Configure FTD Multi-Instance High-availability on Firepower 4100

Contents

Introduction
<u>Prerequisites</u>
Requirements
Components Used
Background Information
Network Diagram
Configurations
Step 1. Pre-configure Interfaces
Step 2. Add 2 Resource Profiles for Container Instances.
Step 3. (Optional)Add a MAC Pool Prefix of virtual MAC address for Container Instance Interfaces.
Step 4. Add a Standalone Instance.
Step 5. Configure Interfaces
Step 6. Add High Availability Pair For Each Instance.
<u>Verify</u>
Troubleshoot
<u>Reference</u>

Introduction

This document describes how to configure Failover in FTD Container Instances (Multi-Instance).

Prerequisites

Requirements

Cisco recommends that you have knowledge of Firepower Management Center and Firewall Threat Defense.

Components Used

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Before deploying FTD Multi-Instance, it is important to understand how it can impact your system

performance and to plan accordingly. Always refer to Cisco official documentation or consult with a Cisco technical representative to ensure optimal deployment and configuration.

Background Information

Multi-Instance is a feature of Firepower Threat Defense (FTD) which is similar to ASA multiple context mode. It allows you to run multiple, separate container Instances of FTD on a single piece of hardware. Each container Instance allows hard resource separation, separate configuration management, separate reloads, separate software updates, and full threat defense feature support. This is particularly useful for organizations that require different security policies for different departments or projects, but do not want to invest in multiple separate hardware appliances. The Multi-Instance feature is currently supported on the Firepower 4100 and 9300 series security appliance running FTD 6.4 and later.

This document uses Firepower4145 which supports maximum 14 Container Instances. For the maximum Instances supported in Firepower Appliance, please refer to <u>Maximum Container Instances and Resources</u> <u>per Model.</u>

Network Diagram

This document introduces the configuration and verification for HA in Multi-Instance on this diagram.



Logical Configuration Diagram



Physical Configuration Diagram

Configurations

Step 1. Pre-configure Interfaces

a. Navigate to Interfaces on FCM. Set 2 mgmt interfaces. In this example Ethernet1/3 and Ethernet1/7.

Overview Interface	s Logical Devices	Security Engine	Platform Settings						System	Tools Help	admin
			Network Module 1	5 7 5 8	Network Module 2 :	Empty	Network Module 3 : Em	pty			
All Interfaces Hardware	Bypass] [Dhus	
Interface	Туре	Admin Speed	Operational Speed	Instances	VLAN	Admin Duplex	Auto Negotiation	Operation State	Add New	ritter	
MGMT	Management										
Port-channel48	cluster	10gbps	indeterminate			Full Duplex	no	admin-down		J 🗟	
Ethernet1/1	data	lgbps	1gbps			Full Duplex	yes	up		ø	
Ethernet1/2	data	lgbps	1gbps			Full Duplex	yes	up		0	
Ethernet1/3	mgmt	lgbps	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	1gbps	1gbps			Full Duplex	yes	up		0	

Pre-configure Interfaces

Step 2. Add 2 Resource Profiles for Container Instances.

a. Navigate to **Platform Settings** > **Resource Profiles** > **Add** on FCM. Set 1st resource profile.

In this example :

- Name : Instance01
- Number of Cores : 10



Note: For HA of container Instance pair, they must use the same resource profile attributes.

Set the name of the profile between 1 and 64 characters. Note that you cannot change the name of this profile after you add it.

Set the number of cores for the profile, between 6 and the maximum.

Overview Interfaces Logic	cal Devices Security Engine Plat	tform Settings			System Tools Help admin
NTP SSH SNMP	Name	Description	Cores	Add 🛛	
HTTPS AAA Syslog DNS SERS and Conserve Coloria	Default-Small	Auto-created application resource-profile with 6 cpu-cores	6	/ 5	
Access List MAC Pool • Resource Profiles Network Control Policy		Add Resource Profile Name:* Instance01 Description:			
Chassis URL		Number of Cores:* 10 Range: 6 to 86 Specify even value for number of cores.			
		OK Cancel			

Add 1st Resource Profile

b. Repeat a. in Step 2, to configure 2nd resource profile.

In this example :

- Name : Instance02
- Number of Cores : 20

Overview Interfaces Log	cal Devices Security Engine	Platform Settings			System Tools Help admin
NTP SSH				Add	
SNMP	Name	Description	Cores		
HTTPS AAA	Default-Small	Auto-created application resource-profile with 6 cpu-cores	6	/ 5	
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 Image: Specify even value for number of cores. OK			

Add 2nd Resource Profile

c. Check 2 resource profiles are added successfully.

