

CD-FMCで管理されるAzure FTDに冗長データインターフェイスを展開する

内容

はじめに

このドキュメントでは、冗長マネージャアクセスデータインターフェイス(RMI)機能を使用するようにcdFMC管理仮想FTDを設定する手順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ファイアウォール管理センター
- Cisco Defense Orchestrator

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。

- クラウドで提供されるFirewall Management Center
- Azure CloudでホストされるVirtual Secure Firewall Threat Defenseバージョン7.3.1。

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。

関連製品

このドキュメントは、次のバージョンのハードウェアとソフトウェアにも使用できます。

- Firepower Threat Defense(FTD)バージョン7.3.0以降を実行できる物理アプライアンス。

背景説明

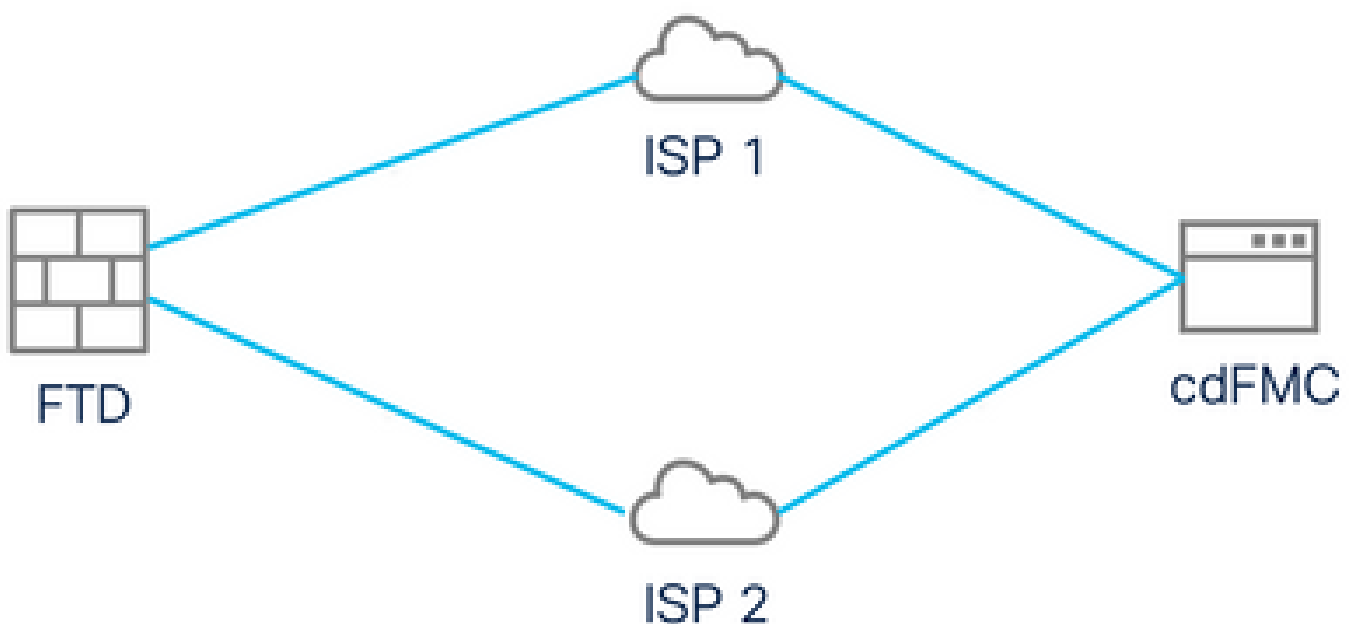
このドキュメントでは、管理目的で2つのデータインターフェイスを使用するようにcdFMC管理

対象vFTDを設定および確認する手順を示します。この機能は、お客様が第2のISPを使用してインターネット経由でFTDを管理するために第2のデータインターフェイスを必要とする場合に役立ちます。デフォルトでは、FTDは両方のインターフェイス間の管理トラフィックに対してラウンドロビン方式でロードバランシングを行います。このロードバランシングは、このドキュメントで説明するように、アクティブ/バックアップの導入に変更できます。

管理用冗長データインターフェイス機能は、Secure Firewall Threat Defenseバージョン7.3.0で導入されました。vFTDは、CDOアクセス用のURLを解決できるネームサーバに到達できることが前提となっています。

コンフィギュレーション

ネットワーク図



ネットワーク図

管理アクセス用のデータインターフェイスの設定

コンソールを使用してデバイスにログインし、`configure network management-data-interface` コマンドを使用して、管理アクセス用のデータインターフェイスの1つを設定します。

```
<#root>
```

```
>
```

```
configure network management-data-interface
```

Note: The Management default route will be changed to route through the data interfaces. If you are connecting to the device with SSH, your connection may drop. You must reconnect using the console port.

Data interface to use for management:

```
GigabitEthernet0/0
```

```
Specify a name for the interface [outside]:
```

```
outside-1
```

```
IP address (manual / dhcp) [dhcp]:
```

```
manual
```

```
IPv4/IPv6 address:
```

```
10.6.2.4
```

```
Netmask/IPv6 Prefix:
```

```
255.255.255.0
```

```
Default Gateway:
```

