Configurazione di FTD dal file di configurazione ASA con lo strumento di migrazione Firepower

Sommario

Introduzione Prerequisiti Requisiti Componenti usati Premesse Configurazione Verifica Bug noti relativi allo strumento di migrazione Firepower Informazioni correlate

Introduzione

Questo documento descrive un esempio di migrazione di Adaptive Security Appliance (ASA) a Firepower Threat Defense (FTD) su FPR4145.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenze base di ASA
- Conoscenza di Firepower Management Center (FMC) e FTD

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- ASA versione 9.12(2)
- FTD versione 6.7.0
- FMC versione 6.7.0
- Firepower Migration Tool versione 2.5.0

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Esportare il file di configurazione ASA in formato **.cfg** o **.txt**. Il CCP deve essere installato con un FTD registrato.

Configurazione

1. Scaricare Firepower Migration Tool da <u>software.cisco.com</u> come mostrato nell'immagine.



2. Esaminare e verificare i requisiti nella sezione <u>Linee guida e limitazioni</u> per lo strumento di migrazione Firepower.

3. Se si prevede di eseguire la migrazione di un file di configurazione di grandi dimensioni, configurare le impostazioni di sospensione in modo che il sistema non passi alla modalità sospensione durante un'operazione push di migrazione.

3.1. Per Windows, selezionare Opzioni risparmio energia nel Pannello di controllo. Fare clic su **Modifica impostazioni combinazione** accanto alla combinazione per il risparmio di energia corrente. Modifica **Sospensione computer** impostata su **Mai**. Fare clic su **Salva modifiche**.

3.2. Per MAC, passare a **Preferenze di sistema > Risparmio energetico**. Selezionare la casella accanto a per impedire che il computer si spenga automaticamente quando lo schermo è spento e trascinare **Spegni schermo** dopo il dispositivo di scorrimento su Mai.

Nota: Questo avviso viene visualizzato quando gli utenti MAC tentano di aprire il file scaricato. Ignorare l'avviso e seguire il passo 4 A.



4. A. Per MAC: utilizzare il terminale ed eseguire questi comandi.

```
CAROLDSO-M-WGYT:~ caroldso$ cd Downloads/
CAROLDSO-M-WGYT:Downloads caroldso$ chmod 750 Firepower_Migration_Tool_v2.5-6263
.command
CAROLDSO-M-WGYT:Downloads caroldso$ ./Firepower_Migration_Tool_v2.5-6263.command
[75653] PyInstaller Bootloader 3.x
[75653] LOADER: executable is /Users/caroldso/Downloads/Firepower_Migration_Tool
_v2.5-6263.command
[75653] LOADER: homepath is /Users/caroldso/Downloads
[75653] LOADER: homepath is /Users/caroldso/Downloads
[75653] LOADER: mEIPASS2 is NULL
[75653] LOADER: archivename is /Users/caroldso/Downloads/Firepower_Migration_Too
1_v2.5-6263.command
[75653] LOADER: archivename is /Users/caroldso/Downloads/Firepower_Migration_Too
1_v2.5-6263.command
[75653] LOADER: Cookie found at offset 0x219AE08
[75653] LOADER: Extracting binaries
[75653] LOADER: Extracting binaries
```

```
127.0.0.1 - - [23/Nov/2021 14:49:47] "GET /inline.318b50c57b4eba3d437b.bundle.js

HTTP/1.1" 200 -

127.0.0.1 - - [23/Nov/2021 14:49:47] "GET /cui-font.880241c0aa87aa899c6a.woff2 H

TTP/1.1" 200 -

2021-11-23 14:49:47,999 [INFO | cco_login] > "EULA check for an user"

127.0.0.1 - - [23/Nov/2021 14:49:48] "GET /assets/cisco.svg HTTP/1.1" 200 -

2021-11-23 14:49:48,013 [DEBUG | common] > "session table records count:1"

127.0.0.1 - [23/Nov/2021 14:49:48] "GET /api/eula_check HTTP/1.1" 200 -

127.0.0.1 - [23/Nov/2021 14:49:48] "GET /api/eula_check HTTP/1.1" 200 -

127.0.0.1 - [23/Nov/2021 14:49:48] "GET /assets/icons/login.png HTTP/1.1" 200 -

127.0.0.1 - [23/Nov/2021 14:49:48] "GET /assets/images/1.png HTTP/1.1" 200 -

127.0.0.1 - [23/Nov/2021 14:49:48] "GET /assets/images/3.png HTTP/1.1" 200 -

127.0.0.1 - [23/Nov/2021 14:49:48] "GET /assets/images/3.png HTTP/1.1" 200 -

127.0.0.1 - [23/Nov/2021 14:49:48] "GET /assets/images/3.png HTTP/1.1" 200 -

127.0.0.1 - [23/Nov/2021 14:49:48] "GET /assets/images/3.png HTTP/1.1" 200 -

127.0.0.1 - [23/Nov/2021 14:49:48] "GET /assets/images/3.png HTTP/1.1" 200 -

127.0.0.1 - [23/Nov/2021 14:49:48] "GET /assets/images/3.png HTTP/1.1" 200 -

127.0.0.1 - [23/Nov/2021 14:49:48] "GET /assets/images/3.png HTTP/1.1" 200 -

127.0.0.1 - [23/Nov/2021 14:49:48] "GET /assets/images/3.png HTTP/1.1" 200 -

127.0.0.1 - [23/Nov/2021 14:49:48] "GET /assets/images/3.png HTTP/1.1" 200 -

127.0.0.1 - [23/Nov/2021 14:49:48] "GET /assets/images/2.png HTTP/1.1" 200 -

127.0.0.1 - [23/Nov/2021 14:49:48] "GET /assets/images/2.png HTTP/1.1" 200 -

127.0.0.1 - [23/Nov/2021 14:49:48] "GET /assets/images/2.png HTTP/1.1" 200 -

127.0.0.1 - [23/Nov/2021 14:49:48] "GET /assets/images/2.png HTTP/1.1" 200 -

127.0.0.1 - [23/Nov/2021 14:49:48] "GET /favicon.ico HTTP/1.1" 200 -
```

