Configure High Availability on FMC

Contents

ntroduction
Prerequisites
Requirements
Components Used
Background Information
Before You Begin
Configure
Configure Secondary FMC
Configure Primary FMC
Verification

Introduction

This document describes a configuration example of High Availability (HA) on a Firewall Management Center (FMC).

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on the Secure FMC for VMware v7.2.5.

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.

Background Information

Specific requirements for this document include:

- Both FMC peers are required to be on the same software version, intrusion rule update, vulnerability database, and Lightweight Security Package
- Both FMC peers are required to have the same capacity or hardware version
- Both FMCs require a separate license

For a full set of requirements, you can visit the Administration Guide.



Warning: If there is a mismatch in the requirements listed, you cannot configure HA.

This procedure is supported on all hardware appliances.

Before You Begin

- Ensure administrator access to both FMCs
- Ensure connectivity between management interfaces
- Take a moment to review software versions and ensure that all the necessary upgrades are done

Configure

Configure Secondary FMC

Step 1. Log in to the Graphical User Interface (GUI) of the device of the FMC that is going to take the role of Secondary/Standby.



Log in to FMC

Step 2. Navigate to **Integration** tab.

Firewall Management Center Overview / Dashboards / Dashboard	Overview	Analysis Policie	s Devices	Objects	Integration	Deploy Q	📀 🌣 🕜 admin	• diali- cisco SECURE
								Reporting
Summary Dashboard (exitch dashboard) Provides a summary of activity on the appliance								
Network × Threats Intrusion Events	Status Geo	olocation QoS	+			Show the Last	1 hour	• II
								Add Widgets
 Unique Applications over Time 	$- \times$	Top Web Appli	cations Seen		$- \times$	Top Client Application	is Seen	- ×
No Data								
No Data			No Dat	ta		No	No Data	
Click here to register a device.			Click here to regis	ter a device.		Click he	ere to register a device	
Last updated 3 minutes ago		Last undated 3 minut	es ado			Last undated 3 minutes app		
			69.690					
 Traffic by Application Risk 	- ×	Top Server App	lications Seen		$-\times$	Top Operating System	ns Seen	- ×
N. 5.4								
No Data	1	1			1	1		

Navigate to integration

Step 3. Click Other Integrations.

Integration	Deploy	Q 🥝 🔅 🕜 admin 🔻 🖞	
SecureX Security Analytics & Lo Other Integrations AMP AMP Management Dynamic Analysis Conr	gging	Incidents Sources Elements Settings	-

Navigate to Other Integration

Step 4. Navigate to the High Availability tab.

Firewall Integration /	Managen Other Integra	nent Center ations / Cloud Services	Overview	Analysis	Policies	Devices	Objects	Integration
Cloud Services	Realms	Identity Sources	High Availability	eStreamer	Host Input	Client	Smart Software	Manager On-Prem
Navigate to High Av	vailability							

Step 5. Click Secondary.

Firewall Management Center Integration / Other Integrations / High Availability	Overview	Analysis	Policies	Devices	Objects	Integration	Deploy	۹	0	₽	🕜 admin 🕶	cisco SECURE
												Peer Manager
Cloud Services Realms Identity Sources	High Availability	eStreamer	Host Input (Client Sm	art Software N	lanager On-Prem						
Select a role for this Management Center and	specify peer detai	ls to setup hiç	gh availability	ι.								
Role For This Firewall Management Center:												
 Standalone (No High Availability) 												
O Primary												
 Secondary 												

Input information and select desired role for current FMC

Step 6. Enter information of the Primary/Active peer and click Register.

Cloud Services	Realms	Identity Sources	High Availability	eStreamer	Host Input Client	Smart Software Manager On-Prem	Peer Manager
Select a role for	this Manag	ement Center and	specify peer detail	s to setup high	h availability.		
Role For This Firew	vall Managen o High Availa	nent Center: bility)					
O Primary							
 Secondary 							
Peer Details:							
After Firewall Mana Primary Firewall M	agement Cer anagement C	ter high availability is Center Host:	configured in virtual c	r cloud environr	ment, each registered	Firewall Threat Defense consumes an additional Firepower MCv Device license.	
Registration Key*:							
cisco123							
Unique NAT ID:							
Register † Either host or NAT I	D is required.						



Note: Take note of the registration key, since it is going to be used on the active FMC.

Warning

This operation may affect critical processes running in the background. Do you want to continue?





Note: Ensure there is no other task running as while HA is being created, the GUI restarts.

Step 8. Confirm that you want to register the primary peer.





Warning: All information on the Devices/Policy/Configuration is going to get removed from Secondary FMC once HA is created.

Step 9. Verify that the Secondary FMC status is pending.

[Firewall I Integration /	Managem Other Integra	tions / Peer Manager	Overview	Analysis	Policies	Devices	Objects	Integration	Deploy	Q	0	¢	Ø admin ▼	cisco SEC	CURE
	Cloud Services	Realms	Identity Sources	High Availability	eStreamer	Host Inp	ut Client	Smart Softwar	e Manager On-Prem							
	Host		Last Modif	hed			s	itatus				S	tate			
	10.18.19.31		2023-09-	28 13:53:56			P	ending Registratio	n			•			/	Ť.

Configure Primary FMC

Repeat Steps 1 - 4 on the Primary/Active FMC.

Step 5. Click **Primary**.

