Firepower Threat Defenseからクラウド提供の Firewall Management Centerへの移行

内容			
<u>はじめに</u>			
<u>前提条件</u>			
<u>要件</u>			

はじめに

このドキュメントでは、Firepower Thread Defense(FTD)をオンプレミスFMCからクラウド配信 FMCに移行する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

クラウド提供のFirepower Management Center(cdFMC) Cisco Defense Orchestrator(CDO) セキュアなFirepower Threat Defense(FTDv) Firepower Management Center (FMC)

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアのバージョンに基づいています。

- FTD7.2.7
- cdFMC(入手可能)
- FMC 7.4.1

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始していま す。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認して ください。

背景説明

Cisco Defense Orchestratorの管理者ユーザは、バージョン7.2以降を実行しているオンプレミスの管理センターから、クラウド配信のファイアウォール管理センターに脅威防御デバイスを移行

できます。さらに、オンプレミスの管理センター1000/2500/4500からクラウド配信のファイアウ ォール管理センターにデバイスを移行できます。

移行プロセスを開始する前に、オンプレミスのManagement CenterモデルをCDO対応バージョン にアップグレードし、CDOにオンボーディングすることが重要です。この手順の後でのみ、オン プレミス管理センターに関連付けられているデバイスの移行に進むことができます。

設定

1.- OnPrem FMCのCDOテナントへのオンボード

次の図は、OnPrem FMCをCDOテナントにオンボーディングするために必要な初期セットアップ プロセスを示しています。

CDOのホームページから、 Tools & Services > Firewall Management Center. に移動します。Firepower Management Center(FMC)ページで、画面の右上に青色の追加ボタンがあることに注意して、追加ボタンを選択します。

.1 1.1 1. cisco	Defense Orchestrator		Serv	vices					C	L Search
≡	Hide Menu									_ 🗖
	Dashboard	(Q	Search by Device Name, IP A	Address, or Serial Num	nber				2 +
\bigcirc	Multicloud Defense		FMC	Secure Connectors						
	Inventory		•	Name		Version	Devices	Туре	Status	Last Heartbeat
Conf	figuration			Cloud-Delivered FMC		20240307	⊜1	Cloud-Delivered FMC	 Active 	05/14/2024, 15:00:10
٢	Policies	>								
\odot	Objects	>								
<u>ە</u>	VPN	>								
Ever	nts & Monitoring									
	Analytics	>								
٩	Change Log									
(<u>*</u>)	Jobs									
*	Tools & Services	>								
 	Settings	>								

画像 1.Firepower Management Center(FMC)ページ

Firewall Management Centerを選択します。

cisco	Defense Orchestrato	r Services				Q Search	⊳ ••	۵. و	<u>⊾</u> ?•
≡	Hide Menu								
	Dashboard		What would you like to on	board?				Cancel	
\bigcirc	Multicloud Defense								
	Inventory				Select a Service				
Conf	iguration			A	⇔	→ ←			
٢	Policies	·		<u> </u>	$\square \rightarrow$	···· →			
\otimes	Objects	>		Firewall Management Center	Secure Event Connector	Secure Device Connector			
•Å•	VPN	>		FMC	SEC	SDC			
Even	ts & Monitoring								
\mathcal{N}	Analytics	>							
٩	Change Log								
(*)	Jobs								
R	Tools & Services	>							
{\$}	Settings	>							



Use Credentialsを選択します。

cisco Defense Orchestra	tor Services			Q Search	¢ 7 -	¢- e	h (?∙
Hide Menu		Follow the steps below				Cancel	
C Multicloud Defense							
Configuration			Discover From SecureX	Generation Use Credentials			
Policies	•		Account Auto-discovery of On-Prem FMCs	Onboarding a device using an IP address or host name and a username and nassword (Version 6.4+)			
Objects	>	Firewall Management Center	from SecureX tenant	ana pasana a (renami a.e.)			
•ð• VPN Events & Monitoring	>	Center					
√ Analytics	>						
Change Log							
📥 Jobs							
Tools & Services	>						
251 onrenilla							

