# firepower 4100에서 FTD 다중 인스턴스 고가용성 구성

목차
<u>소개</u>
사전 요구 사항
<u>요구 사항</u>
<u>사용되는 구성 요소</u>
<u>배경 정보</u>
네트워크 다이어그램
<u>48</u>
<u>1단계. 인터페이스 사전 구성</u>
<u>2단계. 컨테이너 인스턴스에 대한 리소스 프로필 2개를 추가합니다.</u>
<u>3단계. (선택 사항) 컨테이너 인스턴스 인터페이스에 대한 가상 MAC 주소의 MAC 풀 접두사를 추</u> <u>가합니다.</u>
<u>4단계. 독립형 인스턴스를 추가합니다.</u>
<u>5단계. 인터페이스 구성</u>
<u>6단계, 각 인스턴스에 고가용성 쌍을 추가합니다.</u>
<u>다음을 확인합니다.</u>
문제 해결
<u>참조</u>

## 소개

이 문서에서는 FTD 컨테이너 인스턴스(다중 인스턴스)에서 장애 조치를 구성하는 방법에 대해 설 명합니다.

## 사전 요구 사항

## 요구 사항

Cisco에서는 Firepower Management Center 및 방화벽 위협 방어에 대해 알고 있는 것이 좋습니다.

## 사용되는 구성 요소

Cisco Firepower Management Center Virtual 7.2.5 Cisco Firepower 4145 FTD(NGFW Appliance) 7.2.5 Firepower eXtensible 운영 체제(FXOS) 2.12(0.498) Windows 10

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.

FTD 다중 인스턴스를 구축하기 전에 시스템 성능에 어떤 영향을 미칠 수 있는지 파악하고 그에 따 라 계획을 세워야 합니다. 최적의 구축 및 구성을 위해 항상 Cisco 공식 문서를 참조하거나 Cisco 기 술 담당자에게 문의하십시오.

## 배경 정보

다중 인스턴스는 ASA 다중 컨텍스트 모드와 유사한 FTD(Firepower Threat Defense)의 기능입니다 . 단일 하드웨어에서 FTD의 여러 개별 컨테이너 인스턴스를 실행할 수 있습니다. 각 컨테이너 인스 턴스는 하드 리소스 분리, 별도의 컨피그레이션 관리, 별도의 리로드, 별도의 소프트웨어 업데이트, 완전한 위협 방어 기능 지원을 허용합니다. 이는 부서나 프로젝트마다 다른 보안 정책이 필요하지 만 여러 개의 개별 하드웨어 어플라이언스에 투자하고 싶지 않은 조직에서 특히 유용합니다. 다중 인스턴스 기능은 현재 FTD 6.4 이상을 실행하는 Firepower 4100 및 9300 Series Security Appliance에서 지원됩니다.

이 문서에서는 최대 14개의 Firepower 인스턴스를 지원하는 Container4145를 사용합니다. Firepower Appliance에서 지원되는 최대 인스턴스는 모델당 <u>최대 컨테이너 인스턴스 및 리소스를</u> <u>참조하십시오.</u>

## 네트워크 다이어그램

이 문서에서는 이 다이어그램에서 다중 인스턴스의 HA에 대한 컨피그레이션 및 확인을 소개합니다



논리적 컨피그레이션 다이어그램



물리적 컨피그레이션 다이어그램

## 설정

1단계. 인터페이스 사전 구성

a. FCM의 인터페이스로 이동합니다. 2개의 관리 인터페이스를 설정합니다. 이 예에서는 Ethernet1/3 및 Ethernet1/7입니다.

Overview Interface	s Logical Devices	Security Engine	Platform Settings						System	n Tools Help	admin
		CONSOLE MGMT	Network Module 1 Network Module 2 : Empty Network Module 2 : Empty Network Module 3 : Empty								
An Internaces naroware	e bypass								Add New	Filter.	×
Interface	Туре	Admin Speed	Operational Speed	Instances	VLAN	Admin Duplex	Auto Negotiation	Operation State	Admin State		
MGMT	Management										
Port-channel48	cluster	10gbps	indeterminate			Full Duplex	no	admin-down		6	
Ethernet1/1	data	1gbps	1gbps			Full Duplex	yes	up		0	
Ethernet1/2	data	1gbps	1gbps			Full Duplex	yes	up		0	
Ethernet1/3	mgmt	1gbps	1gbps			Full Duplex	yes	up		0	
Ethernet1/4	data	1gbps	1gbps			Full Duplex	yes	up		0	
Ethernet1/5	data	1gbps	1gbps			Full Duplex	yes	up		0	
Ethernet1/6	data	1gbps	1gbps			Full Duplex	yes	up		0	
Ethernet1/7	mgmt	1gbps	1gbps			Full Duplex	yes	up		0	
Ethernet1/8	data	lgbps	1gbps			Full Duplex	yes	up		0	

인터페이스 사전 구성

2단계. 컨테이너 인스턴스에 대한 리소스 프로필 2개를 추가합니다.

a. Platform Settings(플랫폼 설정) > Resource Profiles(리소스 프로파일) > Add on FCM(FCM에 추가)으로 이동합니다. 첫 번째 리소스 프로필을 설정합니다.

이 예에서는 다음을 수행합니다. ·이름: Instance01 · 코어 수: 10



참고: 컨테이너 인스턴스 쌍의 HA에서는 동일한 리소스 프로필 특성을 사용해야 합니다.

