# 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 디바 이스는 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) Ac	kd 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-FF	PR9K-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-FP	R9K-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

	Firepower_TD2	Standalone	Status: ok					V. 2. 3	
	Security Module	Application	Version	Management IP	Gateway	Management Port	Status		
8	Security Module 3	FTD	6.0.1.1.1023	10.62.148.69	10.62.148.1	Ethernet1/2	online	Control 🕒 A	
	Ports: Data Interfaces: Ethernet1/4 Ethernet1/5 Ethernet1/6 UID								

FPR9300-2

Firepower_TD	Standalone	Status: ok					M. 28	
Security Module	Application	Version	Management IP	Gateway	Management Port	Status		
Security Module 3	FTD	6.0.1.1.1023	10.62.148.72	10.62.148.1	Ethernet1/2	Online	Contract 🕒 🥂 🍌	
Ports:     Attributes:       Data Interfaces:     Ethernet1/4     Ethernet1/5     Cluster Operational Status : not-applicable       Ethernet1/6     Firegower_Management IP : 10.82.148.72       UUID     : Mtdps//10.62.148.73/								

# 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.

Add High Availat	oility Pair	? ×								
Name:*	Name:* FTD9300_HA									
Device Type:	Firepower Threat Defense	~								
Primary Peer:	FTD9300-1	*								
Secondary Peer:	FTD9300-2	~								
Threat Defense High Availability pair will have primary device configuration. Licenses from primary peer will be converted to their high availability versions and applied on both peers.										
Continue Cancel										

▲ 경고: 올바른 유닛을 기본 유닛으로 선택해야 합니다. 선택한 기본 유닛의 모든 컨피그레이션 이 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 이름 을 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.

Interface:*	Ethernet1/4	*	Interface:*	Same as LAN Failover L
Logical Name:*	fover_link		Logical Name:*	fover_link
Primary IP:*	1.1.1.1		Primary IP:*	1.1.1.1
	Use IPv6 Address			Use IPv6 Address
Secondary IP:*	1.1.1.2		Secondary IP:*	1.1.1.2
Subnet Mask:*	255.255.255.0		Subnet Mask:*	255.255.255.0
Sec Encryption				
Key Generation:	Auto	٣		
I AN failover link	is used to sync coefin	uration e	tateful failover link is us	ed to sync application contr
LAN failover link	is used to sync config	uration, s	tateful failover link is us	ed to sync application cont

# 4단계. 데이터 인터페이스(기본 및 대기 IP 주소) 구성

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

aligned FTD9300_HA     Cisco Firepower 9000 Series SM-36 Threat Defense High Availability		\$\$\$ \$\$
FTD9300-1(Primary, Active) 10.62.148.72 - Cisco Firepower 9000 Series SM-36 Threat Defense - v6.0.1.1 - routed Cisco Firepower 9000 Series SM-36 Threat, Malware, URL Filtering	FTD9300	
FTD9300-2(Secondary, Standby) 10.62.148.69 - Cisco Firepower 9000 Series SM-36 Threat, Malware, URL Filtering	FTD9300	

# 5단계. 이미지에 표시된 대로 인터페이스 설정을 구성합니다.

# 이더넷 1/5 인터페이스

Edit Physical	Interface	?	×
Mode:	None		
Name:	Inside Cabled Management Only		
Security Zone:	×		
Description:			
General IPv4	IPv6 Advanced Hardware Configuration		
IP Type: IP Address:	Use Static IP v 192.168.75.10/24 eg. 1.1.1.1/255.255.255.228 or 1.1.1.	1/25	
	OK Cano	el	

이더넷 1/6 인터페이스

Edit Physical	Interfac	æ					? ×
Mode:	None		¥	_			
Name:	Outside		C Enabled	Man	agement Only		
Security Zone:			*				
Description:							
General IPv4	IPv6	Advanced	Hardware Con	figuration	i		
IP Type:		Use Static I	p 🗸				
IP Address:		192.168.76	10/24		eg. 1.1.1.1/255	255.255.228	or 1.1.1.1/25
						04	Constal
						UK	Cancel

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

FTD9300 Cisco Firepower	HA 9000 Series SM-36 Thre	at Defense									a Sa	ve 🛛 C
Summary	High Availability	Devices	Routing	NAT	Interfaces	Inline Sets	DHCP					
High Availab	ility Configuration	n										
High Availabilit	y Link							State Link				
Interface						Ethernet1/4		Interface			Ethernet	1/4
Logical Name						fover_link		Logical Name			fover_	link
Primary IP						1.1.1.1		Primary IP			1.1.	1.1
Secondary IP						1.1.1.2		Secondary IP			1.1.	1.2
Subnet Mask						255.255.255.0		Subnet Mask			255.255.25	5.0
IPsec Encrypti	ion					Disabled		Statistics				۹.
Monitored In	terfaces											
Interface Nam	ne Ac	tive IPv4	Standby I	IPv4	Active IPv6 - S	tandby IPv6			Active Link-Local IPv6	Standby Link-Local IPv6	Monitoring	
🚔 Inside	19	2.168.75.10									×	1
diagnostic											×	8
Cutside	19	2.168.76.10									×	1

7단계. 이미지에 표시된 Inside 인터페이스의 경우.

Edit Inside	? ×
Monitor this interface for failures	
IPv4 IPv6	
Interface Name: Inside	
Active IP Address: 192.168.75.10	
Mask: 24	
Standby IP Address: 192.168.75.11	
OK	Cancel

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

9단계. 이미지에 표시된 대로 결과를 확인합니다.

Monitored Interfaces		
Interface Name	Active IPv4	Standby IPv4
inside	192.168.75.10	192.168.75.11
diagnostic		
Dutside	192.168.76.10	192.168.76.11

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

Failover Trigger Criteria	1	Interface Mac Addresses			0
Failure Limit	Failure of 1 Interfaces	Physical Interface	Active Mac Address	Standby Mac Address	
Peer Poll Time	1 sec		No records to display		
Peer Hold Time	15 sec		no records to display		
Interface Poll Time	5 sec				
Interface Hold Time	25 sec				

11단계. Inside Interface는 그림과 같습니다.

Add Interface Mac Address			? ×
Physical Interface:*	Ethernet1/5	~	
Active Interface Mac Address:*	aaaa.bbbb.1111		
Standby Interface Mac Address:*	aaaa.bbbb.2222		
① Enter the Mac addresses in hexad	ecimal format such as	0123.45	67.89ab
	ок	Ca	ncel

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

13단계. 이미지에 표시된 대로 결과를 확인합니다.

Interface Mac Addresses				
	Physical Interface	Active Mac Address	Standby Mac Address	
	Ethernet1/5	aaaa.bbbb.1111	aaaa.bbbb.2222	J 🖉
	Ethernet1/6	aaaa.bbbb.3333	aaaa.bbbb.4444	a 🖉

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 확인합 니다.

FTD9300 Cisco Firepower	9000 Series SM-36 Thr	eat Defense Hig	h Availability							
Summary	High Availability	Devices	Routing	NAT	Interfaces	Inline Sets	DHCP			
	•									
	General						P	License		
	Name:			FTD930	AH_00			Base:	Yes	s
	Status:			0				Export-Controlled	d Features: Yes	s
	Primary Pe	er:		FTD930	00-1(Active)			Malware:	Yes	s
	Secondary	Peer:		FTD930	00-2(Standby)			Threat:	Yes	5
	Failover His	story:		۹,				URL Filtering:	Yes	s

VPN IKEv2 P2

VPN CTCP upd

VPN SDI upd

VPN DHCP upd

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

```
<#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
                                            rcv
                                                        rerr
                                 xerr
    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
```

SIP Sessi	on	0	0		0		0
SIP Tx	0	(	C	0		0	
SIP Pinho	le	0	0		0		0
Route Ses	sion	0		0	0		0
Router ID	0		0		0		0
User-Iden	tity	1		0	0		0
CTS SGTNA	ME	0	0		0		0
CTS PAC	0		0	0		0	
TrustSec-	SXP	0	C	)	0		0
IP∨6 Rout	e 0	1	0		0		0
STS Table	0		0		0		0
Logical U Recv Q: Xmit Q:	pdate Q Cur 0 0	ueue I Max 10 11	nformat Tot 416 2118	ion al			

>

3단계. 보조 디바이스에서도 같은 작업을 수행합니다.

