Bereitstellung eines Cloud-gestützten FMC (cdFMC) in Cisco Defense Orchestrator (CDO)

Inhalt

Einleitung Voraussetzungen Anforderungen Verwendete Komponenten Hintergrundinformationen Konfigurieren Bereitstellung eines Cloud-basierten FirePOWER Management Center auf CDO Integration einer FTD in einem Cloud-basierten FMC Zugehörige Informationen

Einleitung

Dieses Dokument beschreibt die Bereitstellung und den integrierten Prozess von Cloud-basiertem FMC auf der CDO-Plattform.

Voraussetzungen

Anforderungen

Cisco empfiehlt, sich mit folgenden Themen vertraut zu machen:

- Cloud-fähiges FirePOWER Management Center (cdFMC)
- Cisco Defense Orchestrator (CDO)
- Firepower Threat Defense Virtual (FTDv)

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- cdFMC 7.2.0
- FTDv 7.2.0

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Hintergrundinformationen

Cisco Defense Orchestrator (CDO) ist die Plattform für das Cloud-basierte Firewall Management Center (cdFMC). Das über die Cloud bereitgestellte Firewall Management Center ist ein Softwareas-a-Service (SaaS)-Produkt, das die Verwaltung sicherer Firewall-Geräte zum Schutz vor Bedrohungen ermöglicht. Es bietet viele Funktionen wie eine sichere Firewall vor Ort und einen sicheren Schutz vor Bedrohungen durch die Firewall. Es bietet dasselbe Erscheinungsbild und Verhalten wie ein Secure Firewall Management Center vor Ort und verwendet dieselbe FMC Application Programming Interface (API).

Dieses Produkt wurde für die Migration von den lokalen Secure Firewall Management Centern zur Secure Firewall Management Center SaaS-Version entwickelt.

Konfigurieren

Bereitstellung eines Cloud-basierten FirePOWER Management Center auf CDO

Diese Bilder zeigen den anfänglichen Einrichtungsprozess, der für die Bereitstellung eines Cloudbasierten FMC auf CDO erforderlich ist.

Navigieren Sie zunächst zu Menu > Inventory um ein neues Gerät hinzuzufügen.



Auswählen Firepower Threat Defense (FTD).

cisco Defense Orchestrator	Onboarding				Q	۵.	⇔	• (?)	cmonterr_cdo cmonterr@cisco.com
	What would you like to onboard?								Cancel
Configuration		Se	lect a Device or Service Type	9					
Policies >		(MA	(maxim)	683					
Objects		asa	Multiple ASAs	On-Prom EMC					
-& VPN >		Adaptive Security Appliance (8.4+)	Adaptive Security Appliance (8.4+)	Firepower Management Center (6.4+)					
√r Analytics →			, star						
Change Log				Meraki					
📥 Jobs		FID Firepower Threat Defense	SECN Secure Firewall Cloud Native	Meraki Meraki Security Appliance					
R Tools & Services >	l								
ĝi Settings →		Integrations Enable basis CDO functionality for integrations	Amazon Virtual Private Cloud	Umbrella Umbrella Organization View Umbrella Organization Policies from CDO					
		Import Import Import configuration for offline management							

Auswählen Request FMC um das Cloud-basierte FirePOWER Management Center anzufordern.



Hinweis: Die Option "Request FMC" wird nur angezeigt, wenn im Tenant kein cdFMC vorhanden ist.

Navigieren Sie zu Menu > Tools & Services > Firewall Management Center wenn das cdFMC einsatzbereit ist.



Wählen Sie das gewünschte cdFMC, um die cdFMC-Informationen anzuzeigen.

CISCO Defense Orchestrator	Firewall Management Center				Q	۵.	⊯	•	cmonterr_cdo cmonterr@cisco.com
E Hide Menu									0
Inventory	Name	SFCN Devices	Devices	Status	Last Hearthe	eat			
Configuration	Firewall Management Center	⊖ 0	⇔ 0	Active	13:40:18 0	8/26/2022			
Policies >									
Objects >									
⊷& VPN >									
Events & Monitoring									
√r Analytics >									
Change Log									
🟥 Jobs									
🋠 Tools & Services 🔷 👌									

Um auf die grafische Benutzeroberfläche (GUI) des cdFMC zuzugreifen, wählen Sie eine der Optionen auf der rechten Seite aus.

