Firepower 어플라이언스에서 FTD 고가용성 설정

목차

소개

이 문서에서는 FPR9300에서 FTD(Firepower Threat Defense) HA(고가용성) (활성/대기 페일오버)를 설정 및 확인하는 방법을 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco Firepower 9300 보안 어플라이언스 2개 - FXOS SW 2.0(1.23)
- FTD 버전 10.10.1.1(빌드 1023)
- FMC(Firepower Management Center) - SW 10.10.1.1(빌드 1023)

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.

참고: FTD가 있는 FPR9300 어플라이언스에서는 섀시 간 HA만 구성할 수 있습니다. HA 설정

✎ 의 두 유닛은 여기에 언급된 조건을 충족해야 합니다.

작업 1. 조건 확인

작업 요구 사항:

두 FTD 어플라이언스 모두 메모 요구 사항을 충족하며 HA 유닛으로 구성할 수 있는지 확인합니다.

해결책:

1단계. FPR9300 관리 IP에 연결하고 모듈 하드웨어를 확인합니다.

FPR9300-1 하드웨어를 확인합니다.

```
<#root>

KSEC-FPR9K-1-A#

show server inventory

Server Equipped PID Equipped VID Equipped Serial (SN) Slot Status      Ackd Memory (MB) Ackd Cores
------- ------------ ------------ -------------------- ---------------- ---------------- ----------
1/1     FPR9K-SM-36  V01          FLM19216KK6          Equipped                    262144         36
1/2     FPR9K-SM-36  V01          FLM19206H71          Equipped                    262144         36
1/3     FPR9K-SM-36  V01          FLM19206H7T          Equipped                    262144         36
KSEC-FPR9K-1-A#
```

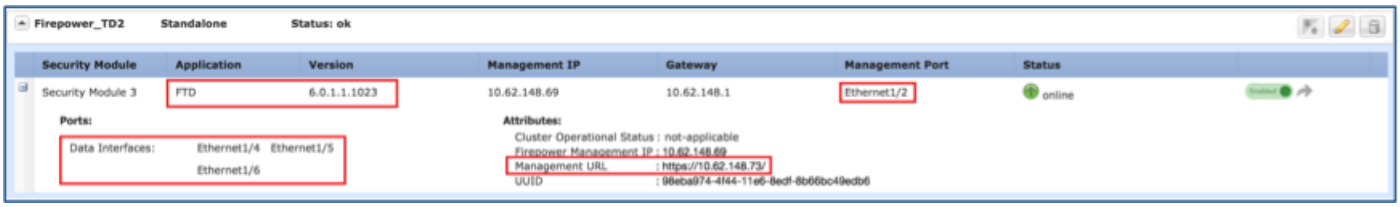
FPR9300-2 하드웨어를 확인합니다.

```
<#root>

KSEC-FPR9K-2-A#

show server inventory

Server  Equipped PID Equipped VID Equipped Serial (SN) Slot Status      Ackd Memory (MB) Ackd Cores
------- ------------ ------------ -------------------- ---------------- ---------------- ----------
1/1     FPR9K-SM-36  V01          FLM19206H9T          Equipped                    262144         36
1/2     FPR9K-SM-36  V01          FLM19216KAX          Equipped                    262144         36
1/3     FPR9K-SM-36  V01          FLM19267A63          Equipped                    262144         36
KSEC-FPR9K-2-A#
```

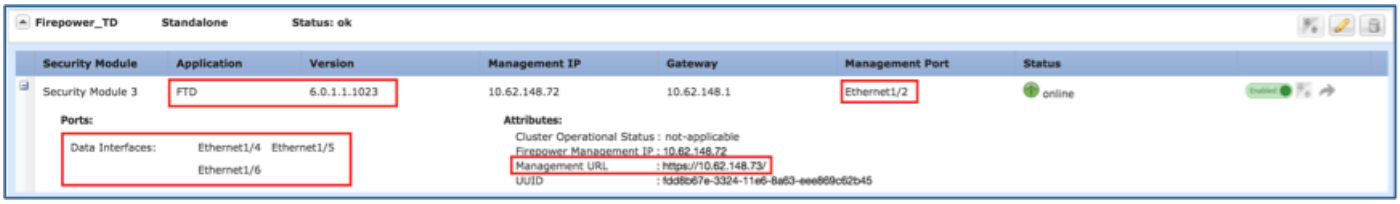
2단계. FPR9300-1 Chassis Manager에 로그인하고 Logical Devices(논리적 디바이스)로 이동합니다.

이미지에 표시된 대로 소프트웨어 버전, 번호 및 인터페이스 유형을 확인합니다.

FPR9300-1



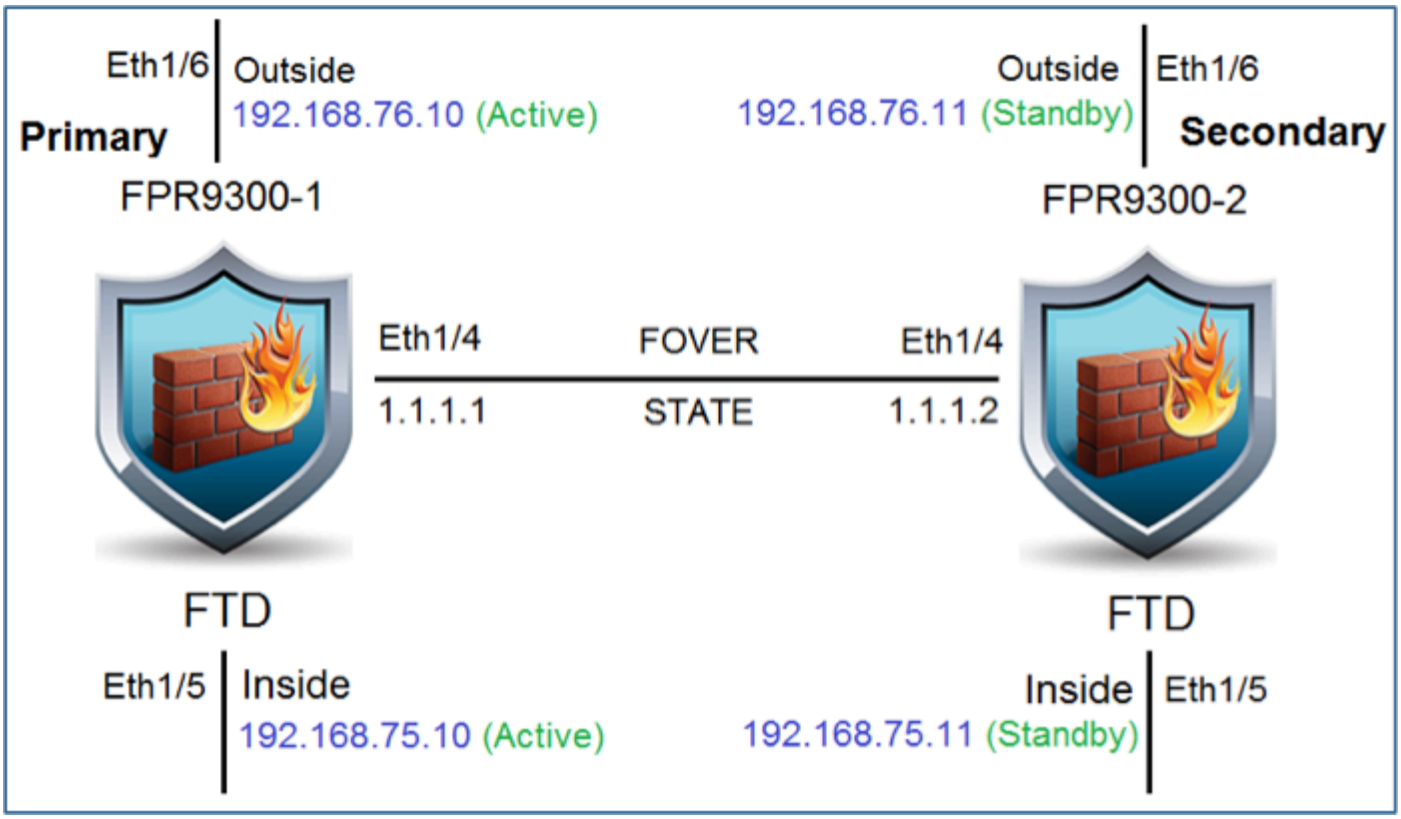
FPR9300-2



작업 2. FPR9300에서 FTD HA 구성

작업 요구 사항:

이 다이어그램에 따라 활성/대기 페일오버(HA)를 설정합니다.



해결책:

두 FTD 디바이스는 이미지에 표시된 것과 같이 FMC에 이미 등록되어 있습니다.

1단계. FTD 장애 조치를 구성하려면 이미지에 표시된 대로 Devices(디바이스) > Device Management(디바이스 관리)로 이동하여 Add High Availability(고가용성 추가)를 선택합니다.

2단계. 이미지에 표시된 대로 Primary Peer(기본 피어)와 Secondary Peer(보조 피어)를 입력하고 Continue(계속)를 선택합니다.

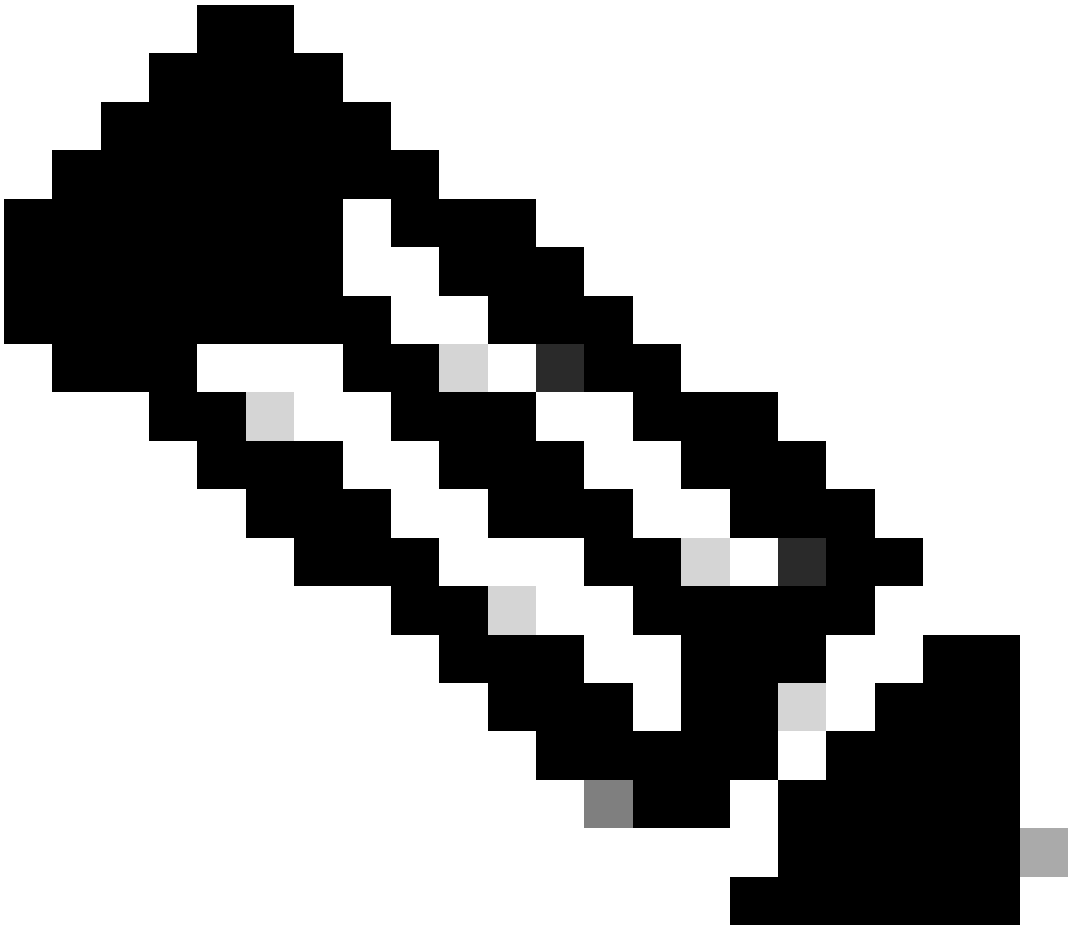
경고: 올바른 유닛을 기본 유닛으로 선택해야 합니다. 선택한 기본 유닛의 모든 컨피그레이션이 선택한 보조 FTD 유닛에 복제됩니다. 복제를 수행하면 보조 유닛의 현재 컨피그레이션을 교체할 수 있습니다.

조건

2개의 FTD 디바이스 간에 HA를 생성하려면 다음 조건을 충족해야 합니다.

- 동일한 모델

- 동일 버전 - 이는 FXOS와 FTD에 적용되며, major(첫 번째 숫자), minor(두 번째 숫자) 및 maintenance(세 번째 숫자)는 동일해야 합니다.
- 동일한 수의 인터페이스
- 동일한 유형의 인터페이스
- 두 디바이스는 FMC에서 동일한 그룹/도메인의 일부입니다.
- 동일한 NTP(Network Time Protocol) 컨피그레이션이 있어야 합니다.
- 커밋되지 않은 변경 사항 없이 FMC에 완전히 구축됩니다.
- 동일한 방화벽 모드(라우팅 또는 투명)에 있어야 합니다.



참고: FTD에서 동일한 모드를 사용하는 경우가 있으므로 FTD 디바이스와 FMC GUI에서 모두 확인해야 하지만 FMC에서는 이를 반영하지 않습니다.

- 인터페이스에 DHCP/PPPoE(Point-to-Point Protocol over Ethernet)가 구성되어 있지 않습니다.
- 두 섀시의 호스트 이름[FQDN(Fully Qualified Domain Name)]이 다릅니다. 섀시 호스트 이름을 확인하려면 FTD CLI로 이동하여 다음 명령을 실행합니다.