4. B. Per Windows - fare doppio clic su Firepower Migration Tool per avviarlo in un browser Google Chrome.

5. Accettare la licenza come illustrato nell'immagine.

$\leftarrow \rightarrow$ C \triangle () localhost:8888/#/eula	
Firepower Migration Tool	
END USER LICENSE AGREEMENT	
This is an agreement between You and Cisco Systems, Inc. or its affiliates ("Cisco") and governs your Use of Cisco Software. "You" and "Your" means the individual or legal entity licensing the Software under this EULA. "Use" or "Using" means to download, install, activate, access or otherwise use the Software. "Software" means the Cisco computer programs and any Upgrades made available to You by an Approved Source and licensed to You by Cisco. "Documentation" is the Cisco user or technical manuals, training materials, specifications or other documentation applicable to the Software and made available to You by an Approved Source. "Approved Source" means (i) Cisco or (ii) the Cisco authorized reseller, distributor or systems integrator from whom you acquired the Software. "Entitlement" means the license detail; including license metric, duration, and quantity provided in a product ID (PID) published on Cisco's price list, claim certificate or right to use notification. "Upgrades" means all updates, upgrades, bug fixes, error corrections, enhancements and other modifications to the Software and backup copies thereof. This agreement, any supplemental license terms and any specic product terms at www.cisco.com/go/softwareterms (collectively, the "EULA") govern Your Use of the Software.	
1. Acceptance of Terms. By Using the Software, You agree to be bound by the terms of the EULA. If you are entering into this EULA on behalf of an entity, you represent that you have authority to bind that entity. If you do not have such authority or you do not agree to the terms of the EULA, neither you nor the entity may Use the Software and it may be returned to the Approved Source for a refund within thirty (30) days of the date you acquired the Software or Cisco product. Your right to return and refund applies only if you are the original end user licensee of the Software.	
2. License. Subject to payment of the applicable fees and compliance with this EULA, Cisco grants You a limited, non-exclusive and non-transferable license to Use object code versions of the Software and the Documentation solely for Your internal operations and in accordance with the Entitlement and the Documentation. Cisco licenses You the right to Use only the Software You acquire from an Approved Source. Unless contrary to applicable law. You are not licensed to Use the Software on	
Proceed	

6. Nella pagina di accesso dello strumento di migrazione Firepower, fare clic sul collegamento di accesso con CCO per accedere all'account Cisco.com con le credenziali di accesso singolo.