Firewall Management Center					Q	۵.	4	• (?)	cmonterr_cdo cmonterr@cisco.com
				ø	>	Firewal Hostname	I Mana	gement	Center
Name	SFCN Devices	Devices	Status	Last Heartbeat		Software Ve	prsion 7.2.0)-build 10364	
Firewall Management Center	⊖ 0	⊕ 0	Active	13:40:18 08/26/2022		Actions			
						Dep Upd Wor API Managem Opdit Opdit Opdit Opdit Opdit Opdit Opdit Sattioge	loyment ates kflows Explorer ent cles ccts		
						♦ Con Sma ♦ AMF ♦ Devi ▲ Aud ♦ Cisc	figuration Int License Managen ice Health it it co Cloud Et	s nent vents	

Nun sehen Sie die Benutzeroberfläche von cdFMC.

Defense Orchesti FMC / System / Health /	rator Analysis Monitor	Policies Devices	Objects Integration		+> Return Home Deploy Q	🗳 🌣 🛛 Imatusci@cisco.com 🕶	tiste SECURE
Monitoring ⇒ Home → Devices (1) ● FTDv	Health Status I total O critical Devices	0 warnings 1 normal	0 disabled C. Filter using device name				Í
	Device		Ve	sion	Model		
	> O FTDV		7.3	.0	Cisco Firepower Threat Defense for Azure		

Integration einer FTD in einem Cloud-basierten FMC

Diese Bilder zeigen, wie man eine FTD einbindet, um auf einem cdFMC mit CLI-Registrierungsschlüssel registriert zu werden.

Wählen Sie zunächst Onboard an FTD auf der CDO-Startseite.



Wählen Sie anschließend die Use CLI Registration Key Option.



Fahren Sie mit der Eingabe der angeforderten und gewünschten FTDv-Informationen fort.

1 Device Name	FTDv			Ed
2 Policy Assignment	Access Control Policy: Default	Access Control Policy		Ed
3 Subscription License	Please indicate if this FTD is physical FTD Device Virtual FTD Device Performance Tier (FTDv 7.0 ai FTDv100 - Tiered (16 cor	nd above only)	 Enable subscription licenses. CDO will attempt to the selected licenses when the device is connec CDO and registered with the supplied Smart Lice Learn more about Cisco Smart Accounts. Note: All virtual FTDs require performance tier lice Make sure your subscription licensing account of 	o enable ted to ense. cense.
	License Type Base License	Includes Base Firewall Capabilities	the available licenses you need. Its important to the tier that matches the license you have in you account. Until you choose a tier, your FTDv defau FTDv50 selection.	choose r ults to
	Malware	 Intrusion Policy File Policy 		
	RA VPN VPNOnly -	URL Reputation		
	Next			
	Next			

Schließlich erstellt das cdFMC eine bestimmte CLI KeyCLI-Schlüssel für Ihr Gerät.



Kopieren Sie CLI Key in die CLI des verwalteten Geräts ein.

> configure manager add cmonterr-cdo.app.us.cdo.cisco.com NaRZpWdiG4waNYJMQVAxdK qsukd2nDTn 6qDJQJAyKn53d0TnEifT0XF5nseZ43pd cmonterr-cdo.app.us.cdo.cisco.com File HA_STATE is not found.								
Manager cmonterr-cdo.app.	us.cdo.cisco.com successfully configured.							
Please make note of reg_k	ey 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							

Das cdFMC initiiert eine Registrierungsaufgabe.

crico Defense Orchestrator	Inventory			Q Q	in -
⊟ Hide Menu	T Devices Templates Q Search by Device Name, IP Address, or Serial Number		Displaying 1 of 1 results C 🐵 +	> FTDv @	
E Inventory	AI FTD			Device Details	~
Configuration	Name 0 FTDv	Configuration Status 0	Connectivity \$	Location n/a Model n/a	
	FTD	-	O Unboarding	Version n/a Onboarding Registration Key Method	
•& VPN >				© Registration Pending	
√r Analytics →				Walting for Device Registration to start. Please complete onboarding process by executing the following registrat command on the device (ignore if already done). Make) the ion sure
Change Log				configure manager add cmonterr-cdo.ap.us.cdo.omc	R)
Jobs				Device Actions	
X Tools & Services >				Workflows	
				Monitoring	Ŷ
				Device Management	¥
				Policies	~
				Objects	×
				Label Groups and Labels	÷
				Add Labels 🛛	
				Add label groups and labels	+

Hinweis: Stellen Sie sicher, dass Ihr FTD-Gerät über die Ports 8305 (Sftunnel) und 443 mit dem CDO-Tenant kommuniziert, um den Registrierungsprozess abzuschließen. Lesen Sie die vollständigen <u>Netzwerkanforderungen</u>.