<#root>

firepower#

show chassis-management-url

https://

KSEC-FPR9K-1.cisco.com

:443//

참고: post-6.3 FTD에서는 show chassis detail 명령을 사용합니다.

<#root>

firepower#

show chassis detail

```
Chassis URL              : https://KSEC-FPR4100-1:443//
Chassis IP               : 192.0.2.1
Chassis Serial Number    : JMX12345678
Security Module          : 1
```

두 섀시의 이름이 같은 경우 다음 명령을 사용하여 섀시 중 하나의 이름을 변경합니다.

<#root>

KSEC-FPR9K-1-A#

scope system

KSEC-FPR9K-1-A /system #

set name FPR9K-1new

```
Warning: System name modification changes FC zone name and redeploys them non-disruptively
KSEC-FPR9K-1-A /system* #
```

commit-buffer

FPR9K-1-A /system #

exit

FPR9K-1new-A

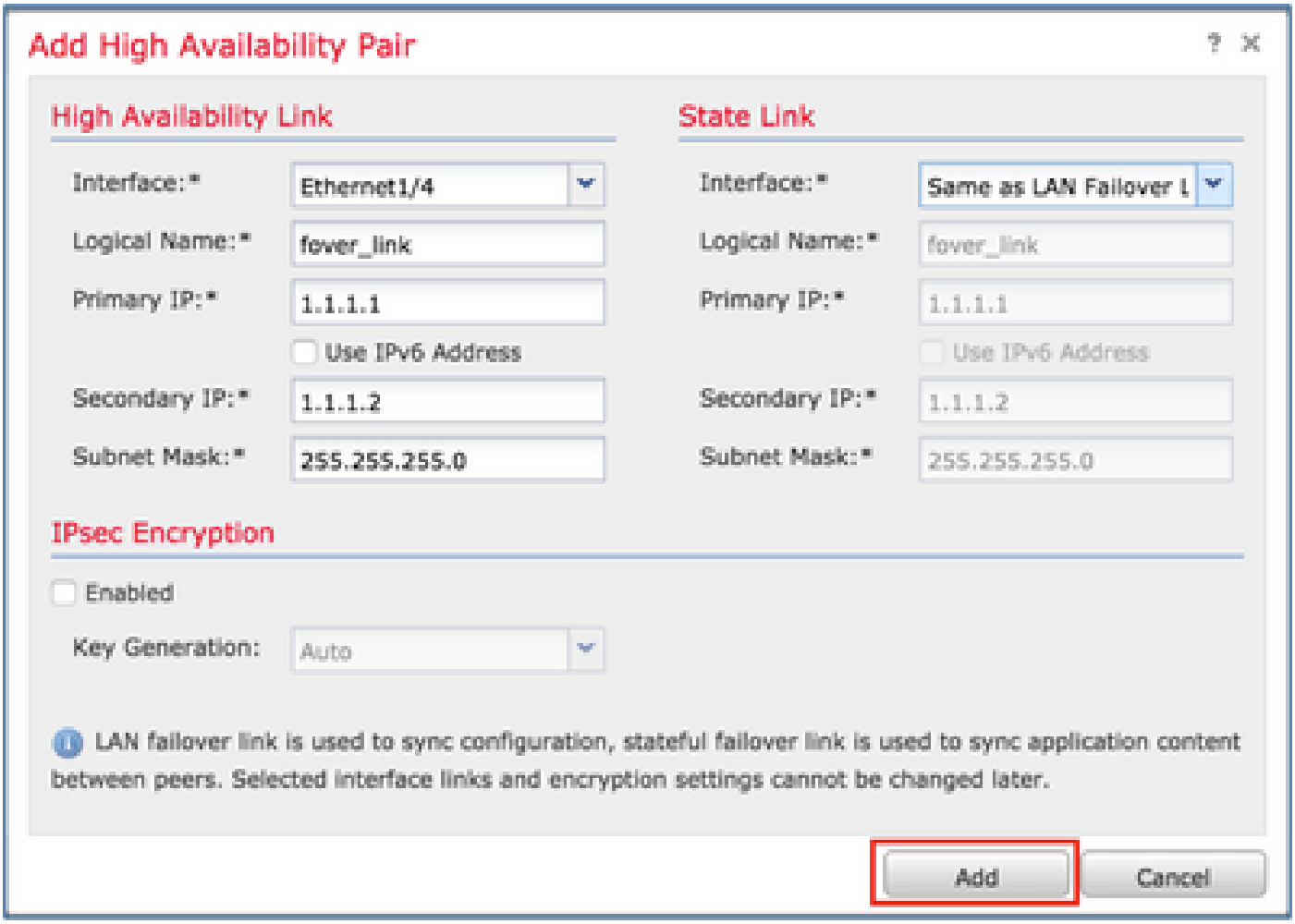
#

섀시 이름을 변경한 후 FMC에서 FTD를 등록 취소하고 다시 등록합니다. 그런 다음 HA 쌍 생성을 진행합니다.

3단계. HA를 구성하고 링크 설정을 지정합니다.

이 경우 상태 링크의 설정은 고가용성 링크와 동일합니다.

Add(추가)를 선택하고 이미지에 표시된 대로 HA 쌍이 구축될 때까지 몇 분간 기다립니다.

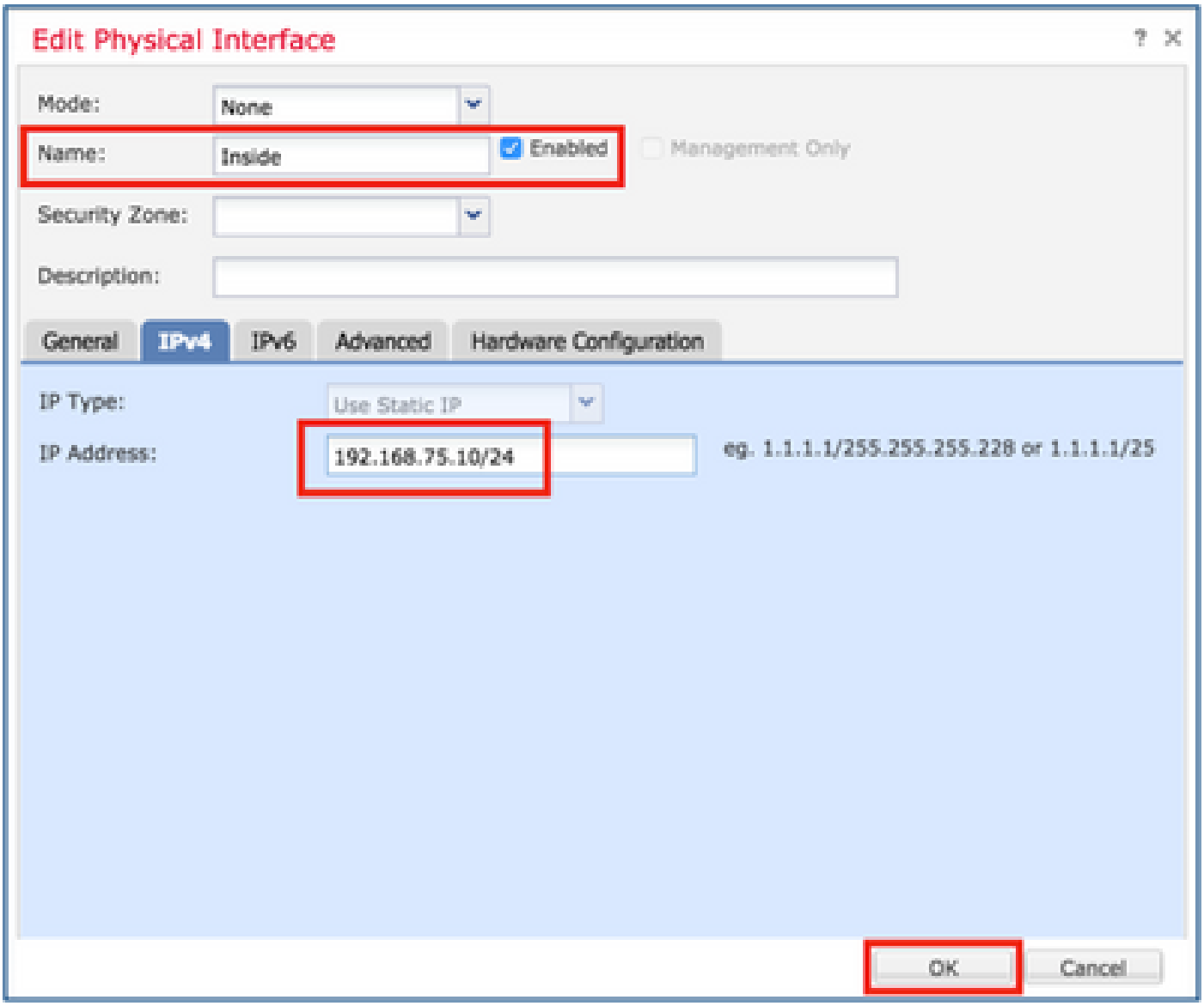


4단계. 데이터 인터페이스(기본 및 대기 IP 주소) 구성

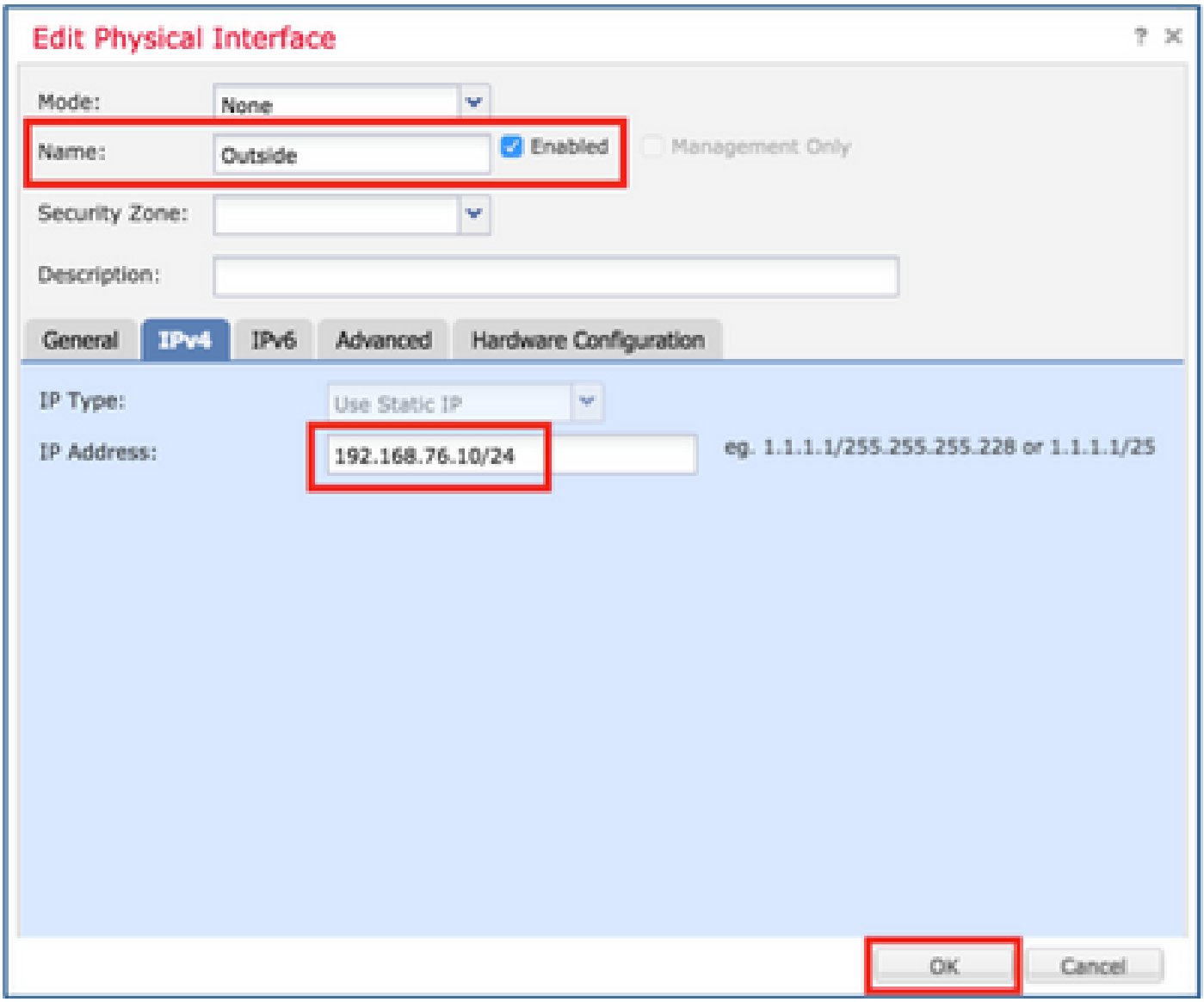
FMC GUI에서 이미지에 표시된 대로 HA Edit(HA 수정)를 선택합니다.

5단계. 이미지에 표시된 대로 인터페이스 설정을 구성합니다.