프로파일 이름을 1~64자로 설정합니다. 이 프로파일을 추가한 후에는 이름을 변경할 수 없 습니다.

프로파일의 코어 수를 6에서 최대 사이로 설정합니다.

Overview Interfaces Logi	cal Devices Security Engine Platfo	rm Settings		System Tools Help admin
Overview Interfaces Logi NTP SSH SNMP HTTPS AAA Syslog DNS FIPS and Common Criteria Access List MAC Pool P Resource Profiles Network Control Policy Chassis URL	cal Devices Security Engine Platfo	Add Resource Profile          Name:*       Instance01         Description:       Range: 6 to 86	Cores 6	System Tools Help admin
		Specify even value for number of cores.      OK Cancel		

첫 번째 리소스 프로필 추가

b. 2단계에서 a.를 반복하여 두 번째 리소스 프로필을 구성합니다.

이 예에서는 다음을 수행합니다. ·이름: Instance02

· 코어 수: 20

Overview Interfaces Logic	al Devices Security Engine	Platform Settings			System Tools Help admin
NTP SSH				Add	
SNMP	Name	Description	Cores		
AAA	Default-Small	Auto-created application resource-profile with 6 cpu-cores	6	/ 8	
Syslog	Instance01		10	/ 8	
DNS FIPS and Common Criteria Access List MAC Pool • Resource Profiles Network Control Policy Chassis URL		Add Resource Profile           Name:*       Instance02         Description:       Range: 6 to 86         Number of Cores:*       20         Specify even value for number of cores.			
		OK Cancel			

두 번째 리소스 프로필 추가

c. 2개의 리소스 프로필이 추가되었는지 확인합니다.

-	Overview I	Interfaces	Logica	al Devic	es Se	curity Engin	e P	Platform	n Settings														System	Tools	Help	admin
	NTP																									
	SSH																			0	Add					
	SNMP			Nam	e							Descri	iption					Cores								
	HTTPS			Defay	ult-Small							Auto-c	reated ap	plication	resource-p	profile with d	5 cpu-cores	6			0	3				
	Syslog			Insta	ince01					_								10	1		28	.				
	DNS																		I 1		~ (					
	FIPS and Cor	mmon Criteria		Insta	ince02													20	1		6P (	3				
	Access List																									
	MAC Pool																									
	Resource P	Profiles																								
	Network Con	ntrol Policy																								
	Chassis URL																									

리소스 프로필 확인

3단계. (선택 사항) 컨테이너 인스턴스 인터페이스에 대한 가상 MAC 주소의 MAC 풀 접두사를 추가합니다.

액티브/스탠바이 인터페이스에 대한 가상 MAC 주소를 수동으로 설정할 수 있습니다. 다중 인스턴 스 기능의 경우 가상 MAC 주소가 설정되지 않은 경우 섀시는 인스턴스 인터페이스에 대한 MAC 주 소를 자동으로 생성하고 각 인스턴스의 공유 인터페이스에서 고유한 MAC 주소를 사용하도록 보장 합니다.

MAC 주소<u>에</u> 대한 자세한<u>내용은 Add a MAC Pool Prefix and View MAC Addresses for Container</u> Instance Interfaces(MAC 풀 접두사 추가 및 컨테이너 인스턴스 인터페이스의 MAC 주소 보기)를 참조하십시오.

4단계. 독립형 인스턴스를 추가합니다.

a. Logical Devices(논리적 디바이스) > Add Standalone(독립형 추가)으로 이동합니다. 첫 번째 인 스턴스를 설정합니다.

이 예에서는 다음을 수행합니다. ·장치 이름 : FTD01

## · 인스턴스 유형: 컨테이너



참고: 컨테이너 애플리케이션을 구축하는 유일한 방법은 Instance Type(인스턴스 유형)이 Container(컨테이너)로 설정된 App-Instance(애플리케이션 인스턴스)를 사전 구축하는 것 입니다. 컨테이너를 선택합니다.

논리적 디바이스를 추가한 후에는 이 이름을 변경할 수 없습니다.

Overview Interfaces Logical Devices Security Engine	Platform Settings	System Tools Help admin
Logical Device List	(0 instances) 100% (86 of 86) Cores Available	C Refresh 🕢 Add 🔸
No logical devices available. Click on Add Device to add a new logical device.		
	Add Standalone	
	Device Name: FTD01	
	Template: Cisco Secure Firewall Threat Defense 💌	
	Image Version: 7.2.5.208	
	Instance Type: Container	
	Before you add the first container instance, you must reinitialize the security module/engine so that the disk has the correct formatting. You only need to perform this action once.	
	OK Cancel	

인스턴스 추가

5단계. 인터페이스 구성

a. Instance01에 대한 자원 프로파일, 관리 인터페이스, 관리 IP를 설정합니다.

이 예에서는 다음을 수행합니다. ·리소스 프로필: Instance01 ·관리 인터페이스 : Ethernet1/3 ·관리IP: x.x.1.1

Overview Interfaces Logical Devices Security Engine Platform S	Settings	System Tools Help admin
Provisioning - FTD01 Standalone   Cisco Secure Firewall Threat Defense   7.2.5.208	Cisco Secure Firewall Threat Defense - Bootstrap Configuration 🖭	Save Cancel
Data Ports	General Information Settings Agreement	
Ethernet1/1 Ethernet1/2 Ethernet1/4 Ethernet1/5 Ethernet1/6 Ethernet1/6	SM 1 - 66 Cores Available          Resource Profile:       Instance01 V         Interface Information       V         Management Interface:       Ethernet1/3 V         Address Type:       IPv4 only V         IPv4       IPv4         Management IP:       1.00100         Network Mask:       255.0.0.0         Network Gateway:       1.00100	
Application Version Resource Profile	rt Status	
FTD 7.2.5.208		
	OK Cancel	

프로필/관리 인터페이스/관리 IP 구성

b. 데이터 인터페이스를 설정합니다.