Hinweis: Wenn Sie keine Verbindung zum Host herstellen können, können Sie die DNS-Konfiguration in der FTD-CLI mit dem folgenden Befehl korrigieren: **configure network dns <Adresse>**.

Um den Registrierungsvorgang zu überwachen, navigieren Sie zu Device Actions > Workflows..

Workflows				۹ ۵.	Cmonterr_cdo
Return to Inventory					
T FIDV (FID)					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

Erweitern Sie die Active angeben, um zusätzliche Informationen zu erhalten, zeigen diese Bilder, wie die FTDv erfolgreich registriert wurde.

	rn to Imatetony					
int int int int int Solution Solution<	rn to Inventory FTDv (FTD)					c
Abde Pietro Piet	Name	Priority	Condition Current	State Last	Active	Time
1044411.0400400000000000000000000000000000000000	ACTION	TIME	START STATE	END STATE	RESULT	
minute min	PollingDelayedCheckAction	15:34:46.812 / 15:34:46.819	POLLING_WAIT_BEFORE_CHECK_REGISTER_FTC	INITIATE_GET_TASK_STATUS	success	
1010000000000000000000000000000000000	FmcRequestGetAction	15:35:17.324 / 15:35:17.724	INITIATE_GET_TASK_STATUS	WAIT_FOR_GET_TASK_STATUS	SUCCESS	
Nonlogeneration 0101201 0100000000000000000000000000000000000	FmcQueryTaskStatusResponseHandler	15:35:18.223 / 15:35:18.244	AWAIT_RESPONSE_FROM_executeFmcRequests	POLLING_WAIT_BEFORE_CHECK_REGISTE	R_FTD JOB_IN_PROG	RESS
	PollingDelayedCheckAction	15:35:18.288 / 15:35:18.299	POLLING_WAIT_BEFORE_CHECK_REGISTER_FTD	INITIATE_GET_TASK_STATUS	SUCCESS	
non-second 10344201 04004/0004/0004/0004 04007/0002/0005/0005/0005/0005/0005/0005/0	FmcRequestGetAction	15:35:48.708 / 15:35:49.173	INITIATE_GET_TASK_STATUS	WAIT_FOR_GET_TASK_STATUS	SUCCESS	
	FmcQueryTaskStatusResponseHandler	15:35:49.639 / 15:35:49.652	AWAIT_RESPONSE_FROM_executeFmcRequests	INITIATE_GET_DEVICE_RECORDS_REGISTE	R_FTD JOB_SUCCEED	DED
	FmcRequestDeviceRecordsAction	15:35:49.674 / 15:35:50.084	INITIATE_GET_DEVICE_RECORDS_REGISTER_FT	WAIT_FOR_DEVICE_RECORDS_REGISTER_	FTD SUCCESS	
ioi ioi ioi ioi Senior Senior Senior Senior Senior	FmceFilterDeviceResponseHandler	15:35:50.496 / 15:35:50.510	AWAIT_RESPONSE_FROM_executeFmcRequests	• DONE	SUCCESS	
been 6000 00 000000000000000000000000000000	ноок	TYPE	TIME	RESULT		
backdblockedebeleviskom bele 533123 / 1531133 conducation Conducation below 533123 / 1531133 conducation	SaveInitialConnectivityStateBeforeHook	Before	15:33:11.229 / 15:33:11.231	Saved Connectivity State to context		
bergen descendendendendendendendendendendendendende	UpdateSMContextWithDeviceVersionHook	Before	15:33:11.231 / 15:33:11.234	setDeviceVersionInSMContext		
inclugate/inductational Bote 102112/1/1230.123 Bote/ 102011/1250.021 Bote/ 102011/1250.	DeviceStateMachineClearErrorBeforeHook	Before	15:33:11.234 / 15:33:11.236	noErrorOccurred		
mdrageneritationarium Adre 193091711305937 Accordantationarium Adre 193091711305937 Accordantationarium Accordantationarium </td <td>FmceRegisterFtdcStatusPreHook</td> <td>Before</td> <td>15:33:11.236 / 15:33:11.289</td> <td>Executed pre hook successfully for FT</td> <td>D device: FTDv</td> <td></td>	FmceRegisterFtdcStatusPreHook	Before	15:33:11.236 / 15:33:11.289	Executed pre hook successfully for FT	D device: FTDv	
http://converting/back/darged/free/back Addr 15250.137/15250.237 Addres/ere Addres/ere Addres/ere Addres/ere Addres/ere Addres/ere Addres/ere Addres/ere Addres/ere Addres/ere Addres/ere Addres/ere Addres/ere Addres/ere Addres/ere Addres/ere Addres/ere Addres/ere Addres/ere Addres/ere Addres/ere Addres/ere Addres/ere Addre	FmceRegisterFtdcStatusHook	After	15:35:50.517 / 15:35:50.519	Executed hook successfully		
isolesticationationationationationationationation	NotifyOnConnectivityStateChangeAfterHook	After	15:35:50.519 / 15:35:50.521	Notification skipped for this event		