4단계. LINA CLI에서 show failover state 명령을 실행합니다.

<#root>

firepower#

show failover state

This host -	State Primary	Last Failure Reason	Date/Time
	Active	None	
Other host -	Secondary		
	Standby Ready	Comm Failure	18:32:56 EEST Jul 21 2016
====Configurat Sync Done ====Communicat Mac set	ion State===		

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
1
interface Ethernet1/2
management-only
nameif diagnostic
security-level 0
no ip address
ï
interface Ethernet1/4
description LAN/STATE Failover Interface
ī
interface Ethernet1/5
nameif Inside
 security-level 0
ip address 192.168.75.10 255.255.255.0
standby 192.168.75.11
1
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.

300 FTD9300_HA     Cisco Firepower 9000 Series SM-36 Threat Defense High Availability	1 <b>3</b> 6	8
FTD9300-1(Primary, Active) 10.62.148.72 - Cisco Firepower 9000 Series SM-36 Threat Defense - v6.0.1.1 - routed Cisco Firepower 9000 Series SM	-36 Thre Base, Threat, Malware, URL Filtering FTD9300	
FTD9300-2(Secondary, Standby) 10.62.148.69 - Cisco Firepower 9000 Series SM-36 Threat Defense - v6.0.1.1 - routed Cisco Firepower 9000 Series SM	-36 Thre Base, Threat, Malware, URL Filtering FTD9300	

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.

Confirm Break		×
Breaking the High Availability pair "FTD930 Control policy from standby peer. Are you s Force break, if standby peer does not respond	0_HA" will erase all configuration e une you want to break the pair?	xcept the Access
	Yes	No

3단계. 그림과 같이 메시지를 기록합니다.



4단계. 이미지에 표시된 대로 FMC GUI에서 결과를 확인합니다.

FTD9300-1 10.62.148.72 - Cisco Firepower 9000 Series SM-36 Threat Defense - v6.0.1.1 - routed	Cisco Firepower 9000 Series SM-36 Thre Base, Threat, Malware, URL Filtering	FTD9300	J 🕄
FTD9300-2 10.62.148.69 - Cisco Firepower 9000 Series SM-36 Threat Defense - v6.0.1.1 - routed	Cisco Firepower 9000 Series SM-36 Thre Base, Threat, Malware, URL Filtering	FTD9300	6

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

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

호스트 이름 firepower	호스트 이름 firepower
비밀번호 8Ry2Yjlyt7RRXU24 암호화 활성화	비밀번호 8Ry2Yjlyt7RRXU24 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
<u>!</u>	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	ngips conn-match vlan-id
access-list CSM_FW_ACL_ advanced permit icmp any rule-id	access-list CSM_FW_ACL_ remark rule-id 정책: FTD9300 - 필수/1
268447744 event-log both access-list CSM_FW_ACL_ remark rule-id 268441600: 액세스	access-list CSM_FW_ACL_ remark rule-io : Allow_ICMP
정책: FTD9300 - 기본값/1 access-list CSM_FW_ACL_ remark rule-id 268441600: L4 규칙	access-list CSM_FW_ACL_ advanced pe 268447744 event-log both
: 기본 작업 규칙 access-list CSM_FW_ACL_ advanced permit ip any rule-id	access-list CSM_FW_ACL_ remark rule-id 정책: FTD9300 - 기본값/1
268441600 !	access-list CSM_FW_ACL_ remark rule-id : 기본 작업 규칙
tcp-map UM_STATIC_TCP_MAP	access-list CSM_FW_ACL_ advanced pe 268441600
tcp-options 범위 6 7 허용	1
tcp-options 범위 9 255 허용	ton-man LIM STATIC TCP MAP
긴급 플래그 허용	top ontions 법인 6.7 원용
!	
호출기 없음	tcp-options 범위 9 255 허용
로깅 사용	긴급 플래그 허용
로깅 타임스탬프	!
로깅 대기	호출기 없음
로깅 버퍼 크기 100000	로깅 사용
로깅 버퍼링된 디버깅	로깅 타임스탬프
로깅 flash-minimum-free 1024	로깅 대기
로깅 flash-maximum-allocation 3076	로깅 버퍼 크기 100000
mtu diagnostic 1500	로깅 버퍼링된 디버깅
mtu 내분 1500	로깅 flash-minimum-free 1024
mtu 1500 이브	로깅 flash-maximum-allocation 3076
자에 ㅈ키	mtu diagnostic 1500
ᅙᇭᆇᄾ ᅶᇲᆘᅎᆗᇉᇗᇲᇇᆋᄖ	mtu 내부 1500
་་་་་་་་་་་་་་་་་་་་་་་་་་་་་་་་་་་་	

장애 조치 lan 인터페이스 fover_link Ethernet1/4	mtu 1500 외부
장애 조치(failover) 복제 http	장애 조치 없음
장애 조치 mac 주소 Ethernet1/5 aaaa.bbb.1111 aaaa bbb 2222	monitor-interface service-module 없음
자애 조치 mag 증소 Ethernot1/6 agag bbb 2222	icmp 연결 불가능 속도 제한 1 버스트 크기
aaaa.bbb.4444	asdm history enable 없음
장애 조치 링크 fover_link Ethernet1/4	arp 시간 초과 14400
장애 조치 인터페이스 ip fover_link 10.10.1.1 255.255.255.0	no arp permit-nonconnected
standby 10.1.2	액세스 그룹 CSM_FW_ACL_ 전역
icmp 연결 불가능 속도 제한 1 버스트 크기 1	시간 제한 xlate 3:00:00
asdm history enable 없음	시간 제한 pat-xlate 0:00:30
arp 시간 초과 14400	timeout conn 1:00:00 half-closed 0:10:00
no arp permit-nonconnected	0:02:00 icmp 0:00:02
액세스 그룹 CSM_FW_ACL_ 전역	시간 제한 sunrpc 0:10:00 h323 0:05:00 h2 0:05:00 mgcp-pat 0:05:00
시간 제한 xlate 3:00:00	  시간 제한 sip 0:30:00 sip_media 0:02:00 s
시간 제한 pat-xlate 0:00:30	disconnect 0:02:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 sctp 0:02:00 icmp 0:00:02	시간 제한 sip-provisional-media 0:02:00 u absolute
시간 제한 sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp	시간 제한 tcp-proxy-reassembly 0:00:30
0:05:00 mgcp-pat 0:05:00	timeout floating-conn 0:00:00
시간 제한 sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip- disconnect 0:02:00	aaa proxy-limit 비활성화
시간 제한 sip-provisional-media 0:02:00 uauth 0:05:00	snmp-server 위치 없음
absolute	snmp-server 연락처 없음
시간 제한 tcp-proxy-reassembly 0:00:30	snmp-server가 트랩 snmp 인증 linkup link
timeout floating-conn 0:00:00	warmstart들 활성화하지 않음
aaa proxy-limit 비활성화	암호화 ipsec 보안 연결 pmtu-에이징 무한 
snmp-server 위치 없음	crypto ca trustpool 정책
snmp-server 연락처 없음	텔넷 시간 초과 5
	ssh stricthostkeycheck