이 예에서는 다음을 수행합니다.

·이더넷1/1(내부용)

·이더넷1/2(외부용)

·Ethernet1/4(HA 링크에 사용)

c	overview Interfaces	Logical Devices Secu	rity Engine Platform Set	tings				System Tools	Help admin
P S	rovisioning - FTD01 itandalone   Cisco Sec	cure Firewall Threat Defense	7.2.5.208					Save	Cancel
D	ata Ports Ethernet1/1 Ethernet1/2 Ethernet1/4 Ethernet1/6 Ethernet1/6			Etherneti Etherneti Etherneti	] ] ]2 ]4	FTD - 7.2.5.208 Etheretiz Click to configure			
ł	Application	Version	Resource Profile	Management IP	Gateway	Management Port	Status		
•	FTD	7.2.5.208	Instance01	1.10001	1.0	Ethernet1/3			
	Interface Name Ethernet1/1 Ethernet1/2 Ethernet1/4	2		Type data data data					

데이터 인터페이스 설정

c. Logical Devices(논리적 디바이스)로 이동합니다. 인스턴스 부팅을 기다리는 중입니다.

(	Overview	Interfaces	Logical Devices	Security Engine	Platform Setting	s				System Tools Help admin
Lo	gical Devic	e List		c	1 Container instanc	e) 100% (86 of 86) Core	is Available			C Refresh 3 Ads -
	FTD01			Standalone	Status:ok					2 I
	Applicat	tion	Version	Resource F	Profile	Management IP	Gateway	Management Port	Status	
	B FTD		7.2.5.208	Instance01		1.111131	1.000000	Ethernet1/3	🐝 Installing	0180 🎋 c 🕍

Instance01의 상태 확인

d. 4.a단계 및 5.a~c단계에서 a.를 반복하여 두 번째 인스턴스를 추가하고 해당 인스턴스에 대한 세 부 정보를 설정합니다.

이 예에서는 다음을 수행합니다.

·장치 이름 : FTD11 ·인스턴스 유형 : 컨테이너

·리소스 프로필 : Instance02 ·관리 인터페이스 : Ethernet1/7 ·ManagementIP: x.x.10.1

·이더넷1/5 = 내부

·이더넷1/6 = 외부

·이더넷1/8 = HA 링크

e. FCM에서 2개의 인스턴스가 온라인 상태인지 확인합니다.

Overview	Interfaces	Logical Devices	Security Engine	Platform Settin	gs				System Tools Help admin
Logical Device	e List			2 Container instand	ces) 66% (56 of 86) Co	ores Available			C Refresh 🕢 Add 🗸
FTD11			Standalone	Status:ok					
Applicat	tion	Version	Resource I	Profile	Management IP	Gateway	Management Port	Status	
B FTD		7.2.5.208	Instance02	3	10.1	1/1-1-111	Ethernet1/7	Online	💌 🕅 🕬
FTD01	]		Standalone	Status:ok					0 I.
Applicat	tion	Version	Resource I	Profile	Management IP	Gateway	Management Port	Status	
H FTD		7.2.5.208	Instance01	]	C: a1.1	1.Converse	Ethernet1/3	Online	💌 🌆 cái

기본 디바이스의 인스턴스 상태 확인

f. (선택 사항) scope ssa 실행 scope slot 1 및 show app-Instance 명령을 사용하여 Firepower CLI에서 2 인스턴스가 온라인 상태임 을 확인합니다.

## <#root>

FPR4145-ASA-K9#

scope ssa

FPR4145-ASA-K9 /ssa #

#### scope slot 1

FPR4145-ASA-K9 /ssa/slot #

#### show app-Instance

Application Instance: App Name Identifier Admin State Oper State Running Version Startup Version Deplo Online

7.2.5 208 7.2.5 208 Container No Instance01 Not Applicable None --> FTD01 Instance is Online ftd FTD11 Online

7.2.5 208 7.2.5 208 Container No Instance02 Not Applicable None --> FTD11 Instance is Online

g. 보조 디바이스에서도 동일하게 수행합니다. 2개의 인스턴스가 온라인 상태인지 확인합니다.

Overview	Interfaces	Logical Devices	Security Engine	Platform Setting	gs				System Tools Help admin
Logical Devic	e List			(2 Container instand	<b>ces)</b> 66% (56 of 86) Cor	es Available			C Refresh 🕢 Add •
FTD12			Standalone	Status:ok					
Applicat	ion	Version	Resource F	Profile	Management IP	Gateway	Management Port	Status	
# FTD		7.2.5.208	Instance02	]	10.2	1.	Ethernet1/7	nline	💌 🕅 C 🚾
FTD02			Standalone	Status:ok					/ I
Applicat	ion	Version	Resource F	Profile	Management IP	Gateway	Management Port	Status	
B FTD		7.2.5.208	Instance01		1.2	1.6	Ethernet1/3	Online	💌 🌆 C 🖄

보조 디바이스의 인스턴스 상태 확인

6단계. 각 인스턴스에 고가용성 쌍을 추가합니다.

a. Devices(**디바이스**) > Add Device on FMC(FMC에 디바이스 추가)로 이동합니다. 모든 인스턴스를 FMC에 추가합니다.