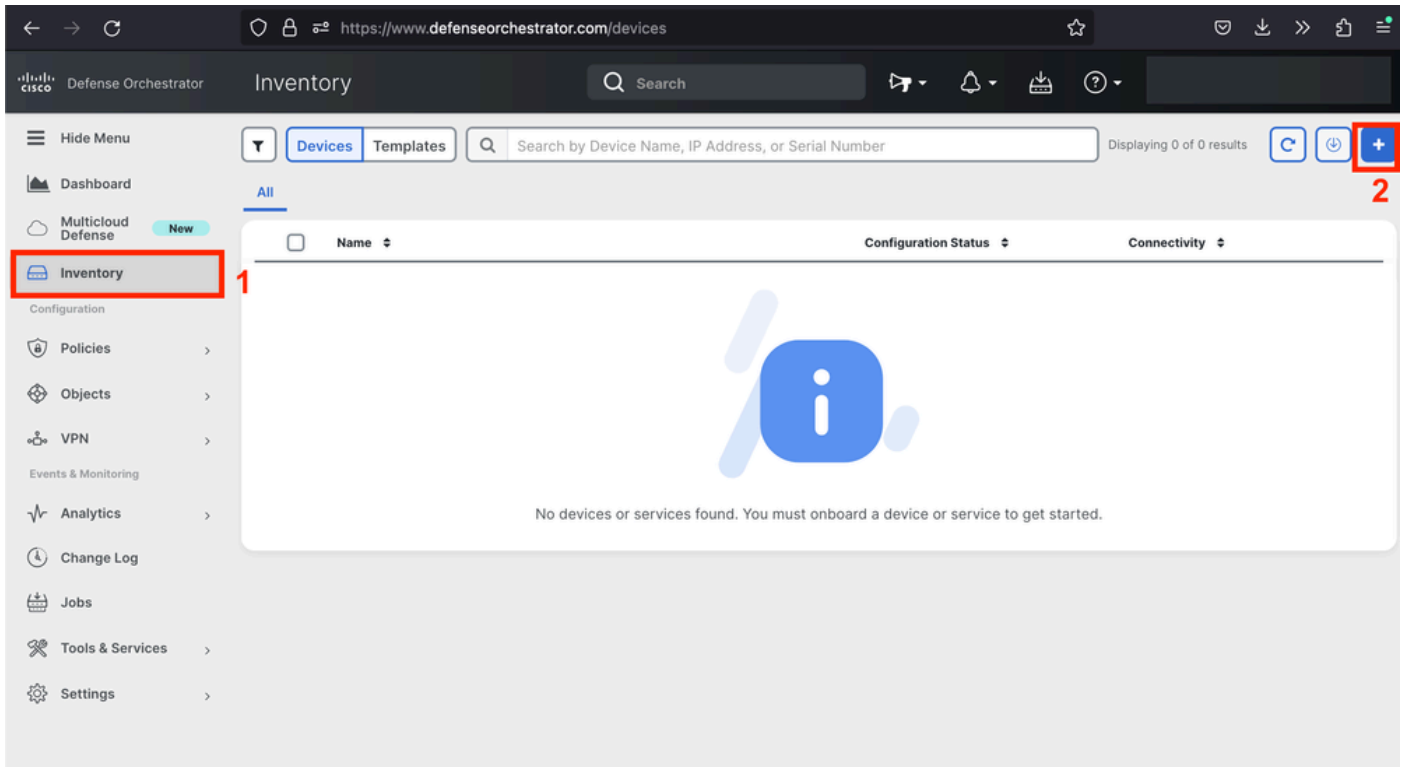
```
10.6.2.1
```

元の管理インターフェイスは、DHCPを使用するように設定できないことに注意してください。これは、show networkコマンドを使用して確認できます。

CDOによるFTDのオンボード

このプロセスはAzure FTDをCDOにオンボードするため、クラウド提供のFMCで管理できます。このプロセスではCLI登録キーを使用します。これは、デバイスにDHCP経由で割り当てられたIPアドレスがある場合に便利です。ログタッチプロビジョニングやシリアル番号などの他のオンボーディング方法は、Firepower 1000、Firepower 2100、またはセキュアファイアウォール3100プラットフォームでのみサポートされます。

ステップ 1 : CDOポータルで、Inventory に移動し、Onboard オプションをクリックします。



インベントリページ

ステップ2:FTDタイルをクリックします。

Select a Device or Service Type

No Secure Device Connector found to communicate with some types of devices. [Set up a Secure Device Connector](#)



ASA

Adaptive Security Appliance
(8.4+)



Multiple ASAs

Adaptive Security Appliance
(8.4+)



FTD

Cisco Secure
Firewall Threat Defense

Meraki

Meraki

Meraki Security Appliance



Integrations

Enable basic CDO functionality for
integrations



AWS VPC

Amazon Virtual Private Cloud



Duo Admin

Duo Admin Panel

Umbrella

Umbrella Organization

View Umbrella Organization Policies
from CDO



Import

Import configuration for offline
management

FTDのオンボーディング

ステップ3 : オプションUse CLI Registration keyを選択します。



Firewall Threat Defense

Important: After onboarding your FTD, it will be managed by Firewall Management Center in CDO. Note that use of the firewall device manager will not be available after onboarding, and all existing policy configurations will be reset. You will need to reconfigure policies from CDO after onboarding. [Learn more](#)



Use CLI Registration Key

Onboard a device using a registration
key generated from CDO and applied
on the device using the Command
Line Interface.
(FTD 7.0.3+ & 7.2+)



Use Serial Number

Use this method for low-touch
provisioning or for onboarding
configured devices using their serial
number.
(FTD 7.2+)



