

FMCによって管理されるFTD上のIP SLAを使用したECMP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](#)

[ネットワーク図](#)

[コンフィギュレーション](#)

[ステップ 0: インターフェイスおよびネットワークオブジェクトの事前設定](#)

[ステップ 1: ECMPゾーンの設定](#)

[ステップ 2: IP SLAオブジェクトの設定](#)

[ステップ 3: ルートトラックを使用したスタティックルートの設定](#)

[確認](#)

[ロード バランシング](#)

[失われたルート](#)

[トラブルシューティング](#)

はじめに

このドキュメントでは、FMCによって管理されるFTDでECMPとIP SLAを設定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 Threat Defense(FTD)のECMP設定
- Cisco Secure Firewall Threat Defense(FTD)のIP SLA設定
- Cisco Secure Firewall Management Center(FMC)

使用するコンポーネント

このドキュメントの情報は、こ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。

- Cisco FTDバージョン7.4.1

- Cisco FMCバージョン7.4.1

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。

背景説明

このドキュメントでは、Cisco FMCによって管理されるCisco FTDでEqual-Cost Multi-Path(ECMP)をインターネットプロトコルのサービスレベル契約(IP SLA)とともに設定する方法について説明します。ECMPを使用すると、FTDでインターフェイスをグループ化し、複数のインターフェイス間でトラフィックのロードバランシングを行うことができます。IP SLAは、通常のパケットの交換を通じてエンドツーエンドの接続を監視するメカニズムです。ECMPとともに、IP SLAを実装して、ネクストホップの可用性を確保できます。この例では、ECMPを使用して、2つのインターネットサービスプロバイダー(ISP)回線に均等にパケットを配信します。同時に、IP SLAは接続を追跡し、障害発生時に利用可能な任意の回線へのシームレスな移行を保証します。

このドキュメントに関する特定の要件は次のとおりです。

- 管理者権限を持つユーザアカウントでデバイスにアクセスする
- Cisco Secure Firewall Threat Defenseバージョン7.1以降
- Cisco Secure Firewall Management Centerバージョン7.1以降

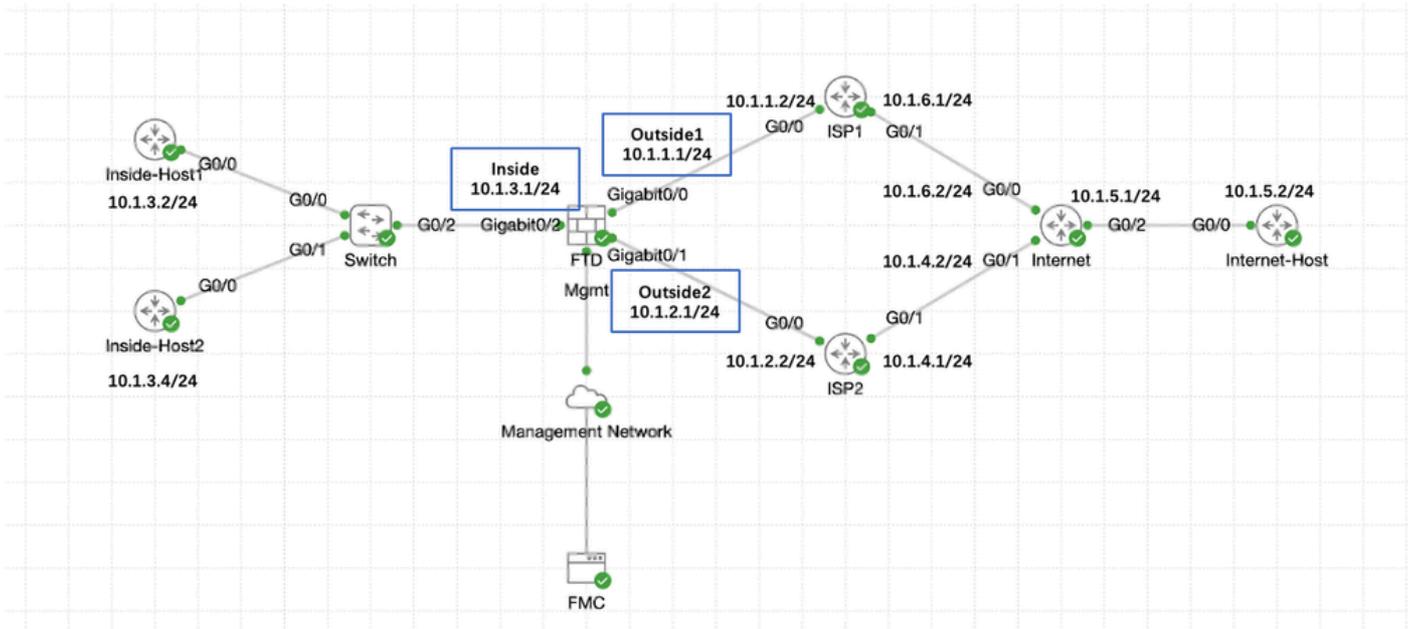
設定

ネットワーク図

この例では、Cisco FTDに2つの外部インターフェイス(outside1およびoutside2)があります。それぞれがISPゲートウェイに接続し、outside1とoutside2はoutsideという名前の同じECMPゾーンに属しています。

内部ネットワークからのトラフィックはFTD経由でルーティングされ、2つのISP経由でインターネットにロードバランシングされます。

同時に、FTDはIP SLAを使用して各ISPゲートウェイへの接続を監視します。いずれかのISP回線で障害が発生した場合、FTDは他のISPゲートウェイにフェールオーバーして、ビジネスの継続性を維持します。



ネットワーク図

コンフィギュレーション

ステップ 0 : インターフェイスおよびネットワークオブジェクトの事前設定

FMCのWeb GUIにログインして、Devices > Device Managementの順に選択し、Editボタンをクリックして脅威対策デバイスを編集します。デフォルトでは、インターフェイスページが選択されています。編集するインターフェイス(この例ではGigabitEthernet0/0)のEditボタンをクリックします。

The screenshot shows the Cisco Firepower Management Center (FMC) Web GUI. The breadcrumb navigation is "Devices > Device Management". The current page is "Interfaces" for the device "10.106.32.250". The "All Interfaces" tab is selected, showing a table of interfaces. The "GigabitEthernet0/0" interface is highlighted with a red box, and its "Edit" button (pencil icon) is also highlighted with a red box.

