

# 管理インターフェイスからデータインターフェイスへのFTDでのマネージャアクセスの設定

## 内容

---

### [はじめに](#)

### [前提条件](#)

#### [要件](#)

#### [使用するコンポーネント](#)

### [背景説明](#)

### [設定](#)

#### [インターフェイスの移行に進む](#)

#### [プラットフォーム設定でのSSHの有効化](#)

### [確認](#)

#### [FMCのグラフィカルユーザインターフェイス\(GUI\)からの確認](#)

#### [FTDコマンドラインインターフェイス\(CLI\)からの確認](#)

### [トラブルシューティング](#)

#### [管理接続ステータス](#)

##### [正常動作シナリオ](#)

##### [正常に動作しないシナリオ](#)

#### [ネットワーク情報の検証](#)

#### [マネージャの状態の検証](#)

#### [ネットワーク接続の検証](#)

##### [Management Centerへのping](#)

##### [インターフェイスのステータス、統計情報、パケットカウントの確認](#)

##### [FMCに到達するためのFTD上のルートの検証](#)

##### [Sftunnelと接続の統計情報の確認](#)

### [関連情報](#)

---

## はじめに

このドキュメントでは、Firepower Threat Defense(FTD)上のManager Access(MA)を管理インターフェイスからデータインターフェイスに変更するプロセス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。

- Firepower Threat Defense ( FTD )
- Firepower Management Center ( FMC )

## 使用するコンポーネント

- Firepower Management Center(FMC)仮想7.4.1
- Firepower Threat Defense(FTD)仮想7.2.5

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。

## 背景説明

各デバイスには、FMCと通信するための単一の専用管理インターフェイスが含まれています。オプションで、専用の管理インターフェイスの代わりにデータインターフェイスを管理用に使用するようにデバイスを設定できます。データインターフェイスのFMCアクセスは、Firepower Threat Defenseを外部インターフェイスからリモートで管理する場合や、個別の管理ネットワークがない場合に役立ちます。この変更は、FMCによって管理されるFTDのFirepower Management Center(FMC)で実行する必要があります。

データインターフェイスからのFMCアクセスには、いくつかの制限があります。

- 1つの物理データインターフェイスでのみマネージャアクセスを有効にできます。サブインターフェイスまたはEtherChannelは使用できません。
- ルーテッドファイアウォールモードのみ。ルーテッドインターフェイスを使用する。
- PPPoEはサポートされていません。ISPがPPPoEを必要とする場合、Firepower Threat Defense(FTD)とWANモデムの間にPPPoEをサポートするルータを配置する必要があります。
- 個別の管理インターフェイスとイベントのみのインターフェイスは使用できません。

## 設定

### インターフェイスの移行に進む

---

注：変更を行う前に、FTDとFMCの両方の最新のバックアップを用意することを強くお勧めします。


---

1. Devices > Device Managementページに移動し、変更するデバイスのEditをクリックします

[Collapse All](#) [Download Device List Report](#)

<input type="checkbox"/>	Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack	Group	
<input type="checkbox"/>	▼ FMT Test (1)								
<input type="checkbox"/>	● FTD-Test Short 3 192.168.1.8 - Routed	FTDv for VMware	7.2.5	N/A	Essentials	Base-ACP	↺		Edit → ↗ ⋮

2. Device > Managementセクションに移動し、Manager Access Interfaceのリンクをクリックします。

Management	
Remote Host Address:	192.168.1.8
Secondary Address:	
Status:	<span style="color: green;">✔</span>
Manager Access Interface:	 Management Interface

Manager Access Interfaceフィールドには、既存の管理インターフェイスが表示されます。リンクをクリックして、新しいインターフェイスタイプを選択します。これは、Manage device byドロップダウンリストのData Interfaceオプションで、Saveをクリックします。

## Manager Access Interface ?

ⓘ This is an advanced setting and need to be configured only if needed. See the [online help](#) for detailed steps.

Manage device by

Management Interface ▼

Management Interface

Data Interface

Close Save

3. 次に、データインターフェイスで管理アクセスをイネーブルにするに進み、Devices > Device Management > Interfaces > Edit Physical Interface > Manager Accessに移動する必要があります。

# Edit Physical Interface



- General
- IPv4
- IPv6
- Path Monitoring
- Hardware Configuration
- Manager Access**
- Advanced

