Migrer FDM vers cdFMC en utilisant FMT dans CDO

Table des matières

ntroduction	
Conditions préalables	
Exigences	
Composants utilisés	
nformations générales	
<u>Configurer</u>	
/érifier	

Introduction

Ce document décrit comment migrer un Firepower Device Manager (FDM) vers le Cloud-Delivered FMC (cdFMC) à l'aide de l'outil de migration Firepower (FMT) dans CDO.

Conditions préalables

Exigences

- Firepower Device Manager (FDM) 7.2+
- · Centre de gestion des pare-feu (cdFMC) fourni dans le cloud
- Outil de migration Firepower (FMT) inclus dans CDO

Composants utilisés

Ce document a été créé sur la base des exigences mentionnées ci-dessus.

- Firepower Device Manager (FDM) version 7.4.1
- Centre de gestion des pare-feu (cdFMC) fourni dans le cloud
- Cloud Defense Orchestrator (CDO)

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Les utilisateurs CDO admin peuvent effectuer des migrations de leurs périphériques vers cdFMC lorsque les périphériques sont sur la version 7.2 ou ultérieure. Dans la migration décrite dans ce

document, cdFMC est déjà activé sur le locataire CDO.

Configurer

1.- Activer les services cloud Cisco sur FDM

Pour commencer la migration, il est nécessaire d'avoir le périphérique FDM sans déploiements en attente et de s'inscrire aux services cloud. Pour vous inscrire aux services cloud, accédez à Paramètres système > En savoir plus > Services cloud.

Dans la section Cloud Services, vous trouvez que le périphérique n'est pas enregistré, par conséquent, il est nécessaire d'effectuer l'inscription avec le type Security/CDO Account. Vous devez configurer une clé d'enregistrement, puis vous inscrire.



Services cloud d'inscription

Sur les services cloud, il est indiqué que n'est pas enregistré. Sélectionnez le type d'inscription Compte CDO et fournissez la clé d'inscription de CDO.



Inscription aux services cloud

La clé d'enregistrement se trouve à l'intérieur de CDO. Accédez à CDO, accédez à Inventory > Add symbol.

Un menu apparaît pour sélectionner le type de périphérique dont vous disposez. Sélectionnez l'option FTD. L'option FDM doit être activée ; sinon, la migration correspondante ne peut pas être effectuée. Le type d'enregistrement utilise Utiliser la clé d'enregistrement. Dans cette option, la clé d'enregistrement apparaît à l'étape 3, que nous devons copier et coller dans le FDM.

disclor cisco Defense Orchestrator	Inventory	Q Search	ଓ १३ - ०० - ⇔ा ० -	
⊟ Hide Menu	Dundens Templates O Casesh bur Dunden Manna ID Address or Cadal Mumbar	Displaying 8 of 8 merula		
A Dashboard	Concest templates C. adarch by banke halle, in Houress, or Senai Houriter			
C Multicloud	All ASA FTD			/
inventory	Name \$	Configuration Status \$	Connectivity \$	

FDM intégré, ajouter une option

Un menu s'affiche pour sélectionner un périphérique ou un type de service.



Sélectionner un périphérique ou un type de service

Pour ce document, l'option Sélectionner la clé d'enregistrement a été sélectionnée.

Follow the steps below				Cancel
FTD 0000	A Important: This method of onbo delivered Firewall Management Sy	parding allows for local co-managem stem, click the FTD button instead.	nent of the firewall via FDM. To man Learn more 🗗	age your device with cloud-
Firewall Threat Defense Management Mode: O FTD O FDM O (Recommended)	Use Registration Key Onboard a device using a registration key generated from CDO and applied on the device using Firepower Device Manager.	Use Serial Number Use this method for low-touch provisioning or for onboarding configured devices using their serial number. (FTD 6.7+, 1000, 2100 and 3100 series only)	Use Credentials (Basic) Onboard a device using its IP address, or host name, and a username and password.	
	X			

Ici, il affiche la clé d'enregistrement nécessaire à l'étape précédente.

FT Fire Man (Red	wall Threat Defense agement Mode: FTD () () FDM () commended)	▲ Important: This method of onboarding allows for local co-management of the firewall via FDM. To manage your device with cloud-delivered Firewall Management System, click the FTD button instead. Learn more C Important: This method of onboarding allows for local co-management of the firewall via FDM. To manage your device with cloud-delivered Firewall Management System, click the FTD button instead. Learn more C Important: This method of onboarding allows for local co-management of the firewall via FDM. To manage your device with cloud-delivered Firewall Management System, click the FTD button instead. Learn more C Important: Use Registration Key Important System Onboard a device using a registration key generated from CDO and applied on the device using Firepower Device Manager. Use Secial Number Important: Important: Important System Important System Important System Important: Important System Important System Important System Important: Important System Important System Important System Important System Important System Impo	•
1	Device Name		
2	Database Updates	Enabled	
3	Create Registration Key	7a53c	
4	Smart License	(Skipped)	
5	Done	Your device is now onboarding. This may take a long time to finish. You can check the status of the device on the Devices and Services page. Add Labels Add label groups and labels Go to Inventory	

Processus d'enregistrement

Une fois la clé d'enregistrement obtenue, copiez-la et collez-la dans le FDM, puis cliquez sur Register. Après l'enregistrement du FDM dans les services cloud, il s'affiche comme Enabled comme indiqué dans l'image.

La licence Smart a été ignorée car le périphérique va être enregistré une fois qu'il sera opérationnel.

