

FMCによって管理されるFTDの管理インターフェイスIPアドレスの変更

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[コンフィギュレーション](#)

[確認](#)

[トラブルシューティング](#)

[関連情報](#)

はじめに

このドキュメントでは、Secure Firewall Management Centerで管理されているファイアウォール脅威対策(FTD)デバイスの管理IPを変更する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

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

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- バージョン7.2.5(1)を実行しているSecure Firewall Management Center(FMC)仮想
- バージョン7.2.4が稼働するCisco Secure Firewall Threat Defense Virtual

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

設定

コンフィギュレーション

ステップ 1 : FMC GUIに移動し、Device > Device Managementに進みます。

ステップ 2 : Deviceを選択し、Managementセクションを見つけます。

The screenshot shows the Cisco Firepower GUI for a device named 'Frepower'. The 'Device' tab is selected in the top navigation bar. The 'Management' section is highlighted with a red box, showing the 'Host' as 192.168.10.42 and the 'Manager Access Interface' as 'Management interface'. The 'Device' tab is also highlighted in the top navigation bar.

Section	Field	Value	
General	Name	Frepower	
	Transfer Packets	Yes	
	Mode	Routed	
	Compliance Mode	None	
	TLS Crypto Acceleration	Disabled	
	Device Configuration	Import Export Download	
	License	Performance Tier	FTDv50 - Tiered (Core 12 / 24 GB)
		Base	Yes
		Export-Controlled Features	No
		Malware	Yes
Threat		Yes	
URL Filtering		Yes	
AnyConnect Apex		No	
AnyConnect Plus		No	
AnyConnect VPN Only		No	
Inspection Engine		Inspection Engine	Snort 3
	Revert to Snort 2	Button	
Inventory Details	CPU Type	CPU Xeon 4100/6100/8100 series 2700 MHz	
	CPU Cores	1 CPU (4 cores)	
	Memory	8192 MB RAM	
	Storage	N/A	
	Chassis URL	N/A	
	Chassis Serial Number	N/A	
	Chassis Module Number	N/A	
	Chassis Module Serial Number	N/A	
	Applied Policies	Access Control Policy	Default
		Prefilter Policy	Default Prefilter Policy
SSL Policy			
DNS Policy		Default DNS Policy	
Identity Policy			
NAT Policy			
Platform Settings Policy			
QoS Policy			
FlexConfig Policy			
System		Model	Cisco Firepower Threat Defense for VMware
	Serial	9A0HJUS0J27	
	Time	2024-04-12 00:57:32	
	Time Zone	UTC (UTC+0:00)	
	Version	7.2.4	
	Time Zone setting for Time based Rules	UTC (UTC+0:00)	
	Management	Host	192.168.10.42
		Status	Initial_Health_Policy 2024-04-08 17:12:48
	Advanced Settings	Application Bypass	No
		Bypass Threshold	3000 ms
Object Group Search		Enabled	
Interface Object Optimization		Disabled	

ステップ 3 : スライダをクリックしてManagementをオフにし、Yesを選択してアクションを確認します。

The screenshot shows the Cisco Firepower GUI for a device named 'Frepower'. The 'Management' section is highlighted with a red box, and a red arrow points to the 'Disable Management' button. A dialog box is displayed in the center, asking 'Disable Management' and 'Managing this device will not be possible if its Management IP is disabled. Do you want to proceed? You can enable it later.' with 'No' and 'Yes' buttons.