Nota: Se non si dispone di un account Cisco.com, crearlo nella pagina di accesso

Cisco.com. Accedere con le credenziali predefinite seguenti: Nome utente—Password amministratore—Admin123.



7. Selezionare la configurazione di origine. In questo scenario, è Cisco ASA (8.4+).



8. Se non si dispone della connettività all'appliance ASA, selezionare Caricamento manuale. In caso contrario, è possibile recuperare la configurazione in esecuzione dall'ASA e immettere i dettagli dell'IP di gestione e di accesso. In questo scenario, è stato eseguito un caricamento manuale.

← → C ☆ ③ localhost.8888/W/home		x 🍳
cisco Firepower Migration Tool		
Extract Cisco ASA (8.4+) Information o		
Extraction Methods		
Manual Upload	Connect to ASA	
 File format is '.ctg' or '.tx'. For Multi-context upload a show tech. For Single-context upload show running. 	Enter the management IP address and connect using admin credentials. IP format should be: <ip.port>.</ip.port>	
Do not upload hand coded configurations.	ASA IP Address/Hostname	
Upload		

Nota: Questo errore viene visualizzato se il file non è supportato. Assicurarsi di modificare il formato in testo normale. (L'errore si verifica nonostante l'estensione .cfg).

$\overline{\otimes}$	Blocked Please upload .txt or .cfg files only	×	
----------------------	---	---	--



9. Una volta caricato il file, gli elementi vengono analizzati fornendo un riepilogo come mostrato nell'immagine:

alitalia cisco	Firepower Migration Tool			00
	Extract Cisco ASA (8.4+) Information	0		Source: Cisco ASA (8.4+)
	Extraction Methods			>
Manual Upload: ASAConfig dg tid				
	Context Selection			>
	Selected Context: Single Context Mode			
	Parsed Summary			~
	Collect Hitcounts: No. Hitcount information is only available of 20 Access Control Lines	ten consected to a live ASA.	18 x Objects	14 Put Objects

10. Immettere le credenziali di accesso e l'indirizzo IP del controller di dominio a cui migrare la configurazione ASA. Verificare che l'indirizzo IP del CCP sia raggiungibile dalla postazione di lavoro.

alialia cisco	Firepower Migration Tool		000
	Select Target 📀	Source: Cloco ASA (8.4+)	
	Connect to FMIC	~	
	PMC IP Address/Hostname 10.106.52:10 Connect		
	Choose FTD	>	
	Select Features	>	
	Rule Conversion/ Process Config	>	

				\times	<
FN	ЛС I	_00	GIN		
IP Address/Hostnar	me				
10.106.52.10					
Username					
1					
Password					

11. Una volta collegato il CCP, vengono visualizzati gli FTD gestiti al suo interno.

altado cisco	Firepower Migration Tool		
	Select Target 💿	Gathering details • •	Source: Cisco ASA (8.4+)
	Connect to FMC		~
	FMC IP Address/Hostname 10.106.52:10 Connect Successfully connected to FMC		
	Choose FTD		>
	Select Features		>
	Rule Conversion/ Process Config		>

12. Scegliere l'FTD su cui eseguire la migrazione della configurazione ASA.

۲	Select FTD Device	Proceed without FTD
	FTD (10.106.52.20) - VMWare (Native)	
	Peace ensure that the firewall mode configured on the target FTD device is the same as in the uploaded ASA configuration file. FABC.	The existing configuration of the FTD device on the FIAC is erased when you push the migrated configuration to the
C	Proceed	

Nota: Si consiglia di selezionare il dispositivo FTD, altrimenti le interfacce, i percorsi e la configurazione della VPN da sito a sito dovranno essere eseguiti manualmente.