Monitoring	Policies	Objects	Device: joroa-fdm-tech
Device Summar Cloud Se	v rvices		
Not Reg	istered		
You can registe use Cisco Defe register with the auto-enroll with want to use See configure Smar register with the	r the device with the device of the device of the device of the device with the device withe device with the device with the device with the device with the d	with the Cisco clo ator (CDO) for m your CDO or oth ecure Firewall Ma device manager which automatica can enable or dis	bud to use additional cloud-based services. If you want to anagement or want to remain in evaluation mode, then her security account registration key. You can alternatively anagement Center using the device serial number. If you for management and are ready to license the device, then ally registers the device with the Cisco cloud. After you sable features as needed.
Enrollment Type	9		
Security/CD0	O Account	Smart Licensing	3
Region US Region			× ()
Registration Ke	y		
7a53c2			
Service En	rollment		
Cisco D	efense Ord	chestrator	
Cisco Defe devices. S account.	ense Orchestr elect this opt	rator is a cloud-b ion if you want to	based management tool used for managing network o register the device in your Cisco Defense Orchestrator
🔽 Enable	e Cisco Defer	nse Orchestrator	
Cisco St	uccess Ne	twork	
Cisco Suco essential fo product an of the proc	cess Network or Cisco to pr d to make yo luct in your n	c enablement pro rovide technical s ou aware of unus etwork.	vides usage information and statistics to Cisco which are support. This information also allows Cisco to improve the ed available features so that you can maximize the value
Check out	the Sample (Data that will be s	sent to Cisco. See more Y
🚦 🔽 Enroll	Cisco Succe	ss Network	
REGISTER	Need he	elp? 🖪	

Enregistrement FDM

Lors de l'enregistrement de FDM, il affiche la location, les services cloud connectés et les services enregistrés.



Enregistrement FDM terminé

Dans CDO, dans le menu Inventaire, le FDM est en cours d'intégration et de synchronisation. La progression et le flux de cette synchronisation peuvent être examinés dans la section Workflows.

Une fois ce processus terminé, il s'affiche sous la forme Synchronisé et En ligne.

elization Defense Orchestrator	Inventory		Q Search	<mark>⊙</mark> ⊳r-	¢ 0 - ≜1	۰.
Hide Menu	Devices Templates Q Search by Device Name, IP Address, or Serial Number		Displaying 9 of 9 results	C 🛛 🕇	> FDM Device Details	2
C Multicloud Defense	AII ASA FTD				Model	Cisco Firepower Threat Defense for
inventory	Name \$	Configuration Status \$	Connectivity \$		Serial	Azure
Configuration			A Unreachable		Version Onboarding Method	7.4.1-172 Registration Key
⊕ Objects →	Гом		O Serial Number Mismatch		Snort Version	3.1.53.100-56
🔥 VPN >	ГТР	O Not Synced	Pending Setup		Syncing CD0 is communica in a moment.	ting with your device. Please check back
√ Analytics →	О гто		Pending Setup		Device Actions	
Jobs	О гто	•	Pending Setup		API Tool Workflows Manage Back	cups
	FDM FDM	Syncing	Online		Remove Management	
	C FTD	•	Online		Notes	
	O FID		Online		🖆 Executive Re	port
	O TTO	O Not Synced	A Unreachable		Check every:	Ion Disabled • Tenant default (24 hours) •
					Label Groups and	Labels
					Add Labels O	

Inventaire CDO FDM intégré

Lorsque les périphériques ont été synchronisés, ils s'affichent comme Online (En ligne) et Synchronized (Synchronisé).

۵	FDM	O Synced	Online

FDM intégré

Lorsque le FDM a été correctement intégré à CDO, nous devons nous déconnecter du FDM. Après vous être déconnecté de FDM, naviguez dans CDO vers Tools & Services > Migration > Firewall Migration Tool.

😤 Tools & Services		Tools & Services	Migrations
	>	Oynamic Attributes Connector	Firewall Migration Tool
		⇒ Secure Connectors	會 ASA to FDM Migration
		G Firewall Management Center	
		ASA Templates	

Cliquez sur le symbole Add, et un nom aléatoire apparaît, indiquant que le nom doit être renommé pour lancer le processus de migration.

(Search for a migration by name	¢	Displaying 0 of 0 results			IC •
Name 2	Status	Created Date 3	Deprevisioning Date: p	Actions	/
	No	nigrations found. Begin migrating AS	A, FDM, Checkpoint, Forlinet, or Palo Alto Networks firewalls to FTD.		

Après avoir renommé, cliquez sur Launch pour commencer la migration.



Initialiser la migration

Cliquez sur Launch pour démarrer la configuration de la migration.

Firewall Migration Tool			Q Search	<mark>ଓ</mark> ⊳,	¢ ? • ≜1	? -	
Search for a migration by name		Displaying 1 of 1 results					i C +
Name 0	Status	Created Date ©	Deprovisioning Date		Actions		
fdm_migration	 Ready to Migrate 	Jun 12, 2024	Jun 19, 2024		C 🔒 Launch		

Processus de lancement de la migration

Après avoir cliqué sur Launch, une fenêtre s'ouvre pour le processus de migration où l'option Cisco Secure Firewall Device Manager (7.2+) est sélectionnée. Comme mentionné précédemment, cette option est activée à partir de la version 7.2.

cisco	Firewall Migration Tool (Version 6.0.1)
Sele	ect Source Configuration 🕕
Source I	Firewall Vendor
Select	Source
Cisco	ASA (8.4+)
Cisco	Secure Firewall Device Manager (7.2+)
Check	k Point (r75-r77)
Check	k Point (r80-r81)
Fortin	net (5.0+)
Palo A	Alto Networks (8.0+)

Configuration source de sélection FMT

Une fois sélectionnées, trois options de migration différentes sont présentées : Configuration partagée uniquement, Inclut les configurations de périphériques et partagées, et Inclut les configurations de périphériques et partagées vers le nouveau matériel FTD.