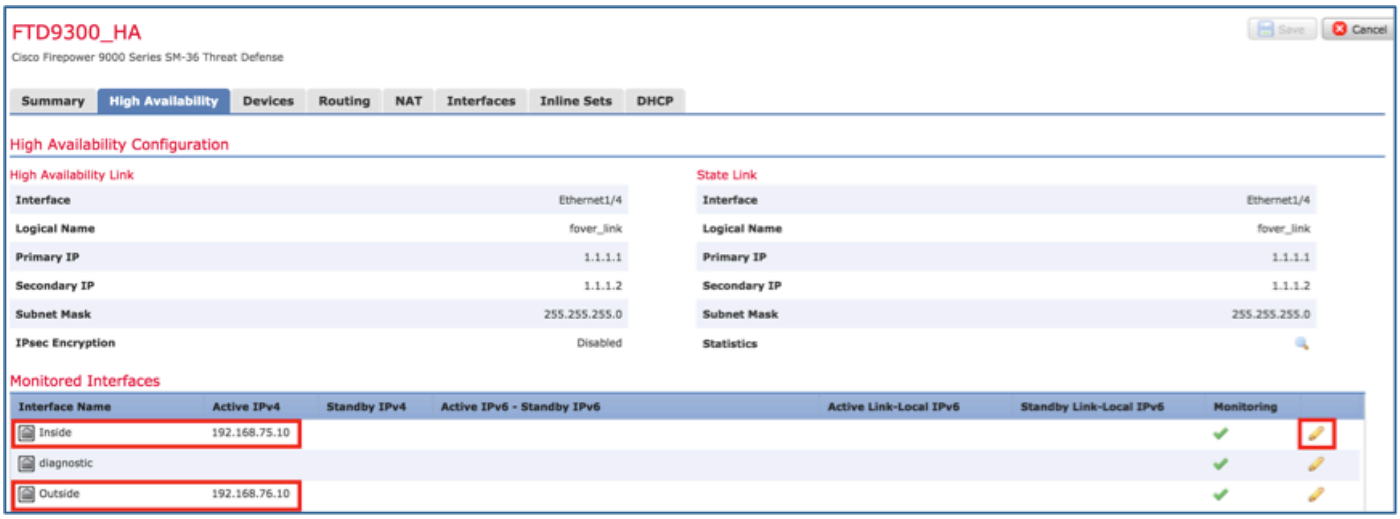
이더넷 1/5 인터페이스


Edit Physical Interface
Mode:
None
Name:
Inside
Enabled
Management Only
Security Zone:
Description:
General
IPv4
IPv6
Advanced
Hardware Configuration
IP Type:
Use Static IP
IP Address:
192.168.75.10/24
eg. 1.1.1.1/255.255.255.228 or 1.1.1.1/25
OK
Cancel

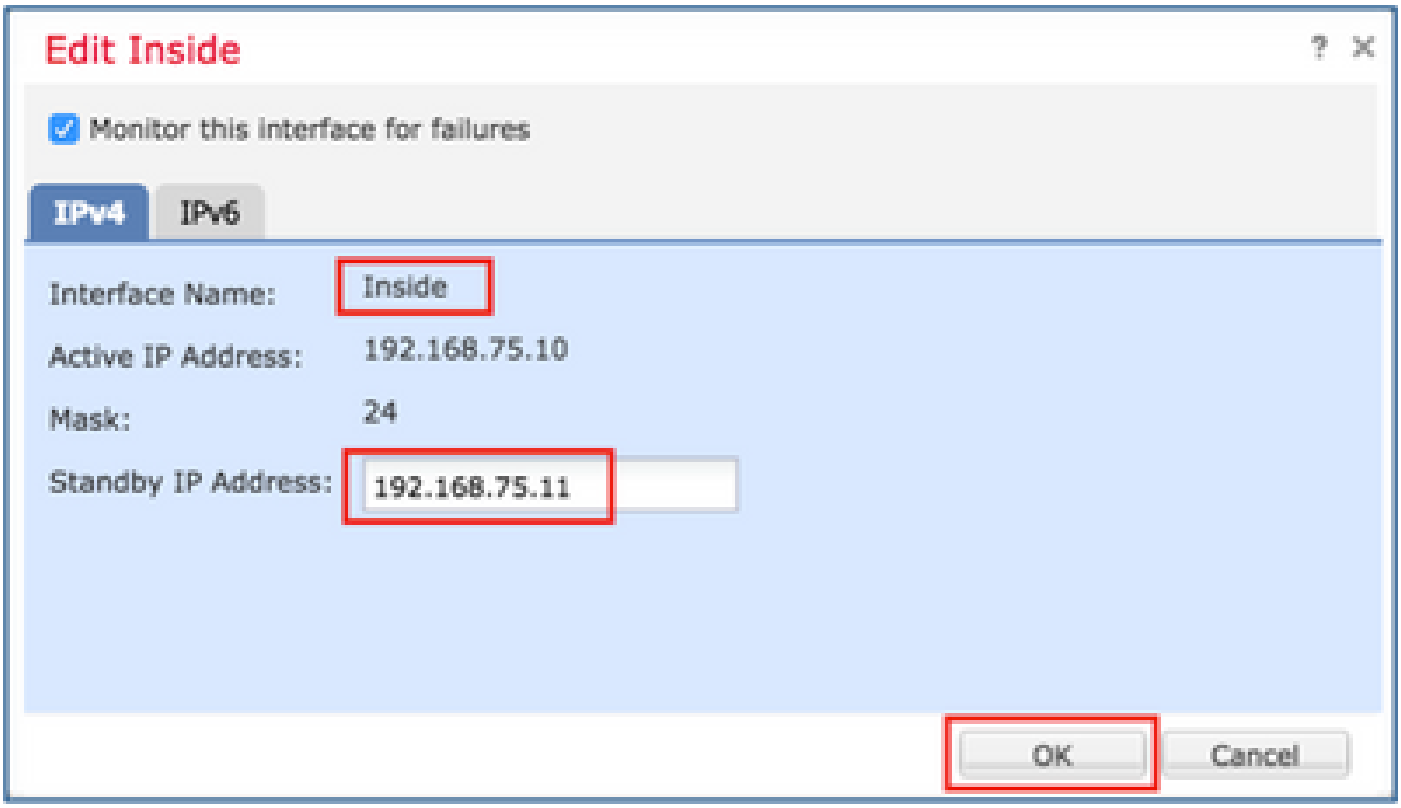
이더넷 1/6 인터페이스



6단계. High Availability(고가용성)로 이동하고 Interface Name Edit(인터페이스 이름 수정)를 선택하여 이미지에 표시된 대로 스탠바이 IP 주소를 추가합니다.

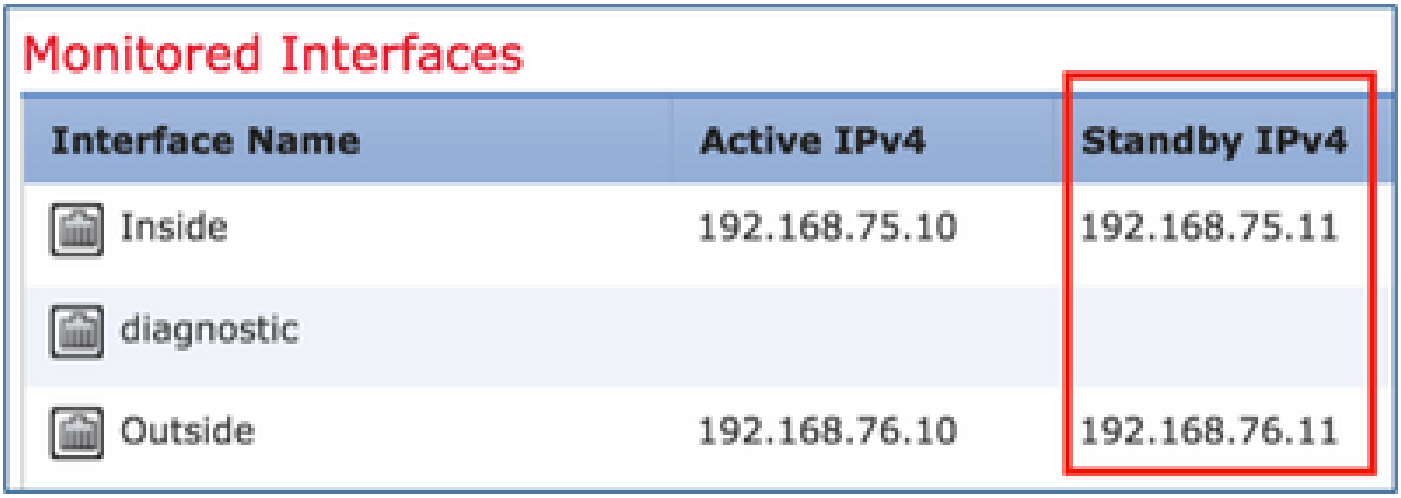


7단계. 이미지에 표시된 Inside 인터페이스의 경우.

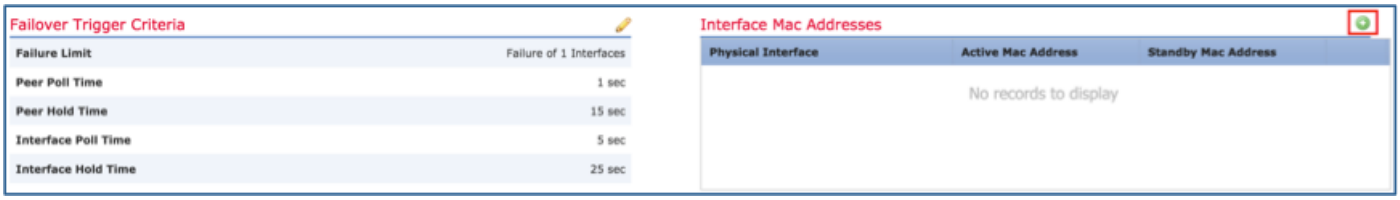


8단계. Outside(외부) 인터페이스에 대해서도 동일한 작업을 수행합니다.

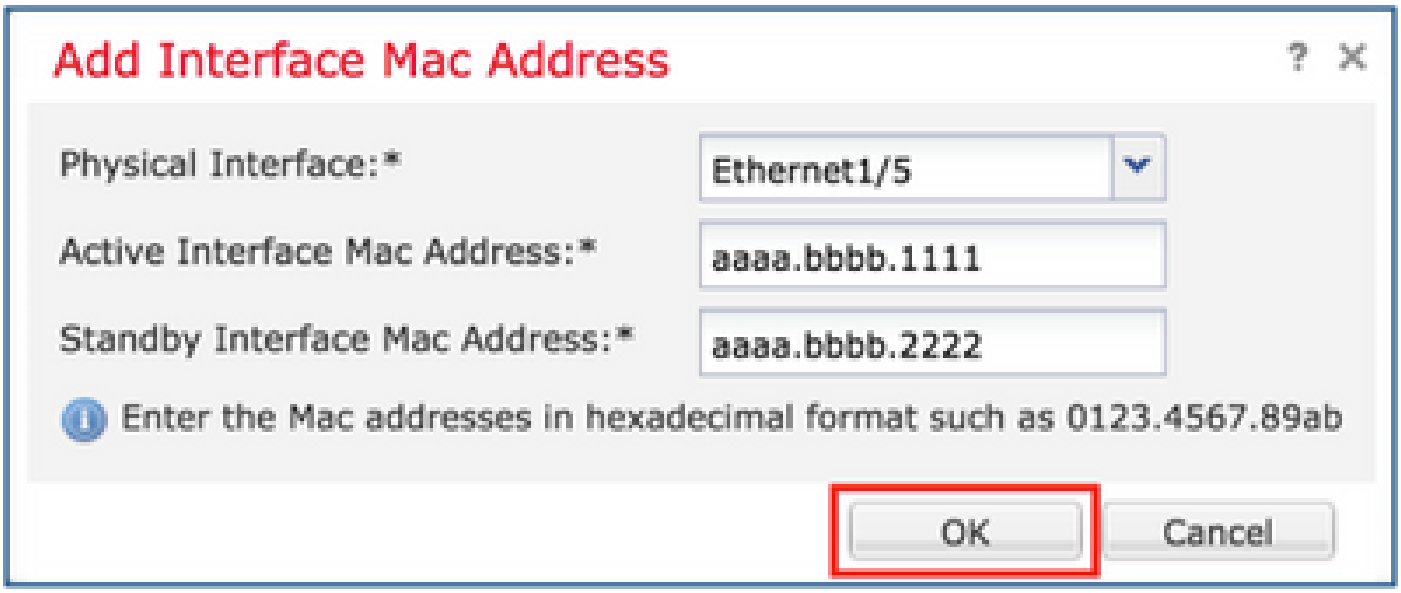
9단계. 이미지에 표시된 대로 결과를 확인합니다.



10단계. High Availability(고가용성) 탭에서 이미지에 표시된 대로 가상 MAC 주소를 구성합니다.



11단계. Inside Interface는 그림과 같습니다.



12단계. Outside(외부) 인터페이스에 대해서도 동일한 작업을 수행합니다.

13단계. 이미지에 표시된 대로 결과를 확인합니다.

14단계. 변경 사항을 구성한 후 저장 및 배포를 선택합니다.

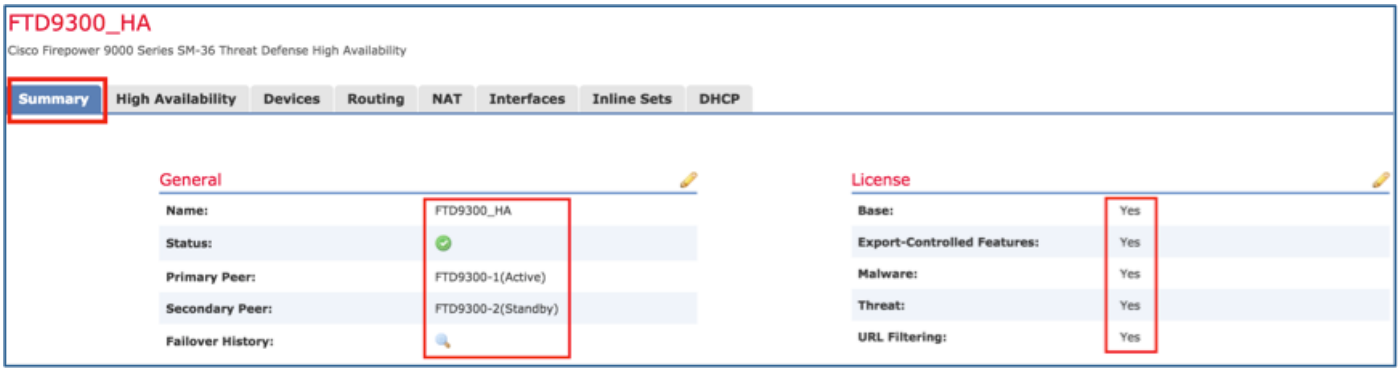
작업 3. FTD HA 및 라이센스 확인

작업 요구 사항:

FMC GUI 및 FTD CLI에서 FTD HA 설정 및 활성화된 라이선스를 확인합니다.