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address	Path Monitoring	Virtual Router	
Management0/0	management	Physical				Disabled	Global	🔍 ↶
GigabitEthernet0/0		Physical				Disabled		✎
GigabitEthernet0/1		Physical				Disabled		✎
GigabitEthernet0/2		Physical				Disabled		✎
GigabitEthernet0/3		Physical				Disabled		✎
GigabitEthernet0/4		Physical				Disabled		✎
GigabitEthernet0/5		Physical				Disabled		✎
GigabitEthernet0/6		Physical				Disabled		✎
GigabitEthernet0/7		Physical				Disabled		✎

Displaying 1-9 of 9 interfaces | Page 1 of 1

インターフェイスGi0/0の編集

Edit Physical InterfaceウィンドウのGeneralタブで、次の操作を行います。

1. Nameを設定します。この例では、Outside1です。
2. Enabledチェックボックスにチェックマークを入れて、インターフェイスを有効にします。
3. Security Zoneドロップダウンリストで、既存のセキュリティゾーンを選択するか、新しいセキュリティゾーンを作成します(この例ではOutside1_Zone)。

Edit Physical Interface ?

General IPv4 IPv6 Path Monitoring Hardware Configuration Manager Access Advanced

Name:
Outside1

Enabled
 Management Only

Description:

Mode:
None

Security Zone:
Outside1_Zone

Interface ID:
GigabitEthernet0/0

MTU:
1500
(64 - 9000)

Priority:
0 (0 - 65535)

Propagate Security Group Tag:

NVE Only:

インターフェイスGi0/0全般

IPv4タブで、次の手順を実行します。

1. IP Typeドロップダウンリストからオプションを1つ選択します。この例では、Use Static IPです。
2. IPアドレス(この例では10.1.1.1/24)を設定します。
3. [OK] をクリックします。

Edit Physical Interface



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

IP Type:
Use Static IP

IP Address:
10.1.1.1/24
eg. 192.0.2.1/255.255.255.128 or 192.0.2.1/25

Cancel OK

インターフェイスGi0/0 IPv4

同様の手順を繰り返して、GigabitEthernet0/1インターフェイスの設定を行います。Edit Physical InterfaceウィンドウのGeneralタブの下に次のように入力します。

1. Nameを設定します。この例では、Outside2です。
2. Enabledチェックボックスにチェックマークを入れて、インターフェイスを有効にします。
3. Security Zoneドロップダウンリストで、既存のセキュリティゾーンを選択するか、新しいセキュリティゾーンを作成します(この例ではOutside2_Zone)。

Edit Physical Interface



General IPv4 IPv6 Path Monitoring Hardware Configuration Manager Access Advanced

Name:
Outside2

Enabled
 Management Only

Description:

Mode:
None

Security Zone:
Outside2_Zone

Interface ID:
GigabitEthernet0/1

MTU:
1500
(64 - 9000)

Priority:
0 (0 - 65535)

Propagate Security Group Tag:

NVE Only:

Cancel OK

インターフェイスGi0/1汎用

IPv4タブで、次の手順を実行します。

1. IP Typeドロップダウンリストからオプションを1つ選択します。この例では、Use Static IPです。
2. IPアドレス(この例では10.1.2.1/24)を設定します。
3. [OK] をクリックします。

Edit Physical Interface

General IPv4 IPv6 Path Monitoring Hardware Configuration Manager Access Advanced

IP Type:
Use Static IP

IP Address:
10.1.2.1/24

eg. 192.0.2.1/24, 2001:200:200:200::1/64, 192.0.2.1/24

Cancel OK

インターフェイスGi0/1 IPv4

同様の手順を繰り返して、GigabitEthernet0/2インターフェイスを設定します。Edit Physical InterfaceウィンドウのGeneralタブで、次のように設定します。

1. Nameを設定します。この例ではInsideです。
2. Enabledチェックボックスにチェックマークを入れて、インターフェイスを有効にします。
3. Security Zoneドロップダウンリストで、既存のセキュリティゾーンを選択するか、新しいセキュリティゾーンを作成します(この例ではInside_Zone)。

Edit Physical Interface



General IPv4 IPv6 Path Monitoring Hardware Configuration Manager Access Advanced

Name:
Inside

Enabled
 Management Only

Description:

Mode:
None

Security Zone:
Inside_Zone

Interface ID:
GigabitEthernet0/2

MTU:
1500
(64 - 9000)

Priority:
0 (0 - 65535)

Propagate Security Group Tag:

NVE Only:

Cancel OK

インターフェイスGi0/2汎用

IPv4タブで、次の手順を実行します。

1. IP Typeドロップダウンリストからオプションを1つ選択します。この例では、Use Static IPです。
2. IPアドレス(この例では10.1.3.1/24)を設定します。
3. [OK] をクリックします。

Edit Physical Interface

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

IP Type:
Use Static IP

IP Address:
10.1.3.1/24

Cancel OK

インターフェイスGi0/2 IPv4

Saveをクリックし、設定をDeployします。

Objects > Object Managementに移動し、オブジェクトタイプのリストからNetworkを選択し、Add NetworkドロップダウンメニューからAdd Objectを選択して、最初のISPゲートウェイ用のオブジェクトを作成します。

Firewall Management Center
Objects / Object Management

Overview Analysis Policies Devices **Objects** Integration

Deploy Filter admin **SECURE**

Network

A network object represents one or more IP addresses. Network objects are used in various places, including access control policies, network variables, intrusion rules, identity rules, network event searches, reports, and so on.