Dans ce cas, la deuxième option, Migrate Firepower Device Manager (Inclut le périphérique et la configuration partagée), est exécutée.

C	lick on text below to get additional details on each of the migration options	
)	Migrate Firepower Device Manager (Shared Configurations Only)	>
)	Migrate Firepower Device Manager (Includes Device & Shared Configurations)	\sim
	 This option migrates both device and shared configuration. Same FTD is moved from FDM managed to FMC managed. 	
	 The migration process is to be done over a scheduled downtime or maintenance window. There is device downtime involved in this migration process. 	
	 Ensure connectivity between FDM device and FMC to move the device from FDM to FMC using FDM. 	
	 User should provide FDM credentials to fetch details. 	
	 FDM Devices enrolled with the cloud management will lose access upon registration with FMC 	
	 Ensure out-of-band access to FTD device is available, to access the device in case of accessibility issues during migration. 	
	 It is highly recommended that a backup (export) of the FDM configuration is performed to restore the original state of the firewall managed by FDM if required. 	
	 If the FTD devices are in a failover pair, failover needs to be disabled (break HA) before proceeding with moving manager from FDM to FMC. 	
	 FDM with Universal PLR cannot be moved from FDM to FMC. 	
	• FDM with flexConfig objects or flexconfig polcies cannot be moved from FDM to FMC. The flexconfig objects and policies must be completely removed from FDM before migration.	
	FMC should be registered to Smart Licensing Server.	

Options de migration

Une fois la méthode de migration sélectionnée, sélectionnez le périphérique dans la liste fournie.

Live Connect to FDM
Select any FDM device onboarded on CDO from the below dropdown.
 Only devices with online connectivity and synced status will be displayed in the dropdown.
 Click on change device status button to update the FDM device status from In-Use to Available. Select FDM Managed Device
Select FDM Managed Device
fdmfdm Available
Connect

Sélection du périphérique FDM

FDM device config extraction successful	
100% Complete	

Extraction de la configuration terminée

Il est recommandé d'ouvrir l'onglet situé en haut de la page pour vérifier et comprendre à quelle étape nous sommes lorsque le périphérique a été sélectionné.



Étapes du processus de migration

En tant que nouvelle migration, sélectionnez Annuler lorsque vous y êtes invité avec l'option « Voulez-vous utiliser une politique de contrôle d'accès, une politique NAT ou RAVPN existante sur FMC ? »

Yes ONO Save Cancel	Do you want to use an Existing Access Control Policy, NAT or RAVPN Policy on FMC.	
Save Cancel	🔾 Yes 💿 No	
	Save Cancel	

Annuler l'option de configuration existante

Par la suite, il y aura des options pour sélectionner les fonctionnalités à migrer comme indiqué dans l'image. Cliquez sur Continuer.

	1		3	4	5	6	7	8	9	
	Extract FDM Information	Select Target	Map FTD Interface	Map Security Zones & Interface Groups	Review & Validate (Shared Config)	Push Shared Config To FMC	Move Manager	Review & Validate (Device Config)	Complete Migration	
	Note: Steps 7,8 and 9 shou	d be carried o	ut in a maintena	nce window.						
Select Target 🕕					^			Selec	ource: Cisco Secure Fi cted Migration: Include	rewall Device Manager (7.24 es Device and Shared Confi
Firewall Management - C	loud-delivered FMC									>
Select Features										~
Device Configuration		SI	ared Configura	tion				Optimization		
✓ Interfaces		~	Access Control					✓ Migrate Only Re	eferenced Objects	
Routes			🧹 Migrate tunn	elled rules as Pref	iter		1	Object Group S	earch 🕕	
ECMP			NAT							
Static		~	Network Objects							
BGP] Port Objects(no	data)						
EIGRP			Access List Obj	ects(Standard, Ext	ended)					
Site-to-Site VPN Tunne	ils (no data)		Access Control I	Policy Objects (Ge	plocation, Applic	ation, URL objects a	nd Intrusion Rul	e		
Policy Based (Cry	oto Map)		' Group) Time based Obi	ects (no data)						
Route Based (VTI			Remote Access	VPN						
Platform Settings			File and Malware	Policy						
- DHCP										
Server										
Relay										
DDNS										
Proceed	•									
Note:Platform settings and	I file and malware policy migra	tion is supporte	d in FMC 7.4 and I	ater versions.						

Fonctionnalités à sélectionner

Puis Lancez La Conversion.

Firewall Migration Tool (Version	6.0.1)									
	(1)	2	3	4	5	6	7	8	9	
	Extract FDM Information	Select Target	Map FTD Interface	Map Security Zones & Interface Groups	Review & Validate (Shared Config)	Push Shared Config To FMC	Move Manager	Review & Validate (Device Config)	Complete Migration	
	Note: Steps 7,8 and 9 shoul	d be carried out i	in a maintena	nce window.		_				
Select Target	0				^	,		Science	ource: Cisco Secure Firewa sted Migration: Includes D	III Device Manager (7.2+) levice and Shared Config
Firewall Manageme	nt - Cloud-delivered FMC									>
Select Features										>
Rule Conversion/ P	rocess Config									~
Start Conversion										

Commencez la conversion.

Une fois le processus d'analyse terminé, deux options peuvent être utilisées : Téléchargez le document et poursuivez la migration en cliquant sur Suivant.



Télécharger le rapport.

Les interfaces des périphériques sont définies pour être affichées. Il est conseillé de cliquer sur Refresh pour mettre à jour les interfaces. Une fois la validation effectuée, vous pouvez continuer en cliquant sur Next (Suivant).