Deploy an FTD to a cloud environment

Deploy an FTD to a supported cloud
environment; AWS, GCP and Azure

CLI登録キーの使用

ステップ 4 : configure managerコマンドから開始してCLIキーをコピーします。

1 Device Name **FTDv-Azure**

2 Policy Assignment **Access Control Policy: Default Access Control Policy**

3 Subscription License **Performance Tier: FTDv, License: Threat, Malware, URL License**

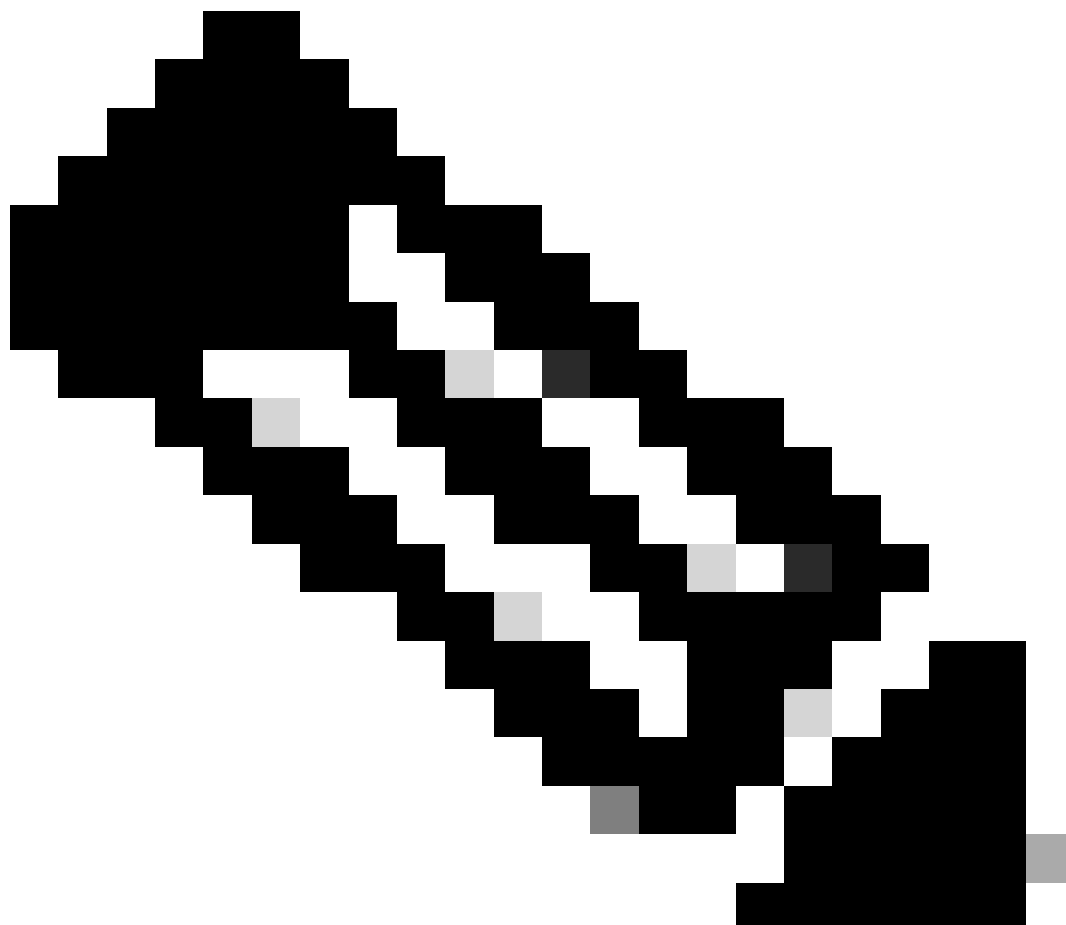
4 CLI Registration Key

- 1 Ensure the device's initial configuration is complete before trying to apply the registration key. [Learn more](#)
- 2 Copy the CLI Key below and paste it into the CLI of the FTD

```
configure manager add cisco-cisco-systems--s1kaau.app.us.cdo.cisco.com  
t67mPqC8cAW6GH2NhhHTUD4poWARdRr7 YJqFWzmpnfbJ6WANBeHTAhXnod9E7c1e cisco-cisco-  
systems--s1kaau.app.us.cdo.cisco.com
```

[Next](#)

Copy Configure Managerコマンド



注:CLIキーは、オンプレミスFMCを使用したFTDの登録で使用される形式と一致します。

ここでは、管理対象デバイスがNATデバイスの背後にある場合に登録を許可するようにNAT-IDを設定できます。configure manager add <fmc-hostname-or-ipv4> <registration-key> <nat-id> <display-name>

ステップ 5 : コマンドをFTD CLIに貼り付けます。通信が成功した場合は、次のメッセージを受信する必要があります。

```
Manager cisco-cisco-systems--s1kaau.app.us.cdo.cisco.com successfully configured.  
Please make note of reg_key as this will be required while adding Device in FMC.
```

手順 6 : CDOに戻り、Nextをクリックします。

3 Subscription License Performance Tier: FTDv, Licen...

4 CLI Registration Key

- 1 Ensure the device's initial
- 2 Copy the CLI Key below a

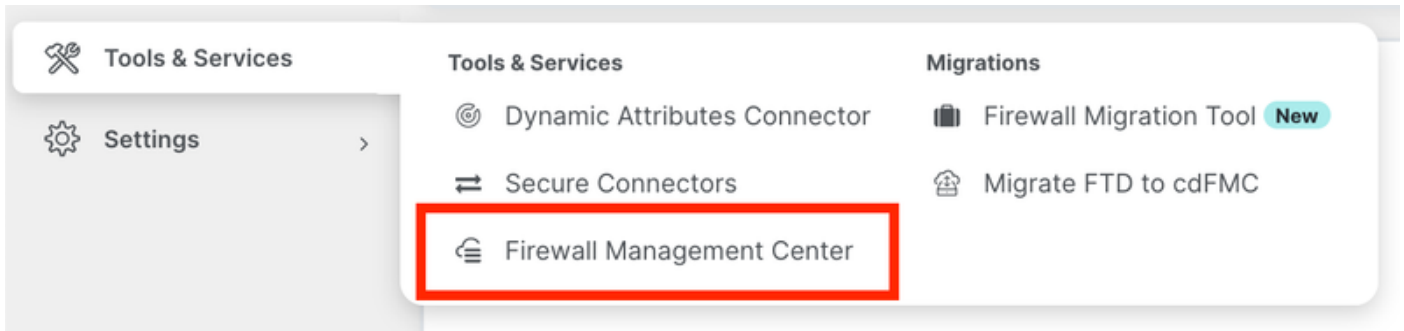
```
configure manager add  
t67mPqC8cAW6GH2NhhhTL  
systems--s1kaau.app.u
```

