# Modificare l'indirizzo IP dell'interfaccia di gestione su FTD Gestito da FMC

## Sommario

Introduzione	
<u>Prerequisiti</u>	
Requisiti	
Componenti usati	
Configurazione	
Configurazioni	
<u>Verifica</u>	
Risoluzione dei problemi	
Informazioni correlate	

### Introduzione

In questo documento viene descritto come modificare l'IP di gestione per il dispositivo Firewall Threat Defense gestito dal centro di gestione Secure Firewall.

# Prerequisiti

#### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Secure Firewall Management Center (FMC)
- Cisco Secure Firewall Threat Defense (FTD)

#### Componenti usati

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

- Secure Firewall Management Center Virtual running versione 7.2.5(1)
- Cisco Secure Firewall Threat Defense Virtual con esecuzione versione 7.2.4

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.

## Configurazione

#### Configurazioni

Passaggio 1. Passare alla GUI di FMC e passare a Device > Device Management (Gestione dispositivi).

Passaggio 2. Selezionare Device, quindi individuare la sezione Management.

Frepower					
Cisco Firepower Threat Defense for VMware					
Device Routing Interfaces In	nline Sets DHCP VTEP				
General	/±∓	License	/	System	0 G
Name:	Frepower	Performance Tier :	FTDv50 - Tiered (Core 12 / 24 GB)	Model:	Cisco Firepower Threat Defense for VMware
Transfer Packets:	Yes	Base:	Yes	Serial:	9A0HJUS0J27
Mode:	Routed	Export-Controlled Features:	No	Time:	2024-04-12 00:57:32
Compliance Mode:	None	Malware:	Yes	Time Zone:	UTC (UTC+0:00)
TLS Crypto Acceleration:	Disabled	Threat:	Yes	Version:	7.2.4
		URL Filtering:	Yes	Time Zone setting for Time based Rules:	UTC (UTC+0:00)
Device Configuration:	Import Export Download	AnyConnect Apex:	No		
		AnyConnect Plus:	No		
		AnyConnect VPN Only:	No		
				<u> </u>	
Inspection Engine		Health		Management	/ 🔍
Inspection Engine:	Snort 3	Status:	•	Host:	192.168.10.42
Revert to Snort 2		Policy:	Initial_Health_Policy 2024-04-08 17:12:48	Status:	•
		Excluded:	None	Manager Access Interface:	Management Interface
Inventory Details	Ċ	Applied Policies	/	Advanced Settings	/
CPU Type:	CPU Xeon 4100/6100/8100 series 2700	Access Control Policy:	Default \varTheta	Application Bypass:	No
00100000	1.0011 (4.0000)	Prefilter Policy:	Default Prefilter Policy	Bypass Threshold:	3000 ms
CPO Coles.	0100 140 00105	SSL Policy:		Object Group Search:	Enabled
Memory.	0142 MD K4M	DNS Policy:	Default DNS Policy	Interface Object Optimization:	Disabled
orunage:	N/A	Identity Policy:			
Chassis URL:	N/A	NAT Policy:			
Chassis Serial Number:	N/A	Platform Settings Policy:			
Chassis Module Number:	N/A	QoS Policy:			
Chassis Module Serial Number:	N/A	ElevConfig Policy:			

Passaggio 3. Disattivare Gestione facendo clic sul dispositivo di scorrimento e confermare l'azione selezionando Sì.

Frepower Cisco Firepower Threat Defense for VMware Device Routing Interfaces Inline	Sets DHCP VTEP				
Ceneral Name: Transfer Packets: Mode: Compliance Mode: TLS Crypto Acceleration: Device Configuration:	✓ ± ∓ Frepower Ves Routed None Disabled	License Performance Tier : Base: Export-Controlled Features: Matware: Threat: URL Filtering: AnyConnect Apex: AnyConnect Plus: AnyConnect VPN O Disable Manageme	FTDvS0 - Tiered (Core 12 / 24 GB) Ves No Ves Ves No No No No	System Model: Serial: Time: Time Zone: Version: Time Zone setting for Time based Rules:	G Cisco Firepower Threat Defense for VMware SA0HJUS027 2024-04-12 01:14:15 UTC (UTC+0:00) 7.2.4 UTC (UTC+0:00)
Inspection Engine Inspection Engine: (Reserve Storr 2)	Short 3	Health Managing this device will possible if it's Managem disabled. Do you want to can enable it later. Excluded:	I not be not B <sup>2</sup> is proceed? You No Yes	Management Host: Manager Access Interface:	192.168.10.42 Management Interface
Inventory Details CPU Type: CPU Cores:	CPU Xeon 4100/6100/6100 series 2700 MHz 1 CPU (4 cores)	Applied Policies Access Control Policy: Prefitter Policy: SSL Policy:	Default @ Default Prefilter Policy	Advanced Settings Application Bypass: Bypass Threshold: Object Group Search:	No 3000 ms Enabled
Memory: Storage:	8192 MB RAM N/A	DNS Policy: Identity Policy:	Default DNS Policy	Interface Object Optimization:	Disabled