	0	-2-		4	5	6	7	8	9	
	Extract FDM Information	Select Target	Map FTD Interface	Map Security Zones &	Review & Validate	Push Shared Config To	Move Manager	Review & Validate	Complete Migration	
				Interface Groups	(Shared Config)	FMC		(Device Config)		
	Note: Steps 7,8 and 9 should	d be carried	out in a maintenar	nce window.						
App ETD Interface	-				<u>^</u>		50	urce: Cisco Sec	ure Firewall Device Mana	ner (7.2+)
viap FTD Interface	0						Se	elected Option:	Includes Device and Sha	red Config
					C	Refresh				
FDM Interface Name		_ 1	FTD Interface Nam	ie –						
GigabitEthernet0/0		Gi	pabitEthernet0/0							
igaoitzmerneturi		Gg	pablemenun							
00										
20 V PRE(0P#98 2 4	A Page 1 of 1 ▶ ▶									~

Interfaces affichées

Accédez à la section Zones de sécurité et groupes d'interfaces, où vous devez ajouter

manuellement avec Add SZ & IG. Pour cet exemple, Auto-Create a été choisi. Cela permet de générer automatiquement les interfaces au sein du FMC vers lequel vous effectuez la migration. Une fois terminé, cliquez sur le bouton Next (Suivant).

Firewall Migration Tool (Version 6.0	.1)				
	1 2- Extract FDM Information Select Target	3 (4) Map FTD Interface Map Security Zo Interface Grow	5 6 nes & Review & Validate Push Shared Conf aps (Shared Confg) FMC	7 8 Ig To Move Manager Review & Validat (Device Config)	9 a Complete Migration
	Note: Steps 7,8 and 9 should be carrie	d out in a maintenance window.			
Map Security Zone	es and Interface Groups 🕕			Add SZ & IG Auto-Create	Source: Cisco Secure Firewall Device Manager (7.2+) Selected Option: Includes Device and Shared Config
FDM Logical Interface .	FDM Security Zones	FTD Interface	FMC Security Zones	FMC Interface Groups	
cutside	outside_zone	GigabitEthernet0/0	outside_zone (A)	Select Interface Groups v	
inside	inside_zone	GigabitEthernet0/1	inside_zone (A)	Select Interface Groups v	
Note Olick on Auto Posta b	uttor to sude may the FDM example as the	and the EMC interface objects of	ed easywity mones. Click on easy built		

Zones de sécurité et groupes d'interfaces

L'option Auto-Create mappe les interfaces FDM aux zones de sécurité FTD existantes et aux groupes d'interfaces dans FMC qui ont le même nom.

		Charot
FTD		e Groups
Gigabiti	Auto-Create	ups
Gigabiti	Auto-create maps FDM interfaces to existing FTD security zones and interface groups in FMC that have the same name. If no match is found, the Migration Tool creates a new FTD security zone and interface group with the same name in FMC.	ups
	Select the objects that you want to map to FDM interfaces	
	Cancel Auto-Create	

Option de création automatique.

Sélectionnez ensuite Suivant.

Firewall Migration Tool (Version 6	5.0.1)						
	Extract FDM Information Select	3 Carget Map FTD Interface Map Security Zon Interface Group	5 6 es & Review & Validate Push Shared C is (Shared Config) FINC	7 Config To Move Manager	8 Review & Validate (Device Config)	9 Complete Mgration	
	Note: Steps 7,8 and 9 should be ca	rried out in a maintenance window.					
Map Security Zo	ones and Interface Groups 🛈					Source: Cisco Secure Firew Selected Option: Includes I	all Device Manager (7.2+) Device and Shared Config
			C	Add SZ & IG Aut	o-Create		
FDM Logical Interfa	ICE N FDM Security Zones	FTD Interface	FMC Security Zones	FMC Interface Gro	ups		
outside	outside_zone	GigabitEthernet0/0	outside_zone (A)	outside_ig (A)	v		
inside	inside_zone	GigabitEthernet0/1	inside_zone (A)	inside_ig (A)	~		
Note:Click on Auto-Crea	te button to auto map the FDM nameif as t	he name of the FMC interface objects and	f security zones. Click on next bu	utton to proceed ahead.			
10 v prif.698981 2	∢ ∢ Page 1 of 1 ▶ ▶						

Option Après la création automatique.

À l'étape 5, comme indiqué dans la barre supérieure, prenez le temps d'examiner les règles ACP (Access Control Policies), les objets et la NAT. Continuez en examinant attentivement chaque élément, puis cliquez sur Valider pour confirmer qu'il n'y a aucun problème avec les noms ou les configurations.

Firewall Migration	n Tool	(Versio	on 6.0.1)			
			1 2 Extract FDM Information Select Target	3 4 3 Map FTD Interface Map Security Zones & Review & Validate Interface Groups (Bared Config)	6 7 Push Shared Config To Move Manager Re FINC (0	8 9 view & Valdate Complete Mgration Device Configi
			Note: Steps 7,8 and 9 should be carried o	ut in a maintenance window.		
	Opti	mize, F	Review and Validate Shared Con	figuration Only 💿	•	Source: Cisco Secure Firewall Device Manager (7.2+ Selected Migration: Includes Device and Shared Config
	Access	Control	Objects NAT Interfaces Routes Site-to-S	ite VPN Tunnels 💿 Remote Access VPN SI		
	Acc	ess List Obj lect all 3 ent	jects Network Objects Port Objects Access Co tries Selected: 0/3 Actions - Save	ntrol Policy Objects VPN Objects Dynamic-Rout	e Objects	Q Search
	•	*	Name Q.	Validation State	Туре С	Value Q
	0	1	OutsidelPv4Gateway	Validation pending	Network Object	172.18.1.1
		2	OutsideIPv4DefaultRoute	Validation pending	Network Object	0.0.0.0/0
		3	Banned	Validation pending	Network Object	103.104.73.155
erpage 1 to3 of3 ∢ ∢	Page _	1 of 1	÷ >			Validate

Contrôle d'accès, objets et configurations NAT

Х Validation Status \odot Successfully Validated Validation Summary (Pre-push) ۱d 3 4 3 Access Control List Lines Network Objects Access Control Policy Objects (Geo, Application, URL objects and Intrusion Rule Group) 2 Network Address Translation

Puis Push Shared Configuration Only

Diffuser la configuration partagée uniquement

Le pourcentage d'achèvement et la tâche spécifique en cours d'exécution peuvent être observés.