이 예에서는 다음을 수행합니다.

·FTD1의 Instance01에 대한 표시 이름: FTD1\_FTD01 ·FTD1의 Instance02에 대한 표시 이름: FTD1\_FTD11 ·FTD2의 Instance01에 대한 표시 이름: FTD2\_FTD02 ·FTD2의 Instance02에 대한 표시 이름: FTD2\_FTD12

이 그림에서는 FTD1\_FTD01에 대한 설정을 보여 줍니다.



FTD 인스턴스를 FMC에 추가

## b. 모든 인스턴스가 정상인지 확인합니다.

Firewall Management Center Overview Analysis Pole	cies Devices Objects &	ntegration			Deploy	Q 📀 🔅 🚱 admin •	dede SECURE						
View By: Group  At (4)													
Collapse All Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack							
🗌 🗸 Ungrouped (4)													
FTD1_FTD01 Snort 3     1	Firepower 4145 with FTD	7.2.5	ER1145-ASA-K9.443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	40	1						
C PTD1_FTD11 Snort 3	Firepower 4145 with FTD	7.2.5	ERATAS-ASA-K9.443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	40	1						
Conc. 5.1.2 - Routed	Firepower 4145 with FTD	7.2.5	Firepower4KHG cisco com 443 IIII Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	*©	11						
FTD2_FTD12_Snort 3     Conc.10.2 - Routed	Firepower 4145 with FTD	7.2.5	Firepower4KHG cisco.com.443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	4Q	11						

FMC에서 인스턴스 상태 확인

c. Devices(**디바이스)** > Add High Availability(고가용성 추가)로 이동합니다. 첫 번째 장애 조치 쌍을 설정합니다.

이 예에서는 다음을 수행합니다.

### ·이름: FTD01\_FTD02\_HA

· 주 피어 : FTD1\_FTD01



**참고**: 올바른 유닛을 기본 유닛으로 선택해야 합니다.

Firewall Management Center Overview Analysis Pol	licies Devices Objects I	integration		Deploy	오 📀 🌣 🔞 admin 🔻	disto SECURE						
Deployment History View By: Oroup •												
All (4)  • Error (0) • Warning (0) • Offline (0) • Normal (4) • De	eployment Pending (0)	(0) • Short 3 (4)			Q, Search Device	Add 🔻						
Collarse: All												
Name	Model	Version Chassis	Licenses	Access Control Policy	Auto RollBack							
Ungrouped (4)		Add High Availability Pair										
FTD1_FTD01 Snort 3	Firepower 4145 with FTD	Name:* FTD01_FTD02_HA	Base, Threat (2 more)	acp-rule	4©	×1						
FTD1_FTD11 Snort 3     10 1 - Routed	Firepower 4145 with FTD	Device Type: Firewall Threat Defense	Base, Threat (2 more)	acp-rule	4©	1						
FTD2_FTD2_Seent 3     1 2 - Routed	Firepower 4145 with FTD	Primary Peer: FTD1_FTD01	Base, Threat (2 more)	acp-rule	4Q	1						
PTD2_FTD12_Snort.3     10.2 - Routed	Firepower 4145 with FTD	Secondary Peer: FTD2_FTD02 +	Base, Threat (2 more)	acp-rule	4Q	×1						
		Threat Defense High Availability pair will have primary configuration. Licenses from primary peer will be converted to their high availability versions and applied on both peers.										
		Cancel Continue										

첫 번째 장애 조치 쌍 추가

d. 첫 번째 장애 조치 쌍에서 장애 조치 링크에 대한 IP를 설정합니다.

이 예에서는 다음을 수행합니다.

## ·고가용성 링크 : Ethernet1/4

## ·상태 링크 : Ethernet1/4

### · 기본 IP: 192.168.90.1/24

## ·보조 IP: 192.168.90.2/24

Firewall Management Center Overview Analysis Policies Devices Objects Integration Deploy Q 💿 Q 💿 admin • 📩 SECURE												
View By: Group	Deployment History											
All (4)  • Error (0)  • Warning (0)  • Offline (0)  • Normal (4)	Deployment	Pending (0)   Upgrade (0)   Snort 3 (4)			Q, Search Device	Add •						
Collacse All												
Name	Model	Add High Availability Pair		Access Control Policy	Auto RollBack							
Ungrouped (4)		Add High Atomosity For	•									
		High Availability Link	State Link									
FID1_FID01 Snort 3	Firepow	Interface:* Ethernet1/4 +	Interface:" Ethernet1/4 +	acp-rule	4Q	/1						
		Logical Name:* ha_link	Logical Name:*									
© FTD1_FTD11 Snort 3	Firepow	Primary IP:* 192.168.90.1	Primary IP:*	acp-rule	49	11						
ETO.1 - Housed		Use IPv6 Address	Use IPv6 Address									
FTD2_FTD02 Snort 3	Firepow	Secondary IP:* 192.168.90.2	Secondary IP:*	acp-rule	4Q	11						
1.2 - Routed		Subnet Mask:* 255.255.255.0	Subnet Mask:*									
FTD2_FTD12 Seert 3	Firepow	IPsec Encryption			40	1:						
		Enabled										
		Key Generation: Auto +										
		<ul> <li>LAN failover link is used to sync configuration, statef between peers. Selected interface links and encryption</li> </ul>	al failover link is used to sync application content settings cannot be changed later.									
			Cancel									