해결책:

1단계. Summary(요약)로 이동하고 이미지에 표시된 대로 HA 설정 및 활성화된 라이센스를 확인합니다.



2단계. FTD CLI에서 다음 명령을 실행합니다.

<#root>

>

show high-availability config

Failover

On

Failover unit

Primary

Failover LAN Interface:

fover_link Ethernet1/4 (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 1 of 1041 maximum
MAC Address Move Notification Interval not set
failover replication http
Version: Ours 9.6(1), Mate 9.6(1)
Serial Number: Ours FLM19267A63, Mate FLM19206H7T
Last Failover at: 18:32:38 EEST Jul 21 2016
    This host: Primary - Active
        Active time: 3505 (sec)
        slot 0: UCSB-B200-M3-U hw/sw rev (0.0/9.6(1)) status (Up Sys)
          Interface diagnostic (0.0.0.0): Normal (Waiting)
        slot 1: snort rev (1.0)  status (up)
        slot 2: diskstatus rev (1.0)  status (up)
    Other host: Secondary - Standby Ready
        Active time: 172 (sec)
        slot 0: UCSB-B200-M3-U hw/sw rev (0.0/9.6(1)) status (Up Sys)
          Interface diagnostic (0.0.0.0): Normal (Waiting)
        slot 1: snort rev (1.0)  status (up)
        slot 2: diskstatus rev (1.0)  status (up)

Stateful Failover Logical Update Statistics
    Link : fover_link Ethernet1/4 (up)
    Stateful Obj     xmit       xerr       rcv        rerr
    General        417        0          416        0
    sys cmd      416        0          416        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

    Logical Update Queue Information
              Cur     Max     Total
    Recv Q:     0     10     416
    Xmit Q:     0     11     2118

>
```

3단계. 보조 디바이스에서도 같은 작업을 수행합니다.

4단계. LINA CLI에서 show failover state 명령을 실행합니다.

<#root>

```
firepower#

show failover state


               State          Last Failure Reason      Date/Time
This host  -   Primary
               Active         None
Other host -   Secondary
               Standby Ready  Comm Failure             18:32:56 EEST Jul 21 2016

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

firepower#
```

5단계. 기본 유닛(LINA CLI)에서 컨피그레이션을 확인합니다.

<#root>

```
firepower#

show running-config failover

failover
failover lan unit primary
failover lan interface fover_link Ethernet1/4
failover replication http
```

```
failover mac address Ethernet1/5

aaaa.bbbb.1111 aaaa.bbbb.2222

failover mac address Ethernet1/6

aaaa.bbbb.3333 aaaa.bbbb.4444

failover link fover_link Ethernet1/4
failover interface ip fover_link 10.10.1.1 255.255.255.0 standby 10.10.1.2
firepower#

firepower#

show running-config interface

!
interface Ethernet1/2
 management-only
 nameif diagnostic
 security-level 0
 no ip address
!
interface Ethernet1/4
 description LAN/STATE Failover Interface
!
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

firepower#
```

작업 4. 장애 조치 역할 전환

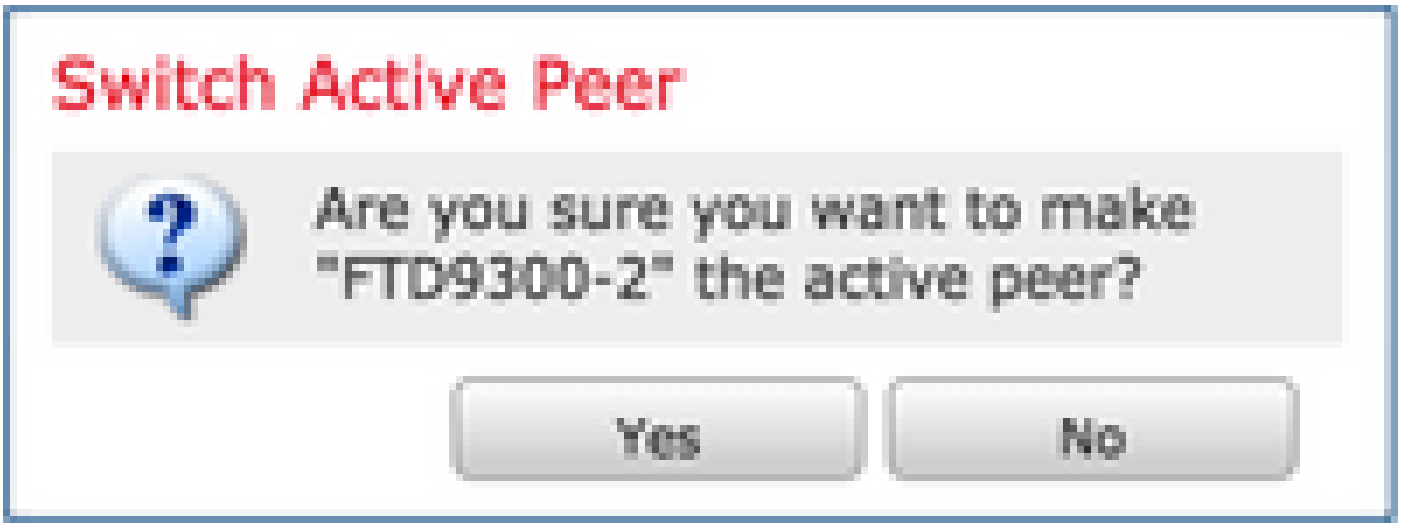
작업 요구 사항:

FMC에서 페일오버 역할을 기본/활성, 보조/대기에서 기본/대기, 보조/활성으로 전환합니다.

해결책:

1단계. 이미지에 표시된 대로 아이콘을 선택합니다.

2단계. 그림과 같이 팝업 창에서 작업을 확인합니다.



3단계. 이미지에 표시된 대로 결과를 확인합니다.

LINA CLI에서 no failover active 명령이 기본/활성 유닛에서 실행되었음을 확인할 수 있습니다.

```
<#root>

Jul 22 2016 10:39:26: %ASA-5-111008: User 'enable_15' executed the '

no failover active

' command.
Jul 22 2016 10:39:26: %ASA-5-111010: User 'enable_15', running 'N/A' from IP 0.0.0.0, executed 'no fail
```

show failover history 명령 출력에서 확인할 수도 있습니다.

