在CDO中使用FMT将FDM迁移到cdFMC

目录			
<u>简介</u>			
<u>先决条件</u>			
<u>要求</u>			
使用的组	<u>件</u>		
<u>背景信息</u>			
<u>配置</u>			
<u>验证</u>			

简介

本文档介绍如何使用CDO中的Firepower迁移工具(FMT)将Firepower设备管理器(FDM)迁移到云交 付的FMC (cdFMC)。

先决条件

要求

- Firepower设备管理器(FDM) 7.2+
- 云交付的防火墙管理中心(cdFMC)
- CDO中包含Firepower迁移工具(FMT)

使用的组件

本文档正是基于上述要求而创建的。

- 版本7.4.1上的Firepower设备管理器(FDM)
- 云交付的防火墙管理中心(cdFMC)
- 云防御协调器(CDO)

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原 始(默认)配置。如果您的网络处于活动状态,请确保您了解所有命令的潜在影响。

背景信息

CDO管理员用户可以在设备使用版本7.2或更高版本时将其设备迁移到cdFMC。在本文档中介绍的 迁移中,cdFMC已在CDO租户上启用。

配置

要开始迁移,必须使FDM设备没有挂起的部署并注册到云服务。要注册到云服务,请导航到系统设置(System Settings) >查看更多(See More) >云服务(Cloud Services)。

在云服务部分中,您发现设备未注册,因此必须使用类型安全/CDO帐户执行注册。您必须配置注册 密钥,然后配置注册。



注册云服务

在云服务上,显示未注册。选择CDO帐户注册类型并提供CDO的注册密钥。

Firewall Device Manager	版 砂 苹王 Monitoring Policies Objects Device	S (a) (b) (c) (c) (c) (c) (c) (c) (c) (c) (c) (c
System Settings +- Management Access Logging Settings	Device Summary Cloud Services Not Registered	
> DHCP DDNS Service DNS Server Management Interface	You can register the device with the Clisco cloud to use additional cloud-based services. If you want to use Clisco Defense Orchestrator (CDO) for management or want to remain in evaluation mode, then register with the cloud using your CDO or other searchy account registration itsy, you can alternatively auto-enroll with CDO or a Secure Firewall Management Clearer using the device serial number, if you want to secure service and the classical security account are ready to learness the device, then cooperate service learned in the classical security account are device to learness the device, then cooperate visit the cloud, you can enable or disable features an ededd.	
Hostname Time Services SSL Settings	Enrollment Type Security/CDO Account Smart Licensing Region	
HTTP Proxy	US Region 🗸 🖉	
Reboot/Shutdown Remote Management	Registration Key Enter Registration Key	
Cloud Services Central Management	Service Enrolment Cisco Defense Orchestrator Cisco Defense Orchestrator Cisco Defense Orchestrator is a cloud-based management tool used for managing network	
Traffic Settings	devices. Select this option if you want to register the device in your Cisco Defense Orchestrator account.	
	Cisco Success Network Cisco Success Network enablement provides usage information and statistics to Cisco which are essential for Cisco to provide technical support. This information also allows Cisco to improve the product and to make you aware of unused available features so that you can maximize the value of the product in your network. Check our the Sample Data that will be sent to Cisco. See more > profile Enrol Cisco Success Network Need help?(5)	

注册云服务

注册密钥可以在CDO中找到。导航至CDO,转至资产>添加符号。

系统将显示一个菜单,用于选择您拥有的设备类型。选择FTD选项。必须启用FDM选项;否则,无 法执行相应的迁移。注册类型使用使用注册密钥。在此选项中,注册密钥出现在第3步中,我们必须 将其复制并粘贴到FDM中。

diade Defense Orchestrator	Inventory	Q Search	१त्र- 众⊚- ≝∎ ७-	•
Hide Menu	Templates Q Search by Device Name, IP Address, or Serial Number	Displaying 8 of 8 results		C () +
Multicloud	All ASA FTD			
inventory	Name \$	Configuration Status \$	Connectivity \$	

板载FDM,添加选项

出现"Select a Device or Service Type(选择设备或服务类型)"菜单。



选择设备或服务类型

对于此文档,已选择"选择注册密钥"。

Follow the steps below				Cancel
FTD JAAAA	A Important: This method of onbo delivered Firewall Management Sy	parding allows for local co-managen 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: FTD FTD FFDM FFDM (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 onlv)	Use Credentials (Basic) Onboard a device using its IP address, or host name, and a username and password.	
	X			

