Migración de un FTD de un FMC a otro FMC

Contenido

Introducción	
Prerequisites	
Requirements	
Componentes Utilizados	
Antecedentes	
<u>Configurar</u>	
Configuraciones	
Verificación	
Troubleshoot	
Información Relacionada	

Introducción

Este documento describe cómo migrar un dispositivo Cisco Firepower Threat Defense (FTD) entre Firepower Management Centers.

Prerequisites

Antes de iniciar el proceso de migración, asegúrese de que se cumplen estos requisitos previos:

- Acceso a los CSP de origen y de destino.
- Credenciales administrativas para los CSP y el FTD.
- Realice una copia de seguridad de la configuración de FMC actual.
- Asegúrese de que los dispositivos FTD que ejecutan una versión de software compatible con el FMC de destino.
- Asegúrese de que el CSP de destino tiene la misma versión que el de origen.

Requirements

- Ambos CSP deben ejecutar versiones de software compatibles.
- Conectividad de red entre el dispositivo FTD y ambos CSP.
- Almacenamiento y recursos adecuados en el CSP de destino para alojar el dispositivo FTD.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

Cisco Firepower Threat Defense Virtual (FTDv) versión 7.2.5

Firepower Management Center Virtual (FMCv) versión 7.2.5

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

La migración de un dispositivo FTD de un FMC a otro implica varios pasos, incluidos la anulación del registro del dispositivo del FMC de origen, la preparación del FMC de destino y el nuevo registro del dispositivo. Este proceso garantiza que todas las políticas y configuraciones se transfieren y aplican correctamente.

Configurar

Configuraciones

1. Inicie sesión en el FMC de origen.

cisco SECURE
Secure Firewall Management Center
Username I Password Log In

2. Navegue hasta Devices > Device Management y seleccione el dispositivo que desea migrar.

Firewall Management Center Devices / Device Management		Overview	Analysis	Policies	Devices	Objects	Integrat	ion	
View By: All (1)	Group • • Error (0) • Warning (0)	Offline (0)	Normal (1)	 Deploymer 	nt Pending (0)	 Upgrad 	de (0)	 Snort 3 (1) 	
Collapse	All								
	Name			Model		Versi	on	Chassis	
□ ~	Ungrouped (1)								
	9 192.168.15.31 Snort 3 192.168.15.31 - Routed			FTDv for VMw	are	7.2.5		N/A	

3. En la sección de dispositivos, navegue hasta el dispositivo y haga clic en exportar para exportar su configuración de dispositivo.

FTD1									
Cisco Firepower Threat Defense for VMware									
Device	Routing	Interfaces	Inline Sets	DHCP	VTEP				
_									
Gener	al					/±∓			
Name:						FTD1			
Transfe	er Packets:					Yes			
Mode:						Routed			
Compli	iance Mode:					None			
TLS Cr	ypto Accelera	ition:				Disabled			
Device	Configuration	c		Import	Export	Download			
						•			

4. Una vez exportada la configuración, debe descargarla.





Nota: el archivo descargado debe contener la extensión .SFO y contiene información de

configuración del dispositivo como direcciones IP, zonas de seguridad, rutas estáticas y otros ajustes del dispositivo.

5. Debe exportar las políticas asociadas al dispositivo, navegar hasta System > Tools > Import/Export, seleccionar las políticas que desea exportar y hacer clic en export.

Deploy	Q 📀 🌣 🔞 adr	min • cisco SECURE
Configuration	Health	Monitoring
Users	Monitor	Audit
Domains	Policy	Syslog
Updates	Events	Statistics
	Exclude	
Licenses	Monitor Alerts	Tools
Smart Licenses		Backup/Restore
Classic Licenses		Scheduling
		Import/Export
		Data Purge

\checkmark Access Control Policy	
test	Access Control Policy
> Contextual Cross-launch	
> Custom Table View	
> Custom Workflow	
> Dashboard	
> Health Policy	
\checkmark NAT Threat Defense	
NAT NAT	NAT Threat Defense
\sim Platform Settings Threat Def	ense
🗹 test	Platform Settings Threat Defense
> Report Template	
Export	



Nota: Asegúrese de que el archivo .SFO se ha descargado correctamente. La descarga se realiza automáticamente después de hacer clic en Export (Exportar). Este archivo contiene las políticas de control de acceso, la configuración de la plataforma, las políticas NAT y otras políticas que son indispensables para la migración, ya que no se exportan junto con la configuración del dispositivo y deben cargarse manualmente en el FMC de destino.

