

	State	Last Failure Reason	Date/Time
This host -	Primary Active	None	
Other host -	Secondary Standby Ready	None	

```
====Configuration State====
```

```
====Communication State====
```

```
Mac set
```

```
>
```

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.