Firewall Manage	ment Center rations / High Availability	Overview	Analysis	Policies	Devices	Objects	Integration	Deploy	۹ (0	🕜 admin 🔻	cisco SECURE
Cloud Services Realms	Identity Sources	High Availability	eStreamer	Host Input Cl	lient Sn	nart Software M	Manager On-Prem					Peer Manager
Select a role for this Mana	gement Center and	specify peer detai	ls to setup hig	ah availability.								
Role For This Firewall Manage	ment Center: ability)											
 Primary Secondary 												
Peer Details:												
Configure the secondary Man After Firewall Management Co Secondary Firewall Managem	agement Center with de Inter high availability is o ent Center Host:	etails of the primary t configured in virtual	pefore registrati or cloud enviror	on. Iment, each reg	gistered Fire	wall Threat Def	ense consumes an a	dditional Fire	power M	Cv Devic	e license.	
Registration Key*:												
Unique NAT ID:												
Register † Either host or NAT ID is required.												

Step 6. Enter the information about Secondary FMC and click **Register**.

							Peer Manager
Cloud Services	Realms	Identity Sources	High Availability	eStreamer	Host Input Client	Smart Software Manager On-Prem	
Select a role for	this Manaç	gement Center and	specify peer detai	ls to setup hig	h availability.		
Role For This Firev	vall Manager o High Availa	nent Center: ibility)					
Primary							
Secondary							
Peer Details:							
Configure the sec After Firewall Man Secondary Firewa	ondary Mana agement Cer II Manageme	gement Center with d nter high availability is nt Center Host:	etails of the primary l configured in virtual	pefore registration or cloud environ	on. ment, each registered	Firewall Threat Defense consumes an additional Firepower MCv Device license.	
10.18.19.32							
Registration Key*:							
cisco123							
Unique NAT ID:							
Register † Either host or NAT	ID is required.						



Note: Use the same Registration Key used as Secondary FMC.

Step 7. This warning asks you to confirm, click Yes.

Warning

This operation may affect critical processes running in the background. Do you want to continue?





Note: Ensure there is no other task running.

Step 8. Confirm that you want to register for Secondary FMC.

Warning

Secondary peer configuration and policies will be removed. After Firewall Management Center high availability is configured in virtual or cloud environment, each registered Firewall Threat Defense consumes an additional Firepower MCv Device license. Do you want to register secondary peer: 10.18.19.32?





Note: Ensure there is no critical information on the Secondary FMC, as accepting this prompt removes all the configurations from the FMC.

Synchronization between Primary and Secondary starts; the duration depends on configuration and devices. This process can be monitored from both units.

F In	irewall Ma itegration / Oti	anagem ther Integra	tions / High Availabili	Overview	Analysis	Policies	Devices	Objects	Integration	Deploy	۹ (¢	admin	diale SECURE
														Peer Manager
Cloud Se	ervices R	Realms	Identity Sources	High Availability	eStreamer	Host Input	t Client Sr	nart Software I	Manager On-Prem					
								5	Switch Peer Roles	∰ E	reak HA		II Pause S	ynchronization
			High a These Databa	vailability operations ar operations include file ise files synchronizatio	e in progress. Th copy which may n: 100% of 379M	e status messa take time to co B transferred	ages and alerts omplete.	on this page are	a temporary. Please cl	heck after high	availabili	ty operat	tions are compl	ete. ×
1.1	Summary	1					S	ystem Statu	S					
	Status		🔺 Temporarily	/ degraded- high ava	ilability operatio F	ons are in progress.			Acti	Local ve - Primary 0.18.19.31)		Stan	Remote dby - Seconda (10.18.19.32)	ary
	Synchroniza	ation			4	A Failed	0	perating Syste	m	7.2.5			7.2.5	
	Active Syste	em			10.1	18.19.31	S	oftware Version	n	7.2.5-208			7.2.5-208	
	Standby Sys	rstem			10.1	18.19.32	Μ	lodel	Secure Fi Cent	rewall Manage er for VMware	ment	S Mana	Secure Firewall agement Cente VMware	r for



Note: While synchronization is taking place, expect to see the status as **Failed** and **Temporary degraded**. This status shows until the process is completed.

Verification

Once the synchronization is completed, the expected output is Status **Healthy** and Synchronization **OK**.

Firewall Management Center Integration / Other Integrations / High Availability	Overview	Analysis Po	olicies Devices	Objects	Integration	Deploy	۹ (¢ 0	admin 🔻	cisco SECURI
Cloud Services Realms Identity Sources	High Availability	eStreamer Ho	ost Input Client	Smart Software N	lanager On-Prem					Peer Manager
				\$	Switch Peer Roles	é B	reak HA		Pause Syr	nchronization
Summary			5	System Status	S					
Status		📀 Hea	Ithy		Active	.ocal		Rei Standby -	mote	DV.
Synchronization		0	OK		(10.	18.19.31)		(10.1	8.19.32)	y
Active System		10.18.19	.31	Operating System	n	7.2.5		7	.2.5	
Standby System		10.18.19	.32	Software Version	7.2	2.5-208		7.2	5-208	
				Model	Secure Firev Center	vall Manage for VMware	ment	Secure Manageme VN	e Firewall ent Center Iware	for

The Primary and Secondary keep synchronizing; this is normal.

Firewall Management Center Integration / Other Integrations / High Availability	Devices Integration		٩ (☆
Cloud Services High Availability eStreamer	Host Input Client			Peer Manager
		🕏 Swit	ch Peer Roles 🛛 🐠 Break HA	II Pause Synchronization
Summary		System Status		
Status	Synchronization task is in progress		Local Standby - Secondary	Remote
Synchronization	📀 ОК		(10.18.19.32)	(10.18.19.31)
Active System	10.18.19.31	Operating System	7.2.5	7.2.5
Standby System	10.18.19.32	Software Version	7.2.5-208	7.2.5-208
		Model	Secure Firewall Management Center for VMware	Secure Firewall Management Center for VMware

Take a moment to review that your devices are showing correctly on both Primary and Secondary.