6. Anule el registro del dispositivo FTD en el FMC, navegue hasta Devices > Device management, haga clic en los tres puntos verticales en el lado derecho y seleccione delete.

þ	Firewall Management Center Overview Analysis	Policies Devices Obje	ects Integra	tion		Deploy Q 💕	🗘 🙆 ad	min • deade- SECU	RE
View	ly: Group -							Deployment History	
Collag	(1) • Error (0) • Warning (0) • Offline (0) • Normal (1) ve All	 Deployment Pending (1) 	Upgrade (0)	 Snort 3 (1) 			Q, Search D	avice Add	
	Namo	Model	Version	Chassis	Licenses	Access Control Policy	Auto Roll	Back	
	Ungrouped (1)								
	© FTD1 Short 3 192.168.15.31 - Routed	FTDv for VMware	7.2.5	N/A	Base, Threat (2 more)	e test	4D	/ Delete	:
								Packet Tracer Packet Capture Revert Upgrade Health Monitor Troubleshoot File	15

- 7. Preparar el CSP de destino:
 - Inicie sesión en el FMC de destino.
 - Asegúrese de que el FMC está listo para aceptar el nuevo dispositivo importando las políticas de FMC de origen que descargó en el paso 5. Navegue hasta System > Tools > Import/Export y haga clic en upload package. Cargue el archivo que desea importar y haga clic en cargar.

	Upload Package						
Firewall Management Center System / Tools / Upload Package	Overview	Analysis	Policies	Devices	Objects	Integration	
Package Name Upload Cancel			Choos	e File ObjectExp	ort4235208.sfo		

8. Seleccione las políticas que desea importar en el FMC de destino.

∼ Ac	cess Control Policy
\checkmark	test
νHe	alth Policy
	Initial_Health_Policy 2024-09-29 18:25:54 Initial Health Policy
\sim N/	AT Threat Defense
\checkmark	NAT
	atform Settings Threat Defense
\checkmark	test
Imp	ort Cancel

9. En el manifiesto de importación, seleccione una zona de seguridad o cree una nueva para asignarla al objeto de interfaz y haga clic en importar.

Import Manifest		
Network and Port objects will be reused if name and content matches with existing objects, in all other cases objects with duplicate names appended to the name.	are imported as new objects with	a number
test (Access Control Policy)		
Initial_Health_Policy 2024-09-29 18:25:54 (Health Policy)		
NAT (NAT Threat Defense)		
test (Platform Settings Threat Defense)		
V Interface Objects		
dmz1 (Routed) ▼ Access Control Policy: test		
Access Control Policy Rule: allowhttps (Source Zone) Access Control Policy Rule: allowssh (Source Zone)		
NAT Policy: NAT	Security Zones	Select
NAT Policy Rule ID: # (Source Zone)		New
		45
labs (Routed) >	Security Zones	Select
Import Cancel		

- 10. Registrar el FTD en el CSP de destino:
 - En el FMC de destino, navegue hasta la pestaña Device > Management y seleccione Add > Device.
 - Complete el proceso de registro respondiendo a las indicaciones.