Add Network
Add Object
Import Object
Add Group

Name	Value	Type	Override
any	0.0.0.0/0 ::0	Group	
any-ipv4	0.0.0.0/0	Network	
any-ipv6	::0	Host	
IPv4-Benchmark-Tests	198.18.0.0/15	Network	
IPv4-Link-Local	169.254.0.0/16	Network	
IPv4-Multicast	224.0.0.0/4	Network	
IPv4-Private-10.0.0.0-8	10.0.0.0/8	Network	
IPv4-Private-172.16.0.0-12	172.16.0.0/12	Network	
IPv4-Private-192.168.0.0-16	192.168.0.0/16	Network	
IPv4-Private-All-RFC1918	10.0.0.0/8 172.16.0.0/12 192.168.0.0/16	Group	
IPv6-IPv4-Mapped	:::ffff:0.0.0.0/96	Network	
IPv6-Link-Local	fe80::/10	Network	
IPv6-Private-Unique-Local-Addresses	fc00::/7	Network	
IPv6-to-IPv4-Relay-Anycast	192.68.99.0/24	Network	

Displaying 1 - 14 of 14 rows Page 1 of 1

ネットワークオブジェクト

New Network Objectウィンドウで、次の操作を行います。

1. Nameを設定します(この例ではgw-outside1)。
2. Networkフィールドで必要なオプションを選択し、適切な値(この例ではHost、10.1.1.2)を入力します。

3. [Save] をクリックします。

New Network Object

Name

gw-outside1

Description

Network

Host Range Network FQDN

10.1.1.2

Allow Overrides

Cancel Save

オブジェクトGw-outside1

同様の手順を繰り返して、2番目のISPゲートウェイ用に別のオブジェクトを作成します。New Network Objectウィンドウで、次の操作を行います。

1. Nameを設定します(この例ではgw-outside2)。
2. Networkフィールドで必要なオプションを選択し、適切な値(この例ではHost、10.1.2.2)を入力します。
3. [Save] をクリックします。

New Network Object



Name

gw-outside2

Description

Network

Host

Range

Network

FQDN

10.1.2.2

Allow Overrides

Cancel

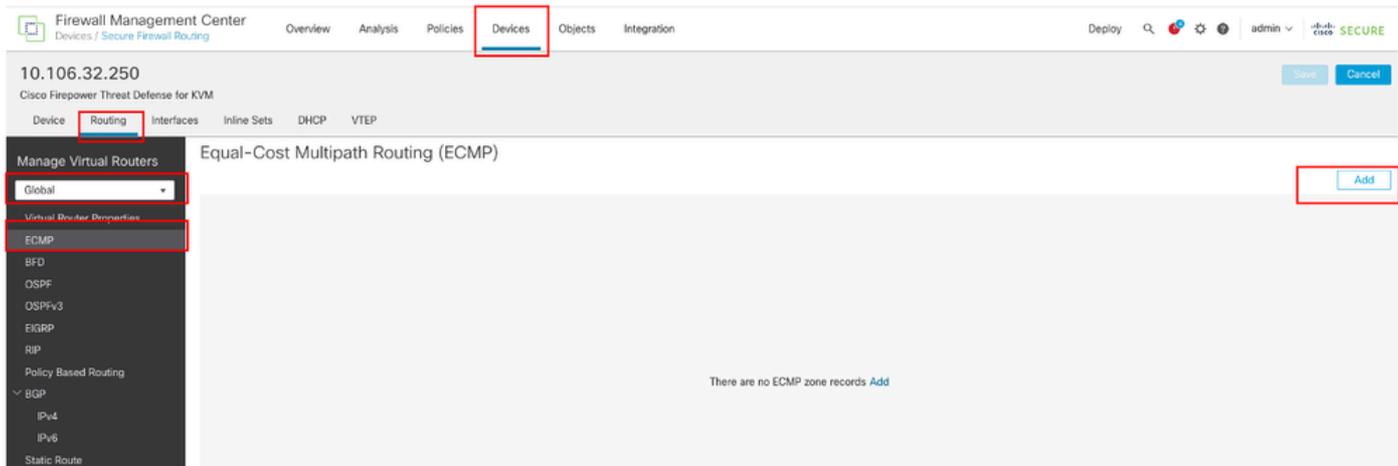
Save

オブジェクトGw-outside2

ステップ 1 : ECMPゾーンの設定

Devices > Device Management に移動し、脅威対策デバイスを編集し、Routingをクリックします。virtual routerドロップダウンから、ECMPゾーンを作成する仮想ルータを選択します。ECMPゾーンは、グローバル仮想ルータとユーザ定義仮想ルータに作成できます。この例では、Globalを選択します。

ECMPをクリックし、次にAddをクリックします。



ECMPゾーンの設定

Add ECMPウィンドウで、次の手順を実行します。

1. ECMPゾーンのNameを設定します。この例ではOutsideです。
2. インターフェイスを関連付けるには、Available Interfacesボックスの下にあるインターフェイスを選択し、Addをクリックします。この例では、Outside1とOutside2です。
3. [OK] をクリックします。

Add ECMP



Name
Outside

Available Interfaces
Inside

Selected Interfaces
Outside1
Outside2

Add

Cancel OK

外部のECMPゾーンの設定

Saveをクリックし、設定をDeployします。

ステップ 2 : IP SLAオブジェクトの設定

Objects > Object Managementに移動し、オブジェクトタイプのリストからSLA Monitorを選択し、Add SLA Monitorをクリックして最初のISPゲートウェイの新しいSLAモニタを追加します。

Firewall Management Center
Objects / Object Management

Overview Analysis Policies Devices **Objects** Integration

Deploy 🔍 ⚙️ 👤 admin 🔒 SECURE

SLA Monitor

Add SLA Monitor 🔍 Filter

SLA monitor defines a connectivity policy to a monitored address and tracks the availability of a route to the address. The SLA Monitor object is used in the Route Tracking field of an IPv4 Static Route Policy. IPv6 routes do not have the option to use SLA monitor via route tracking.