此处显示上一步所需的注册密钥。

FTD 0000 - ===	A Important: This method of onboarding allows for local co-management of the firewall via FDM. To manage your device with cloudelivered Firewall Management System, click the FTD button instead. Learn more
Firewall Threat Defense Management Mode: FTD FTD FFD FFDM F (Recommended)	Use Registration Key Use Serial Number Use Credentials (Basic) Onboard a device using a registration key generated from CDO and applied on the device using Firepower Device Manager. Use Serial Number Use Credentials (Basic) (FTD 6.7+, 1000, 2100 and 3100 series only) Choord a device using the series only) Use Credentials (Basic)
1 Device Name	
2 Database Updates	Enabled
3 Create Registration Key	7a53c
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

注册流程

获取注册密钥后,将其复制并粘贴到FDM中,然后单击注册(Register)。在云服务中注册FDM后 ,其将显示为启用,如图所示。

已跳过智能许可证,因为设备将在启动并运行后进行注册。

Monitoring	Policies	Objects	Device: joroa-fdm-tech
Device Summa Cloud Se	rvices Istered		
You can registe use Cisco Defe register with the auto-enroll with want to use Sec configure Smar	r the device w nse Orchestra e cloud using n CDO or a Se cure Firewall o t Licensing, w	vith the Cisco clo tor (CDO) for m your CDO or oth cure Firewall Ma device manager hich automatica	oud 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
Enrollment Type Security/CDC	e Account	Smart Licensing	
US Region Registration Ke 7a53c2	y		~ ()
 Service En Cisco Defe devices. S account. Enable Cisco Successential for product ar of the prodict ar of the prodict ar Check out Enroll 	rollment efense Orc ense Orchestra elect this option a Cisco Defen uccess Network or Cisco to pro- d to make you duct in your ne the Sample D Cisco Succes	hestrator ator is a cloud-b on if you want to se Orchestrator work enablement pro ovide technical s a ware of unuse stwork. ata that will be s s Network	vased management tool used for managing network o register the device in your Cisco Defense Orchestrator 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 sent to Cisco. See.more V
REGISTER	Need he	lp? 🕑	

FDM注册

注册FDM时,它将显示租户、已连接和已注册的云服务。

题 资 章 和 Find The State	(≥) (admin Administrator ∨ cisco SECURE)
Device Summary Cloud Services Connected Registered Region: US Region	٥ ×
Cisco Defense Orchestrator DISABLE	Cisco Success Network DISABLE Cisco Success Network enablement provides usage information and statistics to Cisco which
Note: If the device is registered to cloud services using smart Licensing, the device will not work with CDD. Please uprecision the device and re-on-board using the registration key method with the "Security/CDD account" option. Cisco Defense Orchestrator (2) allows you to configure multiple devices of different types from a cloud-based configuration portal, allowing deployment across your network.	are essential for Cisco to provide technical support. This information also allows Cisco to improve the product and to make you aware of unused available features so that you can maximize the value of the product in your network. Check out the <u>Sample Data</u> that will be sent to Cisco.
Send Events to the Cisco Cloud ENABLE Disabled	
You can send events to the Cisco cloud server. From there, various Cisco cloud services can access the events. You can then use these cloud applications, such as Cisco SecureX threat response (2, to analyze the events and to evaluate threats that the device might have encountered. When you enable this service, this device will send high priority intrusion, file, malware events and all connection events to the Cisco cloud.	

FDM注册完成

在CDO中的"库存"(Inventory)菜单中,FDM可在入网和同步过程中找到。可以在Workflows部分中查 看此同步的进度和流程。

此过程完成后,将显示为"已同步"和"联机"。

"dialli cisco Defense Orchestrator	Inventory		Q Search 🕐 🏞	¢0• ≜1 ?•
⊟ Hide Menu	T Devices Templates Q Search by Device Name, IP Address, or Serial Number		Displaying 9 of 9 results	> FOM
dia Dashboard	All ASA FTD			Device Details
Multicloud Defense				Model Cisco Firepower Threat Defense for
inventory	Name 2	Configuration Status \$	Connectivity \$	Serial
Configuration			A Unreachable	Version 7.4.1-172 Onboarding Registration Key Method
Objects	D FOM		O Serial Number Mismatch	Snort Version 3.1.53.100-56
🔥 VPN 🔅	O	O Not Synced	Pending Setup	Syncing CDO is communicating with your device. Please check back in a moment.
√ Analytics →	O FTD		Pending Setup	Device Actions
(4) Change Log	O FTD		Pending Setup	♦ API Tool Workflows ③ Manage Backups
Tools & Services	C International	Syncing	Online	Remove Management
JSt certuids			Online	Notes
			Online	Lecutive Report
		Ø Not Synced	A Unreachable	Conflict Detection Check every: Tenant default (24 hours) =
				Label Groups and Labels
				Add Labels O