첫 번째 장애 조치 쌍에 대한 HA 인터페이스 및 IP 설정

e. 장애 조치 상태 확인

·FTD1\_FTD01 : Primay, 활성

· FTD2\_FTD02 : 보조, 대기

E Fire	ewall Management Center Overview Analysis	Policies Devices Object	ts Integratio	n			Deploy Q 😋 🐇	admin • admin • secure				
View By: Group +												
All (4)	Error (0)     Warning (0)     Offline (0)     Normal (4)	<ul> <li>Deployment Pending (0)</li> </ul>	Jpgrade (0)	<ul> <li>Snort 3 (4)</li> </ul>			0,	Search Device Add •				
Collapse All	College Al											
	Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack					
	Ungrouped (3)											
	FTD01_FTD02_HA High Availability							1				
	FTD1_FTD01(Primary, Active) Short 3	Firepower 4145 with FTD	7.2.5	FPR4145-ASA-K9:443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	*Ø	1				
	FTD2_FTD02(Secondary, Standby) Snort 3 CT3.1.2 - Routed	Firepower 4145 with FTD	7.2.5	Firepower4KHG cisco.com:443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	4Ø	I				
	O FTD1_FTD11 Snort 3	Firepower 4145 with FTD	7.2.5	FPR4145-ASA-K9-443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	¢9	1				
	C FTD2_FTD12 Snort 3	Firepower 4145 with FTD	7.2.5	Firepower4KHG.cisco.com.443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	+Ø	11				

첫 번째 장애 조치 쌍의 상태 확인

f. Devices(**디바이스)** > **FTD01\_FTD02\_HA**(이 예에서는) > Interfaces(인터페이스)를 **클릭합니다.** 데이터 인터페이스에 대한 활성 IP를 설정합니다.

이 예에서는 다음을 수행합니다. ·이더넷1/1(내부) : 192.168.10.254/24 ·이더넷1/2(외부): 192.168.20.254/24 ·이더넷1/3(진단): 192.168.80.1/24

## 이 그림에서는 Ethernet1/1의 Active IP에 대한 설정을 보여 줍니다.

Firewall Management Center Devices / Secure Firewall Interfaces	Overview Analysis I	Policies Devices Objects Integration		Deploy Q 💞 🌣 🔕 admin 🕶 📩 SECURE
FTD1_FTD01				You have unsaved changes Save Cancel
Summary High Availability Device Routin	ng Interfaces Inline S	Edit Physical Interface	Edit Physical Interface	eailable for use. X
		General IPv4 IPv6 Path Monitoring Advanced	General IPv6 Path Monitoring Advanced	Add Interfaces *
Interface	Logi	Name: Inside	er sype: Use Static IP v	
Ethernet1/1	inside	Enabled     Management Only	P* Address: 192.168.10.254/24	
© Ethernet1/2	outside	Description:	ing, the second data and set in the second and	
© Ethernet1/3 © Ethernet1/4	ciagnostic	Mode:		
-		None v Security Zone:		
		inside_zone   Interface ID:		Cancel OK
		Ethernet1/1		
		1500		
		(64 - 9184) Priority:		
		0 (0 - 65535) Propagate Security Group Tag:		
		NVE Only:		
			Carcel	

데이터 인터페이스에 대한 활성 IP 설정

g. Devices(**디바이스)** > **FTD01\_FTD02\_HA**(이 예에서) > High Availability(고가용성)를 **클릭합니다.** 데이터 인터페이스의 스탠바이 IP를 설정합니다.

이 예에서는 다음을 수행합니다. ·이더넷1/1(내부) : 192.168.10.253/24 ·이더넷1/2(외부): 192.168.20.253/24 ·이더넷1/3(진단): 192.168.80.2/24

## 이 그림에서는 Ethernet1/1의 Standby IP에 대한 설정을 보여 줍니다.

Firewall Management Devices / High Availability	Center Overview Analysis Policies Devic	es Objects Inte	egration		Deploy	० 🔮 🌣	🕜 admin 🕶 🖏	e SECURE
FTD01_FTD02_HA Cisco Firepower 4145 Threat Defensi Summary High Availability	e Device Routing Interfaces Inline Sets DHCP	VTEP						Cancel
IPsec Encryption	Edit inside	ø	itics					٩
Monitored Interfaces	Monitor this interface for failures		Active Li	ink-Local IPv6	Standby Link-L	ocal IPv6	Monitoring	
outside diagnostic inside	Interface Name: inside Active IP Address: 192.168.10.254 Mask*						0 0 0	/ /
Failover Trigger Criteria	Standby IP Address: 192.168.10.253		face MAC Addresses					+
Failure Limit			cal Interface	Active Mac Addr	ess	Standby Mac	Address	
Peer Poll Time Peer Hold Time		Cancel OK	et1/1	1234.1234.0001		1234.1234.0	002	/=

데이터 인터페이스에 대한 대기 IP 설정

h. 6.c~g 단계를 반복하여 두 번째 장애 조치 쌍을 추가합니다.

이 예에서는 다음을 수행합니다.

