Implante um FMC fornecido em nuvem (cdFMC) no Cisco Defense Orchestrator (CDO)

Contents

Introduction Prerequisites Requirements Componentes Utilizados Informações de Apoio Configurar Implante um Firepower Management Center fornecido em nuvem no CDO. Integrar um FTD em um FMC oferecido em nuvem Informações Relacionadas

Introduction

Este documento descreve o processo de implantação e integração do FMC fornecido em nuvem na plataforma CDO.

Prerequisites

Requirements

A Cisco recomenda o conhecimento destes tópicos:

- Firepower Management Center fornecido em nuvem (cdFMC)
- Cisco Defense Orchestrator (CDO)
- Defesa contra ameaças do Firepower Virtual (FTDv)

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- cdFMC 7.2.0
- FTDv 7.2.0

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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

O Cisco Defense Orchestrator (CDO) é a plataforma para o Firewall Management Center (cdFMC) fornecido em nuvem. O Firewall Management Center fornecido em nuvem é um produto

de software como serviço (SaaS) que gerencia dispositivos Secure Firewall Threat Defense. Ele oferece muitas das mesmas funções que um Secure Firewall Secure Firewall Secure Firewall Threat Defense local. Ele tem a mesma aparência e comportamento de um Secure Firewall Management Center local e usa a mesma API (Application Programming Interface, interface de programação de aplicativos) do FMC.

Este produto foi projetado para migração dos Secure Firewall Management Centers locais para a versão Secure Firewall Management Center SaaS.

Configurar

Implante um Firepower Management Center fornecido em nuvem no CDO.

Essas imagens mostram o processo de configuração inicial necessário para implantar um FMC fornecido em nuvem no CDO.

Primeiro, navegue até Menu > Inventory para adicionar um novo dispositivo.



Selecionar Firepower Threat Defense (FTD).

crisce Defense Orchestrator	Onboarding				Q	۵.	⊯	• (cmonterr_cdo cmonterr@cisco.com
Hide Menu	What would you like to onboard?								Cancel
Inventory		S.	alact a Davice or Service Tur	20					
Configuration		0.	clear a bevice of bervice Typ						
Policies >				r Ba					
Objects			_						
₀ð₀ VPN →		Adaptive Security Appliance	Adaptive Security Appliance	Firepower Management Center					
Events & Monitoring		(8.4+)	(8.4+)	(6.4+)					
√r Analytics →		(Process)	1	Moraki					
Change Log				WEIGKI					
📥 Jobs		FTD Firepower Threat Defense	SFCN Secure Firewall Cloud Native	Meraki Meraki Security Appliance					
😤 Tools & Services >	l								
Settings			VPC	Umbrella					
		Integrations	AWS VPC	Umbrella Organization					
		Enable basic CDO functionality for	Amazon Virtual Private Cloud	View Umbrella Organization Policies					
		Import Import configuration for offline							
		management							

Selecionar Request FMC para solicitar o Firepower Management Center fornecido pela nuvem.

cisco Defense Orchestrator	Onboard FTD Device	Q	٥.	⇔	•	cmonterr_cdo cmonterr@cisco.com
⊟ Hide Menu	Follow the steps below		Cancel			
Inventory						
Configuration	Cloud-Delivered Firewall Management Center now available!					
Policies >	Cisco Defense Orchestrator now provides many of the features and functions available to Secure Firewall Management Center customers.					
Objects	Request FMC			J		
-å-v₽N →						
Events & Monitoring						
√- Analytics →						
Change Log						
📥 Jobs						
X Tools & Services >						

Observação: a opção "Solicitar FMC" será apresentada somente se você não tiver nenhum cdFMC no espaço.

Navegue até Menu > Tools & Services > Firewall Management Center quando o cdFMC estiver pronto para uso.



Selecione o cdFMC desejado para exibir as informações do cdFMC.