CDO资产FDM已注册

设备同步后,将显示为"联机"和"已同步"。

当FDM成功注册到CDO后,我们必须注销FDM。退出FDM后,在CDO中导航到工具和服务>迁移 >防火墙迁移工具。

% Tools & Services		Tools & Services	Migrations		
Settings	>	Oynamic Attributes Connector	Firewall Migration Tool		
		⇒ Secure Connectors	會 ASA to FDM Migration		
		🖨 Firewall Management Center	备 Migrate FTD to cdFMC		
		ASA Templates			

单击Add符号,将显示一个随机名称,表示需要重命名该名称以启动迁移进程。

$\fbox{\begin{tabular}{ c c } \hline \hline Q_{c} & search for a migration by name$		Displaying 0 of 0 needs			1 C 🔹
Name 2	Status	Created Date 2	Depresisioning Date #	Actions	/
		o migrations found. Begin migrating AS	A, FDM, Checkpoint, Forlinet, or Palo Alto Networks firewalls to FTD.		

重命名后,单击Launch开始迁移。

	C Sear
Initialize Migration	×
To initialize the migration process, name this migration and click OK. Cl notify you when the migration tool is ready for use. When ready, select migration and launch the tool.	00 will this named
Name *	
fdm_migration	
This is an auto-generated name. You can change it if you wish.	
Can	cel OK

初始化迁移

单击Launch开始迁移配置。

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

迁移启动流程

单击Launch后,将打开一个窗口,显示选择选项Cisco Secure Firewall Device Manager (7.2+)的迁 移过程。如前所述,此选项从版本7.2开始启用。

Firewall Migration Tool (Version 6.0.1)

Select Source Configuration ()

Source Firewall Vendor	
Select Source	^
Cisco ASA (8.4+)	
Cisco Secure Firewall Device Manager (7.2+)	
Check Point (r75-r77)	
Check Point (r80-r81)	
Fortinet (5.0+)	
Palo Alto Networks (8.0+)	

FMT选择源配置

选择后,系统将显示三种不同的迁移选项:仅共享配置、包括设备和共享配置,以及从"设备和共享 配置"到"FTD新硬件"。

对于此实例,将执行第二个选项"迁移Firepower设备管理器"(Migrate Firepower Device Manager)(包括设备和共享配置)。

	lick on text below to get additional details on each of the migration options	
)	Migrate Firepower Device Manager (Shared Configurations Only)	>
Ì	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.	

迁移选项

选择迁移方法后,继续从提供的列表中选择设备。

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											
fdm_fdm_fdm_fdm_fdm_fdm_fdm_fdm_fdm_fdm_											
Connect											

FDM设备选择



配置提取已完成

建议打开顶部的选项卡,查看并了解选择设备时的步骤。



迁移过程的步骤

作为新迁移,请在系统提示时选择Cancel选项"Do you want to use an Existing Access Control Policy, NAT or RAVPN Policy on FMC?"

Do you want to use an Existing Access Control Policy, NAT or RAVPN Policy on FMC.	
Save Cancel	

现有配置的取消选项

然后,系统将提供用于选择要迁移的功能(如图所示)的选项。单击Proceed。

	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 shou	d be carried o	out in a maintena	nce window.								
Select Target 🕡					^			Science	ource: Cisco Secure I sted Migration: Inclu	Firewall Device Manager (7.2+) des Device and Shared Config		
Firewall Management -	Cloud-delivered FMC									>		
Select Features										~		
Device Configuration		SI	nared Configura	ation				Optimization				
✓ Interfaces		~	Access Control				1	🗸 Migrate Only Re	ferenced Objects			
✓ Routes			🧹 Migrate tunn	elled rules as Pref	lter		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 Tunn	iels (no data)		Access Control Policy Objects (Geolocation, Application, URL objects and Intrusion Rule									
Policy Based (Cr	ypto Map)		 Group) Time based Obii 	ects (no data)								
Route Based (V7	7)		Remote Access	VPN								
Platform Settings			File and Malware	Policy								
- DHCP												
Server												
Relay												
DDNS												
Proceed	-											
Note:Platform settings ar	d file and malware policy migrat	ion is supporte	d in FMC 7.4 and I	ater versions.								

要选择的功能

然后Start Conversion。

rewall Migration Tool (Version 6.0	.1)									
	()	-0	3	4	5	6	7	8	9	
	Extract FOM 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	nce window.		_				
Select Target 🕥					<u> </u>			Sele	ource: Cisco Secure Firew cted Migration: Includes [all Device Manager (7.2+) Device and Shared Config
Firewall Management - C	loud-delivered FMC									>
Select Features										>
Rule Conversion/ Proces	is Config									~
Start Conversion										

开始转换。

解析过程结束后,可以使用两个选项:下载文档并通过点击下一步继续迁移。



下载报告.