画像 3.FMCをオンボードするさまざまな方法。

CDOインベントリに表示できるように、FMCに名前を付けます。

CDOがオンボードプロセスの接続を確立できるように、正しいGUIポートを使用してFMCのIPアドレス、ホスト名、または FQDNを入力します。

esco Defense Orchestrator Services		Q Search 🖙 - 🖧 - 📥 😗
Hide Menu Aboard	Follow the steps below	Cancel
C Multicloud Defense		
Configuration		
(a) Policies >		Account Onboarding a device using an IP Auto-discovery of On-Prem FMCs address or host name and a username
Objects >	Firewall Management Cer	from SecureX tenant and password (Version 8.4+)
eås VPN →	Cisco Secure Firewall Manager Center	nent
Events & Monitoring	O Design Datalia	
√ Analytics >	Device Details	(Version 6.4+)
Change Log		Select Secure Device Connector
(+) Jobs		≓Cloud Connector
R Tools & Services		Device Name
谷 Settings >		MyFMC
r04		
		Next

図 4.FMCの情報。

デバイスの資格情報を入力します。

cisco	Defense Orchestrati	or Services				Q Search	¢ 7 -	¢- e	4 0·
≡	Hide Menu								
	Dashboard		Follow the steps below					Cancel	
0	Multicloud Defense								
	Inventory		a Ha						
Conf	liguration			Discove	r From SecureX Account	Use Credentials			
6	Policies	>	(Auto-discov	ery of On-Prem FMCs	address or host name and a username and password (Version 6.4+)			
¢	Objects	>	Firewall Management C	enter	Securex tenant				
۰Å۰	VPN	>	Cisco Secure Firewall Manag Center	ement					
Even	its & Monitoring		2 Credentials	We recommend	creating a new On-Prem	EMC user with a system-provided Ar	Iministrator usar role or a		
<i></i> ≁	Analytics	>		custom user rol	e with "Devices" and "Sy	stem" permissions for the sole purpos	e of onboarding. If you onboard		
٩	Change Log			onboarding fails Note: Please or	5. Secure the user has Admin	istrator role if you are onboarding this	On-Prom EMC for migrating		
(*)	Jobs			FTDs to Cloud.	sure the user has normal	strator role in you are oncoarding this	on real rise for highering		
R	Tools & Services	>		A Refore proceeding, pl	ease download the certil	ficate and verify that it is authentic			
{\$}	Settings	>		This prevents your crede	entials from being redirect	ted to a third party.			
				Username					
				Username]	
				Password					
				Password				J	
				Next					

図 5.FMCクレデンシャル。

この時点で、オンボーディングプロセスが開始されます。プロセスGo To Services を表示する場合に選択します。

cisco Defense Orcher	strator Services				Q Search	>→- ↔- ₩	?
Hide Menu							
Lashboard		Follow the steps below				Cancel	
C Multicloud Defense							
Inventory		هي الح					
Configuration				Discover From SecureX	Use Credentials		
Policies	>			Account Auto-discovery of On-Prem FMCs	Onboarding a device using an IP address or host name and a username		
Objects	>	Eirourall Management C	Cantar	from SecureX tenant	and password (Version 6.4+)		
₀å₀ VPN	>	Cisco Secure Firewall Manag Center	pement				
Events & Monitoring							
√- Analytics	>	1 Device Details	Name: My	FMC, Location:			
(Change Log		2 Credentials	Successfu	ully connected to MyFMC at 2	_		
(+) Jobs		0					
🛞 Tools & Services	i >	3 Done	O This ma	vice is now onboarding. ay take a long time to finish. You can check th	e status of the device on the Devices and S	ervices page.	
{ô} Settings	>		Add Lab	els 😧		+	
			Go To	Services			