Name	Value
No records to display	

AAA Server
Access List
Address Pools
Application Filters
AS Path
BFD Template
Cipher Suite List
Community List
DHCP IPv6 Pool
Distinguished Name
DNS Server Group
External Attributes
File List
FlexConfig
Geolocation
Interface
Key Chain
Network
PKI
Policy List
Port
Prefix List
Route Map
Security Intelligence
Sinkhole
SLA Monitor
Time Range

SLAモニタの作成

New SLA Monitor Objectウィンドウで、次の操作を行います。

1. SLAモニタオブジェクトの名前を設定します。この例では、sla-outside1です。
2. SLA動作のID番号をSLAモニタIDフィールドに入力します。値の範囲は1 ~ 2147483647です。1つのデバイスに最大2000のSLA動作を作成できます。各ID番号は、ポリシーとデバイス設定に固有である必要があります。この例では、1です。
3. SLA動作によってアベイラビリティをモニタするIPアドレスを、Monitored Addressフィールドに入力します。この例では、10.1.1.2です。
4. Available Zones/Interfacesリストには、ゾーンとインターフェイスグループの両方が表示されます。[ゾーン/インターフェイス]リストで、デバイスが管理ステーションと通信するために使用するインターフェイスを含むゾーンまたはインターフェイスグループを追加します。単一のインターフェイスを指定するには、そのインターフェイス用のゾーンまたはインターフェイスグループを作成する必要があります。この例では、Outside1_Zoneです。
5. [Save] をクリックします。

New SLA Monitor Object



Name:

sla-outside1

Description:

Frequency (seconds):

60

{1-604800}

SLA Monitor ID*:

1

Threshold (milliseconds):

{0-60000}

Timeout (milliseconds):

5000

{0-604800000}

Data Size (bytes):

28

{0-16384}

ToS:

Number of Packets:

1

Monitor Address*:

10.1.1.2

Available Zones/interfaces



Search

Inside_Zone

Outside1_Zone

Outside2_Zone

Add

Selected Zones/interfaces

Outside1_Zone



Cancel

Save

SLAオブジェクトSla-outside1

同様の手順を繰り返して、2番目のISPゲートウェイに別のSLAモニタを作成します。

New SLA Monitor Objectウィンドウで、次の操作を行います。

1. SLAモニタオブジェクトの名前を設定します。この例では、sla-outside2です。
2. SLA動作のID番号をSLAモニタIDフィールドに入力します。値の範囲は1 ~ 2147483647です。1つのデバイスに最大2000のSLA動作を作成できます。各ID番号は、ポリシーとデバイス設定に固有である必要があります。この例では、2です。
3. SLA動作によってアベイラビリティをモニタするIPアドレスを、Monitored Addressフィールドに入力します。この例では10.1.2.2です。
4. Available Zones/Interfacesリストには、ゾーンとインターフェイスグループの両方が表示されます。[ゾーン/インターフェイス]リストで、デバイスが管理ステーションと通信するために使用するインターフェイスを含むゾーンまたはインターフェイスグループを追加します。単一のインターフェイスを指定するには、そのインターフェイス用のゾーンまたはインターフェイスグループを作成する必要があります。この例ではOutside2_Zoneです。
5. [Save] をクリックします。

New SLA Monitor Object



Name:

sla-outside2

Description:

Frequency (seconds):

60

{1-604800}

SLA Monitor ID*:

2

Threshold (milliseconds):

{0-60000}

Timeout (milliseconds):

5000

{0-604800000}

Data Size (bytes):

20

{0-16384}

ToS:

Number of Packets:

1

Monitor Address*:

10.1.2.2

Available Zones/Interfaces

Q Search

Inside_Zone

Outside1_Zone

Outside2_Zone

Add

Selected Zones/Interfaces

Outside1_Zone

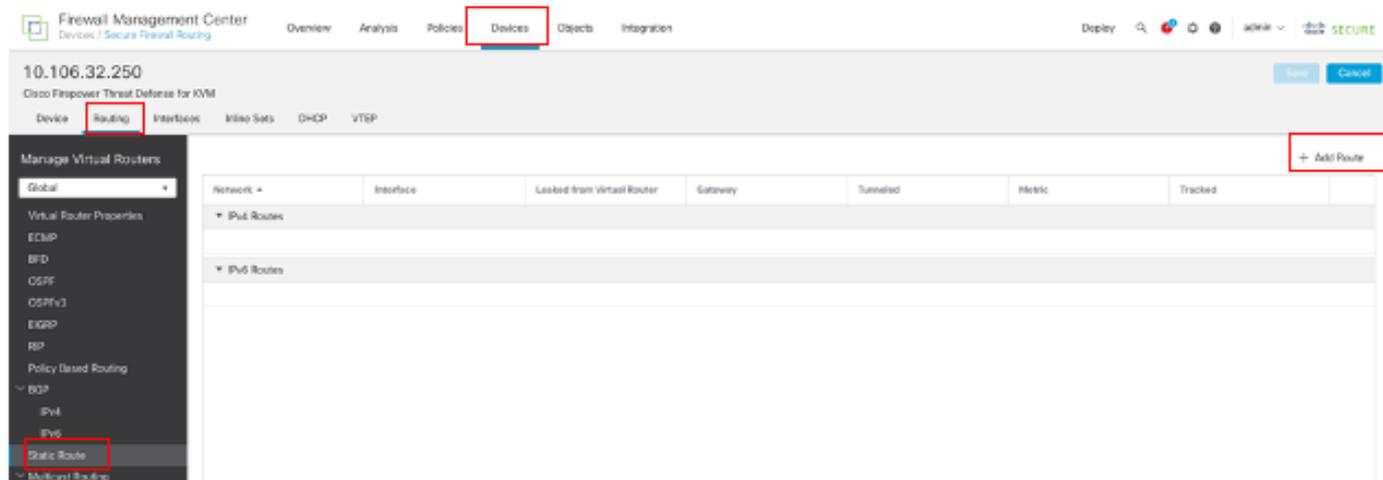
Cancel

Save

ステップ 3 : ルートトラックを使用したスタティックルートの設定

Devices > Device Managementの順に移動し、脅威対策デバイスを編集して、Routingをクリックします。virtual routers ドロップダウンリストから、スタティックルートを設定する仮想ルータを選択します。この例ではGlobalです。

Static Routeを選択し、Add Routeをクリックして、最初のISPゲートウェイにデフォルトルートを追加します。



スタティックルートの設定

Add Static Route Configurationウィンドウで、次の手順を実行します。

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。この例では、IPv4です。
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。この例では、Outside1です。
3. Available Networkリストで、宛先ネットワークを選択します。この例では、any-ipv4です。
4. Gatewayフィールドまたは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。IPアドレスまたはNetworks/Hostsオブジェクトを指定できます。この例では、gw-outside1です。
5. Metricフィールドに、宛先ネットワークへのホップの数を入力します。有効な値の範囲は1 ~ 255です。デフォルト値は1です。この例では、1です。
6. 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SLAモニタオブジェクトの名前をRoute Trackingフィールドで入力または選択します。この例では、sla-outside1です。
7. [OK] をクリックします。

Add Static Route Configuration

Type: IPv4 IPv6

Interface*
Outside1

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

Available Network  + Selected Network

Search

any-ipv4
gw-outside1
gw-outside2
IPv4-Benchmark-Tests
IPv4-Link-Local
IPv4-Multicast

Add

any-ipv4

Gateway*
gw-outside1 +

Metric:
1
(1 = 254)

Tunneled: (Used only for default Routes)

Route Tracking:
sla-outside1 +

Cancel OK

最初のISPにスタティックルートを追加する

同様の手順を繰り返して、2番目のISPゲートウェイにデフォルトルートを追加します。Add Static Route Configurationウィンドウで、次の手順を実行します。

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。この例では、IPv4です。
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。この例では、

Outside2です。

3. Available Networkリストで、宛先ネットワークを選択します。この例では、any-ipv4です。
4. Gatewayフィールドまたは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。IPアドレスまたはNetworks/Hostsオブジェクトを指定できます。この例では、gw-outside2です。
5. Metricフィールドに、宛先ネットワークへのホップの数を入力します。有効な値の範囲は1 ~ 255です。デフォルト値は1です。最初のルート(この例では1)と同じメトリックを必ず指定してください。
6. 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SLAモニタオブジェクトの名前をRoute Trackingフィールドで入力または選択します。この例では、sla-outside2です。
7. [OK] をクリックします。

Add Static Route Configuration



Type: IPv4 IPv6

Interface*

Outside2

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

Available Network



Selected Network

Search

Add

any-ipv4

any-ipv4

gw-outside1

gw-outside2

IPv4-Benchmark-Tests

IPv4-Link-Local

IPv4-Multicast

Gateway*

gw-outside2



Metric:

1

[1 - 254]

Tunneled: (Used only for default Route)

Route Tracking:

sla-outside2



Cancel

OK

2番目のISPへのスタティックルートの追加

Saveをクリックし、設定をDeployします。

確認

FTDのCLIにログインし、`show zone` コマンドを実行して、各ゾーンの一部であるインターフェイスを含む、ECMPトラフィックゾーンに関する情報を確認します。

```
<#root>
```

```
> show zone  
Zone: Outside ecmp  
Security-level: 0
```

```
Zone member(s): 2
```

```
Outside2 GigabitEthernet0/1
```

```
Outside1 GigabitEthernet0/0
```

コマンドshow running-config routeを実行して、ルーティング設定の実行コンフィギュレーションを確認します。この場合、ルートトラックのある2つのスタティックルートがあります。

```
show route
```

```
<#root>
```

```
> show running-config route
```

```
route Outside1 0.0.0.0 0.0.0.0 10.1.1.2 1 track 1
```

```
route Outside2 0.0.0.0 0.0.0.0 10.1.2.2 1 track 2
```

コマンドを実行してルーティングテーブルを確認します。この場合、インターフェイスoutside1とoutside2を通る等コストの2つのデフォルトルートがあり、トラフィックを2つのISP回線間で分散できます。

```
show sla monitor configuration
```

```
<#root>
```

```
> 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 10.1.2.2 to network 0.0.0.0
```

```
S* 0.0.0.0 0.0.0.0 [1/0] via 10.1.2.2, Outside2
```

```
[1/0] via 10.1.1.2, Outside1
```

```
C 10.1.1.0 255.255.255.0 is directly connected, Outside1  
L 10.1.1.1 255.255.255.255 is directly connected, Outside1  
C 10.1.2.0 255.255.255.0 is directly connected, Outside2  
L 10.1.2.1 255.255.255.255 is directly connected, Outside2  
C 10.1.3.0 255.255.255.0 is directly connected, Inside  
L 10.1.3.1 255.255.255.255 is directly connected, Inside
```