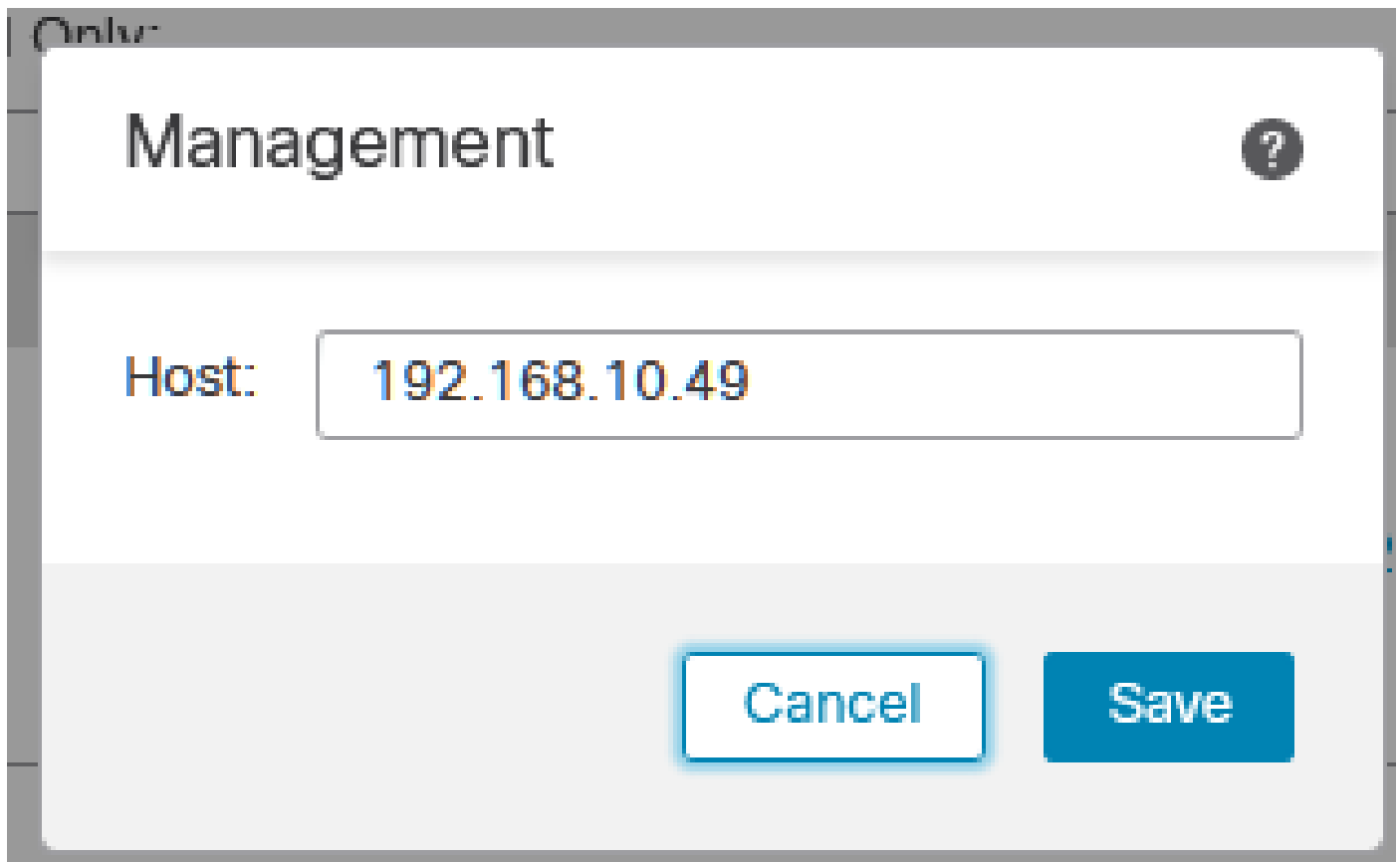
Section	Field	Value	
General	Name	Frepower	
	Transfer Packets	Yes	
	Mode	Routed	
	Compliance Mode	None	
	TLS Crypto Acceleration	Disabled	
	Device Configuration	Import Export Download	
	License	Performance Tier	FTDv50 - Tiered (Core 12 / 24 GB)
		Base	Yes
		Export-Controlled Features	No
		Malware	Yes
Threat		Yes	
URL Filtering		Yes	
AnyConnect Apex		No	
AnyConnect Plus		No	
AnyConnect VPN Only		No	
Inspection Engine		Inspection Engine	Snort 3
	Revert to Snort 2	Button	
Inventory Details	CPU Type	CPU Xeon 4100/6100/8100 series 2700 MHz	
	CPU Cores	1 CPU (4 cores)	
	Memory	8192 MB RAM	
	Storage	N/A	
	Chassis URL	N/A	
	Chassis Serial Number	N/A	
	Chassis Module Number	N/A	
	Chassis Module Serial Number	N/A	
	Applied Policies	Access Control Policy	Default
		Prefilter Policy	Default Prefilter Policy
SSL Policy			
DNS Policy		Default DNS Policy	
Identity Policy			
NAT Policy			
Platform Settings Policy			
QoS Policy			
FlexConfig Policy			
System		Model	Cisco Firepower Threat Defense for VMware
	Serial	9A0HJUS0J27	
	Time	2024-04-12 01:14:15	
	Time Zone	UTC (UTC+0:00)	
	Version	7.2.4	
	Time Zone setting for Time based Rules	UTC (UTC+0:00)	
	Management	Host	192.168.10.42
		Status	Initial_Health_Policy 2024-04-08 17:12:48
	Advanced Settings	Application Bypass	No
		Bypass Threshold	3000 ms
Object Group Search		Enabled	
Interface Object Optimization		Disabled	