-diada cisco	Firepower Migration Tool	000
	Select Target 💿	Source: Cisco ASA (8.4+)
	Connect to FMC	>
	FMC IP Address/Hostname: 10.106.52.10	
	Choose FTD	~
	Select FTD Device Proceed witho	ur FTD
	Select FTD Davice V	
	Interface, Routes and Site-to-Site VPN Tunnels work be migrated	
	Proceed	
	Select Features	>
	Rule Conversion/ Process Config	>

13. Selezionare le funzionalità da migrare, come illustrato nell'immagine.

Device Configuration	Shared Configuration	Optimization
🛃 Interfaces	Access Control	Migrate Only Referenced Objects
Proutes	Populate dostination security zones	Object Group Search ()
Site-to-Site VPN Tunnels	Migrate tunnelled rules as Prefiltor	
Policy Based (Crypto Map)	VINT NAT	Inline Grouping
Route Based (VTI)	W Network Objects	CSM/ASOM
	Port Objects	
	Time based Objects	

14. Selezionare **Avvia conversione** per avviare la pre-migrazione che popolerà gli elementi relativi alla configurazione FTD.

Rule Conversion/ Process Config				~
Start Conversion				
0 parsing errors found. Refer to the pre-migration report for m	ore details.			
Please download the Pre-Migration report for a detailed summ	nary of the parsed configuration. Download Report			
13		98		30
Adoese Control List Unes	Ne	twork Objects		Port. Objectis
2	9	4		1
Logical Interfaces	Static Routes	Network Address Transia	don.	Site-to-Site VPN Tunnels

15. Fare clic su **Scarica report** visualizzato in precedenza per visualizzare il report di premigrazione, come mostrato nell'immagine.

Pre-Migration Rep	bort
e Review all contents of this pre-migration report irepower Threat Defense after the configuration is	carefully. Unsupported rules will not be migrated completely, which can potentially alter your original configuration, restrict some traffic, or permit unwanted traffic. W successfully migrated.
Overall Summary:	
summary of the supported ASA configuration	on elements that can be successfully migrated to Firepower Threat Defense.
Collection Method	Manual
ASA Configuration Name	ASAConfig.cfg.txt
ASA Version	9.12(2)
ASA Hostname	asa
ASA Device Model	FPR4K-SM-12, 56533 MB RAM, CPU Xeon E5 series 2200 MHz, 1 CPU (24 cores)
Hit Count Feature	No
IP SLA Monitor	0
Total Extended ACEs	13
ACEs Migratable	13
Site to Site VPN Tunnels	1
Logical Interfaces	2
Network Objects and Groups	98
Service Objects and Groups	30
Static Routes	9
NAT Rules	4

16. Mappare le interfacce ASA alle interfacce FTD come richiesto, come mostrato nell'immagine.

		Refresh
ASA Interface Name	FTD Interface Name	
	Select Interface	
Ethernet1/2	GigabitEthernet0/0	,
Ethernet1/3	✓ GigabitEthernet0/1	

17. Assegnare zone di sicurezza e gruppi di interfacce alle interfacce FTD.

uluiju cisco	Firepower Migration Tool						0	00
	Map Security Zones and Inte	rface Groups 📀					Source: Osco ASA (8.4+) Target FTD: FTD	
					Add 52 & 10 Au	Al-Create		
	ASA Logical Interface Name	FTD Interface	FMC Security Zones		FMC Interface Groups			
	Inside	Gipabil@hernet01	(Telect Decurity Zone V)	Select Interface Ortops	~		
	Outside	GpARTrenet02	Select Security Zone		Salect Interface Orouge	~		

R. Se nel CCP sono già state create zone di sicurezza e gruppi di interfacce, è possibile selezionarli in base alle esigenze:

✓ Select Security Zone	-
outside	
inside	-

B. Se è necessario creare aree di sicurezza e un gruppo di interfacce, fare clic su Add SZ & IG come mostrato nell'immagine.

	Add SZ & IG	
Security Zones (SZ) Interface	Groups (IG)	
Add	Max 48 characters for Interface	Group name. Allowed special characters are+
Interface Groups	Туре	Actions
Inside	ROUTED	🗴 📀
	0-0of0 ∢ ∢ _ 1 ▶	▶]
	Close	

C. In caso contrario, selezionare l'opzione **Auto-Create** per creare le zone di sicurezza e i gruppi di interfacce denominati rispettivamente **ASA logical interface_sz** e **ASA logical interface_ig**.