·이름: FTD11\_FTD12\_HA ·주 피어: FTD1\_FTD11 ·세컨더리 피어 : FTD2\_FTD12

· High Availability Link : 이더넷1/8 ·주 링크 : 이더넷1/8 ·이더넷1/8(ha\_link Active): 192.168.91.1/24

·이더넷1/5(내부 액티브): 192.168.30.254/24 ·이더넷1/6(외부 액티브): 192.168.40.254/24 ·이더넷1/7(진단 활성): 192.168.81.1/24

·이더넷1/8(ha\_link Standby): 192.168.91.2/24

·이더넷1/5(Inside Standby): 192.168.30.253/24 ·이더넷1/6(Outside Standby): 192.168.40.253/24 ·이더넷1/7(진단 대기): 192.168.81.2/24

i. Logical Devices(**논리적 디바이스)** > Add Standalone(독립형 **추가)으로 이동합니다**. 내부에서 외부로의 트래픽을 허용하도록 ACP 규 칙을 설정합니다.

Firewall Management Center Policies / Access Control / Policy Editor	Iverview Analy	sis Policies	Devices	Objects In	egration					Deploy	Q 🔮 🌣	@ admin	• os	de SEC	URE
acp-rule     Try New UI Layout ( Analyze Hit Counts Save Cancel     Enter Description															
Rules Security Intelligence HTTP Responses Logging Advanced Prefitter Policy: Default Prefitter Policy: Default Prefitter Policy: Default Prefitter Policy: None Identity Policy: None															
Filter by Device Search Rules									×	Show Rule Conf	flicts 🛛 🕂	vdd Catego	y +	- Add R	tule
g Name Source Zones Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applications	Source Ports	Dest Ports	URLs	Source Dynamic Attributes	Destination Dynamic Attributes	Action	F5 0 F5	A 🗆		¢
Mandatory - acp-rule (1-1)	_														
1 ftd_ha_acp inside_zone outside_zone	Any	Any	Any	Any	Any	Any	Any	Any	Any	Any	Allow	15. V. D.	<u>冷</u> 回	0	11
✓ Default - acp-rule (-)															
There are no rules in this section. Add Rule or Add Category															

#### ACP 규칙 설정

#### j. FTD에 설정을 구축합니다.

#### k. CLI에서 HA 상태 확인

각 인스턴스의 HA 상태는 ASA와 동일한 Firepower CLI에서도 확인됩니다.

FTD1\_FTD01(Primary Instance01)의 HA 상태를 확인하려면 show running-config failover 실행 및 show failover 명령

#### <#root>

// confrim HA status of FTD1\_FTD01 (Instance01 of Primary Device) >

#### show running-config failover

failover failover lan unit primary failover lan interface ha\_link Ethernet1/4 failover replication htt

#### show failover

Failover On Failover unit Primary Failover LAN Interface: ha\_link Ethernet1/4 (up) ..... This host: P ..... Other host: Secondary - Standby Ready <---- InstanceO1 of FPRO2 is Standby Interface diagnostic

실행 show running-config failover 및 show failover 명령을 사용하여 FTD1\_FTD11(Primary Instance02)의 HA 상태를 확인합니다.

#### <#root>

// confrim HA status of FTD1\_FTD11 (Instance02 of Primary Device) >

#### show running-config failover

failover failover lan unit primary failover lan interface ha\_link Ethernet1/8 failover replication htt

#### show failover

Failover On Failover unit Primary Failover LAN Interface: ha\_link Ethernet1/8 (up) ..... This host: P Other host: Secondary - Standby Ready <---- Instance02 of FPR02 is Standby Interface diagnostic (192.16

FTD2\_FTD02(Secondary Instance01)의 HA 상태를 확인하려면 show running-config failover 실행 및 show failover 명령을 수행합니 다.

<#root>

// confrim HA status of FTD2\_FTD02 (Instance01 of Secondary Device) >

#### show running-config failover

failover failover lan unit secondary failover lan interface ha\_link Ethernet1/4 failover replication h

#### show failover

Failover On Failover unit Secondary Failover LAN Interface: ha\_link Ethernet1/4 (up) ..... This host: Other host: Primary - Active <---- Instance01 of FPR01 is Active Active time: 31651 (sec) slot 0: UCSB-

FTD2\_FTD12(보조 인스턴스02)의 HA 상태를 확인하려면 실행 show running-config failover 및 show failover 명령을 수행합니다.

#### <#root>

// confrim HA status of FTD2\_FTD12 (Instance02 of Secondary Device) >

#### show running-config failover

failover failover lan unit secondary failover lan interface ha\_link Ethernet1/8 failover replication h Other host: Primary - Active <---- Instance02 of FPR01 is Active Active time: 31275 (sec) slot 0: UCSB-

1. 라이센스 사용 확인

모든 라이센스는 컨테이너 인스턴스가 아니라 보안 엔진/섀시별로 소비됩니다.

· 보안 엔진/섀시당 1개의 베이스라인이 자동으로 할당됩니다.

· 기능 라이센스는 각 인스턴스에 수동으로 할당되지만, 기능 /보안 엔진/섀시당 하나의 라이센스만 소비합니다. 특정 기능 라이센스 의 경우 사용 중인 인스턴스 수와 상관없이 총 1개의 라이센스만 있으면 됩니다.

이 표에서는 이 문서에서 라이센스가 소비되는 방식을 보여줍니다.