Next

[Next] をクリックします。

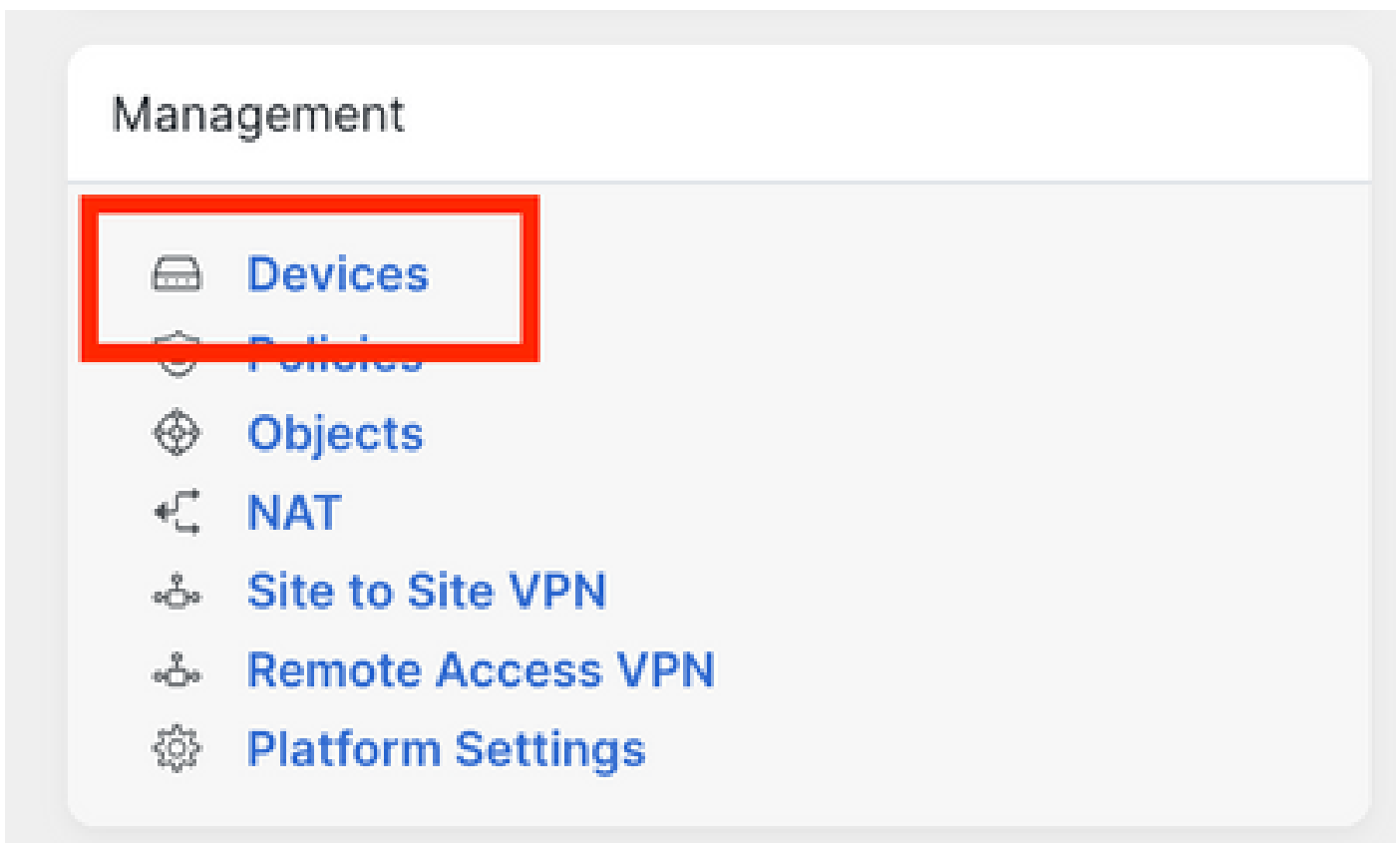
CDOは登録プロセスを続行し、完了までに長い時間がかかることを示すメッセージが表示されま
す。登録プロセスのステータスを確認するには、サービスページのデバイスリンクをクリックし
ます。

手順 7 : Tools & ServicesページからFMCにアクセスします。



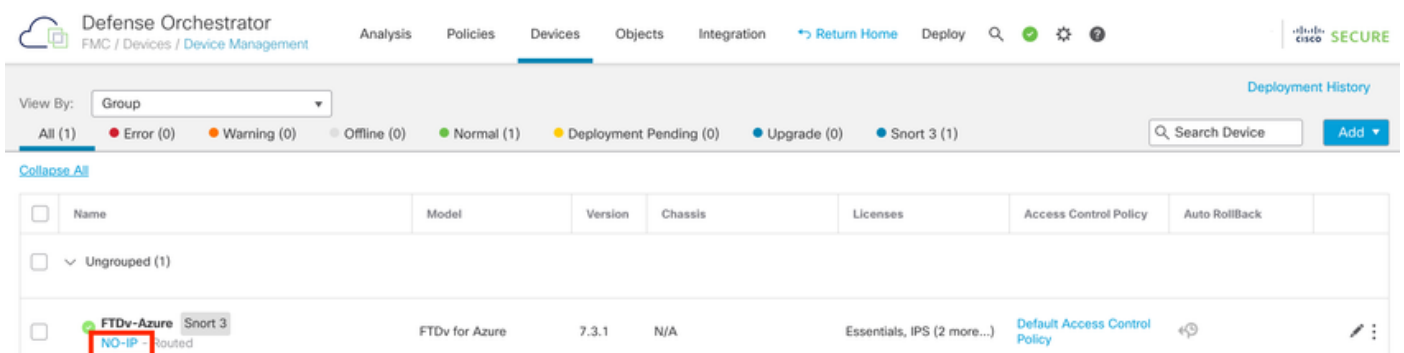
cdFMCへのアクセス

Devices リンクをクリックします。



Devicesをクリックします

これでFTDがCDOにオンボーディングされ、クラウド配信のFMCで管理できるようになります。次の図では、デバイス名の下にNO-IPが表示されています。これは、CLI登録キーを使用したオンボーディングプロセスで必要になります。



マネージャアクセス用の冗長データインターフェイスの設定

このプロセスでは、管理アクセス用に2番目のデータインターフェイスを割り当てます。

ステップ 1 : Devicesタブで、鉛筆アイコンをクリックしてFTD編集モードにアクセスします。

Defense Orchestrator
FMC / Devices / Device Management

Analysis Policies **Devices** Objects Integration [Return Home](#) Deploy 🔍 ⚙️ ⓘ

View By: Group Deployment History

All (1) ● Error (0) ● Warning (0) ● Offline (0) ● Normal (1) ● Deployment Pending (0) ● Upgrade (0) ● Snort 3 (1) 🔍 Search Device [Add](#)

[Collapse All](#)