Ov	erview Interfaces Log	jical	Devices	Security Engine	e Pla	atform Settings	5								System	Tools	Help	admin
N	ITP																	
s	SH												0	Add				
s	NMP		Name					 Description			Cores							
A	ITTPS AA		Default-	Small				Auto-created application	resource-profile with 6 cp	pu-cores	6			6				
s	yslog		Instance	01							10	1		a 🖉				
0	NS		Instance	02							20	L		/ 6				
A	ccess List		_															
N	IAC Pool																	
 B 	tesource Profiles																	
N	letwork Control Policy																	
C	hassis URL																	

Confirm Resource Profile

Step 3. (Optional)Add a MAC Pool Prefix of virtual MAC address for Container Instance Interfaces.

You can set virtual MAC address for Active/Stanby interface manually. If Virtual MAC Addresses are not set, for multi-Instance capability, the chassis automatically generates MAC addresses for Instance interfaces, and guarantees that a shared interface in each Instance uses a unique MAC address.

Please check Add a MAC Pool Prefix and View MAC Addresses for Container Instance Interfaces for more detail about MAC address.

Step 4. Add a Standalone Instance.

a. Navigate to Logical Devices > Add Standalone. Set 1st Instance.

In this example :

- Device Name : FTD01
- Instance Type : Container



Note: The only way to deploy a container application is to pre-deploy an App-Instance with **Instance Type** set to **Container**. Ensure to select **Container**.

You cannot change this name after you add the logical device.

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 Secu	ure Firewall Threat Defense	
	Image Version: 7.2.5.208	*	
	Instance Type: Container	×	
	Before you add the first conta the security module/engine s formatting. You only need to	iner instance, you must reinitialize o that the disk has the correct perform this action once. OK Cancel	

Add Instance

Step 5. Configure Interfaces

a. Set Resource Profile, Management Interface, Management IP for Instance01.

In this example :

- Resource Profile : Instance01
- Management Interface : Ethernet1/3
- ManagementIP : x.x.1.1

Overview Interfaces Logical Devices Security Engine Platform	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 Ethernet1/6 Ethernet1/8	SM 1 - 66 Cores Available Resource Profile: Instance01 Interface Information Management Interface: Ethernet1/3 Address Type: IPv4 only IPv4 Management IP: 1:::::1 Network Mask: 255.0.0 Network Gateway: 1^^	
Application Version Resource Profile	rt Status	
∃ FTD 7.2.5.208		
	OK Cancel	

Configure Profile/Management Interface/Management IP

b. Set Data Interfaces.

In this example :

- Ethernet1/1 (used for inside)
- Ethernet1/2 (used for outside)
- Ethernet1/4 (used for HA link)

c	overview Interfaces	Logical Devices Secu	rity Engine Platform Sett	ings				System Tools	Help admin
P	rovisioning - FTD01 itandalone Cisco Sec	cure Firewall Threat Defense	7.2.5.208					Save	Cancel
	ata Ports Ethernet1/1 Ethernet1/2 Ethernet1/4 Ethernet1/6 Ethernet1/6			Ethernet1/ Ethernet1/	2 4	FTD - 7.2.5.208 EthernetJ3 Click to configure			
ļ	Application	Version	Resource Profile	Management IP	Gateway	Management Port	Status		
	FTD Interface Name Ethernet1/1 Ethernet1/2 Ethernet1/4	7.2.5.208	Instance01	1.1000011 Type data data data	1. <u>C.****</u>)	Ethernet1/3			

Set Data Interfaces

c. Navigate to Logical Devices. Waiting for Instance bootup.

	Overview	Interfaces	Logical Devices	Security Engine	Platform Setting	<u>js</u>				System Tools Help admin
L	gical Devic	e List			(1 Containe r instanc	e) 100% (86 of 86) Cores Ava	ailable			C Refresh 🔾 Add •
	FTD01			Standalone	Status:ok					2 I
	Applicat	ion	Version	Resource I	Profile	Management IP	Gateway	Management Port	Status	
	FTD		7.2.5.208	Instance01		1	1.0-0-000	Ethernet1/3	😽 Installing	000 🎋 c 🕍

d. Repeat a. in Step 4.a and Step 5.a through c to add 2nd Instance and set detail for it.

In this example :

- Device Name : FTD11
- Instance Type : Container
- Resource Profile : Instance02
- Management Interface : Ethernet1/7
- · ManagementIP : x.x.10.1
- Ethernet1/5 = inside
- Ethernet1/6 = outside
- Ethernet1/8 = HA link
- e. Confirm 2 Instances are Online status on FCM.