Auto-Create
Auto-create maps ASA 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 ASA interfaces
Security Zones Interface Groups
Cancel Auto-Create

ſ

diada cisco	Firepower Migration Tool									
Map Security Zones and Interface Groups 🕖										
					Add SZ & IG Auto-C	Create				
	ASA Logical Interface Name	FTD Interface	FMC Security Zones		FMC Interface Groups					
	Inside	GigabitEthernet0/1	inside	~	Inside_ig (A)	~				
	Outside	GigabitEthemet0/2	outside	~	Outside_ig (A)	~				

18. Esaminare e convalidare ogni elemento FTD creato. Gli avvisi vengono visualizzati in rosso, come mostrato nell'immagine.

See	rct all 13 entrie	a Selected 0/13	Actions with	See.						C, Search	
_	-			ECURCE	1.00		DESTINATION				
	1.	0.	0.	Q.		0	Q.	0	0.0	Action 1	ACE COURT
0		Outside_access_in_#1	subide	#19	ANY	ANY			V G D B	Alex	1
0	2	Outside_access_in_#2	eutride	any	1817	4907	-	-	VECE	Alex	1
	3	Outside_access_in_#3	eutside	any	ANY	A807	-	-	JAGE	Nor	2
0	4	Outside_access_in_61	outside	any	ANY	A907		-	JAGGE	Alex	4
	5	Outside_access_in_#5	eutoide	any	ANY	ABCY	-	_		Nor	1
	6	Outside_access_in_#6	eutside	any	ANY	4807			• • • • B	Non	1
	7	Outside_access_in_#7	outside	any .	ANY	ANY		-	• • • • B	Non	3
	8	Outside_access_in_#8	eutride	any	ANY	ANY			• • • • • •	Non	1
	9	Outside_access_in_#9	outside	any	AMPY	ANY			● 🗸 🤤 🖯 🖻	Alter	4
	10	Outside_access_in_#10	0.45-00	any	ANY	ANY			🗩 🗸 9, 6, 8,	Alex	7
0	11	Outside_access_in_#11	outside	any	AMY	ANY	-		🗩 🗸 🧣 🕒 🖻	Alex	2
0	12	Outside_access_in_#12	e utai de	any	ANY	ANY	_		• • • • • B	Allen	1
	9 10 11 12	Outside_access_in_89 Outside_access_in_810 Outside_access_in_811 Outside_access_in_812	outside outside outside outside	479 479 479 479 479	AMP AMP	4807 4807 4807 4807	2			Non Non Non Non	

19. Le azioni di migrazione possono essere selezionate come mostrato nell'immagine se si desidera modificare qualsiasi regola. In questa fase è possibile aggiungere funzioni FTD e criteri IPS.

ACP	Pre-filter			
Selection	t all 13 entries	Selected: 13 / 13	Actions - Save	
			MIGRATION ACTIONS SOURCE	CE
×.	#	Name	Do not migrate twork	
		Q	RULE ACTIONS	_
✓	1	Outside_access_in_#1	File Policy	
v	2	Outside_access_in_#2		
v	3	Outside_access_in_#3	IPS Policy	
v	4	Outside_access_in_#4	Log	
v	5	Outside_access_in_#5	Rule Action	
	6	Outside_access_in_#6	outside any	

Nota: Se i criteri file esistono già nel FMC, verranno popolati come illustrato nell'immagine. Lo stesso vale per i criteri IPS e i criteri predefiniti.

	File Policy	
Select File Policy *		
eicer		^
None		
	Cancel Select	

Èpossibile eseguire la configurazione del registro per le regole richieste. In questa fase è possibile selezionare la configurazione del server Syslog esistente nel FMC.

		>	<
Log			
Log at the beginning of connection			
Send connection events to:			
Syslog			
	\sim		
Cancel Save			

Le azioni selezionate verranno evidenziate di conseguenza per ogni regola.



20. Analogamente, NAT, oggetto di rete, oggetti porta, interfacce, route, oggetti VPN, tunnel VPN da sito a sito e altri elementi in base alla configurazione possono essere rivisti passo dopo passo.