设备接口设置为显示。最佳做法是单击Refresh更新接口。验证完成后,您可以点击下一步继续。

	1 Extract FDM Information	2 Select Target	3 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 Confg)	9 Complete Migration				
Note: St	eps 7,8 and 9 should	d be carried	out in a maintenar	ice window.									
Map FTD Interface 🗿						Refresh	So	ource: Cisco Seco elected Option: I	ure Firewall Device Mana ncludes Device and Shar	ger (7.2+) ed Config			
FDM Interface Name		'	FTD Interface Nam	e									
inabitFthernet0/0		Gia	abiEthernet0/0										
GigabitEthernet0/1		Gio	abitEthernet0/1										
20 v pergoagei2 ∣⊲ ⊰ Page	1 of 1 🕨 🕨										e	Success	
										Back	Next	Success	ally gathered

显示的接口

导航到安全区域和接口组部分,需要在这里使用添加SZ和IG手动添加。 对于本示例,已选择Auto-Create。这有助于在要迁移到的FMC内自动生成接口。完成后,单击Next按钮。

Firewall Migration Tool (Version 6.0.1)

	1 Extract FDM Information	2 3 Select Target Map FTD Inte	rface Map Security Zones & Review & Va Interface Groups (Shared Co	6 Idate Push Shared Config To fig) FMC	7 Move Manager Revi (De	8 ew & Validate vice Config)	9 Complete Mgration	
	Note: Steps 7,8 and 9 shoul	ld be carried out in a main	tenance window.					
Map Security Zone	es and Interface Grou	ips 🛈	<u> </u>	Add Si	Z & IG Auto-Cr	eate	Source: Cisco Secure Firew Selected Option: Includes (all Device Manager (7.2+) Device and Shared Config
FDM Logical Interface	FDM Security Zone	FTD Interfac	ce FMC Secur	ity Zones FI	MC Interface Groups			
cutside	outside_zone	GigabitEthernet0/	0 outside_zone (A)	Sele	ct Interface Groups	~		
inside	inside_zone	GigabitEthernet0/	1 inside_zone (A)	Sele	ct interface Groups	×		

安全区域和接口组

Auto-Create选项将FDM接口映射到具有相同名称的现有FTD安全区域和FMC中的接口组。

FTD		Group
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. Select the objects that you want to map to FDM interfaces Security Zones Interface Groups Cancel Auto-Create	ups

Auto-Create选项。

然后选择Next。

Firewall Migration	n Tool (Version 6.0.1))					
		Extract FDM Information Select	2 3 4 t Target Map FTD Interface Map Security Z Interface Gro	5 6 ones & Review & Validate Push Shared pugs (Shared Confg) PMC	Config To Move Manager Review (Device	9 Validate Complete Migration Config)	
	No	ote: Steps 7,8 and 9 should be c	arried out in a maintenance window				
	Map Security Zones a	and Interface Groups ()			Source: Cisco Secure Firewa Selected Option: Includes D	I Device Manager (7.2+) evice and Shared Config
					Add SZ & IG Auto-Crea	e	
	FDM Logical Interface N	FDM Security Zones	FTD Interface	FMC Security Zones	FMC Interface Groups		
	outside	outside zone	Gigabi/Ethernet0/0	outside zone (A)	outside in (A)		
	inside	inside zone	GigabitEthernet0/1	inside_zone (A)	inside_ig (A)	v	
	Note;Click on Auto-Create butto	n to auto map the FDM nameif as	the name of the FMC interface objects a	ind security zones. Click on next t	button to proceed ahead.		
	10 v pmr.sPB38 2 4 4	Page 1 of 1 ▶ ▶					
							Back Next

After-Creation选项。

在步骤5中,如顶部栏中所示,请花时间检查访问控制策略(ACP)、对象和NAT规则。继续仔细检查 每个项目,然后单击Validate确认名称或配置没有问题。

Firewall Migration 1	Tool (Ve	rsion 6.0	.1)											
			Extract FDM Information Set	2 lect Target	3 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	Mgration		
			Note: Steps 7,8 and 9 should be	carried ou	t in a maintena	nce window.								
C	Optimize	e, Reviev	w and Validate Share	d Confi	guration C	Only 🕠	^	,		Sele	ource: C	Cisco Secure Fire gration: Includes	vall Device Manager Device and Shared ((7.2+) Config
A	ccess Contro	ol Objects	NAT Interfaces Routes		e VPN Tunnels 🌘	Remote Acce								
	Access Lis	st Objects	letwork Objects Port Objects A	Access Cont	trol Policy Object	s VPN Objects	Dynamic-Rout	e Objects						
C	Select all	3 entries s	Selected: 0/3 Actions +									Q Search		
	• *	Nam Q	e		Validation State			Туре Q			Value Q			
C	1	Outsidel	Pv4Gateway		Validation pending			Network Object			172.18.1.1			
0	2	Outside	Pv4DefautRoute		Validation pending			Network Object			0.0.0.0/	0		_
ierpage 1 to 3 of 3 [4 ≼ Pa	age 🚺	of1 ► ►I												
												/		
											Validat	10		