Overview	Interfaces	Logical Devices	Security Engine	Platform Setting	gs				System Tools Help admin
Logical Devic	e List			2 Container instanc	ves) 66% (56 of 86) Co	es 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	1/202020	Ethernet1/7	Online	💌 🕅 🕬
FTD01]		Standalone	Status:ok					0 I.
Applicat	tion	Version	Resource #	Profile	Management IP	Gateway	Management Port	Status	
H FTD		7.2.5.208	Instance01]	Cartana	1.Constants	Ethernet1/3	Online	💌 🕅 Cú

Confirm Instance Status In Primary Device

f. (Optional)Run scope ssa, scope slot 1 and show app-Instance command to confrim 2 Instances are Online status on Firepower CLI.

<#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 Deploy Type Turbo Mode Profi _____ ____ ftd FTD01 Enabled Online 7.2.5 208 7.2.5 208 Container No Instance01 Not Applicable None --> FTD01 Instance is Online ftd FTD11 Enabled Online 7.2.5 208 7.2.5 208 Container No Instance02 Not Applicable None --> FTD11 Instance is Online

g. Do the same on the Secondary device. Confirm 2 Instances are Online status.

Overview	Interfaces	Logical Devices	Security Engine	Platform Setting	gs				System Tools Help admin
Logical Devic	e List		(2 Container instand	ces) 66% (56 of 86) Cor	es Available			C Refresh 🕢 Add •
FTD12			Standalone	Status:ok					<i>2</i> :
Applicat	tion	Version	Resource F	rofile	Management IP	Gateway	Management Port	Status	
# FTD		7.2.5.208	Instance02		10.2	1.	Ethernet1/7	nline	🚾 🌃 c 🕍
FTD02			Standalone	Status:ok					01
Applicat	tion	Version	Resource F	rofile	Management IP	Gateway	Management Port	Status	
B FTD		7.2.5.208	Instance01			1.6	Ethernet1/3	Online	🕶 🏹 🖙

Confirm Instance Status In Secondary Device

Step 6. Add High Availability Pair For Each Instance.

a. Navigate to **Devices** > **Add Device** on FMC. Add all Instances to FMC.

In this example :

- Dispaly Name for Instance01 of FTD1 : FTD1_FTD01
- Dispaly Name for Instance02 of FTD1 : FTD1_FTD11
- Dispaly Name for Instance01 of FTD2 : FTD2_FTD02
- Dispaly Name for Instance02 of FTD2 : FTD2_FTD12

This image shows the setting for FTD1_FTD01.

Firewall Management Center Overview Analyte Devices / Device Management	Add Device	Deploy	Q 🧬 🕸 💿 admin 🔹 🔤 esco SECURE
View By: Group • A8 (0) • Error (0) • Warning (0) • Offine (0) • Normal (CDD Managed Device		Deployment History Q, Search Device Add •
Collecte All Name Ungrouped (f)	Display Name: FTD1_FTD01 Registration Key:*	Licenses Access Control Policy	Auto BollBack
	George: • None • Access Control Policy** • Scp-rude • Smart Licensing • Mark surge york Smart Licensing account contains the wisilable licenses you need. It's important to choose the tier that matches the license you have in your account. Click have for information about the Ferwall Threat Defense performance-tierer licensing. Unit you choose a tier, your Frewall Threat Defense virtual defaults to the FTDv50 selection. Profermance Tierer (Jord Frewall Threat Defense virtual 2.0 and above): • Intro / Variable • Otherwale • URL Filtering Advanced Linque NAT ID: • Otherwale Threat Defense • Variable • Starting Threat Defense • Starting Packets •		
	Cancel Register		

Add FTD Instance To FMC

b. Confirm all Instances are Normal.

þ	Firewall Management Cer Devices / Device Management	nter _{Overview} Analysis Pol	icies Devices Objects I	integration			Deploy	Q 📀 🌣 🚱 admin 🔹	dede SECURE					
View E	Inverse Caroop • Deployment Hatory Ait (4) • Error (0) • Warning (0) • Offline (0) • Deployment Pending (0) • Upgrade (0) • Snort 3 (4) Q, Search Device Add •													
Collect	Name		Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack						
C	V Ungrouped (4)													
	FTD1_FTD01 Snort 3 1_0_1.1.1 - Routed 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	¹ ⁰	/:					
	FTD2_FTD02 Short 3		Firepower 4145 with FTD	7.2.5	Security Module - 1 (Container) Firepower4KHG.cisco.com:443 Security Module - 1 (Container)	Base, Threat (2 more) Base, Threat (2 more)	acp-rue acp-rule	10 10	/1					
C	© FTD2_FTD12 Snort 3		Firepower 4145 with FTD	7.2.5	Erepower4KHG cisco com 443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	4Q	11					

Confirm Instance Status In FMC

c. Navigate to **Devices** > **Add High Availability**. Set 1st failover pair.

In this example :

· Name : FTD01_FTD02_HA

- Primary Peer : FTD1_FTD01
- Secondary Peer : FTD2_FTD02

Note: Ensure to select the correct unit as the primary unit.