コマンドを実行して、SLAモニタの設定を確認します。

```
show sla monitor operational-state
```

```
<#root>
```

```
> show sla monitor configuration
SA Agent, Infrastructure Engine-II
Entry number: 1
Owner:
Tag:
```

```
Type of operation to perform: echo
```

```
Target address: 10.1.1.2
```

```
Interface: Outside1
```

```
Number of packets: 1
Request size (ARR data portion): 28
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Verify data: No
Operation frequency (seconds): 60
Next Scheduled Start Time: Start Time already passed
Group Scheduled : FALSE
Life (seconds): Forever
Entry Ageout (seconds): never
Recurring (Starting Everyday): FALSE
Status of entry (SNMP RowStatus): Active
Enhanced History:
```

```
Entry number: 2
```

Owner:
Tag:

Type of operation to perform: echo

Target address: 10.1.2.2

Interface: Outside2

Number of packets: 1
Request size (ARR data portion): 28
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Verify data: No
Operation frequency (seconds): 60
Next Scheduled Start Time: Start Time already passed
Group Scheduled : FALSE
Life (seconds): Forever
Entry Ageout (seconds): never
Recurring (Starting Everyday): FALSE
Status of entry (SNMP RowStatus): Active
Enhanced History:

コマンドを実行して、SLAモニタの状態を確認します。この場合、コマンド出力に「**Timeout occurred: FALSE**」と表示されていれば、ゲートウェイへのICMPエコーが応答していることを示します。したがって、宛先インターフェイスを経由するデフォルトルートはアクティブであり、ルーティングテーブルにインストールされています。

<#root>

```
> show sla monitor operational-state
Entry number: 1
Modification time: 09:31:28.785 UTC Thu Feb 15 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 82
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
```

Timeout occurred: FALSE

```
Over thresholds occurred: FALSE
Latest RTT (milliseconds): 1
Latest operation start time: 10:52:28.785 UTC Thu Feb 15 2024
Latest operation return code: OK
RTT Values:
RTTAvg: 1 RTTMin: 1 RTTMax: 1
NumOfRTT: 1 RTTSum: 1 RTTSum2: 1
```

```
Entry number: 2
Modification time: 09:31:28.785 UTC Thu Feb 15 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 82
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
```

Timeout occurred: FALSE

```
Over thresholds occurred: FALSE
Latest RTT (milliseconds): 1
Latest operation start time: 10:52:28.785 UTC Thu Feb 15 2024
Latest operation return code: OK
RTT Values:
RTTAvg: 1 RTTMin: 1 RTTMax: 1
NumOfRTT: 1 RTTSum: 1 RTTSum2: 1
```

ロード バランシング

FTDを介した最初のトラフィックにより、ECMPゾーンのゲートウェイ間でECMPロードバランシングがトラフィックを処理するかどうかを確認します。この場合、Inside-Host1(10.1.3.2)とInside-Host2(10.1.3.4)からInternet-Host(10.1.5.2)に向けてTelnet接続を開始し、コマンド `show conn` を実行して、トラフィックが2つのISPリンク間でロードバランスされていることを確認します。Inside-Host1(10.1.3.2)はインターフェイスoutside1を通過し、Inside-Host2(10.1.3.4)はインターフェイスoutside2を通過します。

```
> show conn
```

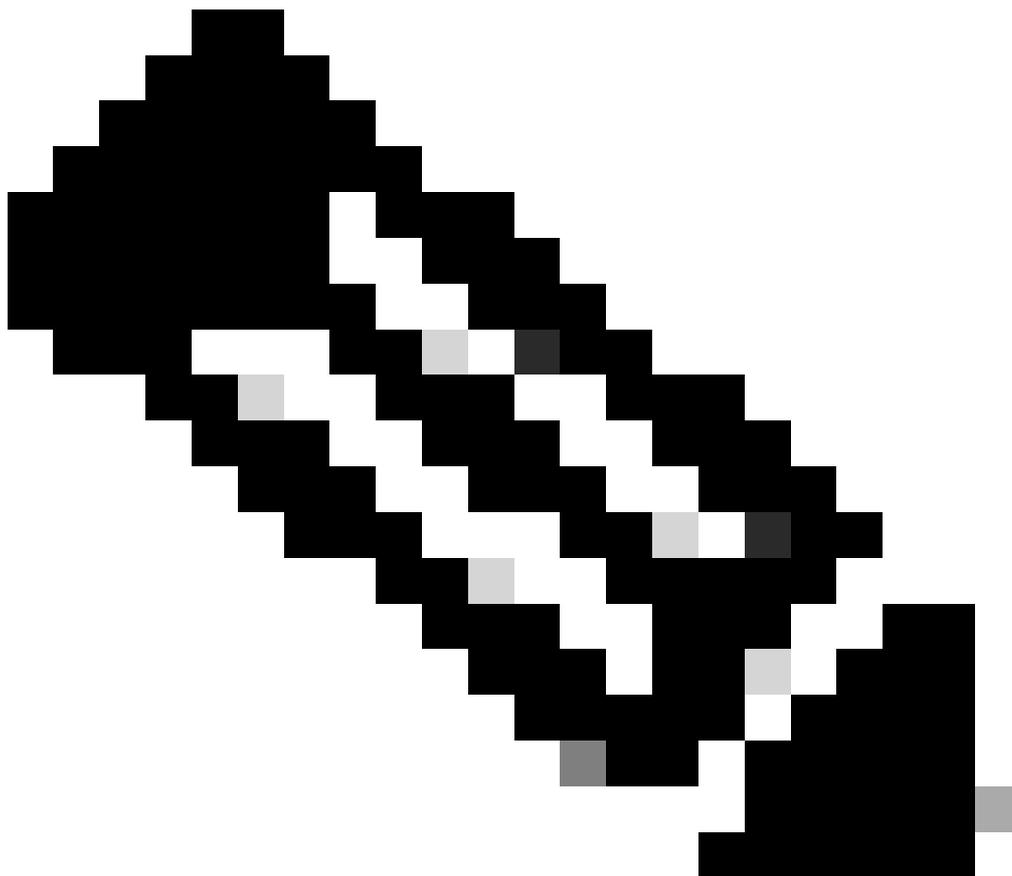
```
2 in use, 3 most used
```

```
Inspect Snort:
```

```
preserve-connection: 2 enabled, 0 in effect, 2 most enabled, 0 most in effect
```

```
TCP Inside 10.1.3.2:46069 Outside1 10.1.5.2:23, idle 0:00:24, bytes 1329, flags UIO N1
```

```
TCP Inside 10.1.3.4:61915 Outside2 10.1.5.2:23, idle 0:00:04, bytes 1329, flags UIO N1
```