访问控制、对象和NAT配置

然后仅推送共享配置

		Successfully Validat	be	
dation Summary (Pre-pu	ush)		eu	
3		4		3
ccess Control List Lines		Network Objects		Access Control Policy Objects (Geo, Application, URL objects and Intrusion Rule Group)
2	Not selected for migration			
Network Address Translation				

仅推送共享配置

可以观察到完成的百分比和正在处理的特定任务。

Firewall Migrati	on Tool (Version 6.0.1)			
	Push Shared Config to I	FMC	PUSHING	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 summ	hary. Download Report	

推送百分比

完成步骤5后,继续执行步骤6(如顶部栏所示),此时将将共享配置推送到FMC发生。此时,请选 择Next按钮前进。

	1 Extract FCM Information	2 Select Target Map	3 FTD interface	4 Map Security Zones & Interface Groups	5 Review & Validate (Shared Config)	Push Shared Config To FINC	7 Move Manager	8 Review & Validate (Device Config)	9 Complete Migration	
	Note: Steps 7,8 and 9 shou	Id be carried out in a	a maintenanc	e window.						
Push Shared Cor	fig to FMC				^			Solution	Source: Cisco Secure Firev	vall Device Manager
Migration Status								Jen	ected migration. Includes	Device and onlared c
Live Connect: Selected Context: Single Co Migration Summary (Post P	ntext Mode Jsh)			4					3	
Live Connect: Selected Context: Single Co Migration Summary (Post P 3 Access Control List Line	ntext Mode Jsh)			4	biects				3 Access Control Policy O	biects
Live Connect: Selected Context: Single Co Migration Summary (Post P 3 Access Control List Line	ntext Mode ush) Hot se Acc (Standard			4 Network Of	bjects				3 Access Control Policy O (Geo, Application, URL obje lithrusion Rule Group)	bjects cts and)
Live Connect: Selected Context: Single Co Migration Summary (Post P 3 Access Control List Liner Not selected for migratio	ntext Mode Ish) Hot se C(Slander)	Aected for migration ess List Objects 1, Edanded used is BORY RAVIPAGEORY 2		4 Network Of	bjects r migration				3 Access Control Policy O (Geo, Application, URL obje Intrusion Rule Group) Not selected for migra	bjects ts and bion
Live Connect: Selected Context: Single Co Migration Summary (Post P 3 Access Control List Line: Not selected for migratio Dynamic-Roote Objects	ntext Mode ush) Not se Clander	Alected for migration ess List Objects 1, Edended used is BORY RAVPRECARP 2 k Address Translation		4 Network Of Not selected for Logical Inte	bjects r migration rrfaces				3 Access Control Policy O (Geo, Application, URL obje- intrusion Rule Group) Not selected for migra	bjects cts and bion

将共享配置推送到FMC已完成

此选项会触发确认消息,提示继续管理器迁移。

Confirm Move Manager

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



确认移动管理器

继续管理员迁移需要拥有管理中心ID和NAT ID,这是必不可少的。通过选择Update Details,可以 检索这些ID。此操作将启动一个弹出窗口,在此窗口中输入cdFMC中FDM表示的所需名称,然后保 存更改。

Firewall Migration Tool (Version 6.0	0.1)									
	1			-(5)		•	8	9		
	Extract FDM Information	Select Target Map FTD Inte	rface 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	I be carried out in a main	tenance window.		_					
Move Manager				^			Selec	ource: Cisco Se ted Migration:	cure Firewall Device Includes Device and	Manager (7.2+) Shared Config
Update Deta	ils	a downtime window. Af	ter you register the de	avice with the m	anagement center	or Cloud-delive	ered FMC. vou ca	an no longer use	the device manager	r to manage it.
Management Cent	Management Cente (NAT ID	Threat D	efense Hostn	DNS Serve	r Group	Managemen	nt Center/	Data Interface	
cisco cdi	»		1	Lcloud	app.n CiscoUmbrellaDN	SServerGroup ~	💿 Data 🔵 Ma	anagement	Select Data Interface	×

管理员中心ID和NAT ID

	Extract FOW information See	2 Upda	te Device Name for F	X	B Darpine Migration (Davice Config)		
	Note: Steps 7,8 and 9 should be	carried -					
Move Manager			Cancel Save		Source: Cisco Sec Selected Migration: I		
Update Det	als						
This step is mandatory a	nd should be performed during a d	downtime			d FMC, you can no longer use t	the device manager to m	anage it.
This step is mandatory a Management Cent	nd should be performed during a C	NAT ID 💿	Threat Defense Hostn	DNS Server Group	d FMC, you can no longer use I Management Center/	the device manager to m Data Interface	anage it.
This step is mandatory a Management Cent cisco-mex-refre-tac spp us cd	nd should be performed during a d Management Cente 3	Iowntime NAT ID 💿	Threat Defense Hostn	DNS Server Group CiscoUmbrelisDNSServerGroup ~	d FMC, you can no longer use t Management Center/ Data Management	the device manager to m Data Interface Select Data Interface	anage it.