CISCO Defense Orchestrator	Firewall Management Center				Q Q. 🖄	(?) ▼ cmonterr_cdo ↓ cmonterr@cisco.com ▼
⊟ Hide Menu						0
Inventory	Name	SFCN Devices	Devices	Status	Last Heartbeat	
Configuration	Firewall Management Center	⇔ 0	⊖ 0	Active	13:40:18 08/26/2022	
Policies >						
Objects >						
•Å• VPN →						
√r Analytics >						
Change Log						
di Jobs						
🛠 Tools & Services 💦 💡						

Para acessar a interface gráfica do usuário (GUI) do cdFMC, selecione qualquer uma das opções disponíveis no lado direito.

Firewall Management Center					Q	۵.	4	?•	cmonterr_cdo cmonterr@cisco.com
				c	•	Firewa	II Mana	gement	Center p.us.cdo.cisco.com
Name	SFCN Devices	Devices	Status	Last Heartbeat		Software V	ersion 7.2.0	0-build 10364	4
Firewall Management Center	⊕ 0	⊕ 0	Active	13:40:18 08/26/2022		Actions			
						Dep Dep Upd Wor API Managem Obj -: NAT Settings Con	koyment lates kflows Explorer ent cles ects figuration		
						AMI	ert License P Managen	s nent	
						illa Aud Cisc	it co Cloud E	vents	

Agora você pode ver a GUI do cdFMC.

Defense Orchesti FMC / System / Health /	rator Analysis	Policies D	Devices Objects	Integration	👈 Return Home Deploy Q 🗳 🌣 🚱 Im	atuscl@cisco.com • diada SECURE
Monitoring ⇒ Home → Devices (1) ● FTDv	Health Status 1 total 0 critical Devices ••••••••••••••••••••••••••••••••••••	0 warnings 1 i	normal 0 disabled	Q. Filter using device name		
	Device			Version	Model	
	> © FTDv			7.2.0	Cisco Firepower Threat Defense for Azure	

Integrar um FTD em um FMC oferecido em nuvem

Essas imagens mostram como integrar um FTD para ser registrado em um cdFMC com a chave de registro da Interface de Linha de Comando (CLI).

Primeiro, selecione Onboard an FTD na página inicial do CDO.



Em seguida, selecione a opção Use CLI Registration Key opção.



Continue para inserir as informações de FTDv solicitadas e desejadas.

1 Device Name	FTDv			Edit
2 Policy Assignment	Access Control Policy: Default A	Access Control Policy		Edit
3 Subscription License	 Please indicate if this FTD is physic Physical FTD Device Virtual FTD Device Performance Tier (FTDv 7.0 and FTDv100 - Tiered (16 core 	cal or virtual: d above only) / 32 GB) v	 Enable subscription licenses. CDO will attempt to e the selected licenses when the device is connected CDO and registered with the supplied Smart Licens Learn more about Cisco Smart Accounts. Note: All virtual FTDs require performance tier licen Make sure your subscription licensing account continues. 	to e.
	License Type Base License	Includes Base Firewall Capabilities	the available licenses you need. Its important to che the tier that matches the license you have in your account. Until you choose a tier, your FTDv defaults FTDv50 selection.	to
	Malware	 Intrusion Policy File Policy 		
	RA VPN VPNOnly -	URL Reputation		
	Next			

Por fim, o cdFMC cria um cLI ĸeyChave CLI do dispositivo.



Copie o CLI Key na CLI do dispositivo gerenciado.

> configure manager add cm qsukd2nDTn 6qDJQJAyKn53d0T File HA_STATE is not found	onterr-cdo.app.us.cdo.cisco.com NaRZpWdiG4waNYJMQVAxdK nEifT0XF5nseZ43pd cmonterr-cdo.app.us.cdo.cisco.com
Manager cmonterr-cdo.app.u	s.cdo.cisco.com successfully configured.
Please make note of reg_ke	y as this will be required while adding Device in FMC.
>	
> show managers	
Туре	: Manager
Host	: cmonterr-cdo.app.us.cdo.cisco.com
Display name	: cmonterr-cdo.app.us.cdo.cisco.com
Identifier	: 6qDJQJAyKn53d0TnEifT0XF5nseZ43pd
Registration	: Pending

O cdFMC inicia uma tarefa de registro.