Nota: la disattivazione di Gestione interrompe la connessione tra il centro di gestione e il dispositivo, ma mantiene il dispositivo all'interno del centro di gestione.

Passaggio 4. Se Management è disattivato, modificare la connessione di gestione selezionando Edit (Modifica).

Passaggio 5. Nella finestra di dialogo Gestione, modificare l'indirizzo IP nel campo dell'indirizzo dell'host remoto, quindi selezionare Salva.



Passaggio 6. Connettersi alla console FTD per modificare l'indirizzo IP di gestione.



Avviso: la modifica dell'indirizzo IP di gestione può causare la perdita della connettività SSH al dispositivo se la sessione viene stabilita tramite l'indirizzo IP di gestione. Pertanto, si consiglia di eseguire questa modifica tramite l'accesso alla console come suggerito da Cisco.

Passaggio 7. In modalità inglese, modificare l'indirizzo IP di gestione con il comando:

> configure network ipv4 manual 192.168.10.49 255.255.0.0 192.168.255.254



Nota: per impostazione predefinita, questa configurazione viene applicata all'interfaccia di gestione.

Passaggio 8. Tornare all'interfaccia utente di FMC e riattivare Gestione spostando il dispositivo di scorrimento sulla posizione On.

Management	/ 🔍
Host:	192.168.10.49
Status:	0
Manager Access Interface:	Management Interface

Passaggio 9. Tenere presente che il ripristino della connessione di gestione può richiedere tempo.

La riuscita della riconnessione è indicata come illustrato nella seguente immagine:

Management	/ 🔍
Host:	192.168.10.49
Status:	0
Manager Access Interface:	Management Interface

## Verifica

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

È possibile verificare la connettività di gestione tramite la CLI FTD. A tal fine, è necessario connettersi alla CLI, in modalità Clish eseguire questo comando:

## Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

• Per verificare lo stato della connessione di gestione nella CLI FTD, eseguire il comando show sftunnel status brief. Osservate l'output di una connessione inattiva, indicata dall'assenza di dettagli connessi per il canale peer e da informazioni heartbeat mancanti.

PEER:192.168.10.40 Registration: Completed. Connection to peer '192.168.10.40' Attempted at Fri Apr 19 21:14:23 2024 UTC Last disconnect time : Fri Apr 19 21:14:23 2024 UTC Last disconnect reason : Both control and event channel connections with peer went down

Una connessione integra tra i dispositivi viene confermata quando il comando sftunnel-status-brief alla CLI di FTD genera un output che include un canale peer connesso alle informazioni e ai dati heartbeat.

> sftunnel-status-brief

PEER:192.168.10.40 Peer channel Channel-A is valid type (CONTROL), using 'eth0', connected to '192.168.10.40' via '192.168 Peer channel Channel-B is valid type (EVENT), using 'eth0', connected to '192.168.10.40' via '192.168.1 Registration: Completed. IPv4 Connection to peer '192.168.10.40' Start Time: Fri Apr 19 21:12:59 2024 UTC Heartbeat Send Time: Fri Apr 19 21:13:00 2024 UTC Heartbeat Received Time: Fri Apr 19 21:13:23 2024 UTC Last disconnect time : Fri Apr 19 21:12:57 2024 UTC Last disconnect reason : Process shutdown due to stop request from PM

• Per controllare la connettività di rete, eseguire il ping del centro di gestione dall'interfaccia di gestione e immettere ping system fmc\_ip nella CLI di FTD.

#### Informazioni correlate

- Nozioni di base sulla gestione dei dispositivi
- Supporto tecnico Cisco e download

#### Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).