snmp-server가 트랩 snmp 인증 linkup linkdown coldstart warmstart를 확성화하지 않음	ssh 시간 초과 5
아ㅎ하Lincoo 보안 여겨 pmtu 에이지 무하	ssh key-exchange 그룹 dh-group1-sha1
김오와 ipsec 또한 한을 pintu-에이징 두한	콘솔 시간 초과 0
crypto ca trustpool 정책	dynamic-access-policy-record DfltAccess
텔넷 시간 초과 5 	!
ssh stricthostkeycheck	class-map inspection_default
ssh 시간 초과 5	  기본 검사 트래픽 일치
ssh key-exchange 그룹 dh-group1-sha1	1
콘솔 시간 초과 0	
dynamic-access-policy-record DfltAccessPolicy	policy-map type inspect dns preset_dns_r
!	매개변수
class-map inspection_default	message-length maximum client auto
기본 검사 트래픽 일치	message-length 최대 512
! !	policy-map type inspect ip-options UM_STATIC_IP_OPTIONS_MAP
policy-map type inspect dns preset_dns_map	매개변수
매개변수	eool 작업 허용
message-length maximum client auto	nop 작업 허용
message-length 최대 512	라우터 알림 작업 허용
policy-map type inspect ip-options	정책 맵 global_policy
	class inspection_default
배개면수	inspect dns preset_dns_map
leool 작업 허용	ftp 검사
nop 작업 허용	검사 h323 h225
라우터 알림 작업 허용	h323 ras 검사
정책 맵 global_policy	  rsh 검사
class inspection_default	 Irtsp 검사

inspect dns preset_dns_map	inspect sqlnet
ftp 검사	inspect skinny
검사 h323 h225	inspect sunrpc
h323 ras 검사	xdmcp 검사
rsh 검사	inspect sip
rtsp 검사	netbios 검사
inspect sqlnet	tftp 검사
inspect skinny	icmp 검사
inspect sunrpc	icmp 검사 오류
xdmcp 검사	dcerpc 검사
inspect sip	inspect ip-options UM_STATIC_IP_OPTI
netbios 검사	class-default
tftp 검사	연결 고급 옵션 설정 UM_STATIC_TCP_I
icmp 검사	!
icmp 검사 오류	서비스 정책 전역 정책 전역
dcerpc 검사	프롬프트 호스트 이름 컨텍스트
inspect ip-options UM_STATIC_IP_OPTIONS_MAP	콜홈
class-default	프로필 CiscoTAC-1
연결 고급 옵션 설정 UM_STATIC_TCP_MAP	활성 상태 없음
!	대상 주소 http
서비스 정책 전역 정책 전역	<u>Mups.//tools.cisco.com/its/service/oddce/</u>
프롬프트 호스트 이름 컨텍스트	구선 구조 이메월 Calinome@cisco.com
콜홈	대경 신중 경직 nup 경고 그를 지다 그도
프로필 CiscoTAC-1	영고 그급 신민 구락
활성 상태 없음	alert group 이벤트리 저기 그도 위
대상 주소 http	puice cubecribe to elect arous 커피그레이셔 조
nups.//tools.cisco.com/its/service/oudce/services/DDCESe	<u>···································</u>

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

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

HA 분리 전	HA 분리 후
firepower# sh 실행	firepower# sh 실행
: 저장됨	: 저장됨
:	:
: 일련 번호: FLM19206H7T	: 일련 번호: FLM19206H7T
: 하드웨어: FPR9K-SM-36, 135841 MB RAM, CPU Xeon E5 Series 2294 MHz, 2 CPU(72코어)	: 하드웨어: FPR9K-SM-36, 135841 MB R Series 2294 MHz, 2 CPU(72코어)
:	:
NGFW 버전 10.10.1.1	NGFW 버전 10.10.1.1
!	!
호스트 이름 firepower	호스트 이름 firepower
비밀번호 8Ry2Yjlyt7RRXU24 암호화 활성화	비밀번호 8Ry2Yjlyt7RRXU24 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	셧다운
!	nameif 없음
interface Ethernet1/5	보안 수준 없음
nameif 내부	ip 주소 없음
보안 수준 0	!
ip 주소 192.168.75.10 255.255.255.0 대기 192.168.75.11	interface Ethernet1/5
!	셧다운
interface Ethernet1/6	nameif 없음
nameif 외부	보안 수준 없음
보안 수준 0	ip 주소 없음
ip 주소 192.168.76.10 255.255.255.0 대기 192.168.76.11	!
!	interface Ethernet1/6
ftp 모드 수동	셧다운
ngips conn-match vlan-id	nameif 없음
access-list CSM_FW_ACL_ remark rule-id 268447744: 액세스	보안 수준 없음
경색: FTD9300 - 월구/1	ip 주소 없음
access-list CSM_FW_ACL_ remark rule-Id 268447744: L4 뉴식 : Allow_ICMP	!
access-list CSM_FW_ACL_ advanced permit icmp any rule-id	ftp 모드 수동
268447744 event-log both	ngips conn-match vlan-id
access-list CSM_FW_ACL_ remark rule-id 268441600: 액세스	

정책: FTD9300 - 기본값/1	access-list CSM_FW_ACL_ remark rule-i
access-list CSM_FW_ACL_ remark rule-id 268441600: L4 규칙 · 기본 작업 규칙	access-list CSM_FW_ACIremark_rule-i
access-list CSM_EW_ACL_advanced permit in any rule-id	: Allow_ICMP
268441600	access-list CSM_FW_ACL_ advanced pe
!	
tcp-map UM_STATIC_TCP_MAP	access-list CSM_FW_ACL_ remark rule-i 정책: FTD9300 - 기본값/1
tcp-options 범위 6 7 허용	access-list CSM_FW_ACL_ remark rule-i
tcp-options 범위 9 255 허용	: 기본 작업 규칙
긴급 플래그 허용	access-list CSM_FW_ACL_ advanced pe 268441600
!	!
호출기 없음	tcp-map UM_STATIC_TCP_MAP
로깅 사용	tcp-options 범위 6 7 허용
로깅 타임스탬프	tcp-options 범위 9 255 허용
로깅 대기	 긴급 플래그 허용
로깅 버퍼 크기 100000	!
로깅 버퍼링된 디버깅	호출기 없음
로깅 flash-minimum-free 1024	 로깅 메시지 106015 없음
로깅 flash-maximum-allocation 3076	로깅 메시지 313001 없음
mtu diagnostic 1500	로깅 메시지 313008 없음
mtu 내부 1500	 로깅 메시지 106023 없음
mtu 1500 외부	  로깅 메시지 710003 없음
장애 조치	  로깅 메시지 106100 없음
장애 조치 lan 유닛 보조	로깅 메시지 302015 없음
장애 조치 lan 인터페이스 fover_link Ethernet1/4	로깅 메시지 302014 없음
장애 조치(failover) 복제 http	  로깅 메시지 302013 없음
장애 조치 mac 주소 Ethernet1/5 aaaa.bbb.1111 aaaa.bbb.2222	로깅 메시지 302018 없음

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

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
<u>!</u>	dynamic-access-policy-record DfltAccess
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	message-length 최대 512
UM_STATIC_IP_OPTIONS_MAP 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_OPTI
연결 고급 옵션 설정 UM_STATIC_TCP_MAP	class-default
!	연결 고급 옵션 설정 UM_STATIC_TCP_N
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	활성 상태 없음
https://tools.clsco.com/its/service/oddce/services/DDCEService	대상 주소 http <u>https://tools.cisco.com/its/service/oddce/s</u>
 대상 전송 방식 http	수신 주소 이메일 callhome@cisco.com
· 경고 그룹 진단 구독	 대상 전송 방식 http
	'

alert-group 환경에 가입	경고 그룹 진단 구독
alert-group 인벤토리 정기 구독 월	alert-group 환경에 가입
subscribe-to-alert-group 컨피그레이션 주기적 매월	alert-group 인벤토리 정기 구독 월
subscribe-to-alert-group telemetry 일별	subscribe-to-alert-group 컨피그레이션 주:
Cryptochecksum:e648f92dd7ef47ee611f2aaa5c6cbd84	subscribe-to-alert-group telemetry 일별
: 끝	Cryptochecksum:08ed87194e9f5cd9149f
firepower 번호	: 끝
	firepower 번호
	1

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.