更新设备名称以进行注册。

执行此操作后,将显示上述字段的ID。



警告:请勿对管理中心界面进行任何更改。默认情况下,Management选项处于选中状态 ,保留该选项为默认设置。

Firewall Migration	n Tool (Version 6.0	.1)										
		Extract FDM information	2 Select Target	3 Map FTD Interface Map	4 Security Zones & Interface Groups	5 Review & Validate (Shared Config)	6 Push Shared Config To FMC	7 Nove Manager	8 Review & Validate (Device Config)	9 Complete Migration		
		Note: Steps 7,8 and 9 should	be carried out	in a maintenance	window.							
	Move Manager					^			Sc Selec	urce: Cisco Sec ted Migration:	cure Firewall Device M Includes Device and	lanager (7.2+) Shared Config
	Update Detai	Is										
	This step is mandatory an	d should be performed during	a downtime w	indow. After you re	gister the dev	vice with the ma	inagement center	or Cloud-delive	red FMC, you ca	n no longer use	the device manager	to manage it.
	Management Cent	Management Cente	NAT ID		Threat De	fense Hostn	DNS Server	Group	Managemer	it Center/	Data Interface	
	cisco us.cdo	ogu 16	6GW 104V	3sPI	fdm-Azu	re	CiscoUmbrellaDN	SServerGroup 🗸	💿 Data 🔵 Ma	nagement	Select Data Interface	~
		L			_						/	

Move Manager

管理中心ID & NAT ID。

选择Update Details选项后,设备将开始同步。

on Tool (Version 6.	0.1)										
	1)- Extract FDM Infor	2 mation Select Target	3 Map FTD Interface	d f				6 9 Review & Validate (Device Config)			
	Note: Steps 7,8 and 9	should be carrie	d out in a maintena	ance window.							
Move Manager								Source: Cisco Selected Migrat	o Secure Firewa ion: Includes De		
Update De	tails	during a downti	me window.	SYN	CING the FDM D	evice	ıd-deliver	ed FMC, vou can no longer	r use the device	manager to ma	anage it.
Management Cent	Management Cen	te 🗊 🛛 🗛	ID 🕢		9% Complete			Management Center/	. Data Int	erface	
								Data Varannat			
cisco us.o	do oguq	166GW. 104			ure			Usta O Management		nternace	

同步FDM设备

完成迁移后,下一步是通过选择验证来检查FDM中配置的接口、路由和DHCP设置。

rewall Migration Too	ol (Versio	on 6.0.1)				
		(1) (2) Extract FDM Information Select Tar	(3) (4) (4) (4) (4) (4) (5) (4) (4) (5) (4) (4) (4) (4) (4) (4) (4) (4) (4) (4	5 6 7 4 Validate Push Shared Config To Move Manager d Config) FMC	9 Review & Validate Complete Migration (Device Config)	
		Note: Steps 7,8 and 9 should be carr	ed out in a maintenance window.			
Opti	imize, F	Review and Validate Device C	onfiguration Page 0	^	Source: Cisco Secure Fir Selected Migration: Include	rewall Device Manager (7.2+) as Device and Shared Config
		Objects NAT Interfaces Routes Site	-to-Site VPN Tunnels 👩 Remote Access VPN	SNMP DHCP		
Sta	atic PPPo8					
Se	elect all 2 ent	tries Selected: 0 / 2			Q Search	+
•		Interface	Zone	IP Address	State	
	1	GigabitEthernet0/0	outside_zone		Enabled	
0	2	GigabitEthernet0/1	inside_zone	45.1	Enabled	
1 to 2 of 2 14 4 Page [1_ of 1	5 F			Validate	

验证FDM配置设置

验证之后,选择Push Configuration以启动配置推送进程,该进程将持续到迁移结束为止。此外,还可以监控正在执行的任务。

	\odot	Successfully Validated		
alidation Summary (Pre-pu	Ish) Not selected for migration	2	1	1
		Logical Interfaces	Routes (Static Routes, ECMP)	DHCP (Server, Relay, DDNS)
	0 Platform Settings	0 Malware & File Policy		