Firewall Management Center Overview Analysis Po Devices / Device Management	licies Devices Objects I	integration		Deploy	Q 🥝 🌣 🔞 admin 🔹	este SECURE
Marchan Comm					Deploy	ment History
All (4) • Error (0) • Warning (0) • Offline (0) • Normal (4) • D	eployment Pending (0)	(0) Snort 3 (4)			Q, Search Device	Add 🔻
Collapse All						
Name	Model	Version Chassis	Licenses	Access Control Policy	Auto RollBack	
Ungrouped (4)		Add High Availability Pair				
FID1_FID01 Seert 3	Firepower 4145 with FTD	Name:* FTD01_FTD02_HA	Base, Threat (2 more)	acp-rule	e@	1
FID1_FID11 Snort 3 TO 1 - Routed	Firepower 4145 with FTD	Device Type: Firewall Threat Defense	Base, Threat (2 more)	acp-rule	e\$9	1
FTD2_FTD02_Short 3	Firepower 4145 with FTD	Primary Peer: FTD1_FTD01	Base, Threat (2 more)	acp-rule	*9	×1
FTD2_FTD12 Short 3	Firepower 4145 with FTD	Secondary Peer: FTD2_FTD02 +	Base, Threat (2 more)	acp-rule	*9	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				

d. Set IP for failover link in 1st failover pair.

In this example :

- High Availability Link : Ethernet1/4
- State Link : Ethernet1/4
- · Primary IP : 192.168.90.1/24
- · Secondary IP : 192.168.90.2/24

Firewall Management Center Overview Analysis Policies	Devices Objects Integration		Deploy	Q 📀 🌣 😧 admin 🔹	deader SECURE
New By: Group				Deploy	ment History
All (4) • Error (0) • Warning (0) = Offline (0) • Normal (4) • Deployment	Pending (0)			Q, Search Device	Add 🔻
Collapse All					
Name Model			Access Control Policy	Auto RollBack	
	Add High Availability Pair	0			
Ungrouped (4)	High Availability Link	State Link			
FTD1_FTD01 Seet 3	Interface:* Ethernet1/4 +	Interface:* Ethernet1/4 +			
1.1 - Routed	Logical Name:* ha_link	Logical Name:*		12	× :
FTD1_FTD11 Snort 3 Firepow	Primary IP:* 192.168.90.1	Primary IP;*	acp-rule	40	1:
	Use IPv6 Address	Use IPv6 Address			
FTD2_FTD02 Snort 3 Firepower	Secondary IP:* 192.168.90.2	Secondary IP:*	acp-rule	49	1:
ILZ - HOURD	Subnet Mask:* 255.255.255.0	Subnet Mask:*			
FTD2_FTD12 Seet 3 Firepowe	IPsec Encryption		acp-rule	<0	1:
	Enabled				
	Key Generation: Auto v				
	LAN failover link is used to sync configuration, stateful	I failover link is used to sync application content			
	between peers, selected interface links and encryption s	enings carnot be changed later.			
		Cancel Add			

Set HA Interface and IP for 1st Failover Pair

e. Confirm the status of failover

• FTD1_FTD01 : Primay, Active

· FTD2_FTD02 : Secondary, Standby

Fin Dev	ewall Management Center Overview Analysis	Policies Devices Obj	ects Integrati	on			Deploy 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 •
Collapse All								
	Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack	
	Ungrouped (3)							
•	 FTD01_FTD02_HA High Availability 							11
	FTD1_FTD01(Primary, Active) Snort 3	Firepower 4145 with FTD	7.2.5	FPR4145-ASA-K9-443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	ф	I
	O FTD2_FTD02(Secondary, Standby) Snott 3 で同見1.2 - Routed	Firepower 4145 with FTD	7.2.5	Firepower4KHG.cisco.com.443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	¢۶	:
	O FTD1_FTD11 Short 3	Firepower 4145 with FTD	7.2.5	FPR4145-ASA-K9-443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	ę.	11
	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	\$P	11

Confirm Status Of 1st Failover Pair

f. Navigate to **Devices** > **Click FTD01_FTD02_HA** (in this example) > **Interfaces.** Set Active IP for Data Interface.

In this example :

- Ethernet1/1 (inside) : 192.168.10.254/24
- Ethernet1/2 (outside) : 192.168.20.254/24
- Ethernet1/3 (diagnostic) : 192.168.80.1/24

This image shows the setting for Active IP of Ethernet1/1.