<input type="checkbox"/>	Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack	
<input type="checkbox"/>	▼ Ungrouped (1)							
<input type="checkbox"/>	● FTDv-Azure <small>Snort 3</small> NO-IP - Routed	FTDv for Azure	7.3.1	N/A	Essentials, IPS (2 more...)	Default Access Control Policy	⚙️	✎

FTDの編集

ステップ 2 : Interfaceタブで、冗長管理インターフェイスとして割り当てるインターフェイスを編集します。これをまだ行っていない場合は、インターフェイス名とIPアドレスを設定します。

ステップ 3 : Manager Accessタブで、Enable management on this interface for the manager チェックボックスをオンにします。

Edit Physical Interface ⓘ

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

Enable management on this interface for the Manager

Available Networks [+](#)

🔍 Search

- any-ipv4
- any-ipv6
- IPv4-Benchmark-Tests
- IPv4-Link-Local
- IPv4-Multicast
- IPv4-Private-10.0.0.0-8

[Add](#)

Allowed Management Networks

any

[Cancel](#) [OK](#)

マネージャのアクセスの有効化

ステップ 4 : General タブで、インターフェイスがセキュリティゾーンに割り当てられていることを確認し、OKをクリックします。

Edit Physical Interface



General IPv4 IPv6 Path Monitoring Hardware Configuration Manager Access Advanced

Name:

Enabled
 Management Only

Description:

Mode:

Security Zone:

冗長データインターフェイスのセキュリティゾーン

ステップ 5 : これで、両方のインターフェイスにManager Accessタグが付けられたことに注目してください。さらに、プライマリデータインターフェイスが別のセキュリティゾーンに割り当てられていることを確認します。

FTDv-Azure Cisco Firepower Threat Defense for Azure Save Cancel

Device Routing Interfaces Inline Sets DHCP VTEP

Search by name Sync Device Add Interfaces

Interface	Logical N...	Typ	Security Z...	MAC Address (Active/Standby)	IP Address	Path...	Virtual Ro...
Diagnostic0/0	diagnostic	Phy				Disa...	Global
GigabitEthernet0/0 (Manager Access)	outside-1	Phy	outside1-sz		10.6.2.4/255.255.255.0(Static)	Disa...	Global
GigabitEthernet0/1 (Manager Access)	outside-2	Phy	outside2-sz		10.6.3.4/255.255.255.0(Static)	Disa...	Global

インターフェイス設定の確認

次のセクションでは、ステップ6 ~ 10は、CDOに到達するために2つの等コストのデフォルトルートを設定することを目的とし、各デフォルトルートは独立したSLAトラッキングプロセスによってモニタされます。SLAトラッキングにより、監視対象インターフェイスを使用してcdFMCと通信するための機能パスが存在することが保証されます。

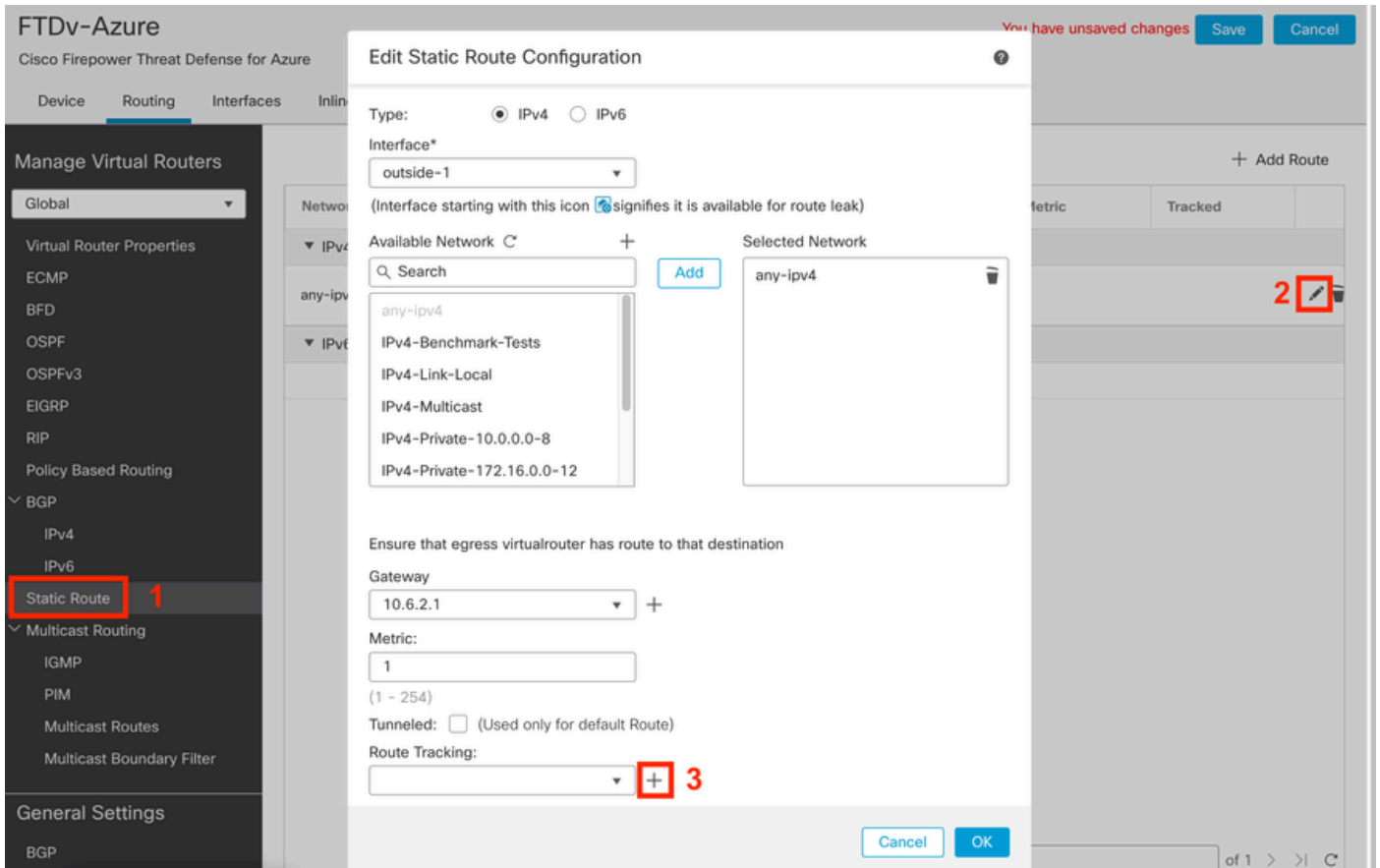
手順 6 : Routingタブに移動し、ECMPメニューで両方のインターフェイスを含む新しいECMPゾーンを作成します。