GB FTD9300_HA     Cisco Firepower 9000 Series SM-36 Threat Defense High Availability			/ 🕏 🖗 🖯
FTD9300-1(Primary, Active) 10.62.148.72 - Cisco Firepower 9000 Series SM-36 Threat Defense - v6.0.1.1 - routed	Cisco Firepower 9000 Series SM-36 Thre Base, Threat, Malware, URL Filtering	FTD9300	
FTD9300-2(Secondary, Standby) 10.62.148.69 - Cisco Firepower 9000 Series SM-36 Threat Defense - v6.0.1.1 - routed	Cisco Firepower 9000 Series SM-36 Thre Base, Threat, Malware, URL Filtering	FTD9300	

2단계. 알림을 확인하고 그림과 같이 확인합니다.

Confirm	m Delete
?	Are you sure you want to delete the high availability, "FTD9300_HA"?
contin "config	Deleting the pair from the FMC does not disable high availability at the device level. The devices will ue to operate as an Active/Standby pair until you disable high availability for each unit using the CLI: gure high-availability disable"
	Yes No

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	firepower# sh 실행
: 저장됨	: 저장됨
:	:
: 일련번호: FLM19267A63	: 일련 번호: FLM19206H7T
: 하드웨어: FPR9K-SM-36, 135839 MB RAM, CPU Xeon E5 Series 2294 MHz, 2 CPU(72코어)	: 하드웨어: FPR9K-SM-36, 135841 MB R Series 2294 MHz, 2 CPU(72코어)
:	:
NGFW 버전 10.10.1.1	NGFW 버전 10.10.1.1
!	!
호스트 이름 firepower	호스트 이름 firepower
비밀번호 8Ry2Yjlyt7RRXU24 암호화 활성화	비밀번호 8Ry2Yjlyt7RRXU24 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	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
i	!
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-i 정책: FTD9300 - 필수/1
access-list CSM_FW_ACL_ remark rule-id 268447744: L4 규칙 : Allow_ICMP	access-list CSM_FW_ACL_ remark rule-i : Allow_ICMP
access-list CSM_FW_ACL_ advanced permit icmp any rule-id 268447744 event-log both	access-list CSM_FW_ACL_ advanced pe 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-i 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-i : 기본 작업 규칙
access-list CSM_FW_ACL_ advanced permit ip any rule-id 268441600	access-list CSM_FW_ACL_ advanced pe 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.bbl aaaa.bbb.2222
장애 조치 mac 주소 Ethernet1/6 aaaa.bbb.3333 aaaa.bbb.4444	장애 조치 mac 주소 Ethernet1/6 aaaa.bbl 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. 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 h 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	snmp-server 연락처 없음
warmstart을 필경와하지 않음 암호화 ipsec 보안 연결 pmtu-에이징 무한	snmp-server가 트랩 snmp 인증 linkup linł 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
	1