```
<#root>

firepower#

show failover history

==========================================================================
From State                  To State                    Reason
10:39:26 EEST Jul 22 2016
Active                      Standby Ready               Set by the config command
```

4단계. 확인 후 기본 유닛을 다시 액티브 상태로 설정합니다.

작업 5. HA 쌍 중단

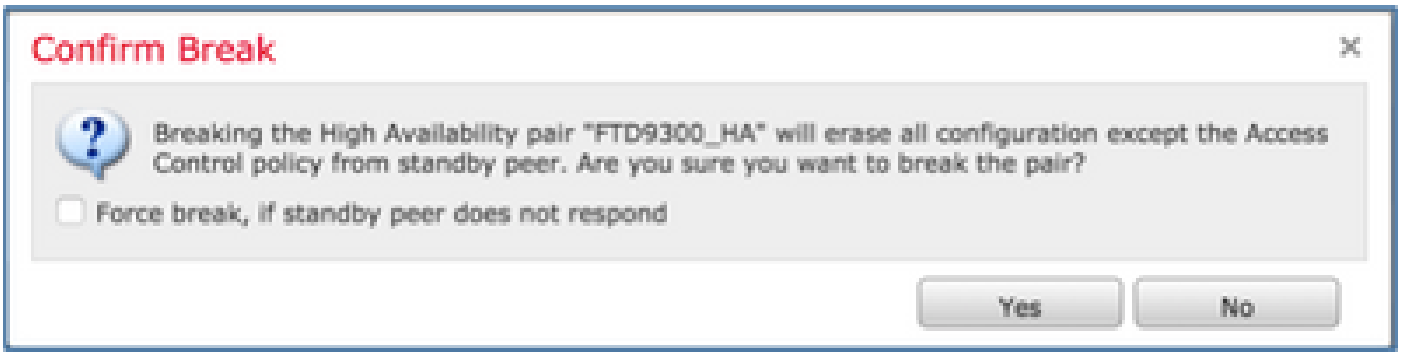
작업 요구 사항:

FMC에서 페일오버 쌍을 분리합니다.

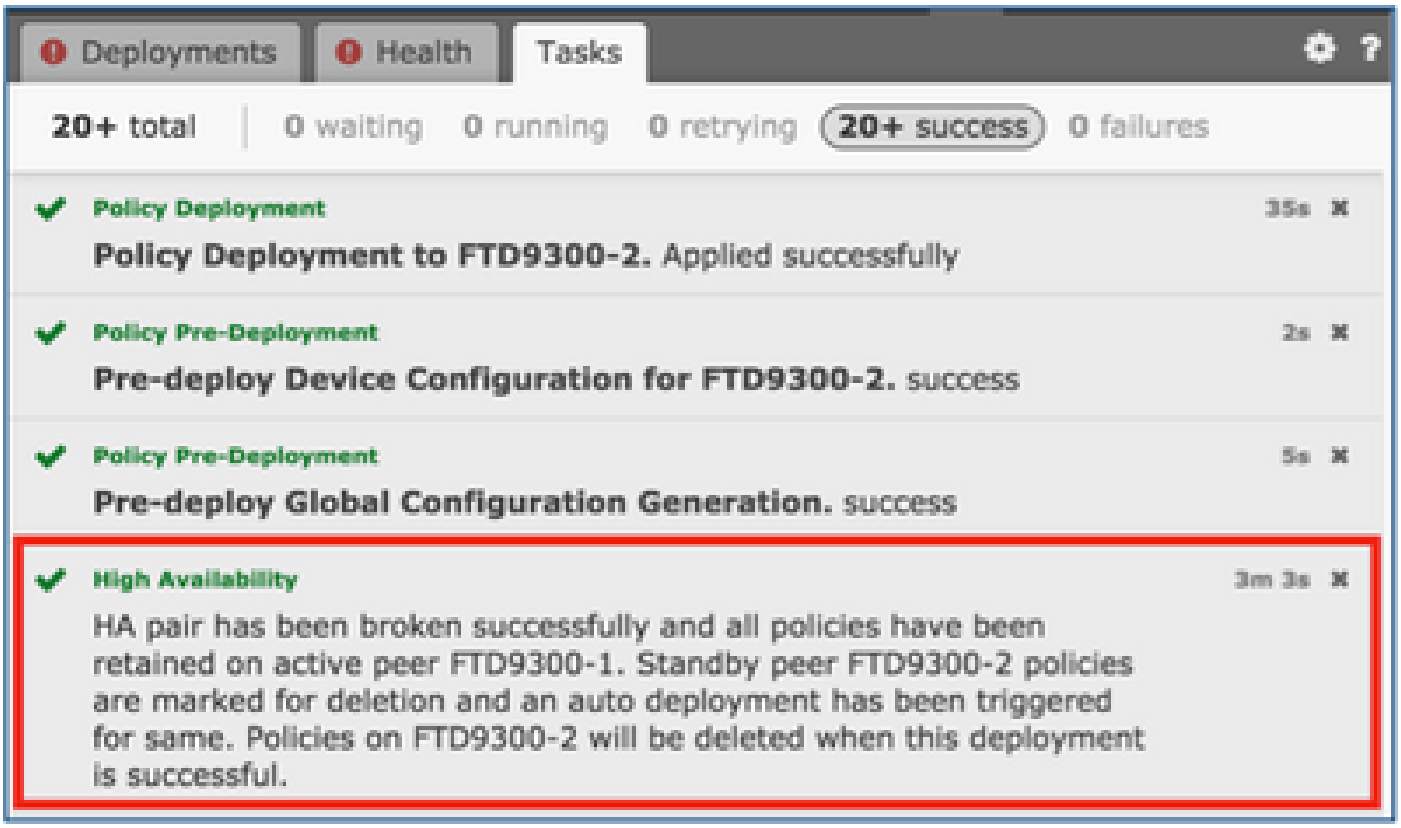
해결책:

1단계. 이미지에 표시된 대로 아이콘을 선택합니다.

2단계. 이미지에 표시된 대로 알림을 확인합니다.



3단계. 그림과 같이 메시지를 기록합니다.



4단계. 이미지에 표시된 대로 FMC GUI에서 결과를 확인합니다.

HA 분리 전과 후에 기본 유닛에서 show running-config 실행:

HA 분리 전	HA 분리 후
firepower# sh 실행 : 저장됨 : : 일련번호: FLM19267A63 : 하드웨어: FPR9K-SM-36, 135839 MB RAM, CPU Xeon E5 Series 2294 MHz, 2 CPU(72코어) : NGFW 버전 10.10.1.1 !	firepower# sh 실행 : 저장됨 : : 일련번호: FLM19267A63 : 하드웨어: FPR9K-SM-36, 135839 MB R Series 2294 MHz, 2 CPU(72코어) : NGFW 버전 10.10.1.1 !

호스트 이름 firepower	호스트 이름 firepower
비밀번호 8Ry2YjIyt7RRXU24 암호화 활성화	비밀번호 8Ry2YjIyt7RRXU24 암호화 활성
이름	이름
!	!
인터페이스 Ethernet1/2	인터페이스 Ethernet1/2
관리 전용	관리 전용
nameif 진단	nameif 진단
보안 수준 0	보안 수준 0
ip 주소 없음	ip 주소 없음
!	!
인터페이스 Ethernet1/4	인터페이스 Ethernet1/4
설명 LAN/STATE Failover Interface	nameif 없음
!	보안 수준 없음
interface Ethernet1/5	ip 주소 없음
nameif 내부	!
보안 수준 0	interface Ethernet1/5
ip 주소 192.168.75.10 255.255.255.0 대기 192.168.75.11	nameif 내부
!	보안 수준 0
interface Ethernet1/6	ip 주소 192.168.75.10 255.255.255.0 대기
nameif 외부	!
보안 수준 0	interface Ethernet1/6
ip 주소 192.168.76.10 255.255.255.0 대기 192.168.76.11	nameif 외부
!	보안 수준 0
ftp 모드 수동	ip 주소 192.168.76.10 255.255.255.0 대기
ngips conn-match vlan-id	!
access-list CSM_FW_ACL_ remark rule-id 268447744: 액세스 정책: FTD9300 - 필수/1	ftp 모드 수동

access-list CSM_FW_ACL_ remark rule-id 268447744: L4 규칙 : Allow_ICMP access-list CSM_FW_ACL_ advanced permit icmp any rule-id 268447744 event-log both access-list CSM_FW_ACL_ remark rule-id 268441600: 액세스 정책: FTD9300 - 기본값/1 access-list CSM_FW_ACL_ remark rule-id 268441600: L4 규칙 : 기본 작업 규칙 access-list CSM_FW_ACL_ advanced permit ip any rule-id 268441600 ! tcp-map UM_STATIC_TCP_MAP tcp-options 범위 6 7 허용 tcp-options 범위 9 255 허용 긴급 플래그 허용 ! 호출기 없음 로깅 사용 로깅 타임스탬프 로깅 대기 로깅 버퍼 크기 100000 로깅 버퍼링된 디버깅 로깅 flash-minimum-free 1024 로깅 flash-maximum-allocation 3076 mtu diagnostic 1500 mtu 내부 1500 mtu 1500 외부 장애 조치 장애 조치 lan 유닛 기본	ngips conn-match vlan-id access-list CSM_FW_ACL_ remark rule-id 정책: FTD9300 - 필수/1 access-list CSM_FW_ACL_ remark rule-id : Allow_ICMP access-list CSM_FW_ACL_ advanced per 268447744 event-log both access-list CSM_FW_ACL_ remark rule-id 정책: FTD9300 - 기본값/1 access-list CSM_FW_ACL_ remark rule-id : 기본 작업 규칙 access-list CSM_FW_ACL_ advanced per 268441600 ! tcp-map UM_STATIC_TCP_MAP tcp-options 범위 6 7 허용 tcp-options 범위 9 255 허용 긴급 플래그 허용 ! 호출기 없음 로깅 사용 로깅 타임스탬프 로깅 대기 로깅 버퍼 크기 100000 로깅 버퍼링된 디버깅 로깅 flash-minimum-free 1024 로깅 flash-maximum-allocation 3076 mtu diagnostic 1500 mtu 내부 1500

장애 조치 lan 인터페이스 fover_link Ethernet1/4

장애 조치(failover) 복제 http

장애 조치 mac 주소 Ethernet1/5 aaaa.bbb.1111 aaaa.bbb.2222

장애 조치 mac 주소 Ethernet1/6 aaaa.bbb.3333 aaaa.bbb.4444

장애 조치 링크 fover_link Ethernet1/4

장애 조치 인터페이스 ip fover_link 10.10.1.1 255.255.255.0 standby 10.1.2

icmp 연결 불가능 속도 제한 1 버스트 크기 1

asdm history enable 없음

arp 시간 초과 14400

no arp permit-nonconnected

액세스 그룹 CSM_FW_ACL_ 전역

시간 제한 xlate 3:00:00

시간 제한 pat-xlate 0:00:30

timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 sctp 0:02:00 icmp 0:00:02

시간 제한 sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00

시간 제한 sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00

시간 제한 sip-provisional-media 0:02:00 uauth 0:05:00 absolute

시간 제한 tcp-proxy-reassembly 0:00:30

timeout floating-conn 0:00:00

aaa proxy-limit 비활성화

snmp-server 위치 없음

snmp-server 연락처 없음

mtu 1500 외부

장애 조치 없음

monitor-interface service-module 없음

icmp 연결 불가능 속도 제한 1 버스트 크기

asdm history enable 없음

arp 시간 초과 14400

no arp permit-nonconnected

액세스 그룹 CSM_FW_ACL_ 전역

시간 제한 xlate 3:00:00

시간 제한 pat-xlate 0:00:30

timeout conn 1:00:00 half-closed 0:10:00 0:02:00 icmp 0:00:02

시간 제한 sunrpc 0:10:00 h323 0:05:00 h2 0:05:00 mgcp-pat 0:05:00

시간 제한 sip 0:30:00 sip_media 0:02:00 s disconnect 0:02:00

시간 제한 sip-provisional-media 0:02:00 u absolute

시간 제한 tcp-proxy-reassembly 0:00:30

timeout floating-conn 0:00:00

aaa proxy-limit 비활성화

snmp-server 위치 없음

snmp-server 연락처 없음

snmp-server가 트랩 snmp 인증 linkup link warmstart를 활성화하지 않음

암호화 ipsec 보안 연결 pmtu-에이징 무한

crypto ca trustpool 정책

텔넷 시간 초과 5

ssh stricthostkeycheck

snmp-server가 트랩 snmp 인증 linkup linkdown coldstart warmstart를 활성화하지 않음

암호화 ipsec 보안 연결 pmtu-에이징 무한

crypto ca trustpool 정책

텔넷 시간 초과 5

ssh stricthostkeycheck

ssh 시간 초과 5

ssh key-exchange 그룹 dh-group1-sha1

콘솔 시간 초과 0

dynamic-access-policy-record DfltAccessPolicy

!

class-map inspection_default

기본 검사 트래픽 일치

!

!

policy-map type inspect dns preset_dns_map

매개변수

message-length maximum client auto

message-length 최대 512

policy-map type inspect ip-options UM_STATIC_IP_OPTIONS_MAP

매개변수

eool 작업 허용

nop 작업 허용

라우터 알림 작업 허용

정책 맵 global_policy

class inspection_default

ssh 시간 초과 5

ssh key-exchange 그룹 dh-group1-sha1

콘솔 시간 초과 0

dynamic-access-policy-record DfltAccessP

!

class-map inspection_default

기본 검사 트래픽 일치

!

!

policy-map type inspect dns preset_dns_r

매개변수

message-length maximum client auto

message-length 최대 512

policy-map type inspect ip-options UM_STATIC_IP_OPTIONS_MAP

매개변수

eool 작업 허용

nop 작업 허용

라우터 알림 작업 허용

정책 맵 global_policy

class inspection_default

inspect dns preset_dns_map

ftp 검사

검사 h323 h225

h323 ras 검사

rsh 검사

rtsp 검사

inspect dns preset_dns_map

ftp 검사

검사 h323 h225

h323 ras 검사

rsh 검사

rtsp 검사

inspect sqlnet

inspect skinny

inspect sunrpc

xdmcp 검사

inspect sip

netbios 검사

tftp 검사

icmp 검사

icmp 검사 오류

dcerpc 검사

inspect ip-options UM_STATIC_IP_OPTIONS_MAP

class-default

연결 고급 옵션 설정 UM_STATIC_TCP_MAP

!

서비스 정책 전역 정책 전역

프롬프트 호스트 이름 컨텍스트

콜홈

프로필 CiscoTAC-1

활성 상태 없음

대상 주소 http https://tools.cisco.com/its/service/oddce/services/DDCEService

inspect sqlnet

inspect skinny

inspect sunrpc

xdmcp 검사

inspect sip

netbios 검사

tftp 검사

icmp 검사

icmp 검사 오류

dcerpc 검사

inspect ip-options UM_STATIC_IP_OPTIC

class-default

연결 고급 옵션 설정 UM_STATIC_TCP_M

!

서비스 정책 전역 정책 전역

프롬프트 호스트 이름 컨텍스트

콜홈

프로필 CiscoTAC-1

활성 상태 없음

대상 주소 http https://tools.cisco.com/its/service/oddce/s

수신 주소 이메일 callhome@cisco.com

대상 전송 방식 http

경고 그룹 진단 구독

alert-group 환경에 가입

alert-group 인벤토리 정기 구독 월

subscribe-to-alert-group 컨피그레이션 주

수신 주소 이메일 callhome@cisco.com 대상 전송 방식 http 경고 그룹 진단 구독 alert-group 환경에 가입 alert-group 인벤토리 정기 구독 월 subscribe-to-alert-group 컨피그레이션 주기적 매월 subscribe-to-alert-group telemetry 일별 Cryptochecksum:933c594fc0264082edc0f24bad358031 : 끝 firepower 번호	subscribe-to-alert-group telemetry 일별 Cryptochecksum:fb6f5c369dee730b9125 : 끝 firepower 번호

show running-config on the Secondary unit before and after the HA break here(여기 표에 나와 있는 것처럼 HA 중단 전후에 보조 유닛에서 running-config를 표시합니다).

HA 분리 전	HA 분리 후
firepower# sh 실행 : 저장됨 : : 일련 번호: FLM19206H7T : 하드웨어: FPR9K-SM-36, 135841 MB RAM, CPU Xeon E5 Series 2294 MHz, 2 CPU(72코어) : NGFW 버전 10.10.1.1 ! 호스트 이름 firepower 비밀번호 8Ry2YjIyt7RRXU24 암호화 활성화 이름 !	firepower# sh 실행 : 저장됨 : : 일련 번호: FLM19206H7T : 하드웨어: FPR9K-SM-36, 135841 MB R Series 2294 MHz, 2 CPU(72코어) : NGFW 버전 10.10.1.1 ! 호스트 이름 firepower 비밀번호 8Ry2YjIyt7RRXU24 암호화 활성 이름 !

인터페이스 Ethernet1/2 관리 전용 nameif 진단 보안 수준 0 ip 주소 없음 ! 인터페이스 Ethernet1/4 설명 LAN/STATE Failover Interface ! interface Ethernet1/5 nameif 내부 보안 수준 0 ip 주소 192.168.75.10 255.255.255.0 대기 192.168.75.11 ! interface Ethernet1/6 nameif 외부 보안 수준 0 ip 주소 192.168.76.10 255.255.255.0 대기 192.168.76.11 ! ftp 모드 수동 ngips conn-match vlan-id access-list CSM_FW_ACL_ remark rule-id 268447744: 액세스 정책: FTD9300 - 필수/1 access-list CSM_FW_ACL_ remark rule-id 268447744: L4 규칙 : Allow_ICMP access-list CSM_FW_ACL_ advanced permit icmp any rule-id 268447744 event-log both access-list CSM_FW_ACL_ remark rule-id 268441600: 액세스	인터페이스 Ethernet1/2 관리 전용 nameif 진단 보안 수준 0 ip 주소 없음 ! 인터페이스 Ethernet1/4 셧다운 nameif 없음 보안 수준 없음 ip 주소 없음 ! interface Ethernet1/5 셧다운 nameif 없음 보안 수준 없음 ip 주소 없음 ! interface Ethernet1/6 셧다운 nameif 없음 보안 수준 없음 ip 주소 없음 ! ftp 모드 수동 ngips conn-match vlan-id

정책: FTD9300 - 기본값/1

access-list CSM_FW_ACL_ remark rule-id 268441600: L4 규칙 : 기본 작업 규칙

access-list CSM_FW_ACL_ advanced permit ip any rule-id 268441600

!

tcp-map UM_STATIC_TCP_MAP

tcp-options 범위 6 7 허용

tcp-options 범위 9 255 허용

긴급 플래그 허용

!

호출기 없음

로깅 사용

로깅 타임스탬프

로깅 대기

로깅 버퍼 크기 100000

로깅 버퍼링된 디버깅

로깅 flash-minimum-free 1024

로깅 flash-maximum-allocation 3076

mtu diagnostic 1500

mtu 내부 1500

mtu 1500 외부

장애 조치

장애 조치 lan 유닛 보조

장애 조치 lan 인터페이스 fover_link Ethernet1/4

장애 조치(failover) 복제 http

장애 조치 mac 주소 Ethernet1/5 aaaa.bbb.1111 aaaa.bbb.2222

access-list CSM_FW_ACL_ remark rule-id
정책: FTD9300 - 필수/1

access-list CSM_FW_ACL_ remark rule-id
: Allow_ICMP

access-list CSM_FW_ACL_ advanced per
268447744 event-log both

access-list CSM_FW_ACL_ remark rule-id
정책: FTD9300 - 기본값/1

access-list CSM_FW_ACL_ remark rule-id
: 기본 작업 규칙

access-list CSM_FW_ACL_ advanced per
268441600

!

tcp-map UM_STATIC_TCP_MAP

tcp-options 범위 6 7 허용

tcp-options 범위 9 255 허용

긴급 플래그 허용

!

호출기 없음

로깅 메시지 106015 없음

로깅 메시지 313001 없음

로깅 메시지 313008 없음

로깅 메시지 106023 없음

로깅 메시지 710003 없음

로깅 메시지 106100 없음

로깅 메시지 302015 없음

로깅 메시지 302014 없음

로깅 메시지 302013 없음

로깅 메시지 302018 없음