ECMPゾーンの設定

OKをクリックして、保存します。

手順 7 : Routingタブから、Static Routesに移動します。

プライマリルートを編集するには、鉛筆アイコンをクリックします。プラス記号をクリックして、新しいSLAトラッキングオブジェクトを追加します。



プライマリルートを編集してSLAトラッキングを追加する

ステップ 8 : 機能的なSLAトラッキングに必要なパラメータは、次の図で強調表示されています。オプションで、Number of Packets、Timeout、Frequencyなどの他の設定を調整できます。

Edit SLA Monitor Object



Name:

outside1-sla

Description:

Frequency (seconds):

60

(1-604800)

SLA Monitor ID*:

1

Threshold (milliseconds):

5000

(0-60000)

Timeout (milliseconds):

5000

(0-604800000)

Data Size (bytes):

28

(0-16384)

ToS:

0

Number of Packets:

1

Monitor Address*:



Available Zones

Search

outside1-sz

outside2-sz

Selected Zones/Interfaces

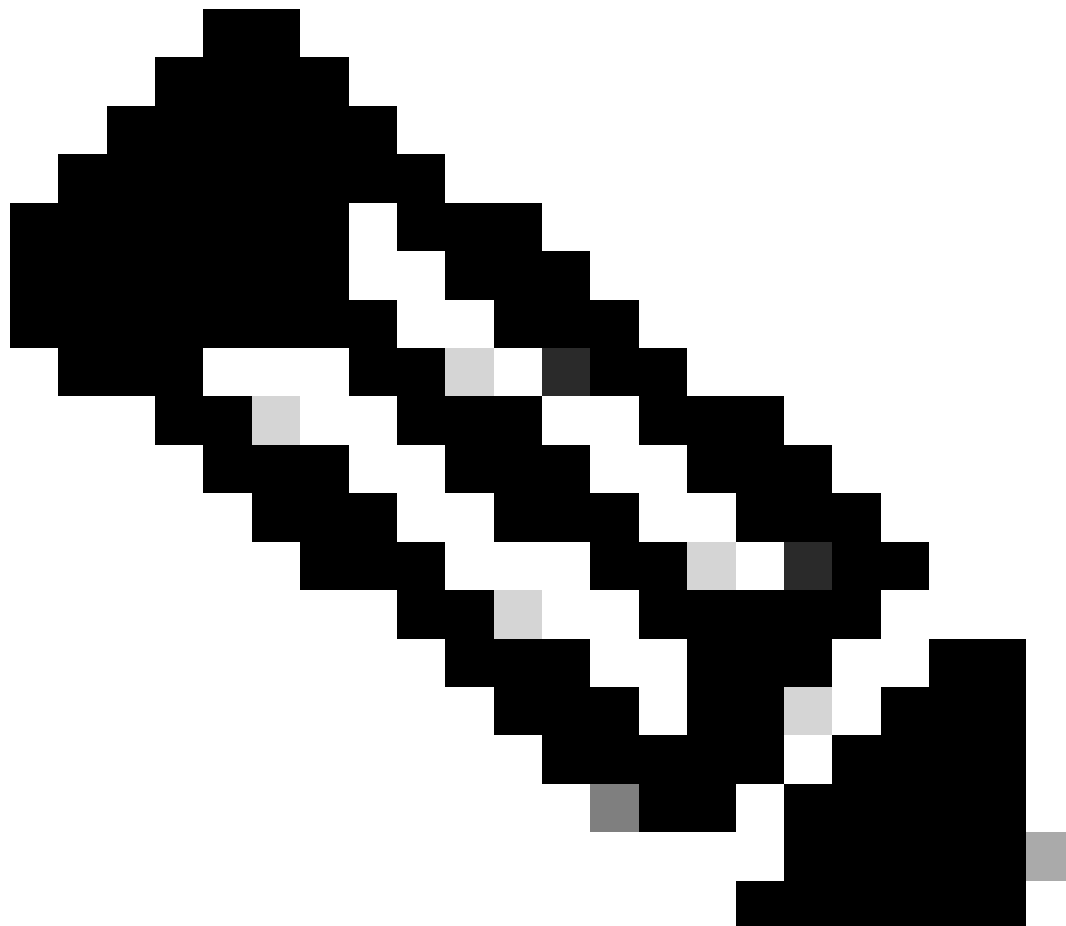
Add

outside1-sz

Cancel

Save

この例では、outside1インターフェイスを介してインターネット（およびCDO）に到達するFTD機能を監視するために、Google DNS IPが使用されました。準備ができたら、okをクリックします。



注：FTD外部インターフェイスから到達可能であると検証済みのIPを追跡していることを確認します。到達不能なIPを持つトラックを設定すると、このFTDでデフォルトルートがダウンし、CDOとの通信機能が停止する可能性があります。

ステップ9：Saveをクリックし、新しいSLAトラッキングがプライマリインターフェイスを指すルートに割り当てられていることを確認します。

Route Tracking:

outside1-sla



外部1 SLAトラッキング

OKをクリックすると、次の警告メッセージを示すポップアップが表示されます。

Warning about Static Route

This Static route is defined on the Defense Orchestrator Access Interface. Ensure the change is not affecting connectivity to the device

OK

構成の警告

ステップ 10 : Add Routeオプションをクリックして、冗長データインターフェイスの新しいルートを追加します。次の図では、ルートのメトリック値が同じであることに注意してください。また、SLAトラッキングには異なるIDが割り当てられています。