Firewall Management Center Overview Analysis Devices / Secure Frewall Interfaces	Policies Devices Objects Integration		Deploy Q 🤣 🌣 🔕 admin 🕶 🐝 SECURE
FTD1_FTD01			You have unsaved changes Save Cancel
Summary High Availability Device Routing Interfaces Inlin	Se Edit Physical Interface	Edit Physical Interface	• Assable for use. A
	General IPv4 IPv6 Path Monitoring Advanced	General IPv6 Path Monitoring Advanced	Add Interfaces +
Interface Logi	Name: inside	er type: Use Static IP v	
Ethernet1/1 inside	Management Only	IP Address: 192.168.10.254/24	
Ethernet1/2 outside	Description:	eg 192.0.2.17265.286.286.128.07.192.0.2.1726	
Ethernet1/3 diagnostic			
Ethernet1/4	Mode:		
	Security Zone:		
	inside_zone *		
	Interface ID:		Cancel OK
	Ethernet1/1		
	MTU:		
	1500		
	(64 - 9184)		
	Priority:		
	Descents Security Course Text		
	M/E Only:		
	-		
		Cancel OK	

Set Active IP for Data Interface

g. Navigate to **Devices** > **Click FTD01_FTD02_HA** (in this example) > **High Availability.** Set Standby IP for Data Interface.

In this example :

- Ethernet1/1 (inside) : 192.168.10.253/24
- Ethernet1/2 (outside) : 192.168.20.253/24
- Ethernet1/3 (diagnostic) : 192.168.80.2/24

This image shows the setting for Standby IP of Ethernet1/1.

Firewall Management Devices / High Availability	Center Overview Analysis Policies Ob	jects Integ	ration		Deploy	९ 🔮 🌣	Ø admin ▼ dia	SECURE
FTD01_FTD02_HA Cisco Firepower 4145 Threat Defense Summary High Availability	Device Routing Interfaces Inline Sets DHCP VTEP							Cancel
IPsec Encryption	Edit inside	ø	itics					Q
Monitored Interfaces	Monitor this interface for failures			Active Link-Local IPv6	Standby Link-	Local IPv6	Monitoring	
outside	Interface Name:						0	1
diagnostic	inside Active IP Address:						0	1
inside	192.168.10.254 Mask: 24						٥	/
	Standby IP Address:							
Failover Trigger Criteria	192.168.10.253		face MAC Addr	esses				+
Failure Limit			al Interface	Active Mac A	ddress	Standby Mac A	lddress	
Peer Poll Time			et1/1	1234.1234.00	001	1234.1234.000	02	/1
Peer Hold Time	Cance							

Set Standby IP for Data Interface

h. Repeat Step 6.c through g, to add 2nd failover pair.

In this example :

- Name : FTD11_FTD12_HA
- Primary Peer : FTD1_FTD11
- Secondary Peer : FTD2_FTD12
- High Availability Link : Ethernet1/8
- State Link : Ethernet1/8
- Ethernet1/8 (ha_link Active) : 192.168.91.1/24
- Ethernet1/5 (inside Active) : 192.168.30.254/24
- Ethernet1/6 (outside Active) : 192.168.40.254/24
- Ethernet1/7 (diagnostic Active) : 192.168.81.1/24
- Ethernet1/8 (ha_link Standby) : 192.168.91.2/24
- Ethernet1/5 (inside Standby) : 192.168.30.253/24
- Ethernet1/6 (outside Standby) : 192.168.40.253/24
- Ethernet1/7 (diagnostic Standby) : 192.168.81.2/24

i. Navigate to **Logical Devices** > **Add Standalone**. Set ACP rule to permit the traffic from inside to outisde.

Firewall Manager Policies / Access Contro	ent Center Policy Editor	Overview Ar	alysis Policies	Devices	Objects Ir	ntegration					Deploy	Q 🔮 🌣	🛛 admi	n• 4	diada: SE	CURE
acp-rule Try New UI Layout () Analyze Hit Counts Save Cancel Enter Description																
Rules Security Intelligen	Rules Security Intelligence HTTP Responses Logging Advanced Prefilter Policy: Default Prefilter Policy: Default Prefilter Policy: None Identity Policy: None															
Eilter by Device	ules									×	Show Rule Cont	flicts 🛛 + A	dd Categ	ory	+ Add	Rule
# Name Source	ones Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applications	Source Ports	Dest Ports	URLs	Source Dynamic Attributes	Destination Dynamic Attributes	Action	15 O I	4.20	-	• •
Mandatory - acp-rule (1-1)																
1 ftd_ha_acp inside	one outside_zone	Any:	Any	Any	Any	Any	Any	Any	Any	Any	Any	C Allow	15 O D	A 0	S 🖬 🤇	11
✓ Default - acp-rule (-)	Default - acp-rule (-)															
There are no rules in this section	Add Rule or Add Cates	pory														

Set ACP Rule

j. Deploy the setting to FTD.

k. Confirm HA status in CLI

The HA status for each Instance is also confirmed in Firepower CLI which is same as ASA.

Run show running-config failover and show failover command to confrim HA status of $FTD1_FTD01$ (Primary Instance01).