장애 조치 mac 주소 Ethernet1/6 aaaa.bbb.3333 aaaa.bbb.4444 장애 조치 링크 fover_link Ethernet1/4 장애 조치 인터페이스 ip fover_link 10.10.1.1 255.255.255.0 standby 10.1.2 icmp 연결 불가능 속도 제한 1 버스트 크기 1 asdm history enable 없음 arp 시간 초과 14400 no arp permit-nonconnected 액세스 그룹 CSM_FW_ACL_ 전역 시간 제한 xlate 3:00:00 시간 제한 pat-xlate 0:00:30 timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 sctp 0:02:00 icmp 0:00:02 시간 제한 sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00 시간 제한 sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00 시간 제한 sip-provisional-media 0:02:00 uauth 0:05:00 absolute 시간 제한 tcp-proxy-reassembly 0:00:30 timeout floating-conn 0:00:00 사용자 ID 기본 도메인 로컬 aaa proxy-limit 비활성화 snmp-server 위치 없음 snmp-server 연락처 없음 snmp-server가 트랩 snmp 인증 linkup linkdown coldstart warmstart를 활성화하지 않음 암호화 ipsec 보안 연결 pmtu-에이징 무한	로깅 메시지 302017 없음 로깅 메시지 302016 없음 로깅 메시지 302021 없음 로깅 메시지 302020 없음 mtu diagnostic 1500 장애 조치 없음 monitor-interface service-module 없음 icmp 연결 불가능 속도 제한 1 버스트 크기 asdm history enable 없음 arp 시간 초과 14400 no arp permit-nonconnected 액세스 그룹 CSM_FW_ACL_ 전역 시간 제한 xlate 3:00:00 시간 제한 pat-xlate 0:00:30 timeout conn 1:00:00 half-closed 0:10:00 0:02:00 icmp 0:00:02 시간 제한 sunrpc 0:10:00 h323 0:05:00 h2 0:05:00 mgcp-pat 0:05:00 시간 제한 sip 0:30:00 sip_media 0:02:00 s disconnect 0:02:00 시간 제한 sip-provisional-media 0:02:00 u absolute 시간 제한 tcp-proxy-reassembly 0:00:30 timeout floating-conn 0:00:00 aaa proxy-limit 비활성화 snmp-server 위치 없음 snmp-server 연락처 없음 snmp-server가 트랩 snmp 인증 linkup link warmstart를 활성화하지 않음

crypto ca trustpool 정책	암호화 ipsec 보안 연결 pmtu-에이징 무한
텔넷 시간 초과 5	crypto ca trustpool 정책
ssh stricthostkeycheck	텔넷 시간 초과 5
ssh 시간 초과 5	ssh stricthostkeycheck
ssh key-exchange 그룹 dh-group1-sha1	ssh 시간 초과 5
콘솔 시간 초과 0	ssh key-exchange 그룹 dh-group1-sha1
dynamic-access-policy-record DfltAccessPolicy	콘솔 시간 초과 0
!	dynamic-access-policy-record DfltAccessI
class-map inspection_default	!
기본 검사 트래픽 일치	class-map inspection_default
!	기본 검사 트래픽 일치
!	!
policy-map type inspect dns preset_dns_map	!
매개변수	policy-map type inspect dns preset_dns_r
message-length maximum client auto	매개변수
message-length 최대 512	message-length maximum client auto
policy-map type inspect ip-options UM_STATIC_IP_OPTIONS_MAP	message-length 최대 512
매개변수	policy-map type inspect ip-options UM_STATIC_IP_OPTIONS_MAP
eool 작업 허용	매개변수
nop 작업 허용	eool 작업 허용
라우터 알림 작업 허용	nop 작업 허용
정책 맵 global_policy	라우터 알림 작업 허용
class inspection_default	정책 맵 global_policy
inspect dns preset_dns_map	class inspection_default
ftp 검사	inspect dns preset_dns_map
검사 h323 h225	ftp 검사

h323 ras 검사	검사 h323 h225
rsh 검사	h323 ras 검사
rtsp 검사	rsh 검사
inspect sqlnet	rtsp 검사
inspect skinny	inspect sqlnet
inspect sunrpc	inspect skinny
xdmcp 검사	inspect sunrpc
inspect sip	xdmcp 검사
netbios 검사	inspect sip
tftp 검사	netbios 검사
icmp 검사	tftp 검사
icmp 검사 오류	icmp 검사
dcerpc 검사	icmp 검사 오류
inspect ip-options UM_STATIC_IP_OPTIONS_MAP	dcerpc 검사
class-default	inspect ip-options UM_STATIC_IP_OPTIC
연결 고급 옵션 설정 UM_STATIC_TCP_MAP	class-default
!	연결 고급 옵션 설정 UM_STATIC_TCP_M
서비스 정책 전역 정책 전역	!
프롬프트 호스트 이름 컨텍스트	서비스 정책 전역 정책 전역
콜홈	프롬프트 호스트 이름 컨텍스트
프로필 CiscoTAC-1	콜홈
활성 상태 없음	프로필 CiscoTAC-1
대상 주소 http https://tools.cisco.com/its/service/oddce/services/DDCEService	활성 상태 없음
수신 주소 이메일 callhome@cisco.com	대상 주소 http https://tools.cisco.com/its/service/oddce/s
대상 전송 방식 http	수신 주소 이메일 callhome@cisco.com
경고 그룹 진단 구독	대상 전송 방식 http

alert-group 환경에 가입 alert-group 인벤토리 정기 구독 월 subscribe-to-alert-group 컨피그레이션 주기적 매월 subscribe-to-alert-group telemetry 일별 Cryptochecksum:e648f92dd7ef47ee611f2aaa5c6cbd84 : 끝 firepower 번호	경고 그룹 진단 구독 alert-group 환경에 가입 alert-group 인벤토리 정기 구독 월 subscribe-to-alert-group 컨피그레이션 주 subscribe-to-alert-group telemetry 일별 Cryptochecksum:08ed87194e9f5cd9149f : 끝 firepower 번호

HA 분리에 대한 중요 사항:

기본 유닛	보조 유닛
모든 페일오버 설정이 제거됨. 스탠바이 IP 주소는 그대로 유지됩니다.	모든 설정이 제거됨.

5단계. 이 작업을 완료한 후 HA 쌍을 다시 생성합니다.

작업 6. HA 쌍 비활성화

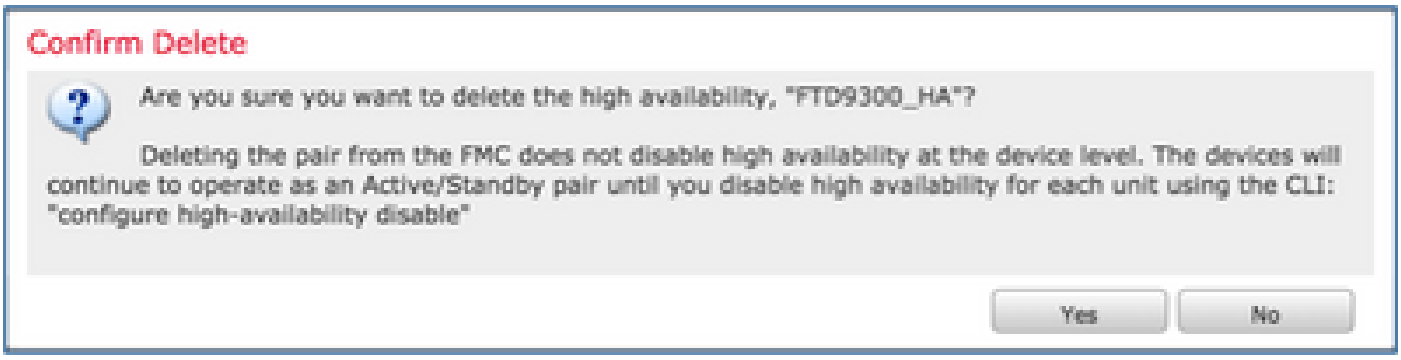
작업 요구 사항:

FMC에서 페일오버 쌍을 비활성화합니다.

해결책:

1단계. 이미지에 표시된 대로 아이콘을 선택합니다.

2단계. 알림을 확인하고 그림과 같이 확인합니다.



3단계. HA를 삭제하면 두 디바이스 모두 FMC에서 등록 취소(제거)됩니다.

LINA CLI의 show running-config 결과는 여기에 있는 표와 같습니다.

기본 유닛	보조 유닛
firepower# sh 실행 : 저장됨 : : 일련번호: FLM19267A63 : 하드웨어: FPR9K-SM-36, 135839 MB RAM, CPU Xeon E5 Series 2294 MHz, 2 CPU(72코어) : NGFW 버전 10.10.1.1 ! 호스트 이름 firepower 비밀번호 8Ry2YjIyt7RRXU24 암호화 활성화 이름 ! 인터페이스 Ethernet1/2 관리 전용 nameif 진단 보안 수준 0 ip 주소 없음	firepower# sh 실행 : 저장됨 : : 일련 번호: FLM19206H7T : 하드웨어: FPR9K-SM-36, 135841 MB R Series 2294 MHz, 2 CPU(72코어) : NGFW 버전 10.10.1.1 ! 호스트 이름 firepower 비밀번호 8Ry2YjIyt7RRXU24 암호화 활성 이름 ! 인터페이스 Ethernet1/2 관리 전용 nameif 진단 보안 수준 0 ip 주소 없음

!	!
인터페이스 Ethernet1/4	인터페이스 Ethernet1/4
설명 LAN/STATE Failover Interface	설명 LAN/STATE Failover Interface
!	!
interface Ethernet1/5	interface Ethernet1/5
nameif 내부	nameif 내부
보안 수준 0	보안 수준 0
ip 주소 192.168.75.10 255.255.255.0 대기 192.168.75.11	ip 주소 192.168.75.10 255.255.255.0 대기
!	!
interface Ethernet1/6	interface Ethernet1/6
nameif 외부	nameif 외부
보안 수준 0	보안 수준 0
ip 주소 192.168.76.10 255.255.255.0 대기 192.168.76.11	ip 주소 192.168.76.10 255.255.255.0 대기
!	!
ftp 모드 수동	ftp 모드 수동
ngips conn-match vlan-id	ngips conn-match vlan-id
access-list CSM_FW_ACL_ remark rule-id 268447744: 액세스 정책: FTD9300 - 필수/1	access-list CSM_FW_ACL_ remark rule-id 정책: FTD9300 - 필수/1
access-list CSM_FW_ACL_ remark rule-id 268447744: L4 규칙 : Allow_ICMP	access-list CSM_FW_ACL_ remark rule-id : Allow_ICMP
access-list CSM_FW_ACL_ advanced permit icmp any rule-id 268447744 event-log both	access-list CSM_FW_ACL_ advanced per 268447744 event-log both
access-list CSM_FW_ACL_ remark rule-id 268441600: 액세스 정책: FTD9300 - 기본값/1	access-list CSM_FW_ACL_ remark rule-id 정책: FTD9300 - 기본값/1
access-list CSM_FW_ACL_ remark rule-id 268441600: L4 규칙 : 기본 작업 규칙	access-list CSM_FW_ACL_ remark rule-id : 기본 작업 규칙
access-list CSM_FW_ACL_ advanced permit ip any rule-id 268441600	access-list CSM_FW_ACL_ advanced per 268441600
!	!

tcp-map UM_STATIC_TCP_MAP	tcp-map UM_STATIC_TCP_MAP
tcp-options 범위 6 7 허용	tcp-options 범위 6 7 허용
tcp-options 범위 9 255 허용	tcp-options 범위 9 255 허용
긴급 플래그 허용	긴급 플래그 허용
!	!
호출기 없음	호출기 없음
로깅 사용	로깅 사용
로깅 타임스탬프	로깅 타임스탬프
로깅 대기	로깅 대기
로깅 버퍼 크기 100000	로깅 버퍼 크기 100000
로깅 버퍼링된 디버깅	로깅 버퍼링된 디버깅
로깅 flash-minimum-free 1024	로깅 flash-minimum-free 1024
로깅 flash-maximum-allocation 3076	로깅 flash-maximum-allocation 3076
mtu diagnostic 1500	mtu diagnostic 1500
mtu 내부 1500	mtu 내부 1500
mtu 1500 외부	mtu 1500 외부
장애 조치	장애 조치
장애 조치 lan 유닛 기본	장애 조치 lan 유닛 보조
장애 조치 lan 인터페이스 fover_link Ethernet1/4	장애 조치 lan 인터페이스 fover_link Ether
장애 조치(failover) 복제 http	장애 조치(failover) 복제 http
장애 조치 mac 주소 Ethernet1/5 aaaa.bbb.1111 aaaa.bbb.2222	장애 조치 mac 주소 Ethernet1/5 aaaa.bbb aaaa.bbb.2222
장애 조치 mac 주소 Ethernet1/6 aaaa.bbb.3333 aaaa.bbb.4444	장애 조치 mac 주소 Ethernet1/6 aaaa.bbb aaaa.bbb.4444
장애 조치 링크 fover_link Ethernet1/4	장애 조치 링크 fover_link Ethernet1/4
장애 조치 인터페이스 ip fover_link 10.10.1.1 255.255.255.0 standby 10.1.2	장애 조치 인터페이스 ip fover_link 10.10.1 standby 10.1.2
icmp 연결 불가능 속도 제한 1 버스트 크기 1	icmp unreachable rate-limit 1 -size 1

asdm history enable 없음	asdm history enable 없음
arp 시간 초과 14400	arp 시간 초과 14400
no arp permit-nonconnected	no arp permit-nonconnected
액세스 그룹 CSM_FW_ACL_ 전역	액세스 그룹 CSM_FW_ACL_ 전역
시간 제한 xlate 3:00:00	시간 제한 xlate 3:00:00
시간 제한 pat-xlate 0:00:30	시간 제한 pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 sctp 0:02:00 icmp 0:00:02	timeout conn 1:00:00 half-closed 0:10:00 0:02:00 icmp 0:00:02
시간 제한 sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00	시간 제한 sunrpc 0:10:00 h323 0:05:00 h2 0:05:00 mgcp-pat 0:05:00
시간 제한 sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00	시간 제한 sip 0:30:00 sip_media 0:02:00 s disconnect 0:02:00
시간 제한 sip-provisional-media 0:02:00 uauth 0:05:00 absolute	시간 제한 sip-provisional-media 0:02:00 u absolute
시간 제한 tcp-proxy-reassembly 0:00:30	시간 제한 tcp-proxy-reassembly 0:00:30
timeout floating-conn 0:00:00	timeout floating-conn 0:00:00
aaa proxy-limit 비활성화	사용자 ID 기본 도메인 로컬
snmp-server 위치 없음	aaa proxy-limit 비활성화
snmp-server 연락처 없음	snmp-server 위치 없음
snmp-server가 트랩 snmp 인증 linkup linkdown coldstart warmstart를 활성화하지 않음	snmp-server 연락처 없음
암호화 ipsec 보안 연결 pmtu-에이징 무한	snmp-server가 트랩 snmp 인증 linkup link warmstart를 활성화하지 않음
crypto ca trustpool 정책	암호화 ipsec 보안 연결 pmtu-에이징 무한
텔넷 시간 초과 5	crypto ca trustpool 정책
ssh stricthostkeycheck	텔넷 시간 초과 5
ssh 시간 초과 5	ssh stricthostkeycheck
ssh key-exchange 그룹 dh-group1-sha1	ssh 시간 초과 5
콘솔 시간 초과 0	ssh key-exchange 그룹 dh-group1-sha1
dynamic-access-policy-record DfltAccessPolicy	콘솔 시간 초과 0

!	dynamic-access-policy-record DfltAccessl
class-map inspection_default	!
기본 검사 트래픽 일치	class-map inspection_default
!	기본 검사 트래픽 일치
!	!
policy-map type inspect dns preset_dns_map	!
매개변수	policy-map type inspect dns preset_dns_r
message-length maximum client auto	매개변수
message-length 최대 512	message-length maximum client auto
policy-map type inspect ip-options UM_STATIC_IP_OPTIONS_MAP	message-length 최대 512
매개변수	policy-map type inspect ip-options UM_STATIC_IP_OPTIONS_MAP
eool 작업 허용	매개변수
nop 작업 허용	eool 작업 허용
라우터 알림 작업 허용	nop 작업 허용
정책 맵 global_policy	라우터 알림 작업 허용
class inspection_default	정책 맵 global_policy
inspect dns preset_dns_map	class inspection_default
ftp 검사	inspect dns preset_dns_map
검사 h323 h225	ftp 검사
h323 ras 검사	검사 h323 h225
rsh 검사	h323 ras 검사
rtsp 검사	rsh 검사
inspect sqlnet	rtsp 검사
inspect skinny	inspect sqlnet
inspect sunrpc	inspect skinny
xdmcp 검사	inspect sunrpc

inspect sip netbios 검사 tftp 검사 icmp 검사 icmp 검사 오류 dcerpc 검사 inspect ip-options UM_STATIC_IP_OPTIONS_MAP class-default 연결 고급 옵션 설정 UM_STATIC_TCP_MAP ! 서비스 정책 전역 정책 전역 프롬프트 호스트 이름 컨텍스트 콜홈 프로필 CiscoTAC-1 활성 상태 없음 대상 주소 http https://tools.cisco.com/its/service/oddce/services/DDCEService 수신 주소 이메일 callhome@cisco.com 대상 전송 방식 http 경고 그룹 진단 구독 alert-group 환경에 가입 alert-group 인벤토리 정기 구독 월 subscribe-to-alert-group 컨피그레이션 주기적 매월 subscribe-to-alert-group telemetry 일별 Cryptochecksum:933c594fc0264082edc0f24bad358031 : 끝 firepower 번호	xdmcp 검사 inspect sip netbios 검사 tftp 검사 icmp 검사 icmp 검사 오류 dcerpc 검사 inspect ip-options UM_STATIC_IP_OPTIC class-default 연결 고급 옵션 설정 UM_STATIC_TCP_M ! 서비스 정책 전역 정책 전역 프롬프트 호스트 이름 컨텍스트 콜홈 프로필 CiscoTAC-1 활성 상태 없음 대상 주소 http https://tools.cisco.com/its/service/oddce/s 수신 주소 이메일 callhome@cisco.com 대상 전송 방식 http 경고 그룹 진단 구독 alert-group 환경에 가입 alert-group 인벤토리 정기 구독 월 subscribe-to-alert-group 컨피그레이션 주 subscribe-to-alert-group telemetry 일별 Cryptochecksum:e648f92dd7ef47ee611f2 : 끝

	firepower 번호

4단계. 두 FTD 디바이스 모두 FMC에서 등록되지 않았습니다.