Nota: L'avviso viene notificato come mostrato nell'immagine per aggiornare la chiave già condivisa, in quanto non viene copiata nel file di configurazione dell'ASA. Selezionare **Azioni > Aggiorna chiave già condivisa** per immettere il valore.

titethe Firepower Migration Tool								000
Optimize, Review and Validate Configuration o		<u> </u>	,		Sov Tar	nce: Cisco ASA (8/ pet FTD: FTD	47)	
Access Control NAT Network Objects Port Objects Interfaces Roules	VPN Objects	Sile-to-Sile VPN Ture	w/s \varTheta					
Select al 1 entites Selected 1/1 Actors V Core					0,	Search		<u>+</u>
A Severa Interfere R., Do not evidate A Severa Interfere R., Do not evidate	RE .	Bit ARD A P.	KENTREN PROP.	Authorit	estion Type PNI Carti	Frain Source Not	Remote Net	
Q. Update Pre-shared Key	Q.	Q.	Q.			Q.	Q.	
50 v per page 1 to 1 of 1 (+ + Page 1 of 1 + +)								
Update the Pre-Shared Key/PRI Cestificate column highlighted in Yolow for each VPN-term	i rows under She	to-Site VPN Termels tab	to validate and proceed with m	igration.				
For additional help, click here.			105					
Lindata Dra S	hor		<u></u>	×				
Opuale Pre-S	nar	euro	ey	\sim				
Pre-Shared Key IKEv2								
Cancel								

21. Infine, fare clic sull'icona **Convalida** nella parte inferiore destra della schermata, come mostrato nell'immagine.



22. Una volta completata la convalida, fare clic su **Push Configuration** (Configurazione push) come mostrato nell'immagine.



PUSHING

0% Complete

Push In progress. Refer FMT Terminal to monitor the migration status.

← → C O O localhost.8888/#/home			\$ Q	87 #0 🛱 👼 🙁 🕸 🌺 (lydare 1	
cisco Firepower Migration Tool			00		
Complete Migration Migration Blatus	PUSHING 50%. Complete Push in progress. Rafter FM migration status.	Taminal to monitor the	Seurce: Carol ASA (B.4*) Target FTD: FTD Status		
Next Disp - Login to FMC to deploy the policy to FTD.				Expand panel to show video	
Live Connect:					
Selected Context: Single Context Mode					
Migration Summary (Post Push)					
13		37	14 Port Objects		
Access Control List Lines	Robert	k Objects			
2	9	4		1	
Logical Interfaces	Static Routes	Network Address Translet	ion Bite-to-5	the VPN Turnels	

23. Una volta completata la migrazione, il messaggio visualizzato viene visualizzato nell'immagine.

cisco	Firepower Migration Tool			G	00			
	Complete Migration o	_	~	Source: Cisco ASA (8.4+) Target FTD: FTD				
	Migration Status		Optimization Status					
	Migration is complete, policy is pushed to FMC. Next Step - Login to FMC to deploy the policy to FTD.		ACL Optimization is not applied for this migration.					
	Live Connect:							
	Selected Context: Single Context Mode							
	Migration Summary (Post Push)							
	13	3	37	14				
	Access Control List Lines	Network	k Objects	Port Objects				
	2	9	4	1				
	Logical Interfaces	Static Routes	Network Address Translatio	n Ste-to-Site VPN Tunnels				
	Please download the Post-Push migration report for a detailed summary.	Download Report						

Nota: Se la migrazione non riesce, fare clic su **Scarica report** per visualizzare il report di post-migrazione.

Complete Migration 💿	Source: Cisco ASA (8.4+) Target FTD: FTD
Migration Status	Optimization Status
Migration Unsuccessfult Internal Server Error.	ACL Optimization is successful but due to migration failure the refined optimized policy cannot be deployed to FMC.
Please roler logs for more details. Download Report Contact Support	

Verifica

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

Convalida sul CCP.

1. Per verificare che l'FTD selezionato sia compilato, selezionare **Criteri > Controllo di accesso > Criteri di controllo di accesso > Assegnazione criteri**.