!	dynamic-access-policy-record DfltAccess
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	message-length 최대 512
에_STATIC_IP_OPTIONS_MAP 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           ttp 검사         netbios 검사           icmp 검사         ttp 검사           icmp 검사 Q류         icmp 검사           icmp 검사 Q류         icmp 검사           dcerpc 검사         icmp 검사 Q.F.           inspect ip-options UM_STATIC_IP_OPTIONS_MAP         dcerpc 검사           class-default         inspect ip-options UM_STATIC_IP_OP           언결 고급 음선 설정 UM_STATIC_TCP_MAP         class-default           !         연결 고급 음선 설정 UM_STATIC_TCP_MAP           tas== 토 호         이름 컨텍스트           서비스 정책 전역 정책 전역         !           프로프로 호         서비스 정책 전역 정책 전역           콜홈         프롬프트 호           프로필 CiscoTAC-1         콜롬           법tbs://tools.cisco.com/its/service/oddce/services/DDCEService         rtb' 주 A           수신 주 소 이메일 callhome@cisco.com         rtb' 주 A           대상 전승 방식 http         수신 주 소 이메일 callhome@cisco.com           건상 전승 방식 http         경고 그룹 진단 구독           alert-group 한경에 가입         alert-group 한경에 가입           subscribe-to-alert-group 컨피그레이션 주기적 매월         alert-group 안벤토리 정기 구독 월           subscribe-to-alert-group 컨피그레이션 주기적 매월         alert-group 컨텍 프리 전기 구독 월           subscribe-to-alert-group 컨피그레이션 <th></th> <th></th>		
netbios 검사inspect sipttp 검사netbios 검사icmp 검사ttp 검사icmp 검사 오류icmp 검사 오류inspect ip-options UM_STATIC_IP_OPTIONS_MAPdcerpc 검사class-defaultinspect ip-options UM_STATIC_IP_OP연결 고급 옵션 설정 UM_STATIC_TCP_MAPclass-default!연결 고급 옵션 설정 UM_STATIC_TCP_MAP서비스 정책 전역 정책 전역!프로프토 호스트 이름 컨텍스트서비스 정책 전역 정책 전역콜홈프롬프트 호스트 이름 컨텍스트프로필 CiscoTAC-1콜홈발성 상태 없음프로필 CiscoTAC-1대상 주소 httphttps://tools.cisco.com/its/service/oddce/services/DDCEService수신 주소 이메일 callhome@cisco.comtrik 장주 & http다상 전승 방식 http수신 주소 이메일 callhome@cisco.com대상 전승 방식 http경고 그룹 진단 구독alert-group 환경에 가입alert-group 환경에 가입subscribe-to-alert-group 컨피그레이션 주기적 매월alert-group 인벤토리 정기 구독 월subscribe-to-alert-group telemetry 일별cryptochecksum:e648f92d7ef47ee61: 끝Cryptochecksum:e648f92d7ef47ee61	inspect sip	xdmcp 검사
thp 검사netbios 검사icmp 검사iftp 검사icmp 검사 오류icmp 검사dcerpc 검사icmp 검사 오류inspect ip-options UM_STATIC_IP_OPTIONS_MAPdcerpc 검사class-defaultinspect ip-options UM_STATIC_TCP_MAP건결 고급 옵션 설정 UM_STATIC_TCP_MAPclass-default!연결 고급 옵션 설정 UM_STATIC_TCP_MAP서비스 정책 전역 정책 전역!프로프트 호스트 이름 컨텍스트서비스 정책 전역 정책 전역플록프트 호스트 이름 컨텍스트서비스 정책 전역 정책 전역필축프로필 CiscoTAC-1감성 상태 없음프로필 CiscoTAC-1대상 주소 httphttps://tools.cisco.com/its/service/oddce/services/DDCEService다상 전송 방식 http수신 주소 이메일 callhome@cisco.com건고 그룹 진단 구독대상 전송 방식 httpalert-group 환경에 가입alert-group 환경에 가입alert-group 한경에 가입alert-group 한경에 가입subscribe-to-alert-group 컨피그레이션 주기적 매월alert-group 인벤토리 정기 구독 월subscribe-to-alert-group 컨피그레이션 주기적 매월subscribe-to-alert-group telemetry 일별: 글Cryptochecksum:e648/92dd7ef47ee61	netbios 검사	inspect sip
icmp 검사ttp 검사icmp 검사 오류icmp 검사 오류inspect ip-options UM_STATIC_IP_OPTIONS_MAPdcerpc 검사class-defaultinspect ip-options UM_STATIC_IP_OP번결 고급 옵션 설정 UM_STATIC_TCP_MAPclass-default반연결 고급 옵션 설정 UM_STATIC_TCP_MAP서비스 정책 전역 정책 전역!포름프트 호스트 이름 컨텍스트서비스 정책 전역 정책 전역콜홈프롬프트 호스트 이름 컨텍스트프로필 CiscoTAC-1콜홈발성 상태 없음프로필 CiscoTAC-1대상 주소 http참성 조소 httphttps://tools.cisco.com/its/service/oddce/services/DDCEService수신 주소 이메일 callhome@cisco.com대상 주소 http감상 전승 방식 http순신 주소 이메일 callhome@cisco.com검고 그를 진단 구독alert-group 환경에 가입alert-group 한경에 가입alert-group 환경에 가입subscribe-to-alert-group 컨피그레이션 주기적 매월alert-group 한경에 가입subscribe-to-alert-group 컨피그레이션 주기적 매월subscribe-to-alert-group 컨피그레이션'''도·''''''''''''''''''''''''''''''''''''	lftp 검사	netbios 검사
icmp 검사 오류icmp 검사dcerpc 검사icmp 검사 오류inspect ip-options UM_STATIC_IP_OPTIONS_MAPdcerpc 검사class-defaultinspect ip-options UM_STATIC_IP_OP연결 고급 옵션 설정 UM_STATIC_TCP_MAPclass-default!연결 고급 옵션 설정 UM_STATIC_TCP_MAP/ 비스 정책 전역 정책 전역!프록프트 호스트 이름 컨텍스트서비스 정책 전역 정책 전역콜홈프로필 CiscoTAC-1탈성 상태 없음프로필 CiscoTAC-1대상 주소 http발성 상태 없음thtps://tools.cisco.com/its/service/oddce/services/DDCEService대상 주소 http수신 주소 이메일 callhome@cisco.comhttps://tools.cisco.com/its/service/oddce/services/DDCEService대상 전속 방식 http출신 상태 없음uta 전속 방식 http수신 주소 이메일 callhome@cisco.com경고 그를 진단 구독대상 전송 방식 httpalert-group 환경에 가입alert-group 환경에 가입subscribe-to-alert group 컨피그레이션 주기적 매월alert-group 인벤토리 정기 구독 월subscribe-to-alert-group telemetry 일별subscribe-to-alert-group 컨피그레이션: 끝Cryptochecksum:933c594fc0264082edc0f24bad358031subscribe-to-alert-group telemetry 일별	icmp 검사	tftp 검사
dcerpc 검사icmp 검사 오류inspect ip-options UM_STATIC_IP_OPTIONS_MAPdcerpc 검사class-defaultinspect ip-options UM_STATIC_IP_OP연결 고급 음션 설정 UM_STATIC_TCP_MAPclass-default1연결 고급 음션 설정 UM_STATIC_TCP서비스 정책 전역 정책 전역!프롬프트 호스트 이름 컨텍스트서비스 정책 전역 정책 전역콜홈프롬프트 호스트 이름 컨텍스트프로필 CiscoTAC-1콜홈법상 상태 없음프로 일 CiscoTAC-1대상 주소 http법상 조소 httphttps://tools.cisco.com/its/service/oddce/services/DDCEService대상 주소 http수신 주소 이메일 callhome@cisco.com대상 주소 http업고 그룹 진단 구독대상 전송 방식 httpalert-group 환경에 가입경고 그를 진단 구독alert-group 한경에 가입alert-group 한경에 가입subscribe-to-alert-group 컨피그레이션 주기적 매월subscribe-to-alert-group 컨피그레이션cryptochecksum:933c594fc0264082edc0f24bad358031subscribe-to-alert-group telemetry 일별	cmp 검사 오류	icmp 검사
inspect ip-options UM_STATIC_IP_OPTIONS_MAP dcerpc 검사 class-default inspect ip-options UM_STATIC_IP_OP 연결 고급 옵션 설정 UM_STATIC_TCP_MAP class-default 1 연결 고급 옵션 설정 UM_STATIC_TCP_MAP l 프롬프트 호스트 이름 컨텍스트 서비스 정책 전역 정책 전역 클홈 프로필 CiscoTAC-1 콜홈 환성 상태 없음 프롬포트 호스트 이름 컨텍스트 대상 주소 http https://tools.cisco.com/its/service/oddce/services/DDCEService rtdy 주소 null일 callhome@cisco.com https://tools.cisco.com/its/service/oddce/services/DDCEService default callhome@cisco.com https://tools.cisco.com/its/service/oddce/services/DDCEService alert-group 환경에 가입 callhome@cisco.com call callhome@cisco.com 경고 그룹 진단 구독 call callhome@cisco.com 강전송 방식 http alert-group 인벤토리 정기 구독 월 callert-group 환경에 가입 subscribe-to-alert-group 컨피그레이션 주기적 매월 subscribe-to-alert-group 컨피그레이션 전기 작독 월 subscribe-to-alert-group 컨피그레이션 주기적 매월 callhome.etal callhome? Cryptochecksum:933c594fc0264082edc0f24bad358031 subscribe-to-alert-group 란피그레이션	dcerpc 검사	icmp 검사 오류
class-defaultinspect ip-options UM_STATIC_IP_OP연결 고급 옵션 설정 UM_STATIC_TCP_MAPclass-default!연결 고급 옵션 설정 UM_STATIC_TCP서비스 정책 전역 정책 전역!프롬프트 호스트 이름 컨텍스트서비스 정책 전역 정책 전역콜홈프롬프트 호스트 이름 컨텍스트프로필 CiscoTAC-1콜홈합성 상태 없음프로필 CiscoTAC-1대상 주소 http합성 상태 없음https://tools.cisco.com/its/service/oddce/services/DDCEService수신 주소 이메일 callhome@cisco.comhttps://tools.cisco.com/its/service/oddce/services/DDCEService대상 전송 방식 http수신 주소 이메일 callhome@cisco.com건고 그룹 진단 구독대상 전송 방식 httpalert-group 환경에 가입리ert-group 환경에 가입alert-group 인벤토리 정기 구독 월alert-group 한경에 가입subscribe-to-alert-group 컨피그레이션 주기적 매월subscribe-to-alert-group 컨피그레이션Cryptochecksum:933c594fc0264082edc0f24bad358031subscribe-to-alert-group 컨피그레이션고고Cryptochecksum:e648f92dd7ef47ee61	inspect ip-options UM_STATIC_IP_OPTIONS_MAP	dcerpc 검사
연결 고급 옵션 설정 UM_STATIC_TCP_MAPclass-default!연결 고급 옵션 설정 UM_STATIC_TCP서비스 정책 전역 정책 전역!포통프트 호스트 이름 컨택스트서비스 정책 전역 정책 전역콜홈프로프트 호스트 이름 컨텍스트프로필 CiscoTAC-1콜홈활성 상태 없음프로필 CiscoTAC-1대상 주소 http활성 상태 없음https://tools.cisco.com/its/service/oddce/services/DDCEService수신 주소 이메일 callhome@cisco.com대상 주소 httphttps://tools.cisco.com/its/service/oddce/services/DDCEService여신 주소 이메일 callhome@cisco.com대상 주소 httphttps://tools.cisco.com/its/service/oddce/services/DDCEService/oddce/services/DDCEService/oddce/services/DDCEService/oddce/services/DDCEService/oddce/services/DDCEService/oddce/services/DDCEService/oddce/services/DDCEService/services/DDCEService/services/DDCEService/service/service/oddce/services/DDCEService/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/serv	class-default	inspect ip-options UM_STATIC_IP_OPTIC