Add Static Route Configuration



Type: IPv4 IPv6

Interface*

outside-2

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

Available Network  +

Search

Add

any-ipv4

IPv4-Benchmark-Tests


IPv4-Link-Local

IPv4-Multicast

IPv4-Private-10.0.0.0-8

IPv4-Private-172.16.0.0-12

Selected Network

any-ipv4 

Gateway*

10.6.3.1



Metric:

1

(1 - 254)

Tunneled: (Used only for default Route)

Route Tracking:

outside2-sla



Cancel

OK

冗長スタティックルートの設定

Edit SLA Monitor Object



Name:

outside2-sla

Description:

Frequency (seconds):

60

(1-604800)

SLA Monitor ID*:

2

Threshold (milliseconds):

5000

(0-60000)

Timeout (milliseconds):

5000

(0-604800000)

Data Size (bytes):

28

(0-16384)

ToS:

0

Number of Packets:

1

Monitor Address*

Available Zones

Search

outside1-sz

outside2-sz

Add

Selected Zones/Interfaces

outside2-sz

Cancel

Save

[Save] をクリックします。

ステップ 11 必要に応じて、Device > Management でセカンダリデータインターフェイスIPを指定できます。ただし、現在のオンボーディング方式ではCLI登録キーププロセスが使用されるため、これは必須ではありません。

FTDv-Azure
Cisco Firepower Threat Defense for Azure

Device Routing Interfaces Inline Sets DHCP VTEP

Rules: UTC (UTC+0:00)

Health
Status: ✔
Policy: Initial_Health_Policy 2023-06-29 17:28:08
Excluded: None

Management ✎
Remote Host Address: NO-IP
Secondary Address:
Status: ✔
Manager Access Interface: Data Interface
Manager Access Details: Configuration

(オプション) Management フィールドで冗長データインターフェイスのIPを指定します

ステップ 12 変更を展開します。

(オプション) アクティブ/バックアップインターフェイスモードのインターフェイスコストを設定します。

デフォルトでは、データインターフェイス上の冗長管理はラウンドロビンを使用して、両方のインターフェイス間に管理トラフィックを分散します。または、一方のWANリンクの帯域幅がもう一方よりも大きく、このリンクをプライマリ管理リンクにして、もう一方をバックアップとして残す場合は、プライマリリンクのコストを1に、バックアップリンクのコストを2に設定します。次の例では、インターフェイスGigabitEthernet0/0がプライマリWANリンクとして維持され、GigabitEthernet0/1がバックアップ管理リンクとして機能しています。

1. Devices > FlexConfig リンクに移動し、flexConfig ポリシーを作成します。flexConfig ポリシーがすでに設定され、FTD に割り当てられている場合は、それを編集します。

Device Management	VPN	Troubleshoot
Device Upgrade	Site To Site	File Download
NAT	Remote Access	Threat Defense CLI
QoS	Dynamic Access Policy	Packet Tracer
Platform Settings	Troubleshooting	Packet Capture
FlexConfig	Site to Site Monitoring	
Certificates		

FlexConfigメニューへのアクセス

2. 新しいFlexConfigオブジェクトを作成します。

- FlexConfigオブジェクトに名前を付けます。
- DeploymentセクションとTypeセクションで、それぞれEverytimeとAppendを選択します。
- 図22に示すように、インターフェイスのコストを次のコマンドで設定します。
- [Save] をクリックします。

```
<#root>
```

```
interface GigabitEthernet0/0
```

```
  policy-route cost 1
```

<=== A cost of 1 means this will be the primary interface for management communication with CDO tenant.

```
interface GigabitEthernet0/1
```

```
  policy-route cost 2
```

<=== Cost 2 sets this interface as a backup interface.

Defense Orchestrator
FMC / Devices / Flexconfig Policy Editor

Analysis Policies Devices Objects Integration

Return Home Deploy

MyFlexconfig

Enter Description

Available FlexConfig

FlexConfig Object

User Defined

System Defined

- Default_DNS_Configure
- Default_Inspection_Protocol_Disable
- Default_Inspection_Protocol_Enable
- DHCPv6_Prefix_Delegation_Configure
- DHCPv6_Prefix_Delegation_UnConfigure
- DNS_Configure
- DNS_UnConfigure
- Eigrp_Configure
- Eigrp_Interface_Configure
- Eigrp_UnConfigure
- Eigrp_Unconfigure_All
- Inspect_IPv6_Configure
- Inspect_IPv6_UnConfigure
- ISIS_Configure
- ISIS_Interface_Configuration
- ISIS_Unconfigure
- ISIS_Unconfigure_All
- Netflow_Add_Destination
- Netflow_Clear_Parameters

Add FlexConfig Object

Name: InterfaceCost

Description:

Copy-pasting any rich text might introduce line breaks while generating CLI. Please verify the CLI before deployment.

Insert Deployment: Everytime Type: Append

```
interface GigabitEthernet0/0
policy-route cost 1
interface GigabitEthernet0/1
policy-route cost 2
```

Variables

Name	Dimension	Default Value	Property (Type:Name)	Override	Description
No records to display					

Cancel Save

Flexconfigオブジェクトの追加

3. 図に示すように、最近作成したオブジェクトを選択し、選択したFlexConfigs追加セクションに追加します。変更を保存し、設定を展開します。

Defense Orchestrator Flexconfig Policy Editor

Analysis Policies Devices Objects Integration [Return Home](#) **Deploy** 5 ✓ ⚙️ ?