注：トラフィックは、送信元と宛先のIPアドレス、着信インターフェイス、プロトコル、送信元と宛先ポートをハッシュするアルゴリズムに基づいて、指定されたゲートウェイ間でロードバランシングされます。テストを実行すると、シミュレートするトラフィックは、ハッシュアルゴリズムのために同じゲートウェイにルーティングできます。これは予想され、ハッシュ結果を変更するために6つのタプル（送信元IP、宛先IP、着信インターフェイス、プロトコル、送信元ポート、宛先ポート）間での値を変更します。

失われたルート

最初のISPゲートウェイへのリンクがダウンしている場合は、シミュレートする最初のゲートウェイルータをシャットダウンします。FTDがSLAモニタオブジェクトで指定されたしきい値タイマー内に最初のISPゲートウェイからエコー応答を受信しない場合、ホストは到達不能と見なされ、ダウンとしてマークされます。最初のゲートウェイへのトラッキング対象ルートもルーティングテーブルから削除されます。

```
show sla monitor operational-state
```

コマンドを実行して、SLAモニタの現在の状態を確認します。この場合、コマンド出力に「Timeout occurred: True」と表示されていれば、最初のISPゲートウェイへのICMPエコーが応答していないことを示しています。

```
show route
```

```
<#root>
```

```
> show sla monitor operational-state
Entry number: 1
Modification time: 09:31:28.783 UTC Thu Feb 15 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 104
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
```

```
Timeout occurred: TRUE
```

```
Over thresholds occurred: FALSE
Latest RTT (milliseconds): NoConnection/Busy/Timeout
Latest operation start time: 11:14:28.813 UTC Thu Feb 15 2024
Latest operation return code: Timeout
RTT Values:
RTTAvg: 0 RTTMin: 0 RTTMax: 0
NumOfRTT: 0 RTTSum: 0 RTTSum2: 0
```

Entry number: 2
Modification time: 09:31:28.783 UTC Thu Feb 15 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 104
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE

Timeout occurred: FALSE

Over thresholds occurred: FALSE
Latest RTT (milliseconds): 1
Latest operation start time: 11:14:28.813 UTC Thu Feb 15 2024
Latest operation return code: OK
RTT Values:
RTTAvg: 1 RTTMin: 1 RTTMax: 1
NumOfRTT: 1 RTTSum: 1 RTTSum2: 1

コマンドを実行して現在のルーティングテーブルをチェックします。インターフェイスoutside1を経由した最初のISPゲートウェイへのルートが削除され、インターフェイスoutside2を経由した2番目のISPゲートウェイへのアクティブなデフォルトルートが1つしかありません。

show conn

<#root>

> 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 10.1.2.2 to network 0.0.0.0

S* 0.0.0.0 0.0.0.0 [1/0] via 10.1.2.2, Outside2

```
C 10.1.1.0 255.255.255.0 is directly connected, Outside1
L 10.1.1.1 255.255.255.255 is directly connected, Outside1
C 10.1.2.0 255.255.255.0 is directly connected, Outside2
L 10.1.2.1 255.255.255.255 is directly connected, Outside2
C 10.1.3.0 255.255.255.0 is directly connected, Inside
L 10.1.3.1 255.255.255.255 is directly connected, Inside
```