Enable management access

Available Networks:  +

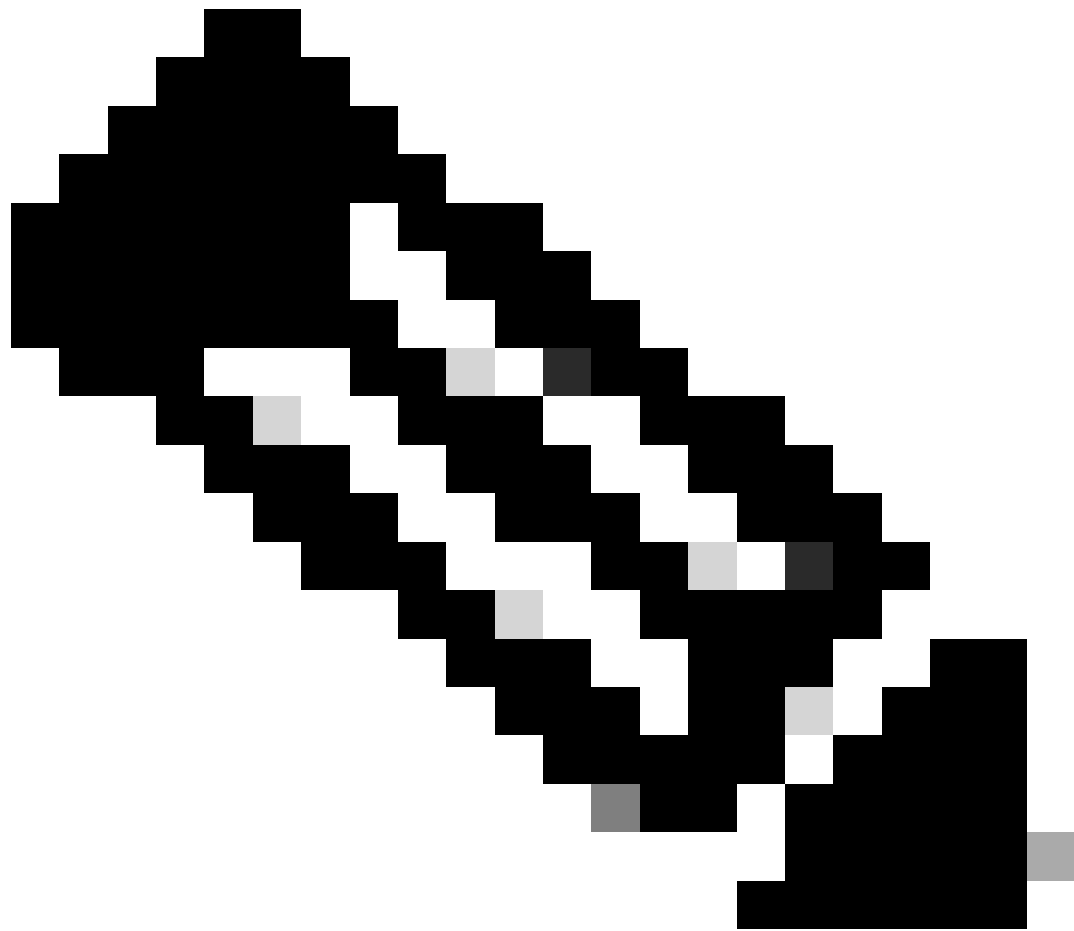
- 
- 10.201.204.129
  - 192.168.1.0\_24
  - any-ipv4
  - any-ipv6
  - CSM
  - Data\_Store

Add

Allowed Management Networks

- any

Cancel OK



---

注: ( オプション ) 冗長性のためにセカンダリインターフェイスを使用する場合は、冗長性のために使用されるインターフェイスで管理アクセスを有効にします。

( オプション ) インターフェイスにDHCPを使用する場合は、Devices > Device Management > DHCP > DDNSの順に選択して、WebタイプのDDNS方式を有効にします。

( オプション ) プラットフォーム設定ポリシーでDNSを設定し、Devices > Platform Settings > DNSでこのデバイスに適用します。

---

4. 脅威対策がデータインターフェイスを介してManagement Centerにルーティングできることを確認し、必要に応じてDevices > Device Management > Routing > Static Routeでスタティックルートを追加します。

1. 追加するスタティックルートのタイプに応じて、IPv4またはIPv6をクリックします。
2. このスタティックルートを適用するインターフェイスを選択します。
3. Available Networkリストから、宛先ネットワークを選択します。
4. GatewayまたはIPv6 Gatewayフィールドで、このルートのネクストホップであるゲートウェイルータを入力または選択します。

( オプション ) ルートの可用性をモニタするには、モニタリングポリシーを定義するサービスレベル契約(SLA)モニタオブジェクトの名前をルートトラッキングフィールドで入力または選択します。

## Add Static Route Configuration



Type:  IPv4  IPv6

Interface\*



(Interface starting with this icon  signifies it is available for route leak)