!       연결 고급 옵션 설정 UM_STATIC_TCP         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       확성 상태 없음         https://tools.cisco.com/its/service/oddce/services/DDCEService       대상 주소 http         수신 주소 이메일 callhome@cisco.com       대상 주소 http         대상 전송 방식 http       수신 주소 이메일 callhome@cisco.com         경고 그룹 진단 구독       대상 전송 방식 http         alert-group 환경에 가입       alert-group 환경에 가입         alert-group 인벤토리 정기 구독 월       alert-group 환경에 가입         subscribe-to-alert-group 컨피그레이션 주기적 매월       alert-group 인벤토리 정기 구독 월         subscribe-to-alert-group 한결미그레이션 주기적 매월       subscribe-to-alert-group 컨피그레이션         : 글       Cryptochecksum:933c594fc0264082edc0f24bad358031       subscribe-to-alert-group telemetry 일별	연결 고급 옵션 설정 UM_STATIC_TCP_MAP	class-default
서비스 정책 전역 정책 전역!프롬프트 호스트 이름 컨텍스트서비스 정책 전역 정책 전역콜홈프롬프트 호스트 이름 컨텍스트프로필 CiscoTAC-1콜홈활성 상태 없음프로필 CiscoTAC-1대상 주소 http https://tools.cisco.com/its/service/oddce/services/DDCEService답상 주소 http신 주소 이메일 callhome@cisco.com대상 주소 http https://tools.cisco.com/its/service/oddce/services/DDCEService전상 전송 방식 http수신 주소 이메일 callhome@cisco.com경고 그룹 진단 구독대상 전송 방식 httpalert-group 환경에 가입경고 그룹 진단 구독alert-group 인벤토리 정기 구독 월alert-group 한경에 가입subscribe-to-alert-group 컨피그레이션 주기적 매월alert-group 인벤토리 정기 구독 월subscribe-to-alert-group 전피그레이션 주기적 매월subscribe-to-alert-group 컨피그레이션 주기적 매월: 끝Cryptochecksum:933c594fc0264082edc0f24bad358031: 끝·································	!	연결 고급 옵션 설정 UM_STATIC_TCP_M
프롬프트 호스트 이름 컨텍스트서비스 정책 전역 정책 전역콜홈프롬프트 호스트 이름 컨텍스트프로필 CiscoTAC-1콜홈할성 상태 없음프로필 CiscoTAC-1업상 주소 http활성 상태 없음https://tools.cisco.com/its/service/oddce/services/DDCEService대상 주소 http수신 주소 이메일 callhome@cisco.comhttps://tools.cisco.com/its/service/oddce/services/DDCEService대상 전송 방식 http수신 주소 이메일 callhome@cisco.com경고 그룹 진단 구독대상 전송 방식 httpalert-group 한경에 가입බert-group 한경에 가입alert-group 인벤토리 정기 구독 월alert-group 인벤토리 정기 구독 월subscribe-to-alert-group 컨피그레이션 주기적 매월alert-group 인벤토리 정기 구독 월subscribe-to-alert-group 컨피그레이션 주기적 매월subscribe-to-alert-group 컨피그레이션Cryptochecksum:933c594fc0264082edc0f24bad358031subscribe-to-alert-group 컨피그레이션: 끝Cryptochecksum:e648f92dd7ef47ee61	서비스 정책 전역 정책 전역	!
공휴목록 트 로 스 트 이 특 컨 텍 스 트 트 프 프 트 트 스 트 이 특 컨 텍 스 트 트 프 프 트 트 스 트 이 특 컨 텍 스 트 트 프 프 트 트 스 트 프 프 E O S C T A C - 1보 전 상 터 없 음프 로 필 C isco T A C - 1대상 주 스 http환성 상 태 없 음https://tools.cisco.com/its/service/oddce/services/DDCEService대상 주 스 http스 신 주 소 이 메 일 callhome@cisco.com대상 주 소 http수신 주 소 이 메 일 callhome@cisco.com수신 주 소 이 메 일 callhome@cisco.com경고 그 급 진단 구 독대상 전송 방 식 httpalert-group 환경에 가 입경고 그 급 진단 구 독alert-group 한 건 이 기 도 페 이 선 준 기 적 의 권 이 가 입alert-group 한 건 이 기 입subscribe-to-alert-group 컨 피 그 리 이 선 주 기 적 매alert-group 인 벤 토 리 정 기 구 독 월subscribe-to-alert-group 한 리 페 이 선 준 기 적 의 관alert-group 한 건 미 그 리 이 선 전Cryptochecksum:933c594fc0264082edc0f24bad358031subscribe-to-alert-group telemetry 일 별고다다	프롬프트 호스트 이름 컨텍스트	서비스 정책 전역 정책 전역
프로필 CiscoTAC-1콜홈확성 상태 없음프로필 CiscoTAC-1대상 주소 http활성 상태 없음https://tools.cisco.com/its/service/oddce/services/DDCEService대상 주소 http수신 주소 이메일 callhome@cisco.com대상 주소 http수신 주소 이메일 callhome@cisco.com수신 주소 이메일 callhome@cisco.com경고 그룹 진단 구독대상 전송 방식 httpalert-group 환경에 가입경고 그룹 진단 구독alert-group 인벤토리 정기 구독 월alert-group 환경에 가입subscribe-to-alert-group 컨피그레이션 주기적 매월alert-group 인벤토리 정기 구독 월도방scribe-to-alert-group 컨피그레이션 주기적 매월alert-group 인벤토리 정기 구독 월subscribe-to-alert-group 컨피그레이션 주기적 매월subscribe-to-alert-group 컨피그레이션도관Cryptochecksum:933c594fc0264082edc0f24bad358031subscribe-to-alert-group telemetry 일별	코홈	프롬프트 호스트 이름 컨텍스트
확성 상태 없음프로필 CiscoTAC-1TVS 주소 http https://tools.cisco.com/its/service/oddce/services/DDCEService / 수신 주소 이메일 callhome@cisco.comTVS 주소 http https://tools.cisco.com/its/service/oddce/services/DDCEService / TVS 주소 http https://tools.cisco.com/its/service/oddce/services/DDCEService건 주소 이메일 callhome@cisco.com주신 주소 이메일 callhome@cisco.com건상 전송 방식 http수신 주소 이메일 callhome@cisco.com경고 그룹 진단 구독대상 전송 방식 httpalert-group 환경에 가입alert-group 환경에 가입alert-group 인벤토리 정기 구독 월alert-group 한경에 가입subscribe-to-alert-group 컨피그레이션 주기적 매월alert-group 인벤토리 정기 구독 월cryptochecksum:933c594fc0264082edc0f24bad358031subscribe-to-alert-group telemetry 일별: 끝Cryptochecksum:e648f92dd7ef47ee61	프로필 CiscoTAC-1	콜홈
대상 주소 http활성 상태 없음https://tools.cisco.com/its/service/oddce/services/DDCEService대상 주소 http수신 주소 이메일 callhome@cisco.comhttps://tools.cisco.com/its/service/oddce/service/oddce/service/oddce/service/oddce/service/oddce/service/oddce/service/oddce/service/oddce/service/oddce/service/oddce/service/oddce/service/oddce/service/oddce/service/oddce/service/oddce/service/oddce/service/oddce/service/oddce/service/oddce/service/oddce/service/oddce/service/oddce/service/oddce/service/oddce/service/oddce/service/oddce/service/oddce/service/oddce/service/oddce/service/oddce/service/oddce/service/oddce/service/oddce/service/oddce/service/oddce/service/oddce/service/oddce/service/oddce/service/oddce/service/oddce/service/oddce/service/oddce/service/oddce/service/oddce/service/oddce/service/oddce/service/oddce/service/oddce/service/oddce/service/oddce/service/oddce/service/oddce/service/oddce/service/oddce/service/oddce/service/oddce/service/oddce/service/oddce/service/oddce/service/oddce/service/oddce/service/oddce/service/oddce/service/oddce/service/oddce/service/oddce/service/oddce/service/oddce/service/oddce/service/oddce/service/oddce/service/oddce/service/oddce/service/oddce/service/oddce/service/oddce/service/oddce/service/oddce/service/oddce/service/oddce/service/oddce/service/service/oddce/service/oddce/service/service/oddce/service/service/oddce/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/service/servic	활성 상태 없음	프로필 CiscoTAC-1
다상 주소 http 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 컨피그레이션 주기적 매월	대상 주소 http https://tools.cisco.com/its/service/oddce/services/DDCEService	활성 상태 없음
대상 전송 방식 http 수신 주소 이메일 callhome@cisco.com 경고 그룹 진단 구독 대상 전송 방식 http 경고 그룹 진단 구독 alert-group 인벤토리 정기 구독 월 alert-group 환경에 가입 subscribe-to-alert-group 컨피그레이션 주기적 매월 alert-group 인벤토리 정기 구독 월 subscribe-to-alert-group telemetry 일별 subscribe-to-alert-group 컨피그레이션 Cryptochecksum:933c594fc0264082edc0f24bad358031 subscribe-to-alert-group telemetry 일별	수신 주소 이메일 callhome@cisco.com	대상 주소 http <u>https://tools.cisco.com/its/service/oddce/s</u>
경고 그룹 진단 구독대상 전송 방식 httpalert-group 환경에 가입경고 그룹 진단 구독alert-group 인벤토리 정기 구독 월alert-group 환경에 가입subscribe-to-alert-group 컨피그레이션 주기적 매월alert-group 인벤토리 정기 구독 월subscribe-to-alert-group telemetry 일별subscribe-to-alert-group 컨피그레이션Cryptochecksum:933c594fc0264082edc0f24bad358031subscribe-to-alert-group telemetry 일별: 끝Cryptochecksum:e648f92dd7ef47ee61	대상 전송 방식 http	수신 주소 이메일 callhome@cisco.com
alert-group 환경에 가입 경고 그룹 진단 구독 alert-group 인벤토리 정기 구독 월 alert-group 환경에 가입 subscribe-to-alert-group 컨피그레이션 주기적 매월 alert-group 인벤토리 정기 구독 월 subscribe-to-alert-group telemetry 일별 subscribe-to-alert-group 컨피그레이션 Cryptochecksum:933c594fc0264082edc0f24bad358031 subscribe-to-alert-group telemetry 일별 : 끝	경고 그룹 진단 구독	대상 전송 방식 http
alert-group 인벤토리 정기 구독 월 alert-group 환경에 가입 subscribe-to-alert-group 컨피그레이션 주기적 매월 alert-group 인벤토리 정기 구독 월 subscribe-to-alert-group telemetry 일별 subscribe-to-alert-group 컨피그레이션 Cryptochecksum:933c594fc0264082edc0f24bad358031 subscribe-to-alert-group telemetry 일별 : 끝 Cryptochecksum:e648f92dd7ef47ee61	alert-group 환경에 가입	경고 그룹 진단 구독
subscribe-to-alert-group 컨피그레이션 주기적 매월 alert-group 인벤토리 정기 구독 월 subscribe-to-alert-group telemetry 일별 subscribe-to-alert-group 컨피그레이션 Cryptochecksum:933c594fc0264082edc0f24bad358031 subscribe-to-alert-group telemetry 일별 : 끝 Cryptochecksum:e648f92dd7ef47ee61	alert-group 인벤토리 정기 구독 월	alert-group 환경에 가입
subscribe-to-alert-group telemetry 일별 subscribe-to-alert-group 컨피그레이션 Cryptochecksum:933c594fc0264082edc0f24bad358031 : 끝 Cryptochecksum:e648f92dd7ef47ee61	subscribe-to-alert-group 컨피그레이션 주기적 매월	alert-group 인벤토리 정기 구독 월
Cryptochecksum:933c594fc0264082edc0f24bad358031 subscribe-to-alert-group telemetry 일별 : 끝 Cryptochecksum:e648f92dd7ef47ee61	subscribe-to-alert-group telemetry 일별	subscribe-to-alert-group 컨피그레이션 주
: 끝 Cryptochecksum:e648f92dd7ef47ee61	Cryptochecksum:933c594fc0264082edc0f24bad358031	subscribe-to-alert-group telemetry 일별
	: 끝	Cryptochecksum:e648f92dd7ef47ee611f2
lfirepower 번호 : 끝	firepower 번호	: 끝