Add double same bid double.double Add 19.559.52/19.159.50.23/1 Add double same bid double.double Double database bid double.double same bid double.double Add Add double same bid double.com B2007022, 32.250 PM B200702, 32.250 PM	UpdateSMContextWithDeviceAsaNgPolicyFlagHook	After	15:35:50.521 / 15:35:50.523	notAsaDevice		
bedoutdevelored develored with the back to	AddDeviceNameToStateMachineDebugAfterHook	After	15:35:50.523 / 15:35:50.528	Added device name to debug record		
box <td>DeviceStateMachineSetErrorAfterHook</td> <td>After</td> <td>15:35:50.528 / 15:35:50.530</td> <td>noErrorOccurred</td> <td></td> <td></td>	DeviceStateMachineSetErrorAfterHook	After	15:35:50.528 / 15:35:50.530	noErrorOccurred		
http://bearding/State/Machine entory entory entory entory entory entory entory entory entory entory entory entory entory entory entory entory entory entory entory entory entory entory entory entory entory entory entory entory entory entory entory entory entory entory entory entory entory entory entory entory entory entory entory entory entory entory entory entory entory entory entory entory entory entory entory entory entory entory entory entory entory entory entory entory entory entory entory entory entory entory entory entory entory entory entory entory						0/00/0000 0.00.50 04 / 0/00/01
novice Tengles Bench ty Docke Rame, P. Address, et Seinel Number FD FD FD FD FD FD FD F	nocOnboardingStateMachine	 On Demand 	Done Done	8/30	/2022, 3:32:50 PM	3:32:50 PM
PD Device Details Image: Construction of the set of	Devices Templates Q Search by Dev	vice Name, IP Address, or Serial Nu	umber	Displaying 1 of 1 results	FTDv Property Prop	
kmm i i i i i i i i i i i i i i i i i i	FTD				Device Detail	S
PTDv © Synced Online Medic Carrier provem Treat Defines for Acros Sired WGATAW24C8 Weision 7.2 Obsending Registration Kay Medic Carrier provem Treat Defines for Acros Sired Washing 7.2 Medic Carrier provem Treat Defines for Acros Sired Washing 7.2 Medic Carrier provem Treat Defines for Acros Sired Washing 7.2 Medic Carrier provem Treat Defines for Acros Manage Learners Carrier provem Treat Defines for Acros Manage Learners Carrier provem Treat Defines for Acros Manage Learners Carrier provem Treat Defines for Acros Manage Learners Carrier provem Treat Defines for Acros Manage Learners Manage Learners Manage Learners Monitoring Monitoring Monitoring Manage Learners Monitoring Monitoring Monitoring Manage Learners Manage Learners Monitoring Monitoring Monitoring Manage Learners Manage Learners Monitoring Monitoring Monitoring Monitoring Manage Learners Manage Learners Monitoring <	Name +		Configuration Status ©	Connectivity ¢	Location	n/a
FD Serial is ACTAVV2CG Obboarding is Registration Kay Registration Kay Serial is activation of the series Serial is activation of the series Serial is activation of the series Serial is activation of the series Serial is activation of the series Serial is activation of the series Serial is activation of the series Serial is activation of the series Serial is activation of the series Serial is activation of the series Serial is activation of the series Serial is activation of the series Serial is activation of the series Serial is activation of the series Serial is activation of the series Series Series is a	FTDv		O Synced	Online	Model	Cisco Firepower Threat Defense for Azure
Window 2013 Window 2013	FTD				Serial	9AGTAFW24C6
Method Method Source Constructions is up-to-date. Configuration is up-to-date. Device Actions Configuration is up-to-date. Workflows Configuration is up-to-date. Method Configuration is up-to-date. Workflows Configurat. Work					Onboarding	Registration Key
Synced but denice's configuration is up-to-date: Device Actions □ Check for Changes □ Check for Changes □ Check for Changes □ Workflows □ Remove Monitoring □ Remove Monitoring □ Device Management □ Device M					Method Snort Versi	on 3.1.21.1-126