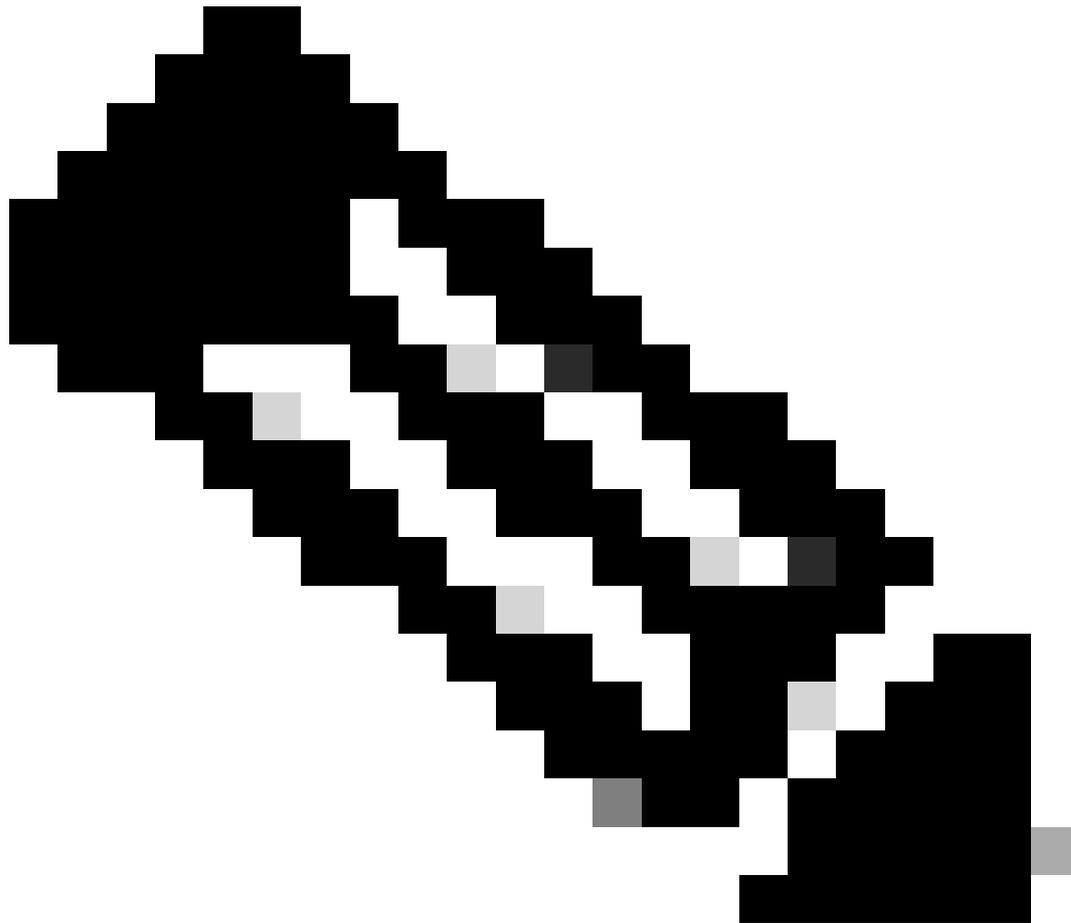
コマンドを実行すると、2つの接続がまだ確立されていることがわかります。Inside-Host1(10.1.3.2)とInside-Host2(10.1.3.4)でも、中断することなくtelnetセッションがアクティブになります。

```
<#root>
```

```
> show conn
2 in use, 3 most used
Inspect Snort:
preserve-connection: 2 enabled, 0 in effect, 2 most enabled, 0 most in effect
```

```
TCP Inside 10.1.3.2:46069 Outside1 10.1.5.2:23, idle 0:00:22, bytes 1329, flags UIO N1
```

```
TCP Inside 10.1.3.4:61915 Outside2 10.1.5.2:23, idle 0:00:02, bytes 1329, flags UIO N1
```



注：show connの出力で、Inside-Host1(10.1.3.2)からのtelnetセッションはインターフェイスoutside1を経由していますが、インターフェイスoutside1を経由するデフォルトルートはルーティングテーブルから削除されています。これは予期された動作であり、設計上、実際のトラフィックはインターフェイスoutside2を経由します。Inside-Host1(10.1.3.2)からInternet-Host(10.1.5.2)への新しい接続を開始すると、すべてのトラフィックがインターフェイスoutside2を通過していることがわかります。

ルーティングテーブルの変更を検証するには、debug ip routingコマンドを実行します。

この例では、最初のISPゲートウェイへのリンクがダウンすると、インターフェイスoutside1を経由するルートがルーティングテーブルから削除されます。

```
show route
```

```
<#root>
```

```
> debug ip routing  
IP routing debugging is on
```

```
RT: ip_route_delete 0.0.0.0 0.0.0.0 via 10.1.1.2, Outside1
```

```
ha_cluster_synced 0 routetype 0
```

```
RT: del 0.0.0.0 via 10.1.1.2, static metric [1/0]NP-route: Delete-Output 0.0.0.0/0 hop_count:1 , via 0.0.0.0
```

```
RT(mgmt-only): NP-route: Update-Output 0.0.0.0/0 hop_count:1 , via 10.1.2.2, Outside2
```

```
NP-route: Update-Input 0.0.0.0/0 hop_count:1 Distance:1 Flags:0X0 , via 10.1.2.2, Outside2
```

コマンドを実行して、現在のルーティングテーブルを確認します。

```
<#root>
```

```
> 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 10.1.2.2 to network 0.0.0.0
```

```
S* 0.0.0.0 0.0.0.0 [1/0] via 10.1.2.2, Outside2
```

```
C 10.1.1.0 255.255.255.0 is directly connected, Outside1  
L 10.1.1.1 255.255.255.255 is directly connected, Outside1  
C 10.1.2.0 255.255.255.0 is directly connected, Outside2  
L 10.1.2.1 255.255.255.255 is directly connected, Outside2  
C 10.1.3.0 255.255.255.0 is directly connected, Inside  
L 10.1.3.1 255.255.255.255 is directly connected, Inside
```

最初のISPゲートウェイへのリンクが再びアップすると、インターフェイスoutside1を経由するルートがルーティングテーブルに追加されます。

```
show route
```

```
<#root>
```

```
> debug ip routing  
IP routing debugging is on
```

```
NP-route: Update-Output 0.0.0.0/0 hop_count:1 , via 10.1.2.2, Outside2
```

```
NP-route: Update-Output 0.0.0.0/0 hop_count:1 , via 10.1.1.2, Outside2
```

NP-route: Update-Input 0.0.0.0/0 hop_count:2 Distance:1 Flags:0X0 , via 10.1.2.2, Outside2

via 10.1.1.2, Outside1

コマンドを実行して、現在のルーティングテーブルを確認します。

<#root>

> 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 10.1.2.2 to network 0.0.0.0

S* 0.0.0.0 0.0.0.0 [1/0] via 10.1.2.2, Outside2

[1/0] via 10.1.1.2, Outside1

C 10.1.1.0 255.255.255.0 is directly connected, Outside1
L 10.1.1.1 255.255.255.255 is directly connected, Outside1
C 10.1.2.0 255.255.255.0 is directly connected, Outside2
L 10.1.2.1 255.255.255.255 is directly connected, Outside2
C 10.1.3.0 255.255.255.0 is directly connected, Inside
L 10.1.3.1 255.255.255.255 is directly connected, Inside

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。