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.	디바이스가 FMC에서 제거됩니다.
FTD 디바이스에서 설정이 제거되지 않음.	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 LAN	Interface: FOVER Ethernet1/3.205	
Failover unit Secondary	( <b>up</b> )		
Failover LAN Interface: not Configured	Reconnect tim	eout 0:00:00	
Reconnect timeout 0:00:00	Unit Poll frequ	ency 1 seconds, holdtime 15	
Unit Poll frequency 1 seconds, holdtime 15	seconds	•	
seconds	Interface Poll	frequency 5 seconds, holdtime 25	
Interface Poll frequency 5 seconds, holdtime 25	seconds		
seconds	Interface Polic	ev 1	
Interface Policy 1	Monitored Int	erfaces 0 of 1041 maximum	
Monitored Interfaces 2 of 1041 maximum	MAC Address	Move Notification Interval not set	
MAC Address Move Notification Interval not set	failover replica	ation http	
>	<b>_</b>	•	
	>		
기보			
		보조	

firepower# show run	firepower# show run
<u>!</u>	!
호스트 이름 firepower	호스트 이름 firepower
비밀번호 8Ry2YjIyt7RRXU24 암호화 활성화	비밀번호 8Ry2Yjlyt7RRXU24 암호화 활성
이름	이름
arp 시간 초과 14400	arp 시간 초과 14400
no arp permit-nonconnected	no arp permit-nonconnected
arp 속도 제한 16384	arp 속도 제한 16384
!	!
인터페이스 GigabitEthernet1/1	인터페이스 GigabitEthernet1/1
nameif 외부	셧다운
cts 설명서	nameif 없음
propagate sgt preserve-untag	보안 수준 없음
policy static sgt disabled trusted	ip 주소 없음
보안 수준 0	!
ip 주소 10.1.1.1 255.255.255.0 < 스탠바이 IP가 제거되었습	인터페이스 GigabitEthernet1/2

니다.	셧다운
!	nameif 없음
인터페이스 GigabitEthernet1/2	보안 수준 없음
nameif 내부	ip 주소 없음
cts 설명서	ļ
propagate sgt preserve-untag	인터페이스 GigabitEthernet1/3
policy static sgt disabled trusted	설명 LAN 장애 조치 인터페이스
보안 수준 0	!
ip 주소 192.168.1.1 255.255.255.0 < 스탠바이 IP가 제거되	인터페이스 GigabitEthernet1/4
있습니다.	설명 상태 장애 조치 인터페이스
! 이터페이스 CiachitEthernet1/2	!
	인터페이스 GigabitEthernet1/5
실명 LAN 상애 소지 인터페이스	셧다운
	nameif 없음
인터페이스 GigabitEthernet1/4	보안 수준 없음
설명 상태 장애 조치 인터페이스 	ip 주소 없음
!	!
인터페이스 GigabitEthernet1/5	인터페이스 GigabitEthernet1/6
· 셧다운	셧다운
nameif 없음	nameif 없음
보안 수준 없음	보안 수준 없음
ip 주소 없음	ip 주소 없음
!	!
인터페이스 GigabitEthernet1/6	인터페이스 GigabitEthernet1/7
셧다운	· · · · · · · · · · · · · · · · · · ·
nameif 없음	nameif 없음
보안 수준 없음	

ip 주소 없음	보안 수준 없음
!	ip 주소 없음
인터페이스 GigabitEthernet1/7	!
셧다운	인터페이스 GigabitEthernet1/8
nameif 없음	셧다운
보안 수준 없음	nameif 없음
ip 주소 없음	보안 수준 없음
!	ip 주소 없음
인터페이스 GigabitEthernet1/8	!
셧다운	인터페이스 관리1/1
nameif 없음	관리 전용
보안 수준 없음	nameif 진단
ip 주소 없음	cts 설명서
!	propagate sgt preserve-untag
인터페이스 관리1/1	policy static sgt disabled trusted
관리 전용	보안 수준 0
nameif 진단	ip 주소 없음
cts 설명서	!
propagate sgt preserve-untag	ftp 모드 수동
policy static sgt disabled trusted	ngips conn-match vlan-id
보안 수준 0	access-list CSM_FW_ACL_ remark rule-id
ip 주소 없음	정찍: 기존 더럴 및 주신군위 정찍
!	access-list CSM_FW_ACL_ remark rule-id 널 작업 규칙
ftp 모드 수동	access-list CSM_FW_ACL_ advanced pe
ngips conn-match vlan-id	9998
access-list CSM_FW_ACL_ remark rule-id 9998: PREFILTER 정책: 기본 터널 및 우선순위 정책	access-list CSM_FW_ACL_ advanced pe 9998