FPR01	인스턴스01	기본, URL 필터링, 악성코드, 위협
	인스턴스02	기본, URL 필터링, 악성코드, 위협
FPR02	인스턴스01	기본, URL 필터링, 악성코드, 위협
	인스턴스02	기본, URL 필터링, 악성코드, 위협

기본	URL 필터링	악성코드	위협
2	2	2	2

## FMC GUI에서 사용된 라이센스 수를 확인합니다.

Smart Licenses			Filter Devices	×	Edit Performance Tier	Edit Licenses
License Type/Device Name	License Status	Device Type		Domain	Group	
V Base (2)	In-Compliance					•
FTD01_FTD02_HA (2) Cisco Firepower 4145 Threat Defense Threat Defense High Availability	In-Compliance	High Availability - Cisco Firepower 4145 Th	reat Defense	Global	N/A	
FTD11_FTD12_HA (2)     Cisco Firepower 4145 Threat Defense Threat Defense High Availability	In-Compliance	High Availability - Cisco Firepower 4145 Th	reat Defense	Global	N/A	
V Mabware (2)	In-Compliance					
FTD01_FTD02_HA (2)     Cisco Firepower 4145 Threat Defense Threat Defense High Availability	In-Compliance	High Availability - Cisco Firepower 4145 Th	reat Defense	Global	N/A	
> FTD11_FTD12_HA (2) Cisco Firepower 4145 Threat Defense Threat Defense High Availability	In-Compliance	High Availability - Cisco Firepower 4145 Th	reat Defense	Global	N/A	
V Threat (2)	In-Compliance					
FTD01_FTD02_HA (2)     Cisco Firepower 4145 Threat Defense Threat Defense High Availability	In-Compliance	High Availability - Cisco Firepower 4145 Th	reat Defense	Global	N/A	
FTD11_FTD12_HA (2) Cisco Firepower 4145 Threat Defense Threat Defense High Availability	In-Compliance	High Availability - Cisco Firepower 4145 Th	reat Defense	Global	N/A	
✓ URL Filtering (2)	In-Compliance					- 1
FTD01_FTD02_HA (2)     Cisco Firepower 4145 Threat Defense Threat Defense High Availability	In-Compliance	High Availability - Cisco Firepower 4145 Thr	eat Defense	Global	N/A	
FTD11_FTD12_HA (2)     Cisco Firepower 4145 Threat Defense Threat Defense High Availability	In-Compliance	High Availability - Cisco Firepower 4145 Thr	eat Defense	Global	N/A	

사용된 라이센스 확인

## 다음을 확인합니다.

FTD1\_FTD01(기본 인스턴스 01)에서 충돌이 발생하면 인스턴스 01의 장애 조치가 트리거되고 스탠바이 측의 데이터 인터페이스가 원래 액티브 인터페이스의 IP/MAC 주소를 인수하여 트래픽(이 문서의 FTP 연결)이 Firepower에 의해 지속적으로 전달되도록 합니다.





장애 조치가 트리거됨

1단계. Win10-01에서 Win10-02로의 FTP 연결을 시작합니다.

2단계. 명령 show conn 을 실행하여 FTP 연결이 두 Instance01에 모두 설정되어 있는지 확인합니다.

## <#root>

// Confirm the connection in Instance01 of FPR01 >

show conn

```
TCP outside 192.168.20.1:21 inside 192.168.10.1:49723, idle 0:00:11, bytes 529, flags UIO N1 // Confirm show conn
```

TCP outside 192.168.20.1:21 inside 192.168.10.1:49723, idle 0:00:42, bytes 530, flags UIO N1

3단계. Win10-03에서 Win10-04로의 FTP 연결을 시작합니다.

4단계. FTP show conn 연결이 두 Instance02에 모두 설정되어 있는지 확인하려면 명령을 실행합니다.

## <#root>

// Confirm the connection in Instance02 of FPR01 >

show conn

TCP outside 192.168.40.1:21 inside 192.168.30.1:52144, idle 0:00:02, bytes 530, flags UIO N1 // Confirm show conn

TCP outside 192.168.40.1:21 inside 192.168.30.1:52144, idle 0:00:13, bytes 530, flags UIO N1

5단계. 실행 connect ftd FTD01 및 system support diagnostic-cli 명령을 사용하여 ASA CLI에 입력합니다. 실행 enable 및 crashinfo force watchdog 명령을 사용하여 기본/액티브 유닛에서 Instance01을 강제로 충돌시킵니다.

### <#root>

Firepower-module1>

connect ftd FTD01

>

system support diagnostic-cli FTD01> enable Password: FTD01# FTD01#

crashinfo force watchdog

reboot. Do you wish to proceed? [confirm]:

6단계. 장애 조치는 Instance01에서 발생하며 FTP 연결이 중단되지 않습니다. FPR02 show failover에서 Instance01의 상태를 확인하려 면 명령 show conn을 실행하고 실행하십시오.

### <#root>

>

#### show failover

Failover On Failover unit Secondary Failover LAN Interface: ha\_link Ethernet1/4 (up) ..... This host: Other host: Primary - Failed Interface diagnostic (192.168.80.2): Unknown (Monitored) Interface inside

show conn

TCP outside 192.168.20.1:21 inside 192.168.10.1:49723, idle 0:02:25, bytes 533, flags U N1

7단계. Instance01에서 발생한 충돌은 Instance02에 영향을 미치지 않았습니다. 실행 show failover 및 show conn 명령을 사용하여 Instance02의 상태를 확인합니다.