Firewall Migrat	ion Tool (Version 6.0.1)			
	Push Shared Config to F	MC	oucume	Source: Cisco Secure Firewall Device Manager (7.2*) Selected Migration: Includes Device and Shared Config
	Migration Status		24% Complete	
	Network Objects	0	Push to Cloud-delivered FMC is In progress. Please wait for entire push process to complete the migration.	
	Network Address Translation	0		
	Access Control Policies	0		
	Policy Assignment			
	Please download the Post-Push migration	n report for a detailed summa		

Pourcentage de poussée

Une fois l'étape 5 terminée, passez à l'étape 6, comme indiqué dans la barre supérieure, où la configuration partagée Push to FMC a lieu. À ce stade, sélectionnez le bouton Next pour avancer.

wall Migration Tool (Versi	ion 6.0.1)				
	Extrac	1 2 (3 4 5 D Interface Map Security Zones & Review & Validate Interface Groups (Shared Confg)	O O T O	9 te Complete Myrston
	Note: Steps 7	,8 and 9 should be carried out in a n	naintenance window.		
Push Shar	red Config to FM	ЛС			Source: Cisco Secure Firewall Device Manager
Migration Status				J	releven migration, includes perce and shared
Migration Next Ste	n of Shared Config is compl p - Login to FMC to deploy	lete, policy is pushed to FMC. the policy to FTD.			
Live Connect: Selected Contex Migration Summ	rt: Single Context Mode ary (Post Push)				
Live Connect: Selected Contex Migration Summ	xt: Single Context Mode ary (Post Push) 3		4		3
Live Connect: Selected Contex Migration Summ Access Cont	kt: Single Context Mode ary (Post Push) 3 Irol List Lines		4 Network Objects		3 Access Control Policy Objects (Gee, Application, URL objects and Intrusion Rule Group)
Live Connect: Selected Contex Migration Summ Access Cont Not selected	<pre>ct: Single Context Mode ary (Post Push) 3 trot List Lines for migration</pre>	Not selected for migration Access List Objects (Standard, Extended used in BGW RAUMWECKIP)	4 Network Objects Not selected for migration		3 Access Control Policy Objects (Geo, Application, URL objects and Intrusion Rule Group) Net selected for migration
Live Connect: Selected Contex Migration Summ Access Cont Not selected Dynamic Ro	tt: Single Context Mode any (Post Push) 3 Info List Lines	Not selected for migration Access List Objects (Slandard, Dominde used is BOAY BAVPIECORP) 2 Network Address Translation	4 Network Objects Not selected for migration Logical Interfaces		3 Access Control Policy Objects (Geo, Application, URL, objects and intrusion Rule Group) Not selected for migration

Diffusion de la configuration partagée vers FMC terminée

Cette option déclenche un message de confirmation, invitant à poursuivre la migration du manager.

Confirm Move Manager

Requires maintainence window to be scheduled FDM manager will be moved to be managed in FMC.



Confirmer le gestionnaire de déplacement

La migration du gestionnaire nécessite la présence de l'ID Management Center et de l'ID NAT, ce qui est essentiel. Ces ID peuvent être récupérés en sélectionnant Mettre à jour les détails. Cette action lance une fenêtre contextuelle dans laquelle le nom souhaité pour la représentation FDM dans cdFMC est entré, puis enregistre les modifications.

Firewall Migration	n Tool (Version 6.	0.1)									
		1				-6	•	8	9		
		Extract FDM Information	Select Target Map FTD Interface	Map Security Zones & Interface Groups	Review & Validate (Shared Config)	Push Shared Config To FMC	Move Manager	Review & Validate (Device Config)	Complete Migration		
		Note: Steps 7,8 and 9 should	be carried out in a maintena	ance window.							
	Move Manager							Sc Selec	ource: Cisco Se ted Migration:	cure Firewall De Includes Device	vice Manager (7.2+) and Shared Config
	Update Del	ails nd should be performed during	a downtime window. After y	ou register the de	vice with the ma	inagement center	or Cloud-delive	red FMC, you ca	ın no longer use	the device man	ager to manage it.
	Management Cent	Management Cente 🕕	NAT ID 🕕	Threat D	efense Hostn	DNS Server	Group	Managemer	nt Center/	Data Interfac	e
	cisco o	so		j.	Lciouda;	pp.n/ CiscoUmbrellaDNS	ServerGroup v	💿 Data 🕥 Ma	inagement	Select Data Interfa	ce ~

ID du centre de gestion et ID NAT

Firewall Migration Tool (Version 6.0	.1) Extract FDM Information Set Note: Steps 7,8 and 9 should be	3 Upd	ate Device Name for f	X	Breve & Malata Consiste Dayates Charles Config						
Move Manager Update Data This step is mandatory an	is d should be performed during a c	downtime	Cancel Save		Source: Cisco Se Selected Migration: d FMC, you can no longer use	cure Firewall Device Mar includes Device and Sha	nager (7.2+) Irred Config manage it,				
Management Cent	Management Cente 🕕	NAT ID 🕕	Threat Defense Hostn	DNS Server Group	Management Center/	Data Interface					
cisco-mex-ngfw-lac.app.us.cdo			joroa-fdm-techzone.internal.cloudapp.n	CiscoUmbrellaDNSServerGroup ~	💿 Data 🔵 Management	Select Data Interface	U I				

Mettre à jour le nom du périphérique pour enregistrement.

