

FDMによって管理されるFTD上のIP SLAを使用したECMPの構成

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/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](#)

[関連情報](#)

はじめに

このドキュメントでは、FDMによって管理されるFTDでIP SLAとともにECMP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 Device Manager(FDM)

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 (ビルド172)

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 FDMによって管理されるCisco FTDでEqual-Cost Multi-Path(ECMP)をInternet Protocol Service Level Agreement(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

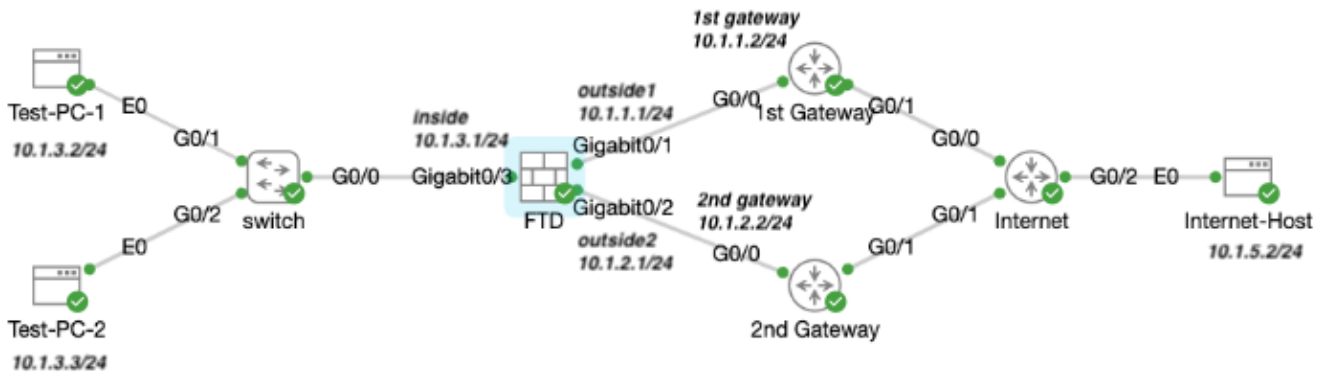
設定

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(外部インターフェイス)と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。