Q Search Devic	ce Add 🔻
	Device
	High Availability
Auto RollI	Cluster
	Group

Add Device				0
CDO Managed Device	,			
Hoste				
1				
Display Name:				
Registration Key:*				
Group:				
None	٠			
Access Control Policy:*				
	*			
Note: All virtual Firewall T Make sure your Smart Lic It's important to choose t Click here for information Until you choose a tier, yo	hreat Defens ensing accor he tier that m about the Fi our Firewall T	e devices require a unt contains the ava atches the license rewall Threat Defen hreat Defense virtue	performance tier licens ilable licenses you neer you have in your accour se performance-tiered al defaults to the FTDv5	se. d. nt. licensing. i0 selection.
Performance Tier (only fo	r Firewall The	reat Defense virtual	7.0 and above):	
Select a recommended	Tier +			
Malware				
Threat				
URL Filtering				
Advanced				
Unique NAT ID:+				
Transfer Packets				
Either host or NAT ID is	equired.		Cancel	

Para obtener más información, consulte la Guía de configuración de Firepower Management Center, <u>Agregar dispositivos a Firepower Management Center</u>

11. Vaya a Device > Device Management > select the FTD > Device y haga clic en import. Aparecerá una advertencia en la que se le solicitará que confirme la sustitución de la configuración del dispositivo. Haga clic en yes (sí).

FTI	D1							
Cisco	o Firepow	ver Threat D	efense for VMv	vare				
De	evice	Routing	Interfaces	Inline Sets	DHCP	VTEP		
_								
(Genera	1				∕±∓		
	Name:					FTD1		
	Transfer Packets:			Yes				
	Mode:			Routed				
	Compliance Mode:			None				
	TLS Cryp	oto Accelera	ition:			Disabled		
	Device C	Configuration	:	Imp	port Export	Download		



12. Seleccione el archivo de configuración de importación, que debe tener la extensión .SFO, haga clic en cargar y aparecerá un mensaje que indica que la importación se ha iniciado.

						20
C > Downloads			~ Ö	Search Dov	inloads	,p
					- EE •	0
Name	Date modified	Туре	Size			
Yesterday (4)						
ObjectExport_20241014235208.sfo	10/14/2024 7:51 PM	SFO File		177 KB		
exportconfig.sfo	10/14/2024 7:46 PM	SFO File		23 KB		
DeviceExport-9fd9088e-7d04-11ef-a474	10/14/2024 7:18 PM	SFO File		23 KB		
DeviceExport-bea34c00-8a80-11ef-88c6	10/14/2024 7:08 PM	SFO File		24 KB		

e exportconfig.sfo	~	All Files	~
		Open	Cancel



13. Por último, se muestra una alerta y se genera un informe automáticamente cuando finaliza la importación, lo que permite revisar los objetos y políticas que se han importado.



Configuration Import Summary

Initiated by: Initiated at: Tue Oct 15 00:40:18 2024

Policies

Policies imported: 3

Туре	Name
PG.PLATFORM.AutomaticApplicationBypassPage	.9fd9088e-7d04-11ef-a474- e9a89b197c24PG.PLATFORM.AutomaticApplicationBypassPage
PG.PLATFORM.PixInterface	.9fd9088e-7d04-11ef-a474-e9a89b197c24PG.PLATFORM.PixInterface
PG.PLATFORM.NgfwInlineSetPage	.9fd9088e-7d04-11ef-a474-e9a89b197c24PG.PLATFORM.NgfwInlineSetPage

Verificación

Después de completar la migración, verifique que el dispositivo FTD esté registrado correctamente y funcione correctamente con el FMC de destino:

- Compruebe el estado del dispositivo en el FMC de destino.
- Asegúrese de que todas las directivas y configuraciones se aplican correctamente.
- Realice una prueba para confirmar que el dispositivo está operativo.

Troubleshoot

Si experimenta algún problema durante el proceso de migración, tenga en cuenta los siguientes pasos para la solución de problemas:

- Verifique la conectividad de red entre el dispositivo FTD y ambos FMC.
- Asegúrese de que la versión del software en ambos CSP es la misma.
- Compruebe las alertas de ambos CSP en busca de mensajes de error o advertencias.

Información Relacionada

- Guía de administración de Cisco Secure Firewall Management Center
- Configuración, verificación y resolución de problemas del registro de dispositivos Firepower

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).