Synced vor device's configuration is up-to-date: Device Actions Check for Changes Check for Changes Check for Changes Workflows ■ Workflows ■ Remove Monitoring Monitoring Device Management ■ Device Manageme						
Image: Longe: Longe						
Device Actions Device Actions Coheck for Changes Check for Changes					O Synced	
Check for Changes Manage Licenses Wintoring Monitoring Were Name Periode Namegement Device Namegement Device Namegement Device Overview S Routing Device Overview S Routing Device Overview S Routing Device Namegement Device Na					Synced Your device	's configuration is up-to-date.
Image Lenses					O Synced Your device' Device Action	's configuration is up-to-date.
Image: Second Secon					O Synced Your device' Device Action	is configuration is up-to-date.
Monitoring Monitoring Weith Device Management ■ Device Overview S Roucing △ Interfaces ⇒ Dirther S Interfaces ⇒ Dirther ⇒ Unitor S Interfaces ⇒ Unitor ⇒					O Synced Your device Device Action O Check f O Manage El Workflor	s configuration is up-to-date. 15 or Changes Licenses ws
↓ Health Device Management □ □ Device Overview ⑤ Roucing □ Interfaces □ Interfaces □ DHCP □ VTEP					Synced Your device' Device Action Check f Manage El Workflor Remove	is configuration is up-to-date. Is or Changes Licenses vs
Device Management					Synced Your device Device Action Check fi Manage El Workfio Remove Monitoring	s configuration is up-to-date. Is or Changes Licenses ws
Device Overview Social Device Overview Device Overview Social Device Overview Device Overview Social Device Overview Social Device Overview Social Device Overview Device Overview Social Device Overview Social Device Overview Device Overview Device Overview Social Device Overview					Synced Your device Device Action Check fi Manage Workfing Remove Monitoring	s configuration is up-to-date. Is or Changes Licenses ws
Becoming Control InderSees DHCP DHCP OVEP					Synced Your device Device Action Check fi Check fi	s configuration is up-to-date. Is or Changes Licenses ws gement
C Interfaces ⊟ Inline Sets ⊟ DHCP ⊟ VTEP					Synced Your device Device Action Check fi Check fi	s configuration is up-to-date. Is or Changes Licenses ws gement Overview
					Synced Your device Device Action Check fi Check fi	s configuration is up-to-date.
					Synced Your device Device Action Check fi Manage Workflor Remove Monitoring + Health Device Manage Check fi Remove Monitoring - Remove Remove - Remove - Remove	s configuration is up-to-date.
					Synced Your device Device Action Check fi Manage Workflor Remove Monitoring + Health Device Manage Check fi Remove Check fi Check fi Remove Check fi Check fi Remove Check fi Check fi	s configuration is up-to-date.

Navigieren Sie abschließend zu Device Management > Device Overview um auf das cdFMC zuzugreifen und den FTDv-Übersichtsstatus zu überprüfen.

Defense Orchestrator FMC / Devices / Secure Firewall Device Summary	Analysis Policies D	evices Objects Integration		🕤 Return Home Deploy Q 💕 🔅	Imatuscl@cisco.com Imatuscl@cisco.com
ETDV Cisco Firepower Threat Defense for Azure Device Routing Interfaces Inline Sets	DHCP VTEP				
General	/±∓	License	/	System	0 G
Name:	FTDv	Performance Tier :	FTDv100 - Tiered (Core 16 / 32 GB)	Model: 0	Disco 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:	0	Host:	NO-IP
Revent to Short 2		Policy:	Initial_Health_Policy 2022-06-04 01:25:03	Status:	0
		Excluded:	None	Manager Access Interface:	Management Interface

Zugehörige Informationen

- Technischer Support und Dokumentation für Cisco Systeme
- Management von Cisco Secure Firewall Threat Defense-Geräten mit Cloud-basiertem Firewall-Management Center

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.