図 6.オンボーディングプロセスを開始する

ステータスが syncedになったら、オンボーディングプロセスは完了です。

Hide Menu								>	MyFMC @		
Dashboard	Q	Search by Device Name, IP Address, or Serial Num	nber				e 🛨		On-Prem FMC	3 🕼	
Multicloud Defense	FMC	Secure Connectors							Device Details		Y
Inventory		Name	Version	Devices	Туре	Status	Last Heartbeat		Location Version Geo Version	3 7.4.1-build 172 None	
Configuration		Cloud-Delivered FMC	20240307	⊜1	Cloud-Delivered FMC	S Active	05/14/2024, 15:30:10		VDB Version	384	
Policies >		MyFMC	7.4.1-build 172	e 1	On-Prem FMC	O Synced	05/14/2024, 15:29:27		Onboarding	credential	
Objects >									Method		
$_{oO_{0}}^{\circ}$ VPN \rightarrow									O Synced		
Events & Monitoring									Your device's co	nfiguration is up-to-date.	
\sqrt{r} Analytics \rightarrow											
Change Log									Actions		v
(*) Jobs									# Reconnect		
😤 Tools & Services 🔷 🔿									 Deploymer Updates 2 	nt 🕑	
∰ Settings →									Workflows API Explore Settings Assign Obj Remove Or devices	i er 🕑 jects n-Prem FMC and its managed	
									Management		÷
									 □ Devices C ○ Policies C ○ Objects C 		

図 7.オンボーディングプロセスが完了します

2.- FTDデバイスをオンプレミスのFMCからcdFMCに移行

オンプレミスFMCのオンボーディングプロセスが完了したら、FTDデバイスの移行を開始できます。

「Tools & Services > Migrate FTD to cdFMC」に移動し、「Migrate FTD to cdFMC」ページで、画面の右上に青色の「add」ボタンが あることに注意して、「add」ボタンを選択します。

disco Defense Orchestrato	r	Migrate FTD to cdFMC			Q Search	⇒ 7 •	\$• ≞	@•	cisco-mex-east Imatuscl@cisco.com
Hide Menu	(Q Search by Name, Device Name or IP Address							C +
bashboard		Name	Number of FTDs	Status		Last Updated			Actions
C Multicloud Defense				No migrations found. Begin FTD Migration to	o cloud				
Inventory									
Configuration									
Policies	>								
Objects	>								
ada VPN	>								
Events & Monitoring									
√ Analytics	>								
(Change Log									
(#) Jobs									
😤 Tools & Services	>								
{\$} Settings	>								

図 8.FTDをcdFMCに移行します。

FTDの移行元のFMCを選択します。

cisco	Defense Orchestrat	or Migrat	e FTD to cdFMC							Q Search		⊳ ∎-	۵.	¢	?-	cisco-mex-east_ Imatuscl@cisco.com
≡	Hide Menu		Migrate FTD to cdFMC Migrate FTD from OnPrem FMC t	to cloud											(Cancel
<u>les</u>	Dashboard		Select OnPrem FMC	1 Ens	sure that you ha	ve onboarded ;	your OnPren	n FMC to CDO	via Credentials or	r SecureX. Onboard an On	Prem FMC or le	arn more				
0	Multicloud Defense		-	- - -	or your Op Drom	ENC has been	onboardod	colocit it from	the list							
	Inventory			Ava	ailable OnPrem FM	Cs (7.2+ only)	onboarded,	, select it from	ine list.							
Con	figuration			M	IyFMC		•									
۲	Policies	>		N	lext											
•	Objects	>														
۰Č•	VPN	>	2 Select Devices													
Ever	nts & Monitoring															
÷	Analytics	>	3 Finish													
٢	Change Log															
	Jobs															
R	Tools & Services															
\{\bar{C}\}	Settings	>														