#### <#root>

>

#### show failover

Failover On Failover unit Secondary Failover LAN Interface: ha\_link Ethernet1/8 (up) ..... This host: Other host: Primary - Active Interface diagnostic (192.168.81.1): Normal (Monitored) Interface inside (199.168.81.1):

TCP outside 192.168.40.1:21 inside 192.168.30.1:52144, idle 0:01:18, bytes 533, flags UIO N1

8단계. FMC에서 Devices > All로 이동합니다. HA 상태를 확인합니다.

#### ·FTD1\_FTD01 : Primay, Standby

#### ·FTD2\_FTD02 : 보조, 활성

Fir Dev	rewall Management Center Overview Analysis	Policies Devices Object	s Integratio	n			Deploy Q	🕽 🌣 🚱 admin 🕶 🔤 dade SECURE			
View By:	w Bry Group										
All (4)	Error (0)     Warning (0)     Offline (0)     Normal (4)	Deployment Pending (0)	pgrade (0)	Snort 3 (4)				Q, Search Device Add •			
Collapse All	olsee Al										
	Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack				
	V Ungrouped (2)										
	FTD01_FTD02_HA High Availability							×1			
	FTD1_FTD01(Primary, Standby) Snort 3	Firepower 4145 with FTD	7.2.5	EPR4145-ASA-K9.443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	49	:			
	FTD2_FTD02(Secondary, Active) Short 3	Firepower 4145 with FTD	7.2.5	Firepower4KHG cisco com:443 Security Module - 1 (Container)	Base, Threat (2 more)	acp+rule	94	1			
	✓ FTD11_FTD12_HA ✓ High Availability							×1			
	FTD1_FTD11(Primary, Active) Short 3     Gramma 10.1 - Routed	Firepower 4145 with FTD	7.2.5	EPR4145-ASA-K9.443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	49	:			
	FTD2_FTD12(Secondary, Standby) Snort 3     To1.u,10.2 - Routed	Firepower 4145 with FTD	7.2.5	Firepower4KHG cisco.com.443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	49	I			

9단계. (선택 사항)FPR01의 Instance01이 정상으로 돌아간 후 HA의 상태를 수동으로 전환할 수 있습니다. 이는 FMC GUI 또는 FRP CLI에서 수행할 수 있습니다.

FMC에서 Devices(**디바이스)** > All(모두)로 이동합니다. FTD01\_FTD02\_HA에 대한 HA 상태를 전환하려면 Switch Active Peer(활성 피어전환)를 클릭합니다.

Fir Des	rewall Management Center Overview Analysis vices / Device Management	Policies Devices Object	s Integratio	n			Deploy Q 🥝 H	admin      didde SECURE
View By:	Group							Deployment History
All (4)	Error (0)     Warning (0)     Offline (0)     Normal (4)	<ul> <li>Deployment Pending (0)</li> </ul>	pgrade (0)	Snort 3 (4)			a	), Search Device Add 🔻
Collapse All								
	Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack	
	Ungrouped (2)							
	FTD01_FTD02_HA High Availability							Switch Active Peer Break
	FTD1_FTD01(Primary, Standby) Short 3     Control, 1,1 - Routed	Firepower 4145 with FTD	7.2.5	EPR4145-ASA-K9:443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	*©	Force refresh node status Delete Revert Upgrade
	Short 3	Firepower 4145 with FTD	7.2.5	Firepower4KHG cisco com.443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	*©	Health Monitor Troubleshoot Files
	V FTD11_FTD12_3AA High Availability							1
	• FTD1_FTD11(Primary, Active) Short 3 CLEm. 10.1 - Routed	Firepower 4145 with FTD	7.2.5	EPR4145-ASA-K9.443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	*Ø	ı
	o FTD2_FTD12(Secondary, Standby) Snort 3 රිස්දු 3.10.2 - Routed	Firepower 4145 with FTD	7.2.5	Firepower4KHG cisco.com:443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	4Q	:

스위치 HA 상태

Firepower CLI에서 ASA CLI connect ftd FTD01를 system support diagnostic-cli 시작하려면 실행 및 명령을 입력합니다. 실행 enable 및 failover active 명령을 사용하여 FTD01\_FTD02\_HA에 대해 HA를 전환합니다.

## <#root>

Firepower-module1>

connect ftd FTD01

>

```
system support diagnostic-cli
```

```
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach. Type help or '?' for a list of available
```

enable

firepower#

failover active

## 문제 해결

장애 조치 상태의 유효성을 검사하려면 명령 show failover 을 show failover history 실행합니다.

## <#root>

>

#### show failover

Failover On Failover unit Secondary Failover LAN Interface: ha\_link Ethernet1/8 (up) ..... This host: Other host: Primary - Active Interface diagnostic (192.168.81.1): Normal (Monitored) Interface inside (1

>

#### show failover history

< debug fover option> 명령을 실행하여 장애 조치의 디버그 로그를 활성화합니다.

### <#root>

#### >

#### debug fover

auth Failover Cloud authentication cable Failover LAN status cmd-exec Failover EXEC command execution of

#### 참조

https://www.cisco.com/c/en/us/support/docs/security/firepower-management-center/212699-configure-ftd-high-availability-on-firep.html https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/multi-Instance/multi-Instance\_solution.html

https://www.cisco.com/c/en/us/support/docs/availability/high-availability/217763-troubleshoot-firepower-threat-defense-hi.html#toc-hId-46641497 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.