crico Defense Orchestrator	Inventory			Q Q - 🖽	· cmonterr_cdo cmonterr@cisco.com
Hide Menu	T Devices Templates Q Search by Device Name, IP Address, or Serial Number		Displaying 1 of 1 results C 🐵 🛨	> FTDv @	
inventory	All FTD			Device Details	
Configuration	Namo 0	Configuration Status ©	Connectivity 0	Location	n/a
Poncies	FTDv FTD	-	 Onboarding 	Serial Version	n/a n/a
Objects >				Onboarding Method	Registration Key
-& VPN >				C Registration Pe	ording
Analytics				Waiting for Device onboarding process	Registration to start. Please complete the s by executing the following registration
Channe Lon				command on the d your FTD can conn	evice (ignore if already done). Make sure ect to cmonterr-cdo.app.us.cdo.cisco.com.
(*)				configure ma	nager add cmonterr-cdo.a_ 🕗
				Device Actions	
X Tools & Services >				El Workflows	
敎 Settings >				Monitoring	÷
				Device Managemer	nt ~
				Policies	
				Objects	
				Label Groups and L	abels ~
				Add Labels 🚱	
				Add label groups	and labels +

Observação: certifique-se de que o dispositivo FTD tenha comunicação nas portas 8305 (sftunnel) e 443 com o locatário CDO para concluir o processo de registro. Consulte todos os <u>requisitos de rede</u>.

Observação: se você não conseguir se conectar ao host, poderá retificar a configuração DNS no FTD-CLI com este comando: **configure network dns <address>**.

Para monitorar o processo de registro, navegue até Device Actions > Workflows..

Workflows				Q 4-	() - Cmonterr_cdo
 Return to Inventory 					
FTDv (FTD)					C 🖲
Name	Priority	Condition	Current State	Last Active	Time
fmceRegisterFtdStateMachine	On Demand	Done	Done	8/30/2022, 3:35:50 PM	8/30/2022, 3:33:11 PM / 8/30/2022, 3:35:50 PM
ftdcOnboardingStateMachine	On Demand	Done	Done	8/30/2022, 3:32:50 PM	8/30/2022, 3:32:50 PM / 8/30/2022, 3:32:50 PM

Expanda a Active para obter informações adicionais, essas imagens mostram como o FTDv foi registrado com êxito.