Après cette action, les ID des champs susmentionnés sont affichés.



Avertissement : n'apportez aucune modification à l'interface Management Center. Par défaut, l'option Management (Gestion) est sélectionnée. Conservez cette option comme paramètre par défaut.

Firewall Migration Tool (/ersion 6.0.1)										
		1 Extract FDM information	2 3 lelect Target Map FTD Interface	4 Map Security Zones & Interface Groups	5 Review & Validate (Shared Config)	6 Push Shared Config To FMC	7 Move Manager	8 Review & Validate (Device Config)	9 Complete Migration		
	Not	e: Steps 7,8 and 9 should b	e carried out in a mainten	ance window.							
Move	Manager					, 		So Select	ource: Cisco Sec ted Migration:	cure Firewall Device Includes Device and	Manager (7.2+) Shared Config
This step i	Update Details s mandatory and <u>sho</u>	ould be performed during a	downtime window. After y	<u>you regi</u> ster the de	vice with the ma	anagement center	or Cloud-delive	red FMC, you ca	n no longer use	the device manager	to manage it
Manage	ement Cent	Management Cente 🕕	NAT ID 🕠	Threat D	efense Hostn	DNS Server	Group	Managemen	nt Center/	Data Interface	
cisco	us.cdo og	gu WEBG	W 104V	3sPM fdm-Azu	re	CiscoUmbrellaDNS	SServerGroup ~	💿 Data 🔵 Ma	inagement	Select Data Interface	×
	L									/	

ID du centre de gestion et ID NAT.

Après avoir choisi l'option Update Details, le périphérique qu'il va commencer à synchroniser.

n Tool (Version 6.0).1)							
	1 Extract FDM Information Se	2 3 alect Target Map FTD Interfac	4 De Map Security Zones & Interface Groups	5 Review & Validate P (Shared Config)	6 To Move Manage	8 9 r Review & Validate Complete Migra (Device Confg)		
	Note: Steps 7,8 and 9 should be	e carried out in a mainter	nance window.					
Move Manager						Source: Cisco Selected Migrati	Secure Firewall Device I on: Includes Device and	
Update Deta This step is mandatory ar	ils Id should be performed during a	downtime window.	SYNG	CING the FDM Dev	ice Id-de	livered FMC, you can no longer	use the device manager	to manage it.
Management Cent	Management Cente 🕕	NAT ID 💿		9% Complete		Management Center/	Data Interface	
cisco us.cd	oguq (66G)	N 104	PMN fdm-Azu	ire	CiscoUmbrellaDNSServerGroup	v OData Management	Select Data Interface	~

Synchronisation du périphérique FDM

Une fois la migration finalisée, l'étape suivante consiste à examiner les interfaces, les routes et les paramètres DHCP configurés dans le FDM en sélectionnant Valider.

ewall Migration	n Tool (Vers	totact FOM Information Select	3 4 Arget Map PTD Interface Map Security Zones & I Interface Orcups	5 6 7 Review & Valdese Push Shared Config To Nove Manager (Shared Config) FMC	Review & Validate Complete (Device Config)	Mgration	
		Note: Steps 7,8 and 9 should be ca	rried out in a maintenance window.	^			
	Optimize,	Review and Validate Device	Configuration Page		Source: Selected Mi	Cisco Secure Firewall Device N igration: Includes Device and	anager (7.2+ Shared Config
		Objects NAT Interfaces Routes S	ite-to-Site VPN Tunnels 👩 Remote Access V	VPN SNMP DHCP			
	Static PPF	PoE					
	Select all 2	entries Selected: 0 / 2				Q Search	+
	- *	Interface	Zone Q	IP Address	State		
	0 1	GigabitEthernet0/0	outside_zone		Enabled		
	2	GigabitEthernet0/1	inside_zone	45.1	Enabled		
1 to 2 of 2 🛛 🛛 🖣	Page 1 of 1	1 > >l					

Valider les paramètres de configuration FDM

Après la validation, choisissez Push Configuration pour lancer le processus de transmission de la configuration, qui va se poursuivre jusqu'à la fin de la migration. En outre, il est possible de surveiller les tâches en cours d'exécution.

alidation Summan//Pro. a	Va Ø	Successfully Validated	3	
Not selected for migration	Not selected for migration	2	1	1
		Logical Interfaces	Routes	DHCP
			(Static Routes, ECMP)	(Server, Relay, DDNS)
	0	0		
	Platform Settings (snmp,http)	Malware & File Policy		

Statut de validation - Configuration push.

Fenêtre contextuelle contenant la configuration de diffusion en pourcentage.

Firewall Migration	n Tool (Version 6.0	0.1)				
		Extract FDM Information 5 Note: Steps 7,8 and 9 should be	2 alect Target Map FTD	PUSHING 10% Complete Push to Cloud-delivered FMC is In progress. Please wait for entire push process to complete the migration.	7)	Berview & Validates Complete Migration (Device Config)
	Complete Migra	tion				Source: Cisco Secure Firewall Device Manager (7.2+) Selected Migration: includes Device and Shared Config
	Migration Status					
	Interfaces	ø				
	Routes	0				
	Policy Assignment					
	Please download the Post-	Push migration report for a detailed s	ummary. Download Re			

Pourcentage de transmission terminé

Une fois terminé, une option permettant d'initier une nouvelle migration est présentée, marquant la fin du processus de migration de FDM à cdFMC.