Available Network  +

Add

Selected Network



10.201.204.129

192.168.1.0\_24

any-ipv4

CSM

Data\_Store

FDM

Gateway\*

+



Metric:

(1 - 254)

Tunneled:  (Used only for default Route)

Route Tracking:

+

Cancel

OK

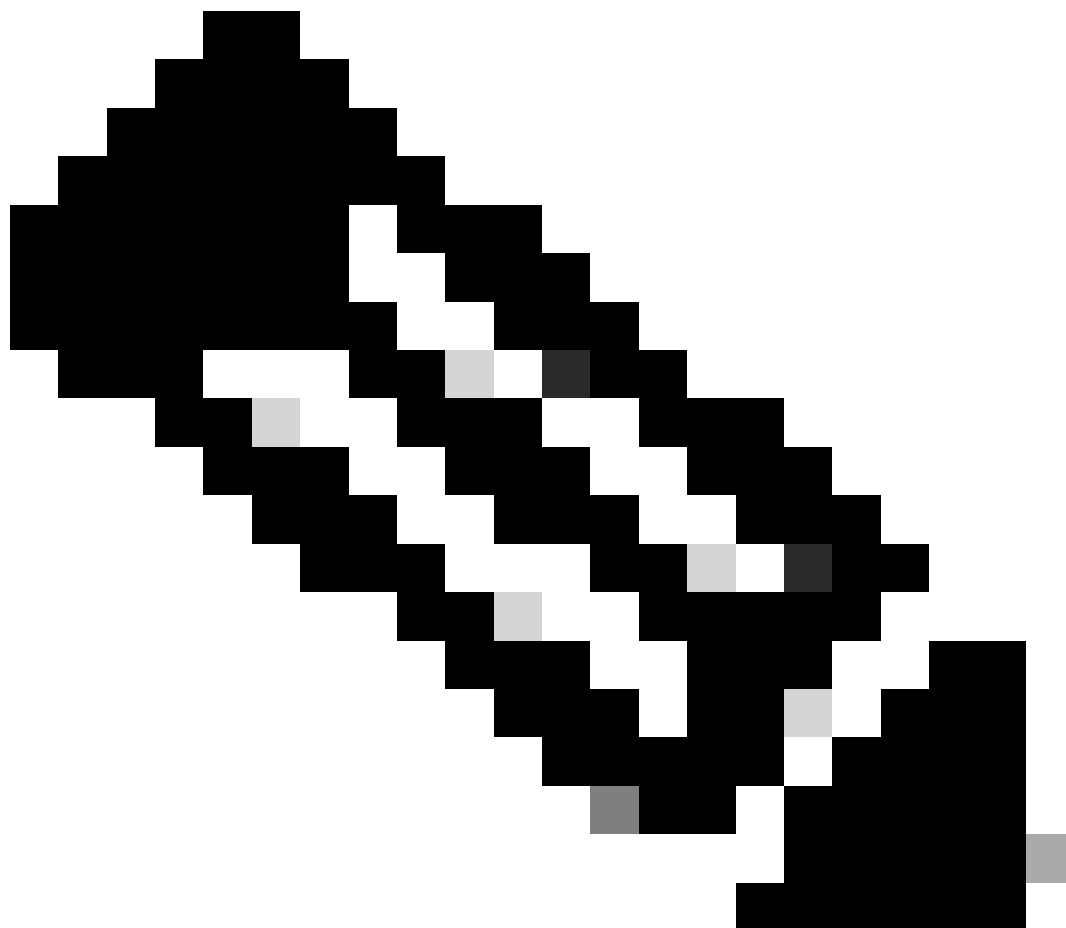
5. 設定変更を導入します。これで、設定変更が現在の管理インターフェイスに適用されます。

6. FTD CLIで、管理インターフェイスにスタティックIPアドレスを使用するように設定し、ゲートウェイにデータインターフェイスを設定します。

- `network {ipv4 | ipv6} manual ip_address netmask data-interfaces`の設定

```
>  
>  
> configure network ipv4 manual IP_ADDRESS 192.168.1.8 NETMASK 255.255.255.0 GATEWAY data-interfaces  
Setting IPv4 network configuration...  
Interface eth0 speed is set to '10000baseT/Full'  
Network settings changed.
```





---



注：管理インターフェイスを使用する予定はありませんが、固定IPアドレスを設定する必要があります。たとえば、ゲートウェイをdata-interfacesに設定できるようにするプライベートアドレスです。この管理は、tap\_nlpインターフェイスを使用してデータインターフェイスに管理トラフィックを転送するために使用されます。