```
<#root>

> show managers

No managers configured.
```

FMC의 HA 비활성화 옵션에 대한 중요 사항:

기본 유닛	보조 유닛
디바이스가 FMC에서 제거됩니다. FTD 디바이스에서 설정이 제거되지 않음.	디바이스가 FMC에서 제거됩니다. FTD 디바이스에서 설정이 제거되지 않음.

5단계. 다음 명령을 실행하여 FTD 디바이스에서 장애 조치 컨피그레이션을 제거합니다.

```
<#root>

>

configure high-availability disable

High-availability will be disabled. Do you really want to continue?
Please enter 'YES' or 'NO':

yes

Successfully disabled high-availability.
```

참고: 두 유닛 모두에서 명령을 실행해야 합니다

결과:

기본 유닛	보조 유닛
> **show failover**	> **show failover** **Failover Off (pseudo-Standby)** **Failover unit Secondary**

Failover Off **Failover unit Secondary** **Failover LAN Interface: not Configured** **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 2 of 1041 maximum** **MAC Address Move Notification Interval not set** >	**Failover LAN Interface: FOVER Ethernet1/3.205 (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 0 of 1041 maximum** **MAC Address Move Notification Interval not set** **failover replication http** >

기본	보조
firepower# show run ! 호스트 이름 firepower 비밀번호 8Ry2YjIyt7RRXU24 암호화 활성화 이름 arp 시간 초과 14400 no arp permit-nonconnected arp 속도 제한 16384 ! 인터페이스 GigabitEthernet1/1 nameif 외부 cts 설명서 propagate sgt preserve-untag policy static sgt disabled trusted 보안 수준 0 ip 주소 10.1.1.1 255.255.255.0 <— 스탠바이 IP가 제거되었습	firepower# show run ! 호스트 이름 firepower 비밀번호 8Ry2YjIyt7RRXU24 암호화 활성 이름 arp 시간 초과 14400 no arp permit-nonconnected arp 속도 제한 16384 ! 인터페이스 GigabitEthernet1/1 셧다운 nameif 없음 보안 수준 없음 ip 주소 없음 ! 인터페이스 GigabitEthernet1/2

니다.

!

인터페이스 GigabitEthernet1/2

nameif 내부

cts 설명서

propagate sgt preserve-untag

policy static sgt disabled trusted

보안 수준 0

ip 주소 192.168.1.1 255.255.255.0 <— 스탠바이 IP가 제거되었습니다.

!

인터페이스 GigabitEthernet1/3

설명 LAN 장애 조치 인터페이스

!

인터페이스 GigabitEthernet1/4

설명 상태 장애 조치 인터페이스

!

인터페이스 GigabitEthernet1/5

셧다운

nameif 없음

보안 수준 없음

ip 주소 없음

!

인터페이스 GigabitEthernet1/6

셧다운

nameif 없음

보안 수준 없음

셧다운

nameif 없음

보안 수준 없음

ip 주소 없음

!

인터페이스 GigabitEthernet1/3

설명 LAN 장애 조치 인터페이스

!

인터페이스 GigabitEthernet1/4

설명 상태 장애 조치 인터페이스

!

인터페이스 GigabitEthernet1/5

셧다운

nameif 없음

보안 수준 없음

ip 주소 없음

!

인터페이스 GigabitEthernet1/6

셧다운

nameif 없음

보안 수준 없음

ip 주소 없음

!

인터페이스 GigabitEthernet1/7

셧다운

nameif 없음

ip 주소 없음

!

인터페이스 GigabitEthernet1/7

셧다운

nameif 없음

보안 수준 없음

ip 주소 없음

!

인터페이스 GigabitEthernet1/8

셧다운

nameif 없음

보안 수준 없음

ip 주소 없음

!

인터페이스 관리1/1

관리 전용

nameif 진단

cts 설명서

propagate sgt preserve-untag

policy static sgt disabled trusted

보안 수준 0

ip 주소 없음

!

ftp 모드 수동

ngips conn-match vlan-id

access-list CSM_FW_ACL_ remark rule-id 9998: PREFILTER 정책: 기본 터널 및 우선순위 정책

보안 수준 없음

ip 주소 없음

!

인터페이스 GigabitEthernet1/8

셧다운

nameif 없음

보안 수준 없음

ip 주소 없음

!

인터페이스 관리1/1

관리 전용

nameif 진단

cts 설명서

propagate sgt preserve-untag

policy static sgt disabled trusted

보안 수준 0

ip 주소 없음

!

ftp 모드 수동

ngips conn-match vlan-id

access-list CSM_FW_ACL_ remark rule-id
정책: 기본 터널 및 우선순위 정책

access-list CSM_FW_ACL_ remark rule-id
널 작업 규칙

access-list CSM_FW_ACL_ advanced per
9998

access-list CSM_FW_ACL_ advanced per
9998

access-list CSM_FW_ACL_ remark rule-id 9998: 규칙: 기본 터널 작업 규칙

access-list CSM_FW_ACL_ advanced permit ipinip any rule-id 9998

access-list CSM_FW_ACL_ advanced permit 41 any rule-id 9998

access-list CSM_FW_ACL_ advanced permit gre any rule-id 9998

access-list CSM_FW_ACL_ advanced permit udp any eq 3544 rule-id 9998

access-list CSM_FW_ACL_ remark rule-id 268435456: 액세스 정책: FTD_HA - 기본값/1

access-list CSM_FW_ACL_ remark rule-id 268435456: L4 규칙: 기본 작업 규칙

access-list CSM_FW_ACL_ advanced permit ip any rule-id 268435456

!

tcp-map UM_STATIC_TCP_MAP

 tcp-options 범위 6 7 허용

 tcp-options 범위 9 18 허용

 tcp-options 범위 20 255 허용

 tcp-options md5 clear

 긴급 플래그 허용

!

호출기 없음

로깅 사용

로깅 타임스탬프

로깅 버퍼링된 디버깅

로깅 flash-minimum-free 1024

로깅 flash-maximum-allocation 3076

access-list CSM_FW_ACL_ advanced per
9998

access-list CSM_FW_ACL_ advanced per
rule-id 9998

access-list CSM_FW_ACL_ remark rule-id
정책: FTD_HA - 기본값/1

access-list CSM_FW_ACL_ remark rule-id
: 기본 작업 규칙

access-list CSM_FW_ACL_ advanced per
268435456

!

tcp-map UM_STATIC_TCP_MAP

 tcp-options 범위 6 7 허용

 tcp-options 범위 9 18 허용

 tcp-options 범위 20 255 허용

 tcp-options md5 clear

 긴급 플래그 허용

!

호출기 없음

로깅 사용

로깅 타임스탬프

로깅 버퍼링된 디버깅

로깅 flash-minimum-free 1024

로깅 flash-maximum-allocation 3076

로깅 메시지 106015 없음

로깅 메시지 313001 없음

로깅 메시지 313008 없음

로깅 메시지 106023 없음

로깅 메시지 710005 없음

로깅 메시지 106015 없음	로깅 메시지 710003 없음
로깅 메시지 313001 없음	로깅 메시지 106100 없음
로깅 메시지 313008 없음	로깅 메시지 302015 없음
로깅 메시지 106023 없음	로깅 메시지 302014 없음
로깅 메시지 710005 없음	로깅 메시지 302013 없음
로깅 메시지 710003 없음	로깅 메시지 302018 없음
로깅 메시지 106100 없음	로깅 메시지 302017 없음
로깅 메시지 302015 없음	로깅 메시지 302016 없음
로깅 메시지 302014 없음	로깅 메시지 302021 없음
로깅 메시지 302013 없음	로깅 메시지 302020 없음
로깅 메시지 302018 없음	mtu 1500 외부
로깅 메시지 302017 없음	mtu 내부 1500
로깅 메시지 302016 없음	mtu diagnostic 1500
로깅 메시지 302021 없음	장애 조치 없음
로깅 메시지 302020 없음	장애 조치 lan 유닛 보조
mtu 1500 외부	장애 조치 lan 인터페이스 FOVER Gigabit
mtu 내부 1500	장애 조치(failover) 복제 http
mtu diagnostic 1500	장애 조치 링크 상태 GigabitEthernet1/4
장애 조치 없음	장애 조치 인터페이스 ip FOVER 10.10.1. 10.1.2
icmp 연결 불가능 속도 제한 1 버스트 크기 1	장애 조치 인터페이스 ip STATE 10.10.2.1 standby 10.10.2.2
asdm history enable 없음	
액세스 그룹 CSM_FW_ACL_ 전역	icmp 연결 불가능 속도 제한 1 버스트 크기
00 커뮤니티 ***** 버전 2c	asdm history enable 없음
snmp-server 위치 없음	액세스 그룹 CSM_FW_ACL_ 전역
snmp-server 연락처 없음	시간 제한 xlate 3:00:00
snmp-server 커뮤니티 *****	시간 제한 pat-xlate 0:00:30

서비스 sw 재설정 버튼

암호화 ipsec 보안 연결 pmtu-에이징 무한

crypto ca trustpool 정책

텔넷 시간 초과 5

콘솔 시간 초과 0

dynamic-access-policy-record DfltAccessPolicy

!

class-map inspection_default

 기본 검사 트래픽 일치

!

!

policy-map type inspect dns preset_dns_map

 매개변수

  message-length maximum client auto

  message-length 최대 512

  tcp 검사 없음

policy-map type inspect ip-options UM_STATIC_IP_OPTIONS_MAP

 매개변수

  eool 작업 허용

  nop 작업 허용

  라우터 알림 작업 허용

정책 맵 global_policy

 class inspection_default

  inspect dns preset_dns_map

  ftp 검사

  검사 h323 h225

timeout conn 1:00:00 half-closed 0:10:00
0:02:00 icmp 0:00:02

시간 제한 sunrpc 0:10:00 h323 0:05:00 h2
0:05:00 mgcp-pat 0:05:00

시간 제한 sip 0:30:00 sip_media 0:02:00 s
disconnect 0:02:00

시간 제한 sip-provisional-media 0:02:00 u
absolute

시간 제한 tcp-proxy-reassembly 0:00:30

timeout floating-conn 0:00:00

timeout conn-holddown 0:00:15

사용자 ID 기본 도메인 로컬

aaa proxy-limit 비활성화

192.168.1.100 커뮤니티 ***** 버전 2c 외부
트

snmp-server 위치 없음

snmp-server 연락처 없음

snmp-server 커뮤니티 *****

서비스 sw 재설정 버튼

암호화 ipsec 보안 연결 pmtu-에이징 무한

crypto ca trustpool 정책

텔넷 시간 초과 5

콘솔 시간 초과 0

dynamic-access-policy-record DfltAccessP

!

class-map inspection_default

 기본 검사 트래픽 일치

!

!

h323 ras 검사

rsh 검사

rtsp 검사

esmtp 검사

inspect sqlnet

inspect skinny

inspect sunrpc

xdmcp 검사

inspect sip

netbios 검사

tftp 검사

icmp 검사

icmp 검사 오류

dcerpc 검사

inspect ip-options UM_STATIC_IP_OPTIONS_MAP

class-default

연결 고급 옵션 설정 UM_STATIC_TCP_MAP

!

서비스 정책 전역 정책 전역

프롬프트 호스트 이름 컨텍스트

콜홈

프로필 CiscoTAC-1

활성 상태 없음

대상 주소 http https://tools.cisco.com/its/service/oddce/services/DDCEService

수신 주소 이메일 callhome@cisco.com

대상 전송 방식 http

policy-map type inspect dns preset_dns_r

매개변수

message-length maximum client auto

message-length 최대 512

tcp 검사 없음

policy-map type inspect ip-options UM_STATIC_IP_OPTIONS_MAP

매개변수

eool 작업 허용

nop 작업 허용

라우터 알림 작업 허용

정책 맵 global_policy

class inspection_default

inspect dns preset_dns_map

ftp 검사

검사 h323 h225

h323 ras 검사

rsh 검사

rtsp 검사

esmtp 검사

inspect sqlnet

inspect skinny

inspect sunrpc

xdmcp 검사

inspect sip

netbios 검사

tftp 검사

경고 그룹 진단 구독 alert-group 환경에 가입 alert-group 인벤토리 정기 구독 월 subscribe-to-alert-group 컨피그레이션 주기적 매월 subscribe-to-alert-group telemetry 일별 Cryptochecksum:768a03e90b9d3539773b9d7af66b3452	icmp 검사 icmp 검사 오류 dcerpc 검사 inspect ip-options UM_STATIC_IP_OPTI class-default 연결 고급 옵션 설정 UM_STATIC_TCP_ ! 서비스 정책 전역 정책 전역 프롬프트 호스트 이름 컨텍스트 콜홈 프로필 CiscoTAC-1 활성 상태 없음 대상 주소 http https://tools.cisco.com/its/service/oddce/s 수신 주소 이메일 callhome@cisco.com 대상 전송 방식 http 경고 그룹 진단 구독 alert-group 환경에 가입 alert-group 인벤토리 정기 구독 월 subscribe-to-alert-group 컨피그레이션 주 subscribe-to-alert-group telemetry 일별 Cryptochecksum:ac9b8f401e18491fee65

FTD CLI에서 HA 비활성화에 대한 중요 사항:

기본 유닛	보조 유닛
장애 조치 컨피그레이션 및 스탠바이 IP의 시간 초과가 xlate 3:00:00으로	• 인터페이스 설정이 제거됨. • 디바이스가 의사 대기 모드로

만료됨 시간 제한 pat-xlate 0:00:30 timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 sctp 0:02:00 icmp 0:00:02 시간 제한 sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00 시간 제한 sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00 시간 제한 sip-provisional-media 0:02:00 uauth 0:05:00 absolute 시간 제한 tcp-proxy-reassembly 0:00:30 timeout floating-conn 0:00:00 timeout conn-holddown 0:00:15 aaa proxy-limit 비활성화 192.168.1.1 외부의 snmp-server 호스트가 제거되었습니다.	전환됨.

6단계. 작업을 완료한 후 디바이스를 FMC에 등록하고 HA 쌍을 활성화합니다.

작업 7. HA 일시 중단

작업 요구 사항:

FTD CLISH CLI에서 HA 일시 중단

해결책:

1단계. 기본 FTD에서 명령을 실행하고 확인합니다(YES를 입력합니다).

<#root>

> configure high-availability suspend

Please ensure that no deployment operation is in progress before suspending high-availability.
Please enter 'YES' to continue if there is no deployment operation in progress and 'NO' if you wish to

YES

Successfully suspended high-availability.

2단계. 기본 유닛의 변경 사항을 확인합니다.

<#root>

>

show high-availability config

Failover Off

Failover unit Primary
Failover LAN Interface: fover_link Ethernet1/4 (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 1 of 1041 maximum
MAC Address Move Notification Interval not set
failover replication http

3단계. 보조 유닛의 결과:

<#root>

>

show high-availability config
Failover Off (pseudo-Standby)

Failover unit Secondary
Failover LAN Interface: fover_link Ethernet1/4 (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 1 of 1041 maximum
MAC Address Move Notification Interval not set
failover replication http

4단계. 기본 유닛에서 HA 다시 시작:

<#root>