验证状态-推送配置。

包含百分比推送配置的弹出窗口。

Firewall Migration	on Tool (Version 6.0	0.1)				
		Estract FDM Information S Note: Stops 7,8 and 9 should b	elect Target Map FTD	PUSHING 10% Complete Push to Cloud-delivered FMC is In progress. Please wait for entire rush process to complete the micration	7) danager	Beview & Valdane Complete Migration (Device Confg)
	Complete Migra Migration Status	ition		nen so entre part process to comprese the regeneror.		Source: Cisco Secure Firewall Device Manager (7.2+) Selected Migration: Includes Device and Shared Config
	Interfaces	0				
	Routes					
	Policy Assignment					
L	Please download the Post-	Push migration report for a detailed :	summary. Download Re			

推送完成百分比

完成后,将显示启动新迁移的选项,标记从FDM到cdFMC的迁移过程的结束。

ration Tool (Version 6.0.	1)			
	2 Extract FDM Information Select Target	3 4 5 Map PTD Interface Map Security Zones & Review & Validan Interface Groups (Shared Config)	6 7 8 e Push Shared Config To Move Manager Review & PMC (Device	Valdam Complete Migration Config)
	Note: Steps 7,8 and 9 should be carried out i	in a maintenance window.		
Complete Migrati	on			Source: Cisco Secure Firewall Device Manager (7.24 Selected Migration: Includes Device and Shared Confi
Migration Status		7		
Migration is complet Next Step - Login to	, policy is pushed to FMC. FMC to deploy the policy to FTD.			
Live Connect:				
Selected Context: Single Co	ntext Mode			
Migration Summary (Post P	ush)			
3		4		3
Access Control List Line:	Access List Objects	Network Objects		Access Control Policy Objects
				(Geo, Application, URL objects and
				Intrusion Rule Group)
				Intrusion Rule Group)
	(Standard, Extended used in BOR RAVPRICEORP)	2	1	Intrusion Rule Group)
	(Stender, Detender used in BOX RAVIPSECOP)	2 Logical Interfaces	1 Routes	Intrusion Rule Group)
	(Stender, Extended used in BCR RAVINECORP) n Network Address Translation	2 Logical interfaces	1 Routes (Static Routes, ECMP)	Intrusion Rule Group)

完成迁移

验证

验证FDM是否已成功迁移到cdFMC。

导航到CDO > Tools & Services > Firepower Management Center。您会发现注册设备的数量已增加。

altali cisco	Defense Orchestrat	or	Ser	vices					Q Search		ଓ 🕅	-	۵۰ ⇔	D (P)	-	•
≡	Hide Menu											>	Cloud-D	elivered I	FMC	
in.	Dashboard			Search by Davice Name ID Address	or Carial Ma	mbar							Version	20240514		
0	Multicloud Defense		FMC	Secure Connectors	, or overlar inc								Actions			
	Inventory		-										0.00	-		
Con	figuration			"Auto onboard On-Prem FMCs from Sec	ureX tenant"	setting is not enabled. Click here to e	enable setting	g.					d Deplo	yment	15	
۲	Policies	>											 Updat Workt 	es lows		
¢	Objects	>	2	Name		Version	Devices	Туре	Status	Last Heartbeat			O APLE	plorer		
-&-	VPN	>		Cloud-Delivered FMC		20240514	⊜ 3	Cloud-Delivered FMC	Active	06/12/2024, 12:42:21			Managemer	e		
Eve	ts & Monitoring					7.2.7-build 500	00	On-Prem FMC	A Unreachable	*			Devic	es		
*	Analytics	>											 Polici Object 	15		
۲	Change Log												< NAT			
	Jobs												-> Site to	Site VPN te Access VP	PN	
R	Tools & Services		Tools I	& Services N	ligrations								Platfo	rm Settings		
٢	Settings	>	00	Dynamic Attributes Connector	Firewall !	Migration Tool							System			
			# S	Secure Connectors	ASA to F	DM Migration							O Confi	guration		
				SA Templates	ar migrate i	TD to cormo							Smart AMP	Licenses Management	e	
				and the property of									+ Devic	a Health		
													Cisco	Cloud Event	ts	