---

7. Management CenterでManagementを無効にします。Devices > Device Management > Device > Managementの順に選択して、脅威対策のEditをクリックし、Remote Host Address IP addressesおよび(Optional)Secondary Addressを更新し、接続をイネーブルにします。

Management		 
Remote Host Address:		192.168.1.8
Secondary Address:		
Status:		
Manager Access Interface:		 <a href="#">Data Interface</a>
Manager Access Details:		<a href="#">Configuration</a>

## プラットフォーム設定でのSSHの有効化

Platform Settings policyでデータインターフェイスのSSHを有効にし、Devices > Platform Settings > SSH Accessでこのデバイスに適用します。[Add] をクリックします。

1. SSH接続を許可しているホストまたはネットワーク。
2. SSH接続を許可するインターフェイスを含むゾーンを追加します。ゾーンに含まれないインターフェイスの場合は、Selected Zones/Interfacesフィールドにinterface nameを入力して、Addをクリックします。
3. [OK] をクリックします。 変更を展開します。

## Add Secure Shell Configuration



IP Address\*

+



Available Zones/Interfaces

C

- DMZ
- Inside
- outside

Add



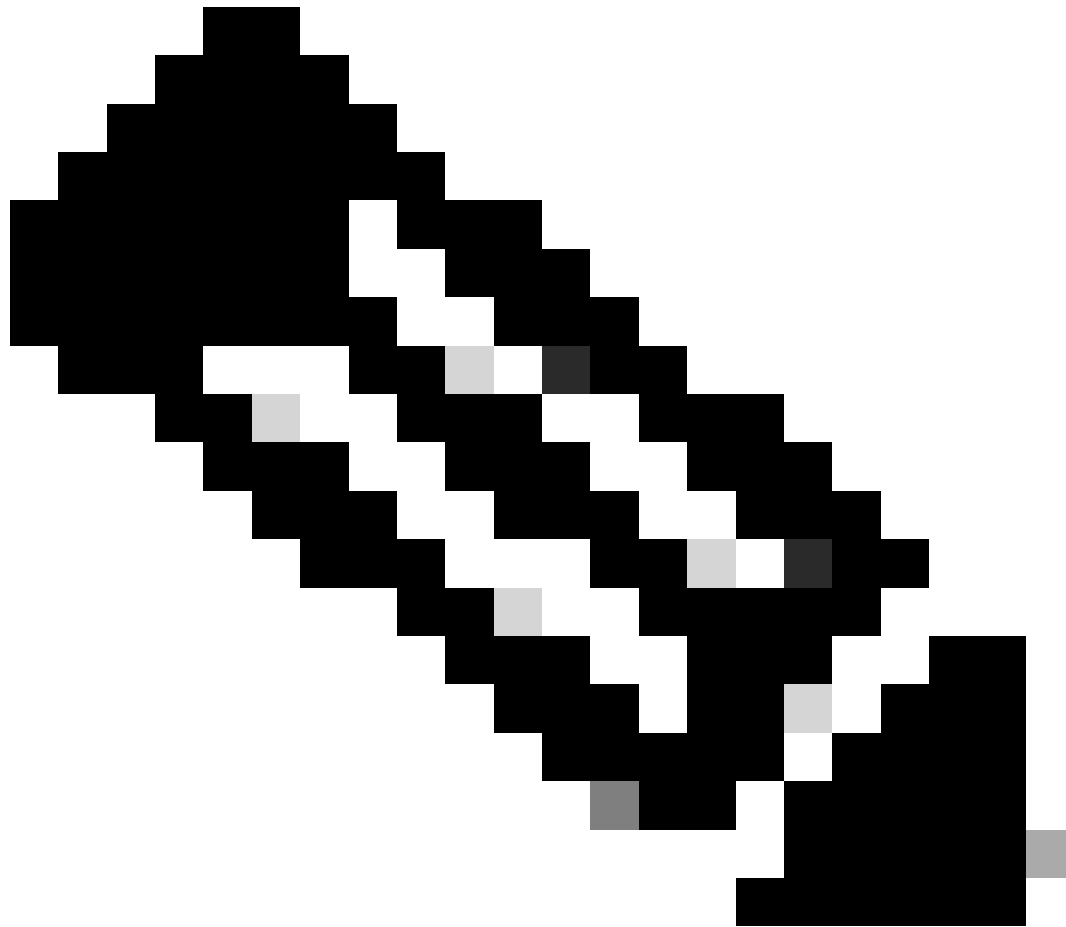
Selected Zones/Interfaces

Interface Name

Add

Cancel

OK



注：データインターフェイスではSSHはデフォルトで有効になっていないため、SSHを使用して脅威対策を管理する場合は、明示的に許可する必要があります。




---

## 確認

データインターフェイス経由で管理接続が確立されていることを確認します。

FMCのグラフィカルユーザインターフェイス(GUI)からの確認

Management Centerで、Devices > Device Management > Device > Management > Manager Access - Configuration Details > Connection Statusページの管理接続のステータスを確認します。