MyFlexconfig Migrate Config Preview Config **Save** 4 Cancel

Enter Description Policy Assignments (1)

Available FlexConfig FlexConfig Object

- ✓ User Defined
 - InterfaceCost** 1
- System Defined
 - Default_DNS_Configure
 - Default_Inspection_Protocol_Disable
 - Default_Inspection_Protocol_Enable
 - DHCPv6_Prefix_Delegation_Configure
 - DHCPv6_Prefix_Delegation_UnConfigure
 - DNS_Configure
 - DNS_UnConfigure
 - Eigrp_Configure
 - Eigrp_Interface_Configure
 - Eigrp_UnConfigure
 - Eigrp_Unconfigure_All
 - Inspect_IPv6_Configure
 - Inspect_IPv6_UnConfigure
 - ISIS_Configure
 - ISIS_Interface_Configuration
 - ISIS_Unconfigure
 - ISIS_Unconfigure_All
 - Netflow_Add_Destination

Selected Prepend FlexConfigs

#	Name	Description

Selected Append FlexConfigs

#	Name	Description
1	InterfaceCost	

Flexconfigポリシーへのオブジェクトの割り当て

4. 変更を展開します。

確認

1. 確認するには、show networkコマンドを使用します。冗長管理インターフェイスの新しいインスタンスが形成されます。

```
> show network
```

```
<<----- output omitted for brevity ----->>
```

```
=====[ eth0 ]=====
State : Enabled
Link : Up
Channels : Management & Events
Mode : Non-Autonegotiation
MDI/MDIX : Auto/MDIX
MTU : 1500
MAC Address : 60:45:BD:D8:62:D7
-----[ IPv4 ]-----
Configuration : Manual
```

```

Address : 10.6.0.4
Netmask : 255.255.255.0
-----[ IPv6 ]-----
Configuration : Disabled

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

=====[ GigabitEthernet0/0 ]=====
State : Enabled
Link : Up
Name : outside-1
MTU : 1500
MAC Address : 60:45:BD:D8:6F:5C
-----[ IPv4 ]-----
Configuration : Manual
Address : 10.6.2.4
Netmask : 255.255.255.0
Gateway : 10.6.3.1
-----[ IPv6 ]-----
Configuration : Disabled

=====[ GigabitEthernet0/1 ]=====
State : Enabled
Link : Up
Name : outside-2
MTU : 1500
MAC Address : 60:45:BD:D8:67:CA
-----[ IPv4 ]-----
Configuration : Manual
Address : 10.6.3.4
Netmask : 255.255.255.0
Gateway : 10.6.3.1
-----[ IPv6 ]-----
Configuration : Disabled

```

2. インターフェイスがsftunnelドメインの一部になりました。これは、show sftunnel interfacesコマンドとshow running-config sftunnelコマンドで確認できます。

```
<#root>
```

```
>
```

```
show sftunnel interfaces
```

```

Physical Interface Name of the Interface
GigabitEthernet0/0 outside-1
GigabitEthernet0/1 outside-2

```

```
>
```

```
show running-config sftunnel
```

```

sftunnel interface outside-2
sftunnel interface outside-1

```

```
sftunnel port 8305
sftunnel route-map FMC_GEN_19283746_RBD_DUAL_WAN_RMAP_91827346
```

3. ポリシーベースのルートは自動的にスペルアウトされます。インターフェイスコストを指定しなかった場合、adaptive-interfaceオプションはラウンドロビン処理を設定して、両方のインターフェイス間で管理トラフィックのロードバランシングを行います。

```
<#root>
```

```
>
```

```
show running-config route-map
```

```
!
route-map FMC_GEN_19283746_RBD_DUAL_WAN_RMAP_91827346 permit 5
 match ip address FMC_GEN_056473829_RBD_DUAL_WAN_ACL_165748392
 set adaptive-interface cost outside-1 outside-2
```

```
>
```

```
show access-list FMC_GEN_056473829_RBD_DUAL_WAN_ACL_165748392
```

```
access-list FMC_GEN_056473829_RBD_DUAL_WAN_ACL_165748392; 1 elements; name hash: 0x8e8cb508
access-list FMC_GEN_056473829_RBD_DUAL_WAN_ACL_165748392 line 1 extended permit tcp any any eq 8305 (hi
```

4. show running-config interface <interface> コマンドを使用してインターフェイス設定を確認します。

```
<#root>
```

```
>
```

```
show running-config interface GigabitEthernet 0/0
```

```
!
interface GigabitEthernet0/0
 nameif outside-1
 security-level 0
 zone-member outside-ecmp
 ip address 10.6.2.4 255.255.255.0
 policy-route cost 1
```

```
>
```

```
show running-config interface GigabitEthernet 0/1
```

```
!
interface GigabitEthernet0/1
 nameif outside-2
 security-level 0
 zone-member outside-ecmp
 ip address 10.6.3.4 255.255.255.0
```

```
policy-route cost 2
```

いくつかの追加コマンドを使用して、設定されたルートのトラッキングを確認できます。

```
<#root>
```

```
>
```

```
show track
```

```
Track 1
```

```
Response Time Reporter 2 reachability
```

```
Reachability is Up
```

```
<===== Ensure reachability is up for the monitored interf
```

```
2 changes, last change 09:45:00
```

```
Latest operation return code: OK
```

```
Latest RTT (milliseconds) 10
```

```
Tracked by:
```

```
STATIC-IP-ROUTING 0
```

```
Track 2
```

```
Response Time Reporter 1 reachability
```

```
Reachability is Up
```

```
<===== Ensure reachability is up for the monitored interf
```

```
2 changes, last change 09:45:00
```

```
Latest operation return code: OK
```

```
Latest RTT (milliseconds) 1
```

```
Tracked by:
```

```
STATIC-IP-ROUTING 0
```

```
>
```

```
show route
```

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
```

```
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
```

```
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
```

```
E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
```

```
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
```

```
ia - IS-IS inter area, * - candidate default, U - per-user static route
```

```
o - ODR, P - periodic downloaded static route, + - replicated route
```

```
SI - Static InterVRF, BI - BGP InterVRF
```

```
Gateway of last resort is 10.6.3.1 to network 0.0.0.0
```

```
S* 0.0.0.0 0.0.0.0 [1/0] via 10.6.3.1, outside-2
```

```
[1/0] via 10.6.2.1, outside-1
```

```
C 10.6.2.0 255.255.255.0 is directly connected, outside-1
```

```
L 10.6.2.4 255.255.255.255 is directly connected, outside-1
```

```
C 10.6.3.0 255.255.255.0 is directly connected, outside-2
```

```
L 10.6.3.4 255.255.255.255 is directly connected, outside-2
```

関連情報

- [シスコのテクニカルサポートとダウンロード](#)

- [Cisco Defense Orchestratorのクラウド配信ファイアウォール管理センターを使用したファイアウォール脅威対策の管理](#)

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。