Overvi	ew Analysis	Policies Do			eligence											y admin	
Access	Control + Acce	as Control N	rtwork Discovery	Application	Detectors Correla	tion Actions											
FTD-	Mig-ACP-1	63774379	6											Analyze	a Cauras 📄 Sana	O Cano	
Profilar	Pelliny: Extinut. P	of Barr Parks			SSL Policy:	Naca .			Identity Policy:	Back							
														To Interter	en Saturga (🖂 Palley	Assignments ()	10
Rules	Security Intel	Igence INTER	exponses Loppie	ng Advance	4												
A 12.	by Device	Search Rules											X D Shee	Rule Conflicts 10	A AM Category	O ANI RA	
. 1	ana	Seurce Zenes	Dest Zones	Source Net	n Dest Networks	VLAN Tage	Dears	Applications	Ecurca Porta	Dest Parts	Ulta	Deuros DGT	Dert SCT	Action			
w Har	dalary - FTD-Hij	- ACP- 1437743794	F(-)														
There is	te no rules in this i	INCOME AND AND AND AN	ARE CARRIENY		blicy Assignments							7 ×					
* 24	ult - ITO-Hig-A	CP-1437743794 (1	-13)		Targeted Devices												
1 0	dekin_necen_in_	* A ministe	Arr	Burt	Select devices to which	were want to appl	ly this parks.						Any	of Allow	a00.8±.	B + 1	0
2 0	AND NORMAL	A Transfer		States.	Available Devices				Selected De	wices .				of Allow	800.80	8 . 1	8
3 0	state access in	4 1,00540		The same	Search by name o	r value			10 MIL			8		of Allow	AUD.84	Re 1	
4 0	utside access in	r outrete		(B. MY	₩ 10.44.171.31 ⊕ /TD ₩ M2P5									af 100au	010.80	8. 1	0
								Add to Part	a.								
5 0	data, accas, n.	r 🚠 satade		10 mr					Impectore D	evices				of Allow	a:0.8±	R+ 2	9
* 0	.e.,	r _{da} outside		(Barr										of Allow	00.80	8 - 1	8
		· · ·					_				04	Carvosi	- 13 of 13 rules	e e Paga 💼 a	1) > 1 6 (Raim)	per page: 100	

Nota: Il criterio di controllo dell'accesso alla migrazione dovrebbe avere un nome con il prefisso **FTD-Mig-ACP**. Se al punto 2.8 non è stato selezionato alcun FTD, l'FTD deve essere selezionato sul CCP.

2. Spostare il criterio nell'FTD. Passare a **Distribuisci > Distribuzione > Nome FTD > Distribuisci** come mostrato nell'immagine.

Overview	Analysis	Policies	Devices	Objects	АМР	Intelligence						0, Deploy System	Holp v admin v
												Deployment	Deployment History
													Enging
- Deserv	a result cesso	e rieme, type	e, comien, g	roup or seens				-	-				
	Device						Inspect Interruption	Type	Group	Last Deploy Time	Preview	Status	
> 0	10.88.17	1.31					🔶 Yes	PTD		Nov 23, 2021 11:24 PM	53.	Pending	
> 0	NG2PS							fienser .			3	Pending	
> D	FTD						🖛 Yasi	FTD		Nov 23, 2021 11:17 PH	3	Completed	

Bug noti relativi allo strumento di migrazione Firepower

- ID bug Cisco <u>CSCwa56374</u> Lo strumento FMT si blocca sulla pagina di mappatura della zona a causa di un errore dovuto all'elevato utilizzo della memoria
- Cisco ID bug <u>CSCvz88730</u> Errore di push dell'interfaccia per il tipo di interfaccia di gestione del canale della porta FTD
- ID bug Cisco <u>CSCvx21986</u> Migrazione porta-canale alla piattaforma di destinazione FTD virtuale non supportato
- ID bug Cisco <u>CSCvy63003</u> Lo strumento di migrazione deve disabilitare la funzione di interfaccia se FTD fa già parte del cluster
- ID bug Cisco <u>CSCvx08199</u> È necessario suddividere l'ACL quando il riferimento all'applicazione è superiore a 50

Informazioni correlate

- Migrazione di ASA Firewall a Threat Defense con lo strumento di migrazione del firewall
- Documentazione e supporto tecnico Cisco Systems