Management 	
Remote Host Address:	192.168.1.30
Secondary Address:	
Status:	Connected  
Manager Access Interface:	Data Interface
Manager Access Details:	Configuration

## FTDコマンドラインインターフェイス(CLI)からの確認

threat defenseCLIで、thesftunnel-status-briefコマンドを入力して、管理接続のステータスを表示します。

```
>  
> sftunnel-status-brief  
  
PEER:192.168.1.2  
Peer channel Channel-A is valid type (CONTROL), using 'tap_nlp', connected to '192.168.1.2' via '169.254.1.2'  
Peer channel Channel-B is valid type (EVENT), using 'tap_nlp', connected to '192.168.1.2' via '169.254.1.2'  
Registration: Completed.  
IPv4 Connection to peer '192.168.1.2' Start Time: Tue Jul 16 22:23:54 2024 UTC  
Heartbeat Send Time: Tue Jul 16 22:39:52 2024 UTC  
Heartbeat Received Time: Tue Jul 16 22:39:52 2024 UTC  
Last disconnect time : Tue Jul 16 22:17:42 2024 UTC  
Last disconnect reason : Both control and event channel connections with peer went down
```

ステータスには、データインターフェイスの接続が成功したことが示され、内部のtap\_nlpインターフェイスが示されます。

## トラブルシューティング

Management Centerで、Devices > Device Management > Device > Management > Manager Access - Configuration Details > Connection Statusページの管理接続のステータスを確認します。

threat defenseCLIで、thesftunnel-status-briefコマンドを入力して、管理接続のステータスを表示します。また、usestunnel-statusを使用して詳細な情報を表示することもできます。

## 管理接続ステータス

### 正常動作シナリオ

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

```
PEER:192.168.1.2
Peer channel Channel-A is valid type (CONTROL), using 'eth0', connected to '192.168.1.2' via '192.168.1.8'
Peer channel Channel-B is valid type (EVENT), using 'tap_nlp', connected to '192.168.1.2' via '169.254.1.2'
Registration: Completed.
IPv4 Connection to peer '192.168.1.2' Start Time: Wed Jul 17 06:21:15 2024 UTC
Heartbeat Send Time: Wed Jul 17 17:15:20 2024 UTC
Heartbeat Received Time: Wed Jul 17 17:16:55 2024 UTC
Last disconnect time : Wed Jul 17 06:21:12 2024 UTC
Last disconnect reason : Process shutdown due to stop request from PM
```

## 正常に動作しないシナリオ

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

```
PEER:192.168.1.2
Registration: Completed.
Connection to peer '192.168.1.2' Attempted at Wed Jul 17 17:20:26 2024 UTC
Last disconnect time : Wed Jul 17 17:20:26 2024 UTC
Last disconnect reason : Both control and event channel connections with peer went down
```

## ネットワーク情報の検証

脅威に対する防御のCLIで、管理およびマネージャアクセスデータインターフェイスのネットワーク設定を表示します。

```
> show network
```

```
> show network
===== [ System Information ] =====
Hostname                : ftdcdo.breakstuff.com
Domains                 : breakstuff.com
DNS Servers             : 192.168.1.103
DNS from router        : enabled
Management port        : 8305
IPv4 Default route
  Gateway               : data-interfaces
IPv6 Default route
  Gateway               : data-interfaces

===== [ eth0 ] =====
State                   : Enabled
Link                    : Up
Channels                : Management & Events
Mode                    : Non-Autonegotiation
MDI/MDIX                : Auto/MDIX
MTU                     : 1500
MAC Address             : 00:0C:29:54:D4:47
----- [ IPv4 ] -----
Configuration           : Manual
Address                 : 192.168.1.8
Netmask                 : 255.255.255.0
Gateway                 : 192.168.1.1
----- [ IPv6 ] -----
Configuration           : Disabled

===== [ Proxy Information ] =====
State                   : Disabled
Authentication          : Disabled

===== [ System Information - Data Interfaces ] =====
DNS Servers             :
Interfaces              : GigabitEthernet0/0

===== [ GigabitEthernet0/0 ] =====
State                   : Enabled
Link                    : Up
Name                    : Outside
MTU                     : 1500
MAC Address             : 00:0C:29:54:D4:5B
```

## 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。