図 9.OnPrem FMCを選択します。

cdFMCに移行するFTDを選択します。ドロップダウンメニューからCommit Action を選択する必要があります。

「Onprem FMCで分析のために保持」または「OnPrem FMCからFTDを削除」の2つのオプションがあります。

Hide Menu		Migrate FTD to cdFMC Migrate FTD from OnPrem FMC to	cloud			Cancel
ashboard		Select OnPrem EMC	OnPrem EMC: MyEMC	1		
C Multicloud Defense		Jelect OliFiell PMG	on Plein Pino. MyPino			
Inventory		2 Select Devices	Select FTD device(s) to migrate from OnPrem	FMC to cloud, and specify an action in bu	lk or per device.	Ensure that the DNS and other required configurations are correct for the
Configuration			Last Synced time : 9 minutes ago Sync from OnF	frem FMC now		selected FTD(s) to reach CDO. Learn
Policies	>		Q Name	Multi-Device Act	ion Retain on OnPrem FMC for Analytics	 It's possible to revert the device back
Objects	>		Name Name	Domain	Commit Action	to its previously-managed On-Prem FMC within 14 days of successfully
.å. VPN	>		FTDv-cloud	Global	Retain on OnPrem FM	minimize to the cloud-delivered FMC.
Events & Monitoring					Delete ETD from OnPu	e with the actions you have
√- Analytics	>					n you. Learn more
(Change Log						
(+) Jobs						
😤 Tools & Services	>					
{ Settings	,					
			1 device/e) selected		Diselation 1 of 1 results	
			Auto deploy to FTDs after successful m	igration 0	propriet and a contraction	
			Migrate FTD to cdFMC			

図 10.Devicesを選択します。

移行が正常に完了した後にFTDに設定を自動導入するチェックボックスが、デフォルトで有効になっていることに注意してください。後で変更を適用する場合は、自動展開タスクを無効にするオプションがあります。

移行プロセスMigrate to cdFMC を開始する場合に選択します。

⊟ Hide Menu		Migrate FTD to cdFMC Migrate FTD from OnPrem FMC to o	cloud			Cancel
ashboard		Select OnPrem FMC	OnPrem FMC: MyFMC			
Multicloud Defense		-				
Inventory		2 Select Devices	Select FTD device(s) to migrate from OnPrem I	MC to cloud, and specify an action in bulk	or per device.	Ensure that the DNS and other required configurations are correct for the
Configuration			Last Synced time : 9 minutes ago Sync from OnPi	em FMC now		selected FTD(s) to reach CDO. Learn
Policies	>		Q Name	Multi-Device Action	Multiple Actions Selected	It's possible to revert the device back
Objects	>		Name Name	Domain	Commit Action	to its previously-managed On-Prem FMC within 14 days of successfully
₀Å₀ VPN	>		FTDv-cloud	Global	Delete FTD from OnPrem FMC	migrating to the cloud-delivered FMC. After 14 days, the migration job is
Events & Monitoring						committed with the actions you have selected without requiring further
√- Analytics	>					action from you. Learn more
(Change Log						
📥 Jobs						
😤 Tools & Services						
Settings	>					
			1 device(s) selected		Displaying 1 of 1 results	
			Auto deploy to FTDs after successful mi	gration 0		
			Migrate FTD to cdFMC			

図 11.移行プロセスを開始します。

移行プロセスが開始されました。通常、移行プロセスが完了するまでに約15分かかります。

ステータスが successfulになったら、移行プロセスは完了です。

Hide Menu	Q	Search by Name, Device Name or IP Address	Displaying 1 of	f 1 results		C +
Dashboard		Name	Number of FTDs	Status	Last Updated	Actions
Multicloud Defense		B MyFMC_ftd-migration_2024-05-14-214124	1 devices	O Migrate FTD to cdFMC job is successful	May 14, 2024, 3:52:39 PM	
Inventory						
Configuration						
(a) Policies	>					
Objects	>					
₀Ô₀ VPN	>					
Events & Monitoring						
√- Analytics	>					
(Change Log						
📥 Jobs						
😤 Tools & Services	*					
 Settings 	>					