注：Managementをオフにすると、Management Centerとデバイス間の接続は停止しますが、デバイスはManagement Center内に保持されます。

ステップ 4：Managementを無効にした状態で、Editを選択して管理接続を編集します。

ステップ 5：Managementダイアログボックスで、remote Host addressフィールドのIPアドレスを変更し、Saveを選択します。



手順 6 : FTDコンソールに接続して、管理IPアドレスを変更します。



警告：管理IPアドレスを変更すると、その管理IPアドレスを使用してセッションを確立した場合に、デバイスへのSSH接続が失われる可能性があります。したがって、シスコが推奨するように、この変更はコンソールアクセスを介して行うことをお勧めします。


手順 7：Clishモードで、次のコマンドを使用して管理IPアドレスを変更します。

```
> configure network ipv4 manual 192.168.10.49 255.255.0.0 192.168.255.254
```




注：この設定は、デフォルトで管理インターフェイスに適用されます。

ステップ 8：FMC GUIに戻り、スライダをオンの位置に切り替えて、管理を再度アクティブにします。

Management 	
Host:	192.168.10.49
Status:	
Manager Access Interface:	Management Interface

ステップ 9：管理接続の再確立には時間がかかる場合があることに注意してください。再接続が成功したことは、次の図に示すように示されています。

Management 	
Host:	192.168.10.49
Status:	
Manager Access Interface:	Management Interface

確認

ここでは、設定が正常に機能しているかどうかを確認します。

管理接続は、FTD CLIを使用して確認できます。これを行うには、CLIに接続し、Clishモードで次のコマンドを実行します。

```
> sftunnel-status
```

```
SFTUNNEL Start Time: Fri Apr 12 01:27:55 2024
```

```
-----OUTPUT OMITTED-----
```

```
*****
```

```
**RPC STATUS**192.168.10.40*****
```

```
'last_changed' => 'Fri Apr 12 01:09:19 2024',  
'active' => 1,  
'ipv6' => 'IPv6 is not configured for management',  
'uuid_gw' => '',  
'uuid' => '4a6e43f6-f5c7-11ee-97d5-a1dcfaf53393',  
'name' => '192.168.10.40',  
'ip' => '192.168.10.40'
```

```
Check routes:
```

```
No peers to check
```

トラブルシューティング

ここでは、設定のトラブルシューティングに使用できる情報を示します。

- FTD CLIで管理接続のステータスを確認するには、`show sftunnel status brief`コマンドを実行します。接続がダウンしている場合の出力を観察します。これは、ピアチャンネルの接続詳細が存在せず、ハートビート情報が欠落しているためです。

```
> sftunnel-status-brief
```

```
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

FTD CLIのsftunnel-status-briefコマンドによって、情報とハートビートデータに接続されたピアチャンネルを含む出力が生成されると、デバイス間の接続が正常であることが確認されます。

```
> 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 '192.168.10.40'
```

```
Peer channel Channel-B is valid type (EVENT), using 'eth0', connected to '192.168.10.40' via '192.168.10.40'
```

```
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
```

- ネットワーク接続を確認するには、管理インターフェイスからManagement Centerにpingを実行し、FTD CLIでping system fmc_ipと入力します。

関連情報

- [デバイス管理の基本](#)
- [シスコのテクニカルサポートとダウンロード](#)

翻訳について

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