	1 2 3 Extract FDM Information Select Target Map FTD Into	4 5	6 7 8	te Complete Micration
		Interface Groups (Shared Config)	FMC (Device Confi	1)
	Note: Steps 7,8 and 9 should be carried out in a main	ntenance window.		
Complete Migrati	ion			Source: Cisco Secure Firewall Device Manager (7.2 Selected Migration: includes Device and Shared Con
Migration Status				
Migration is complete Next Step - Login to	e, policy is pushed to FMC. FMC to deploy the policy to FTD.			
Live Connect:				
LIFE CONFECT				
Selected Context: Single Co	ontext Mode			
Selected Context: Single Co	ontext Mode			
Selected Context: Single Co Migration Summary (Post P	ontext Mode Push) Not selected for migration	4		3
Selected Context: Single Co Migration Summary (Post P 3 Access Control List Line	sontext Mode Push) Not selected for migration Access List Objects	4 Network Objects		3 Access Control Policy Objects
Selected Context: Single Co Migration Summary (Post P 3 Access Control List Line	antext Mode Push) Not selected for migration Access List Objects (Blander, Extended, Extended and In BOV EXV/NECORP)	4 Network Objects		3 Access Control Policy Objects (Ore, Application, URL objects and Intrusion Rule Group)
Selected Context: Single Co Migration Summary (Post P 3 Access Control List Line	sontext Mode sush) Not selected for migration Access List Objects (Standard, Extended used in BOPP RAVPRESCRP)	4 Network Objects		3 Access Control Policy Objects (Geo, Application, URL objects and Intrusion Rule Orcup)
Selected Context: Single Co Migration Summary (Post P 3 Access Control List Line Not selected for migratic	ontext Mode Push) s Not selected for migration Access List Objects (Blandard, Extended used in BDV RAVYNELDRY)	4 Network Objects 2	Not selected for migration Part Objects	3 Access Control Policy Objects (Gee, Application, URL ebjects and Intrusion Rule Group)
Selected Context: Single Cr Migration Summary (Post P 3 Access Control List Line Not selected for migratic Dynamic-Route Object	entext Mode Push) * Not selected for migration Access List Objects (Standard, Demodel and B BDV RAV/NECOBY) on 2 Network Address Translation	4 Network Objects 2 Logical Interfaces	Not selected for migration Port Objects 1 Routes	3 Access Control Policy Objects (Gee, Application, URL objects and Intrusion Rule Group) 1 DHCP

Migration complète

Vérifier

Pour vérifier que le FDM a été correctement migré vers le cdFMC.

Accédez à CDO > Tools & Services > Firepower Management Center. Là, vous constatez que le nombre de périphériques enregistrés a augmenté.

cisco Defense Orches	strator	Ser	vices					Q Search		<mark>ଓ</mark> ⊳¶≁	۵.	±1 ()	-	-
Hide Menu		_							_	,	Cloud Hostname Version	Delivered	FMC	
C Multicloud Defense		FMC	Search by Device Name, IP Address Secure Connectors	i, or Serial Num	iber	J			6		Actions			
Configuration	>		"Auto onboard On-Prem FMCs from Se	cureX tenant" se	tting is not enabled. Click here to	enable settin	9.				O Cr ≙ De ⊕ Up	eck For Change ployment plates	es	
Objects	>	•	Name		Version	Devices	Туре	Status	Last Heartbeat		O AS	rkflows I Explorer		
«Č» VPN	>		Cloud-Delivered FMC	2	20240514	⊜3	Cloud-Delivered FMC	O Active	06/12/2024, 12:42:21		Manage	ment		
Events & Monitoring				7	7.2.7-build 500	⊜ 0	On-Prem FMC	A Unreachable				vices		
√r Analytics ④ Change Log ∰ Jobs	>										③ Po ④ Ot < N/ 소 Sil 소 Ro ③ Pi	licies ijects IT to Site VPN mote Access V atform Settings	(PN	
Settings	•	© C	Services Dynamic Attributes Connector	figrations	gration Tool						System			
			Gecure Connectors	요 ASA to FDM	M Migration D to cdFMC						O CC III Ser O AN → De A O Ci	nfiguration sart Licenses IP Managemen vice Health adit sco Cloud Even	rt NS	

périphériques enregistrés cdFMC

Vérifiez le périphérique dans Périphériques > Gestion des périphériques. En outre, dans les tâches du FMC, vous pouvez trouver quand le périphérique a été correctement enregistré et quand le premier déploiement s'est terminé avec succès.

Defense Orchestrator FMC / Devices / Secure Firewall Device Summary	Analysis Policies De	evices Objects Integration	+5 F	Return Home Deploy Q. O 🧬 🌣 🛛 📕	 dealer secure
-fdm-Azure			Deployments	Upgrades Health O Tasks	± ● Show Notifications
Cisco Firepower Threat Defense for Azure			20+ total 0	waiting 0 running 0 retrying 6 success 20+ failures	Q. Filter
Device Interfaces Inline Sets Routing DHCP	VTEP		Policy Deployment	ent	
			Policy Deploys	ment to -fdm-Azure. Applied successfully	1m 54s 🗙
General	/±∓	License			
Name:	-fdm-Azure	Performance Tier :	FTI O Health Policy		
Transfer Packets:	No	Essentials:	Apply Initial_H Health Policy ap	sealth_Policy 2023-06-29 17:28:08 to film-Azure plied successfully	1m 40s ×
Troubleshoot:	Logs CLI Download	Export-Controlled Features:			
Mode:	Routed	Malware Defense:	 Discovery 		
Compliance Mode:	None	IPS:	fdm-Azur	e - Discovery from the device is successful.	2m 10s 🗙
Performance Profile:	Default	Carrier:	 SETurnel 		
TLS Crypto Acceleration:	Disabled	URL:	-fdm-Azur	e - SFTunnel connection established successfully.	- ×
		Secure Client Premier:			
Device Configuration:	port Export Download	Secure Client Advantage:	Register		
OnBoarding Method:	Registration Key	Secure Client VPN Only:		Remove completed tasks	
Inspection Engine		Health		Management	/ 🔍
Inspection Engine:	Snort 3	Status:	0	Remote Host Address:	NO-IP
Revert to Short 2		Policy: Initial_Health_Policy 20	23-06-29 17:28:08	Secondary Address:	
		Excluded:	None	Status:	0
				Manager Access Interface:	Management Interface
Inventory Details	c	Applied Policies	1	Advanced Settings	1
×₩ ¤ + i					