図 12.移行プロセスが完了しました

3.-変更の確定

最後に、移行の変更を確定します。移行の変更をコミットするのに14日間あります。変更に納得し、Cisco Defense Orchestratorが 変更を自動コミットするのを待っていない場合は、移行の変更を手動でコミットすることをお勧めします。「移行の変更をコミッ ト」ウィンドウには、クラウド配信のファイアウォール管理センターへの移行をコミットする、またはデバイスをオンプレミスの 管理センターに戻すための残りの日数が表示されます。

変更を確定するには、画面の右側にあるkebabメニューを開き、 Commit Migration Changes.

Hide Menu		Q Search by Name, Device Name or IP Address	Displaying 1 of	f 1 results			C
Dashboard		Name	Number of FTDs	Status	Last Update	1	Actions
Multicloud Defense		MyFMC_ftd-migration_2024-05-14-214124	1 devices	O Migrate FTD to cdFMC job is successful	May 14, 20	24, 3:53:46 PM	
Inventory						El Workflows	
Configuration						Download Report	
Policies	`					✓ Commit Migration Changes	1
Objects	>					B Remove Migration Job	
₀å₀ VPN	>					L	
Events & Monitoring							
√- Analytics	>						
(Change Log							
(#) Jobs							
😤 Tools & Services	->						
ô} Settings	>						

図 13.移行の変更をコミットします。

こ Commit Action れが正しいことを確認し、変更をコミットするデバイスを選択します。

Q Search by Name, Device Name or IP Address	Commit Migration Changes X		C +
Name	You have 13 days remaining to commit migration to cloud or revert FTD management to On-Prem FMC.	Last Updated	Actions
B MyFMC_ftd-migration_2024-05-14-214124	Clicking Commit implements your specified actions now. You cannot "unde" later. If you do not implement the changes now, your specified actions will be applied automatically after the 14-day	May 14, 2024, 3:53:46 PM	
	evaluation period ends.		
	Would you like to change any actions or revert any manager choices for the following devices?		
	Q Name Retain on OnPrem FMC for Analytics *		
	FTDv-cloud Delete FTD from OnPrem FMC -		
	O device(s) selected Displaying 1 of 1 results The action for all chosen davines in final and can not be rewarted once committed		
	The action for an chosen dences is man and can not be reference committee.		
	Cancel		
	Q Search by Name, Device Name or IP Address Name Image: Comparison of the Address of	Control by Name, Device Name of IP Address Control Physics Name Name Name Name Name NyFMC_ftd-migration_2024-05-14-21412 Control Physics Control Phys	Control PhyNourse, Doublee Name or IP Address Name Name Name

図 14.変更の検証をコミットします。

変更のコミットが開始されました(通常は完了まで約15分)。

⊟ Hide Menu	Q Search by Name, Device Name or IP Address	Displaying 1 of	1 results		C +
Lashboard	Name	Number of FTDs	Status	Last Updated	Actions
C Multicloud Defense	B MyFMC_ftd-migration_2024-05-14-214124	1 devices	Committing migrate FTD to cdFMC job is in progress	May 14, 2024, 4:02:19 PM	
Inventory					
Configuration					
(a) Policies >					
Objects >					
₀Ĝ₀ VPN →					
Events & Monitoring					
√ Analytics >					
(Change Log					
Jobs					
😤 Tools & Services 💦 🔿					
ố) Settings >					