a lauranteau							
o Inventory Dv (FTD)							c
me	Priority	Condition	Current State	Last Active		Time	
CTION	TIME	START STATE	END STATE		RESULT		
ollingDelayedCheckAction	15:34:46.812 / 15:34:46.819	POLLING_WAIT_BEFORE_CHECK_I	EGISTER_FTD @INITIATE_GET_TASK_ST	ATUS	SUCCESS		
mcRequestGetAction	15:35:17.324 / 15:35:17.724	INITIATE_GET_TASK_STATUS	WAIT_FOR_GET_TASK_	STATUS	SUCCESS		
mcQueryTaskStatusResponseHandler	15:35:18.223 / 15:35:18.244	AWAIT_RESPONSE_FROM_execute	FmcRequests POLLING_WAIT_BEFORE	E_CHECK_REGISTER_FTD	JOB_IN_PROGRES	s	
ollingDelayedCheckAction	15:35:18.288 / 15:35:18.299	POLLING_WAIT_BEFORE_CHECK_I	REGISTER_FTD INITIATE_GET_TASK_ST.	ATUS	SUCCESS		
incRequestGetAction	15:35:48.708 / 15:35:49.173	INITIATE_GET_TASK_STATUS	WAIT_FOR_GET_TASK_	STATUS	SUCCESS		
mcQueryTaskStatusResponseHandler	15:35:49.639 / 15:35:49.652	AWAIT_RESPONSE_FROM_execute	FmcRequests INITIATE_GET_DEVICE_F	RECORDS_REGISTER_FTD	JOB_SUCCEEDED		
mcRequestDeviceRecordsAction	15:35:49.674 / 15:35:50.084	INITIATE_GET_DEVICE_RECORDS_	REGISTER_FTD @WAIT_FOR_DEVICE_REC	CORDS_REGISTER_FTD	SUCCESS		
mceFilterDeviceResponseHandler	15:35:50.496 / 15:35:50.510	AWAIT_RESPONSE_FROM_execute	FmcRequests OONE		SUCCESS		
юок	TYPE	TIME	RESULT				
aveInitialConnectivityStateBeforeHook	Before	15:33:11.229 / 15:33:11.231	Saved Connectivity	y State to context			
IpdateSMContextWithDeviceVersionHook	Before	15:33:11.231 / 15:33:11.234	setDeviceVersionIn	SMContext			
leviceStateMachineClearErrorBeforeHook	Before	15:33:11.234 / 15:33:11.236	noErrorOccurred				
inceRegisterFtdcStatusPreHook	Before	15:33:11.236 / 15:33:11.289	Executed pre hook	successfully for FTD device: FTDv			
mceRegisterPtdcStatusHook	After	15:35:50.517 / 15:35:50.519	Executed hook suc	cessfully			
lotifyOnConnectivityStateChangeAfterHook	After	15:35:50.519 / 15:35:50.521	Notification skipper	d for this event			
IpdateSMContextWithDeviceAsaNgPolicyFlagHook	After	15:35:50.521 / 15:35:50.523	notAsaDevice				
ddDeviceNameToStateMachineDebugAfterHook	After	15:35:50.523 / 15:35:50.528	Added device nam	e to debug record			
leviceStateMachineSetErrorAfterHook	After	15:35:50.528 / 15:35:50.530	noErrorOccurred				
						8/30/2022. 3:32:50 PM / 8/	/30/20
cOnboardingStateMachine	On Demand	Done	Done	8/30/2022, 3:32:50	PM	3:32:50 PM	
Devices Templates Q Search by Devic	ce Name, IP Address, or Serial Nu	mber	Displaying 1 of 1 results	C ⊕ + >	FTDV @	a 🕂 Imatusci@cisc	xo.com
TD					Device Details		
Name \$		Configuration Status	Connectivity C	_	Location	n/a	
FTDv FTD		Q Synced	Online		Model Serial Version Onboarding Method Snort Version	Cisco Firepower Threat Defen Azure 9AGTAFW24C8 7.2.0 Registration Key 3.1.21.1-126	se for
					O Synced Your device's co Device Actions	nfiguration is up-to-date.	
					C Check for C C Manage Lic Workflows Remove	hanges enses	
					I. Hardth		
					The mean of the second		
					Device Managem Device Over Routing Interfaces	rview	

Por fim, navegue até Device Management > Device Overview para acessar o cdFMC e revisar o status de visão geral do FTDv.

Defense Orchestrator FMC / Devices / Secure Firewall Device Summar	y Analysis Policies D	evices Objects Integration		🕤 Return Home Deploy Q 💕 🔅	Imatuscl@cisco.com v sector
ETDV Cisco Firepower Threat Defense for Azure Device Routing Interfaces Inline Sets	DHCP VTEP				
General	/±∓	License	1	System	© G
Name:	FTDv	Performance Tier :	FTDv100 - Tiered (Core 16 / 32 GB)	Model:	Cisco Firepower Threat Defense for Azure
Transfer Packets:	No	Base:	Yes	Serial:	9AGTAFW24C6
Mode:	Routed	Export-Controlled Features:	No	Time:	2022-08-30 21:04:27
Compliance Mode:	None	Malware:	No	Time Zone:	UTC (UTC+0:00)
TLS Crypto Acceleration:	Disabled	Threat:	No	Version:	7.2.0
		URL Filtering:	No	Time Zone setting for Time based Rules:	UTC (UTC+0:00)
Device Configuration:	Import Export Download	AnyConnect Apex:	No		
		AnyConnect Plus:	No		
		AnyConnect VPN Only:	No		
Inspection Engine		Health		Management	/ 🔍
Inspection Engine:	Snort 3	Status:	•	Host:	NO-IP
Revent to Snort 2		Policy:	Initial_Health_Policy 2022-06-04 01:25:03	Status:	•
		Excluded:	None	Manager Access Interface:	Management Interface

Informações Relacionadas

- <u>Suporte Técnico e Documentação Cisco Systems</u>
- <u>Gerencie dispositivos de defesa contra ameaças do Cisco Secure Firewall com o Centro de</u> gerenciamento de firewall fornecido em nuvem

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.