<#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 http
failover link ha_link Ethernet1/4
failover interface ip ha_link 192.168.90.1 255.255.255.0 standby 192.168.90.2

```
>
```

show failover

Failover On Failover unit Primary Failover LAN Interface: ha_link Ethernet1/4 (up) This host: Primary - Active <---- Instance01 of FPR01 is Active Interface diagnostic (192.168.80.1): Normal (Monitored) Interface inside (192.168.10.254): Normal (Monitored) Interface outside (192.168.20.254): Normal (Monitored) Other host: Secondary - Standby Ready <---- Instance01 of FPR02 is Standby Interface diagnostic (192.168.80.2): Normal (Monitored) Interface inside (192.168.10.253): Normal (Monitored) Interface outside (192.168.20.253): Normal (Monitored)

Run show running-config failover and show failover command to confrim HA status of FTD1_FTD11 (Primay Instance02).

```
<#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 http
failover link ha_link Ethernet1/8
failover interface ip ha_link 192.168.91.1 255.255.0 standby 192.168.91.2

>

show failover

Failover On Failover unit Primary Failover LAN Interface: ha_link Ethernet1/8 (up) This host: Primary - Active <---- Instance02 of FPR01 is Active Interface diagnostic (192.168.81.1): Normal (Monitored) Interface inside (192.168.30.254): Normal (Monitored) Interface outside (192.168.40.254): Normal (Monitored) Other host: Secondary - Standby Ready <---- Instance02 of FPR02 is Standby Interface diagnostic (192.168.81.2): Normal (Monitored) Interface inside (192.168.30.253): Normal (Monitored) Interface outside (192.168.40.253): Normal (Monitored) Run show running-config failover and show failover command to confrim HA status of FTD2_FTD02 (Secondary Instance01).

```
<#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 http
failover link ha_link Ethernet1/4
failover interface ip ha_link 192.168.90.1 255.255.0 standby 192.168.90.2

```
>
```

show failover

Failover On Failover unit Secondary Failover LAN Interface: ha_link Ethernet1/4 (up) This host: Secondary - Standby Ready <---- Instance01 of FPR02 is Standby Interface diagnostic (192.168.80.2): Normal (Monitored) Interface inside (192.168.10.253): Normal (Monitored) Interface outside (192.168.20.253): Normal (Monitored) Other host: Primary - Active <---- Instance01 of FPR01 is Active Active time: 31651 (sec) slot 0: UCSB-B200-M3-U hw/sw rev (0.0/9.18(3)53) status (Up Sys) Interface diagnostic (192.168.80.1): Normal (Monitored) Interface inside (192.168.10.254): Normal (Monitored) Interface outside (192.168.20.254): Normal (Monitored)

Run show running-config failover and show failover command to confrim HA status of FTD2_FTD12 (Seconday Instance02).

<#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 http
failover link ha_link Ethernet1/8
failover interface ip ha_link 192.168.91.1 255.255.255.0 standby 192.168.91.2

> show failover
Failover On

```
Failover unit Secondary
Failover LAN Interface: ha_link Ethernet1/8 (up)
.....
This host: Secondary - Standby Ready <---- Instance02 of FPR02 is Standby
Interface diagnostic (192.168.81.2): Normal (Monitored)
Interface inside (192.168.30.253): Normal (Monitored)
Interface outside (192.168.40.253): Normal (Monitored)
.....
Other host: Primary - Active <---- Instance02 of FPR01 is Active
Active time: 31275 (sec)
slot 0: UCSB-B200-M3-U hw/sw rev (0.0/9.18(3)53) status (Up Sys)
Interface diagnostic (192.168.81.1): Normal (Monitored)
Interface inside (192.168.30.254): Normal (Monitored)
Interface outside (192.168.40.254): Normal (Monitored)</pre>
```

1. Confirm license consumption

All licenses are consumed per security engine/chassis, and not per container Instance.

• Baselicenses are automatically assigned: one per security engine/chassis.

• Feature licenses are manually assigned to each Instance, but you only consume one license per feature persecurity engine/chassis. For a specific feature license, you only need a total of 1 license, regardless of the number of Instances in use.

This table show how the licenses are consumed in this document.

FPR01	Instance01	Base, URL Filtering, Malware, Threat
	Instance02	Base, URL Filtering, Malware, Threat
FPR02	Instance01	Base, URL Filtering, Malware, Threat
	Instance02	Base, URL Filtering, Malware, Threat

Total Number of Licenses

Base	URL Filtering	Malware	Threat
2	2	2	2

Confirm the number of consumed licenses in FMC GUI.