図 15.進行中の変更をコミットします。

移行ステータスが Succesful で、コミットステータスが Comittedであることが確認できたら、移行は完了です。

⊟ Hide Menu	(Q Search by Name, Device Name or IP Address	Disp	alaying 1 of 1 re	results				0	•
Lashboard		Name	Number of	FTDs St	itatus			Last Updated	Actions	
Multicloud Defense		B MyFMC_ftd-migration_2024-05-14-214124	1 devices	•	Migrate FTD to cdFMC job is	s successful		May 14, 2024, 4:04:27 Pt	N	
Inventory		DEVICE NAME	MIGRATION STATUS				COMMIT STATUS		LAST UPDATED	
Configuration		FTDv-cloud	 Migration Successful. Delete 	ed device from	m On-Prem FMC successfully.		Committed. Delet	ed FTD from On-Prem FMC.	May 14, 2024, 4:02:44	4 PM
Policies										
Objects	>									
"Å» VPN	>									
Events & Monitoring										
√r Analytics	>									
(Change Log										
📛 Jobs										
😤 Tools & Services	->									
ô Settings	>									

図 16.移行プロセスと変更のコミットが完了しました。

確認

Tools & Services > Firepower Manager Centerに移動し、OnPrem FMCのデバイス番号が減少したことを確認します。

一方、cdFMCのデバイス番号がどのように増加したかを確認できます。これは、移行プロセスが完了したことを意味します。

Hide Menu Hide Menu Dashboard Multicloud		Q FMC	Search by Device Name, IP Address, or Serial No Secure Connectors	imber				•	, (Cloud-Delivered FMC lostname cdo-cisco-mer-east s85mg.app.us.cdo.cisco.com 20240307
			Name	Version	Devices	Туре	Status	Last Heartbeat		Actions
Configuration			Cloud-Delivered FMC	20240307	⊜1	Cloud-Delivered FMC	O Active	05/14/2024, 16:00:10		O Check For Changes
 Policies Objects 	<u>,</u>	0	MyFMC	7.4.1-build 172	⊖0	On-Prem FMC	O Synced	05/14/2024, 16:04:25		Updates Workflows
& VPN	,									API Explorer
Events & Monitoring										Management
\sqrt{r} Analytics	>									Devices Devices
Change Log										Objects Objects
🖶 Jobs										Site to Site VPN
😤 Tools & Services	*									Remote Access VPN Platform Settings
{§} Settings	>									System
										Configuration Smart Licenses MAP Management → Device Health Audit Cisco Cloud Events

図 17. *Firepower Management Center*(FMC)リスト。

OnPrem FMCにログインして完了したタスクを検証すると、FTDがどのようにOnPrem FMCから移行および登録解除されたかを確認できます。

Firewall Management Center Devices / Device Management	Overview A	nalysis Policies	Devices	Objects	Integration		Deploy Q	🔮 🌣 (admin ~	cisco SECURE
View By: Group •						Deployments Upgrades 9 Health	Tasks		± 💽 si	now Notifications
All (0) • Error (0) • Warning (0)	Offline (0) Norr	nal (0) 🛛 😐 Deploym	ent Pending (0)	 Upgr 	rade (0)	20+ total 0 waiting 0 running 0 retrying	20+ success	0 failures	्, Filter	
Collapse All Name		Model	Versio	m C	hassis	 Register Unregistration Urregistration completed. FTDv-cloud - Device unregistered successfully 				$_{95}$ \times
Ungrouped (0)						 Register Migration state change for 1 devices successfully completed 				$\frac{25}{2}$ ×
						Device Configuration Export Export file uploaded to edge.us.cdo.cisco.com Download Export Package	1			<u>5s</u> ×
						 Register CDO state change for migration on 1 devices 				8s ×
						Remo	we completed ta:	sks		

図 18.オンプレミスFMCタスクの検証。

関連情報

- <u>脅威対策をクラウド配信のファイアウォール管理センターに移行</u>
- <u>テクニカル サポートとドキュメント Cisco Systems</u>

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人に よる翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっ ても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性につ いて法的責任を負いません。原典である英語版(リンクからアクセス可能)もあわせて参照する ことを推奨します。