access-list CSM_FW_ACL_ remark rule-id 9998: 규칙: 기본 터 널 작업 규칙	access-list CSM_FW_ACL_ advanced pe 9998
access-list CSM_FW_ACL_ advanced permit ipinip any rule-id 9998	access-list CSM_FW_ACL_ advanced pe rule-id 9998
access-list CSM_FW_ACL_ advanced permit 41 any rule-id 9998	access-list CSM_FW_ACL_ remark rule-i 정책: FTD_HA - 기본값/1
access-list CSM_FW_ACL_ advanced permit gre any rule-id 9998	access-list CSM_FW_ACL_ remark rule-i : 기본 작업 규칙
access-list CSM_FW_ACL_ advanced permit udp any eq 3544 rule-id 9998	access-list CSM_FW_ACL_ advanced pe 268435456
access-list CSM_FW_ACL_ remark rule-id 268435456: 액세스	!
	tcp-map UM_STATIC_TCP_MAP
access-list CSM_FW_ACL_ remark rule-ld 208435450: L4 규칙 : 기본 작업 규칙	tcp-options 범위 6 7 허용
access-list CSM_FW_ACL_ advanced permit ip any rule-id	tcp-options 범위 9 18 허용
268435456	tcp-options 범위 20 255 허용
!	tcp-options md5 clear
tcp-map UM_STATIC_TCP_MAP	긴급 플래그 허용
tcp-options 범위 6 7 허용	!
tcp-options 범위 9 18 허용	호출기 없음
tcp-options 범위 20 255 허용	로깅 사용
tcp-options md5 clear	로깅 타임스탬프
긴급 플래그 허용	로깅 버퍼링된 디버깅
!	로깅 flash-minimum-free 1024
호출기 없음	로깅 flash-maximum-allocation 3076
로깅 사용	  로깅 메시지 106015 없음
로깅 타임스탬프	  로깅 메시지 313001 없음
로깅 버퍼링된 디버깅	  로깅 메시지 313008 없음
로깅 flash-minimum-free 1024	  로깅 메시지 106023 없음
로깅 flash-maximum-allocation 3076	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.
icmp 연결 불가능 속도 제한 1 버스트 크기 1	10.1.2 
asdm history enable 없음	standby 10.10.2.2
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	timeout conn 1:00:00 half-closed 0:10:00
암호화 ipsec 보안 연결 pmtu-에이징 무한	
crypto ca trustpool 정책	시간 제한 sunrpc 0:10:00 h323 0:05:00 h2 0:05:00 mgcp-pat 0:05:00
텔넷 시간 초과 5	시간 제한 sip 0:30:00 sip_media 0:02:00 s
콘솔 시간 초과 0	disconnect 0:02:00
dynamic-access-policy-record DfltAccessPolicy	시간 제한 sip-provisional-media 0:02:00 u absolute
!	시간 제한 tcp-proxy-reassembly 0:00:30
class-map inspection_default	timeout floating-conn 0:00:00
기본 검사 트래픽 일치	timeout conn-holddown 0:00:15
!	사용자 ID 기본 도메인 로컬
!	aaa proxy-limit 비활성화
policy-map type inspect dns preset_dns_map	  192.168.1.100 커뮤니티 ***** 버전 2c 외부
매개변수	
message-length maximum client auto	snmp-server 위치 없음
message-length 최대 512	snmp-server 연락처 없음
tcp 검사 없음	snmp-server 커뮤니티 *****
policy-map type inspect ip-options	서비스 sw 재설정 버튼
UM_STATIC_IP_OPTIONS_MAP	암호화 ipsec 보안 연결 pmtu-에이징 무한
매개변수	crypto ca trustpool 정책
eool 작업 허용	텔넷 시간 초과 5
nop 작업 허용	콘솔 시간 초과 0
라우터 알림 작업 허용	dynamic-access-policy-record DfltAccess
정책 맵 global_policy	!
class inspection_default	class-map inspection_default
inspect dns preset_dns_map	 기본 검사 트래픽 일치
ftp 검사	!
검사 h323 h225	!

h323 ras 검사	policy-map type inspect dns preset_dns_r
rsh 검사	매개변수
rtsp 검사	message-length maximum client auto
esmtp 검사	message-length 최대 512
inspect sqlnet	tcp 검사 없음
inspect skinny	policy-map type inspect ip-options UM_STATIC_IP_OPTIONS_MAP
inspect sunrpc	매개변수
xdmcp 검사	eool 작업 허용
inspect sip	nop 작업 허용
netbios 검사	라우터 알림 작업 허용
tftp 검사	정책 맵 global_policy
icmp 검사	class inspection_default
icmp 검사 오류	inspect dns preset_dns_map
dcerpc 검사	ftp 검사
inspect ip-options UM_STATIC_IP_OPTIONS_MAP	검사 h323 h225
class-default	h323 ras 검사
연결 고급 옵션 설정 UM_STATIC_TCP_MAP	rsh 검사
!	rtsn 검사
서비스 정책 전역 정책 전역	osmto 714
프롬프트 호스트 이름 컨텍스트	
콜홈	
프로필 CiscoTAC-1	inspect skinny
활성 상태 없음	inspect sunrpc
대상 주소 http	xdmcp 검사
https://tools.cisco.com/its/service/oddce/services/DDCEService	inspect sip
수신 주소 이메일 callhome@cisco.com	netbios 검사
대상 전송 방식 http	tftp 검사

경고 그룹 진단 구독	icmp 검사
alert-group 환경에 가입	icmp 검사 오류
alert-group 인벤토리 정기 구독 월	dcerpc 검사
subscribe-to-alert-group 컨피그레이션 주기적 매월	inspect ip-options UM_STATIC_IP_OPT
subscribe-to-alert-group telemetry 일별	class-default
Cryptochecksum:768a03e90b9d3539773b9d7af66b3452	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 <u>https://tools.cisco.com/its/service/oddce/s</u>
	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 즉
	subscribe-to-alert-group telemetry 일별
	Cryptochecksum:ac9b8f401e18491fee65

# FTD CLI에서 HA 비활성화에 대한 중요 사항:

기본 유닛	보조 유닛
장애 조치 컨피그레이션 및 스탠 IP의 시간 초과가 xlate 3:00:00으	<ul><li>✤ 인터페이스 설정이 제거됨.</li><li>.로</li><li>▪ 디바이스가 의사 대기 모드로</li></ul>

만료됨	전환됨.
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 호 스트가 제거되었습니다.	

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.

> .

>

<#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 보 여줍니다.

#### <#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 액 티브 상태일 때 다시 로드하면 어떻게 됩니까? 활성/활성 시나리오가 됩니다(기술적으로는 활성/장애 조치 해제이지만). 특히, 유닛이 가동되면 페 일오버는 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 startupconfig에 저장되지 않음). 두 가지 방법으로 장치를 재부팅/다시 로드할 수 있으며, 두 번째 방법에서 는 주의해야 합니다.

사례 1. CLI에서 재부팅

CLISH에서 재부팅해도 확인을 요청하지 않습니다. 따라서 설정 변경 사항은 startup-config에 저장 되지 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 192.0.2.1 255.255.0 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 피어 를 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 192.0.2.1 255.255.0 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.

<u>Cisco Secure Firewall Threat Defense 설명서 탐색</u>

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

<u>Cisco Firepower 4100/9300 FXOS 설명서 탐색</u>

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

<u>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</u>

• firepower 기술과 관련된 모든 컨피그레이션 및 문제 해결 TechNotes

<u>Cisco Secure Firewall 관리 센터</u>

• <u>기술 지원 및 문서 - Cisco Systems</u>

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 번 역 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.