cdFMC注册设备

在Devices > Device Management中检查设备。此外,在FMC的任务中,您可以找到设备成功注册 和首次部署成功完成的时间。

Defense Orchestrator FMC / Devices / Secure Firewall Device Sum	mmary Analysis Policies De	vices Objects Integration	*> F	Return Home Deploy Q 💿 🍘 🗭 📕	~ dudu SECURE
-fdm-Azure			Deployments	Upgrades Health OTasks	🛨 🌑 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 Routin	Ig DHCP VTEP		Policy Deployme	ent	
		-	Policy Deploy	ment to -fdm-Azure. Applied successfully	1m 54s 🗙
General	∕±∓	License			
Name:	-fdm-Azure	Performance Tier :	FTI Health Policy		
Transfer Packets:	No	Essentials:	Apply Initial_H Health Policy ap	Health_Policy 2023-06-29 17:28:08 to fdm-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:	 SETional 		
TLS Crypto Acceleration:	Disabled	URL:	-1dm-Azur	e - SFTunnel connection established successfully.	- X
		Secure Client Premier:			
Device Configuration:	Import 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
Revent to Snort 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	/
X III 🖙 + 1					

cdFMC注册任务已完成。

设备位于cdFMC > Device > Device Management中。

Defense Orchestrator FMC / Devices / Device Management	Analysis	Policies	Devices Objects Integ	ration		Return Home Deploy	୦ 🚱 ଓଡ଼ି 📕	~	sco SECURE
View By: Group All (3) Error (0) Warning (0)	Offline (0)	Normal (3)	 Deployment Pending (3) 	• Upgrade (0)	 Snort 3 (3) 		6	Migrate Deployme	ent History Add 💌
Collapse All								Download Dev	ice List Report
Name			Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack	
Ungrouped (3)									
-fdm-Azure Snort 3 N/A - Routed			FTDv for Azure	7.4.1	N/A	Essentials	None	e\$9	11

在Policies > Access Control下迁移的访问控制策略。

CONTRACTOR POLICIES / Access Control / Access Control	Analysis Poli	cies Devices	Objects	Integration		+> Return Home	Deploy	Q	•	6 2 (0		~	diada SECURE
						Object Ma	anagement	Intr	usion	Netw	ork An	alysis Policy	DNS	Import/Export
														New Policy
Access Control Policy		Status			Last Modified		Lock !	Status						
Default Access Control Policy Default Access Control Policy with default action block		Targeting 0 devices			2024-06-11 22:28:19 Modified by "Firepower System"									60∕¥
FTD-Mig-ACP-1718216278		Targeting 1 devices Up-to-date on all targ	eted devices		2024-06-12 12:18:00 Modified by 1									90/0

迁移策略

同样,您可以查看在FDM中创建的对象,这些对象已正确迁移到cdFMC。

Network	Add Network	• Q. F	ilter									
		. 5	Show Unused Of	ojects								
A network object represents one or more IP addresses. Network objects are used in various places, including access control policies, network variables, intrusion rules, identity rules, network discovery rules, event searches, reports, and												
Name	Value		Туре	Override								
any	0.0.0.0/0 ::/0		Group		¶a ⊂ ∰ M							
any-ipv4	0.0.0.0/0		Network		唱く言め							
any-ipv6	::/0		Host		唱く言め							
Banned	103.104.73.155		Host	0	有人资格							
Gw_test01	172.22.2.1		Host		%/ ₽₩							
Inside_Network_IP	192.168.192.10		Host	0	┗/〒め							
IPv4-Benchmark-Tests	198.18.0.0/15		Network		₽ < ₩							
IPv4-Link-Local	169.254.0.0/16		Network		¶a q ∦ M							
IPv4-Multicast	224.0.0.0/4		Network		¶a q ∦ M							
IPv4-Private-10.0.0.0-8	10.0.0/8		Network		¶a 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		¶∎ Q ≣ #8							
IPv6-IPv4-Mapped	::##:0.0.0.0/96		Network		¶∎ Q ≣ M							
					B A - H							

从FDM迁移到cdFMC的对象

已迁移对象管理接口。

FMC / Objects / Object Ma	ator Analysis	Policies Device	s Objects	Integration		•> Return	Home	Deploy	۹	o 🧬	° 0		~ d	see SECURE
AAA Server Access List Address Pools Application Eliters	Interface	it your network to help y	ou manage and e	classify traffic flow. An in	terface object simply groups interfaces. These groups	i may span mul	ltiple dev	Add	an also c	onfigure m	• ultiple inte	Q, Filter	n a single de	Ivice.
AS Path BFD Template Cipher Suite List	Name *				Type Interface Group		Interfac Routed	е Туре					/	¥ #
DHCP IPv6 Pool Distinguished Name DNS Server Group External Attributes	A inside_zone A inside_tone	•			Security Zone		Routed						1	¥ M.
File List > FlexConfig Geolocation		5			Interface Group		Routed						1	₽ A
Key Chain Network > PKI	> A outside_zone	2			Security Zone		Routed						/	¥ M

已迁移对象管理接口。

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言,希望全球的用户都能通过各 自的语言得到支持性的内容。

请注意:即使是最好的机器翻译,其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任,并建议您总是参考英文原始文档(已提供 链接)。