Smart Licenses			Filter Devices	×	Edit Performance Tier	Edit Licenses
License Type/Device Name	License Status	Device Type		Domain	Group	
∨ Base (2)	 In-Compliance 					^
FTD01_FTD02_HA (2) Cisco Firepower 4145 Threat Defense Threat Defense High Availability	In-Compliance	High Availability - Cisco Firepower 4145 Thre	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 Thre	eat Defense	Global	N/A	
✓ Malware (2)	In-Compliance					
FTD01_FTD02_HA (2) Cisco Firepower 4145 Threat Defense Threat Defense High Availability	 In-Compliance 	High Availability - Cisco Firepower 4145 Thre	eat Defense	Global	N/A	
FTD11_FTD12_HA (2) Clsco Firepower 4145 Threat Defense Threat Defense High Availability	 In-Compliance 	High Availability - Cisco Firepower 4145 Thre	eat Defense	Global	N/A	
∨ Threat (2)	In-Compliance					
> FTD01_FTD02_HA (2) Cisco Firepower 4145 Threat Defense Threat Defense High Availability	 In-Compliance 	High Availability - Cisco Firepower 4145 Thre	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 Thre	eat Defense	Global	N/A	
✓ URL Fittering (2)	In-Compliance					- 1
FTD01_FTD02_HA (2) Cisco Firepower 4145 Threat Defense Threat Defense High Availability	In-Compliance	High Availability - Cisco Firepower 4145 Thre	at Defense	Global	N/A	
> FTD11_FTD12_HA (2) Cisco Firepower 4145 Threat Defense Threat Defense High Availability	In-Compliance	High Availability - Cisco Firepower 4145 Thre	at Defense	Global	N/A	

Confirm Consumed Licenses

Verify

When crash occured on FTD1_FTD01 (Primary Instance01), the failover of Instance01 is triggered and data interfaces on the Standby side takes over the IP/MAC address of the original Active Interface, ensuring the traffic (FTP connection in this document) to be continuously passed by Firepower.

Before Crash

Failover Is Triggered

Step 1. Initiate FTP connection from Win10-01 to Win10-02.

Step 2. Run show conn command to confrim FTP connection is established in both of Instance01.

```
// 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 the connection in InstanceO1 of FPRO2

show conn

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

Step 3. Initiate FTP connection from Win10-03 to Win10-04.

Step 4. Run show conn command to confrim FTP connection is established in both of Instance02.

<#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 the connection in Instance02 of FPR02

>

show conn

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

Step 5. Run connect ftd FTD01 and system support diagnostic-cli command to enter into ASA CLI. Run enable and crashinfo force watchdog command to force crash Instance01 in Primary/Active unit.

<#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]:

Step 6. Failover occurs in Instance01 and the FTP connection is not interrupted. Run show failover and show conn command to confirm the stauts of Instance01 in FPR02.

<#root>

>

show failover