```
>

configure high-availability resume

Successfully resumed high-availablity.

> .

    No Active mate detected
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Beginning configuration replication: Sending to mate.
End Configuration Replication to mate

>
```

<#root>

```
>

show high-availability config

Failover On

Failover unit Primary
Failover LAN Interface: fover_link Ethernet1/4 (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 1 of 1041 maximum
MAC Address Move Notification Interval not set
failover replication http
```

5단계. HA를 재개한 후 보조 유닛의 결과는 다음과 같습니다.

<#root>

```
> ..


Detected an Active mate

Beginning configuration replication from mate.


WARNING: Failover is enabled but standby IP address is not configured for this interface.
WARNING: Failover is enabled but standby IP address is not configured for this interface.
End configuration replication from mate.

>
```

<#root>

```
>
```

show high-availability config

Failover On

```
Failover unit Secondary
Failover LAN Interface: fover_link Ethernet1/4 (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 1 of 1041 maximum
MAC Address Move Notification Interval not set
failover replication http
>
```

FAQ(자주 묻는 질문)

컨피그레이션이 복제되면 즉시(행별로) 저장됩니까? 아니면 복제가 끝날 때 저장됩니까?
복제가 끝날 때 이에 대한 증거는 debug fover sync 명령 출력의 끝에 있으며, 설정/명령 복제를 보여줍니다.

<#root>

```
cli_xml_server: frep_write_cmd: Cmd: access-list CSM_FW_ACL_ line 1506 remark rule-id 268442578: L7 RUL
cli_xml_server: frep_write_cmd: Cmd: access-list CSM_FW_ACL_ line 1507 advanced permit tcp object-group
cli_xml_server: frep_write_cmd: Cmd: access-list CSM_FW_ACL_ line 1508 remark rule-id 268442078: ACCESS
cli_xml_server: frep_write_cmd: Cmd: access-list CSM_FW_ACL_ line 1509 remark rule-id 268442078: L4 RUL
...
cli_xml_server: frep_write_cmd: Cmd: no access-list CSM_FW_ACL_ advanced permit tcp object-group group_
cli_xml_server: frep_write_cmd: Cmd: no access-list CSM_FW_ACL_ line 1510 remark rule-id 268442077: ACC
cli_xml_server: frep_write_cmd: Cmd: no access-list CSM_FW_ACL_ line 1510 remark rule-id 268442077: L7
cli_xml_server: frep_write_cmd: Cmd: no access-list CSM_FW_ACL_ advanced permit tcp object-group group_
cli_xml_server: frep_write_cmd: Cmd: no access-list CSM_FW_ACL_ line 1510 remark rule-id 268440577: ACC
cli_xml_server: frep_write_cmd: Cmd: no access-list CSM_FW_ACL_ line 1510 remark rule-id 268440577: L4
cli_xml_server: frep_write_cmd: Cmd: access-list CSM_FW_ACL_ advanced deny ip any any rule-id 268442078
cli_xml_server: frep_write_cmd: Cmd: crypto isakmp nat-traversal
cli_xml_server: frep_write_cmd: Cmd: no object-group network group_311
cli_xml_server: frep_write_cmd: Cmd: no object-group network group_433
cli_xml_server: frep_write_cmd: Cmd: no object-group network group_6
cli_xml_server: frep_write_cmd: Cmd: no object-group network group_2
cli_xml_server: frep_write_cmd: Cmd:
```

write memory <--

어떤 유닛이 의사 대기 상태(장애 조치 비활성화)에 있고 다른 유닛이 장애 조치를 활성화했으며 액티브 상태일 때 다시 로드하면 어떻게 됩니까?
활성/활성 시나리오가 됩니다(기술적으로는 활성/장애 조치 해제이지만). 특히, 유닛이 가동되면 페일오버는 비활성화되지만 유닛은 활성 유닛과 동일한 IP를 사용합니다. 따라서 다음과 같은 이점이 있습니다.

- 장치-1: 활성
- Unit-2: 장애 조치가 해제되었습니다. 유닛에서는 Unit-1과 동일한 데이터 IP를 사용하지만 MAC 주소는 다릅니다.

장애 조치를 수동으로 비활성화(고가용성 일시 중단 구성)한 다음 디바이스를 다시 로드하면 장애 조치 컨피그레이션은 어떻게 됩니까?
장애 조치를 비활성화하면 영구적인 변경 사항이 아닙니다(명시적으로 변경하지 않는 한 startup-config에 저장되지 않음). 두 가지 방법으로 장치를 재부팅/다시 로드할 수 있으며, 두 번째 방법에서는 주의해야 합니다.

사례 1. CLI에서 재부팅

CLISH에서 재부팅해도 확인을 요청하지 않습니다. 따라서 설정 변경 사항은 startup-config에 저장되지 않습니다.

```
<#root>

>

configure high-availability suspend

Please ensure that no deployment operation is in progress before suspending high-availability.
Please enter 'YES' to continue if there is no deployment operation in progress and 'NO' if you wish to

YES

Successfully suspended high-availability.
```

running-config에 장애 조치가 비활성화되어 있습니다. 이 경우, 액티브/액티브 시나리오를 피하기 위해 디바이스가 스탠바이 상태였고 예상대로 의사 스탠바이 상태가 되었습니다.

```
<#root>

firepower#

show failover | include Failover

Failover Off (

pseudo-Standby

)
Failover unit Secondary
Failover LAN Interface: FOVER Ethernet1/1 (up)
```

startup-config에서 장애 조치가 계속 활성화되어 있습니다.

```
<#root>
```

```
firepower#
```

show startup | include failover

failover

```
failover lan unit secondary
failover lan interface FOVER Ethernet1/1
failover replication http
failover link FOVER Ethernet1/1
failover interface ip FOVER 192.0.2.1 255.255.255.0 standby 192.0.2.2
failover ipsec pre-shared-key *****
```

CLISH에서 디바이스를 재부팅합니다(reboot 명령).

<#root>

```
>
```

reboot

```
This command will reboot the system.  Continue?
Please enter 'YES' or 'NO':
```

YES

```
Broadcast message from root@
Threat Defense System: CMD=-stop, CSP-ID=cisco-ftd.6.2.2.81__ftd_001_JMX2119L05CYRIBVX1, FLAG=''
Cisco FTD stopping ...
```

유닛이 가동되면 페일오버가 활성화되므로 디바이스는 페일오버 협상 단계를 진행하여 원격 피어를 탐지하려고 시도합니다.

<#root>

```
User enable_1 logged in to firepower
Logins over the last 1 days: 1.
Failed logins since the last login: 0.
Type help or '?' for a list of available commands.
firepower> .
```

Detected an Active mate

사례 2. LINA CLI에서 재부팅
LINA에서 재부팅 시(reload 명령) 확인이 요청됩니다. 따라서 Y(Yes)를 선택하면 컨피그레이션 변경 사항이 startup-config에 저장됩니다.

```
<#root>

firepower#

reload

System config has been modified. Save? [Y]es/[N]o:

Y <-- Be careful. This will disable the failover in the startup-config


Cryptochecksum: 31857237 8658f618 3234be7c 854d583a

8781 bytes copied in 0.940 secs
Proceed with reload? [confirm]
firepower#

show startup | include failover

no failover

failover lan unit secondary
failover lan interface FOVER Ethernet1/1
failover replication http
failover link FOVER Ethernet1/1
failover interface ip FOVER 192.0.2.1 255.255.255.0 standby 192.0.2.2
failover ipsec pre-shared-key *****
```

유닛이 가동되면 페일오버가 비활성화됩니다.

```
<#root>

firepower#

show failover | include Fail

Failover Off

Failover unit Secondary
Failover LAN Interface: FOVER Ethernet1/1 (up)
```

참고: 이 시나리오를 방지하려면 메시지가 표시되면 startup-config에 변경 사항을 저장하지 않아야 합니다.

관련 정보

- Cisco Firepower Management Center 설정 가이드의 모든 버전은 여기에서 확인할 수 있습니다.

Cisco Secure Firewall Threat Defense 설명서 탐색

- FXOS Chassis Manager 및 CLI 설정 가이드의 모든 버전은 여기에서 확인할 수 있습니다.

Cisco Firepower 4100/9300 FXOS 설명서 탐색

- 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.

Cisco FTD(Firepower Threat Defense): NGFW(Next-Generation Firewall), NGIPS(Next-Generation Intrusion Prevention System) 및 AMP(Advanced Malware Protection)의 컨피그레이션 및 트러블슈팅 모범 사례

- firepower 기술과 관련된 모든 컨피그레이션 및 문제 해결 TechNotes

Cisco Secure Firewall 관리 센터

- 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.