Tâche d'enregistrement cdFMC terminée.

Le périphérique se trouve sur cdFMC > Device > Device Management.

	Defense Orchestrator FMC / Devices / Device Management	Analysis	Policies	Devices Objects Integration					🕤 Return Home Deploy Q. 💿 🌮 🌣			0	✓ store SECU			
View By All (3	7: Group • 3) • Error (0) • Warning (0)	Offline (0)	Normal (3)	 Deplo 	oyment Pending	g (3) 🔹 I	Upgrade (0)	 Snort 3 (3) 							Migrate Depk	oyment History
Collapse	<u>a Al</u>														Download	Device List Report
	Name			Model			Version	Chassis	Licenses		Acces	ss Contro	I Policy		Auto RollBack	
	V Ungrouped (3)															
	N/A - Routed Snort 3			FTDv fo	r Azure		7.4.1	N/A	Essentials		None				«Ø	1

Périphérique enregistré sur cdFMC

Politique de contrôle d'accès migrée sous Politiques > Contrôle d'accès.

٤	Defense Orchestrator FMC / Policies / Access Control / Access Control	Analysis	Policies	Devices	Objects	Integration		+> Return Home	Deploy	۹	•	6 24	0		~	cisco SECU	JRE
								Object Ma	nagement	Intr	rusion	Netw	ork Ana	alysis Policy	DNS	Import/Export	t
																New Polic	y
	Access Control Policy		St	atus			Last Modified		Lock S	itatus							
	Default Access Control Policy Default Access Control Policy with default action block		Tar	geting 0 devices			2024-06-11 22:28:19 Modified by "Firepower System"									6 0 × i	i
	FTD-Mig-ACP-1718216278		Tary Up-	geting 1 devices to-date on all targ	eted devices		2024-06-12 12:18:00 Modified by 1									5 0 × 1	i

Politique migratoire

De même, vous pouvez revoir les objets créés dans FDM qui ont été correctement migrés vers cdFMC.

Network	Add Network	۲ Q, Fil	ter		
		Sh	ow Unused Ob	jects	
A network object represents one or more IP addresses. Network objects are used in various places, including access control policies, network	rules, event se	arches, report:	, and so on.		
Name	Value		Туре	Override	
any	0.0.0.0/0 ::/0		Group		¶⊒ Q ≣ #
any-ipv4	0.0.0.0/0		Network		¶a, ≣ #
any-ipv6	::/0		Host		唱く言め
Banned	103.104.73.155		Host	0	◎/〒め
Gw_test01	172.22.2.1		Host		┗/〒め
Inside_Network_IP	192.168.192.10		Host	0	┗/〒Ѧ
IPv4-Benchmark-Tests	198.18.0.0/15		Network		¶a ()
IPv4-Link-Local	169.254.0.0/16		Network		¶∎ Q ⊕ M
IPv4-Multicast	224.0.0.0/4		Network		¶a () ₩
IPv4-Private-10.0.0.0-8	10.0.0/8		Network		¶∎ Q 🗑 🕅
IPv4-Private-172.16.0.0-12	172.16.0.0/12		Network		¶∎ Q ≣ M
IPv4-Private-192.168.0.0-16	192.168.0.0/16		Network		¶∎ Q ≣ #
IPv4-Private-All-RFC1918	10.0.0.0/8 172.16.0.0/12 192.168.0.0/16		Group		¶ <u>a</u> q≣#8
IPv6-IPv4-Mapped	::##:0.0.0.0/96		Network		¶∎ Q ≣ M
					B

Objets migrés de FDM vers cdFMC

Interfaces de gestion des objets migrées.

FMC / Objects / Object Mana	D r igement	Analysis	Policies	Devices	Objects	Integration		*> Return H	lome	Deploy	Q	•	¢	0		~	once SECURI
> AAA Server	Inter	face								Add				•	Q, Filter		
Access List Address Pools	Interface	e objects segmen	nt your networ	rk to help you r	manage and c	lassify traffic flow. An in	iterface object simply groups interfaces. These groups	s may span mult	tiple dev	rices; you o	an also	configu	re multipl	e interf	ace objects	on a singk	e device.
Application Filters AS Path	Name	•					Туре		Interfac	е Туре							
BFD Template Cipher Suite List	~ \$ 1	nside_ig					Interface Group		Routed								/ 1 8
> Community List DHCP IPv6 Pool	> =	-fdm-Azure	-														
> Distinguished Name DNS Server Group	× 44	nside_zone					Security Zone		Routed								/ 18
> External Attributes File List	~ #0	outside_ig	_				Interface Group		Routed								/ 28
> FlexConfig Geolocation	>	-fdm-Azure	2														
Interface Key Chain	~ 📥	utside_zone					Security Zone		Routed								/14
Network > PKI	>	-fdm-Azure	2														

Interfaces de gestion des objets migrées.

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.