```
Failover On
Failover unit Secondary
Failover LAN Interface: ha_link Ethernet1/4 (up)
.....
This host: Secondary - Active <---- InstanceO1 of FPRO2 is Switching to Active
Interface diagnostic (192.168.80.1): Normal (Waiting)
Interface inside (192.168.10.254): Unknown (Waiting)
Interface outside (192.168.20.254): Unknown (Waiting)
.....
Other host: Primary - Failed
Interface diagnostic (192.168.80.2): Unknown (Monitored)
Interface inside (192.168.10.253): Unknown (Monitored)
Interface outside (192.168.20.253): Unknown (Monitored)
```

>

show conn

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

Step 7. The crash occurred in Instance01 had no effect to Instance02. Run show failover and show conn command to confirm the stauts of Instance02.

<#root>

>

show failover

Failover On
Failover unit Secondary
Failover LAN Interface: ha_link Ethernet1/8 (up)
.....
This host: Secondary - Standby Ready
Interface diagnostic (192.168.81.2): Normal (Monitored)
Interface inside (192.168.30.253): Normal (Monitored)
Interface outside (192.168.40.253): Normal (Monitored)
.....
Other host: Primary - Active
Interface diagnostic (192.168.81.1): Normal (Monitored)
Interface inside (192.168.30.254): Normal (Monitored)
Interface outside (192.168.40.254): Normal (Monitored)

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

Step 8. Navigate to **Devices** > **All** on FMC. Confirm the HA status.

• FTD1_FTD01 : Primay, Standby

· FTD2_FTD02 : Secondary, Active

Fir Dev	rewall Management Center Overview Analysis	Policies Devices Objec	s Integratio	'n			Deploy Q 🤇	🔅 🙆 admin 🔹 🖂 de de SECURE
View By:	Group							Deployment History
All (4)	Error (0) Warning (0) Offline (0) Normal (4)	Deployment Pending (0)	pgrade (0)	 Snort 3 (4) 				Q, Search Device Add •
Collapse All								
	Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack	
	V Ungrouped (2)							
	✓ FTD01_FTD02_HA High Availability							11
	FTD1_FTD01(Primary, Standby) Snort 3	Firepower 4145 with FTD	7.2.5	III Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	4 9	1
	FTD2_FTD02(Secondary, Active) Snort 3	Firepower 4145 with FTD	7.2.5	IIII Firepower4KHG cisco.com 443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	¢۹	1
	✓ FTD11_FTD12_HA High Availability							11
	FTD1_FTD11(Primary, Active) Short 3 Gramma 10.1 - Routed	Firepower 4145 with FTD	7.2.5	FPR4145-ASA-K9.443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	4Ø	1
	FTD2_FTD12(Secondary, Standby) Snort 3 toticu, 10.2 - Routed	Firepower 4145 with FTD	7.2.5	Enclose Container	Base, Threat (2 more)	acp-rule	֯	1

Confirm HA Status

Step 9. (Optional)After the Instance01 of FPR01 returns to normal, you can manually switch the status of HA. This can be done by either FMC GUI or FRP CLI.

On FMC, navigate to **Devices** > **All**. Click **Switch Active Peer** to switch HA status for **FTD01_FTD02_HA**.

Fi 🗠	rewall Management Center Overview Analysis	Policies Devices Objec	ts Integratio	n			Deploy Q 🥥	O admin • dada SECURE
View By: All (4)	Group ▼ ● Error (0) ● Warning (0) ◎ Offline (0) ● Normal (4)	Deployment Pending (0)	Jpgrade (0)	Snort 3 (4)				Deployment History Q, Search Device Add •
Collapse Al								
	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) Snort 3 Critic 1,1,1 = Routed	Firepower 4145 with FTD	7.2.5	EPR4145-ASA-K9.443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	49	Force refresh node status Delete Revert Upgrade
	FTD2_FTD02(Secondary, Active) Snort 3	Firepower 4145 with FTD	7.2.5	Firepower4KHG.cisco.com.443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	e\$2	Health Monitor Troubleshoot Files
	✓ FTD11_FTD12_HA High Availability							11
	FTD1_FTD11(Primary, Active) Short 3 Comm.10.1 - Routed	Firepower 4145 with FTD	7.2.5	ERATIAS-ASA-K9.443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	49	:
	FTD2_FTD12(Secondary, Standby) Snort 3 Clip110 2 - Routed	Firepower 4145 with FTD	7.2.5	Enclower4XHC cisco.com 443 Security Module - 1 (Container)	Base, Threat (2 more)	ecp-rule	+9	I

Switch HA Status

On Firepower CLI, Run connect ftd FTD01 and system support diagnostic-cli command to enter into ASA CLI. Run enable and failover active command to switch HA for FTD01_FTD02_HA.

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 commands. firepower> enable

firepower#

failover active

Troubleshoot

In order to validate the the status of failover, run show failover and show failover history command.

<#root>

>

show failover

```
Failover On
Failover unit Secondary
Failover LAN Interface: ha_link Ethernet1/8 (up)
.....
This host: Secondary - Standby Ready
Interface diagnostic (192.168.81.2): Normal (Monitored)
Interface inside (192.168.30.253): Normal (Monitored)
Interface outside (192.168.40.253): Normal (Monitored)
.....
Other host: Primary - Active
Interface diagnostic (192.168.81.1): Normal (Monitored)
Interface inside (192.168.30.254): Normal (Monitored)
Interface outside (192.168.40.254): Normal (Monitored)
```

```
>
```

show failover history

From State	To State	Reason
07:26:52 UTC Jan 22 2024 Negotiation	Cold Standby	Detected an Active peer
07:26:53 UTC Jan 22 2024 Cold Standby	App Sync	Detected an Active peer
07:28:14 UTC Jan 22 2024 App Sync	Sync Config	Detected an Active peer

07:28:18 UTC Jan 22 2024 Sync Config	Sync File System	Detected an Active peer
07:28:18 UTC Jan 22 2024 Sync File System	Bulk Sync	Detected an Active peer
07:28:33 UTC Jan 22 2024 Bulk Sync	Standby Ready	Detected an Active peer

Run debug fover <option> command to enable debug log of failover.

<#root>

>

debug fover

auth	Failover Cloud authentication
cable	Failover LAN status
cmd-exec	Failover EXEC command execution
conn	Failover Cloud connection
fail	Failover internal exception
fmsg	Failover message
ifc	Network interface status trace
open	Failover device open
rx	Failover Message receive
rxdmp	Failover recv message dump (serial console only)
rxip	IP network failover packet recv
snort	Failover NGFW mode snort processing
switch	Failover Switching status
sync	Failover config/command replication
synccount	Failover Sync Count
tx	Failover Message xmit
txdmp	Failover xmit message dump (serial console only)
txip	IP network failover packet xmit
verbose	Enable verbose logging
verify	Failover message verify

Reference

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

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