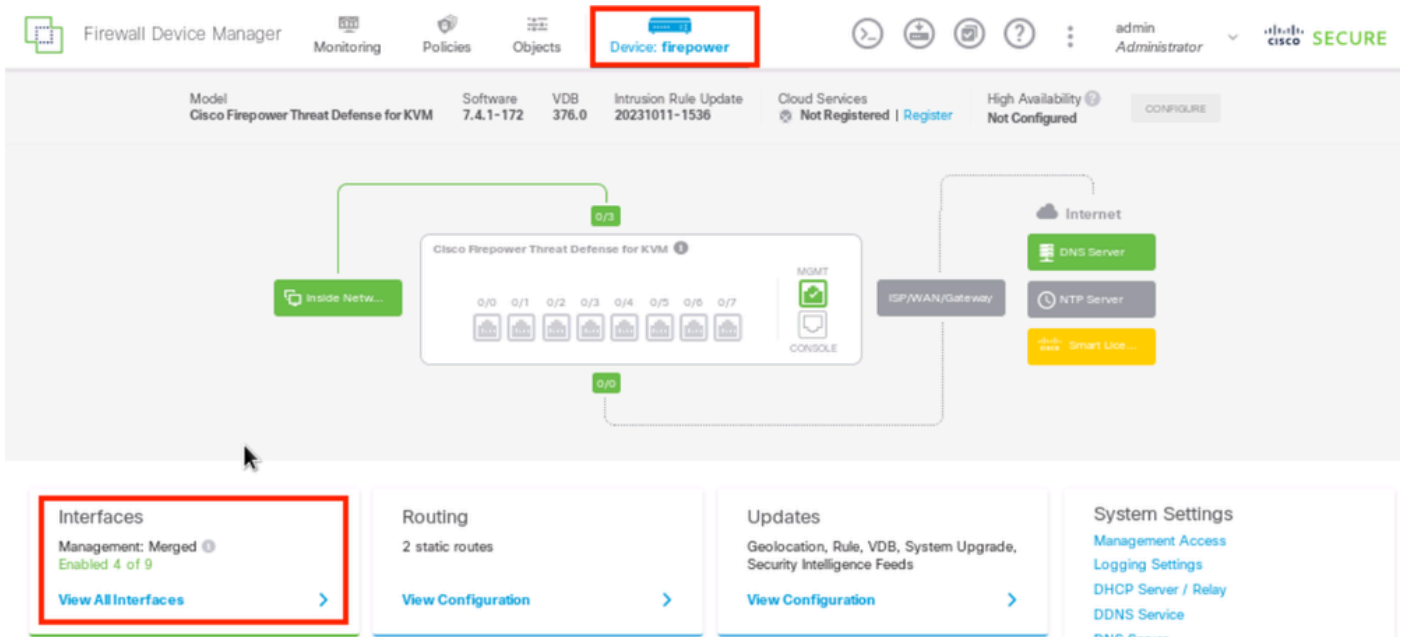


ネットワーク図

コンフィギュレーション

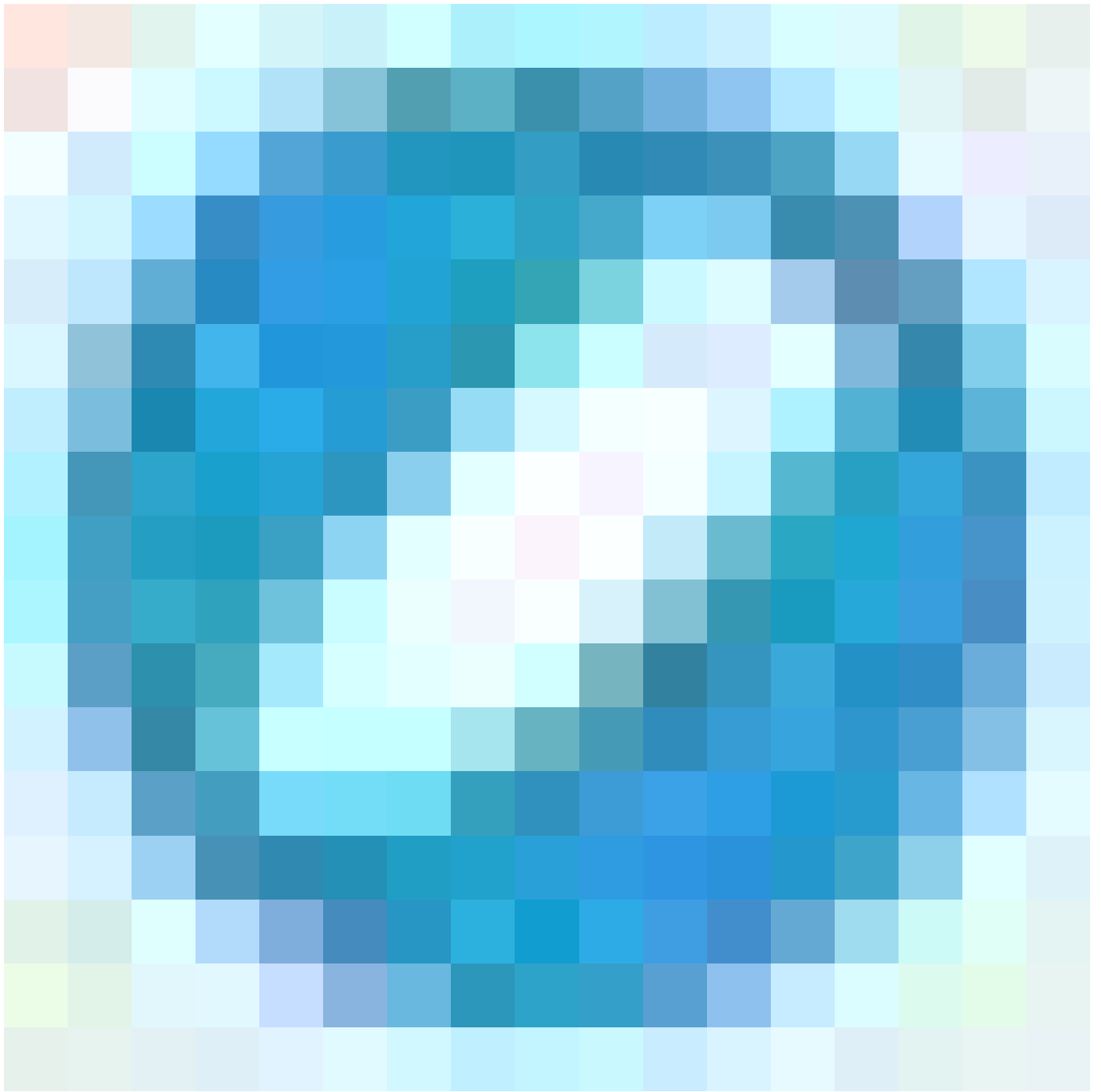
ステップ 0 : インターフェイス/オブジェクトの事前設定

FDM Web GUIにログインし、Deviceをクリックし、次にInterfaces (インターフェイス) の要約のリンクをクリックします。Interfaces リストには、使用可能なインターフェイス、その名前、アドレス、および状態が表示されます。



FDMデバイス・ インタフェース

編集する物理インターフェイスの編集アイコン(



)をクリックします。この例では、GigabitEthernet0/1です。

Device Summary
Interfaces


Cisco Firepower Threat Defense for KVM

0/0 0/1 0/2 0/3 0/4 0/5 0/6 0/7

MGMT
CONSOLE

Interfaces Virtual Tunnel Interfaces

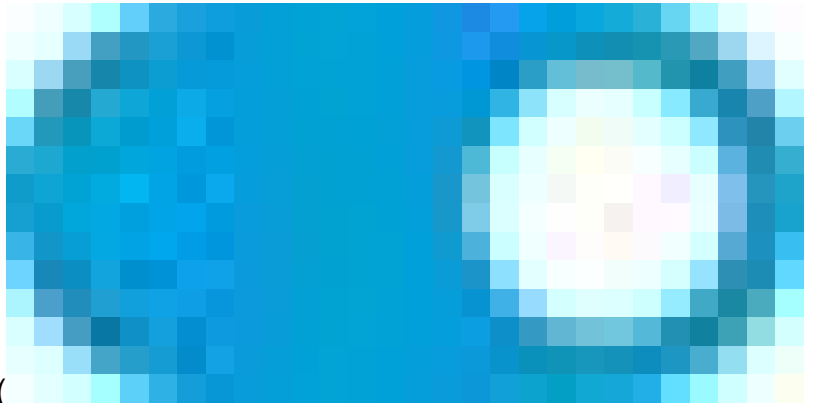
9 Interfaces

NAME	LOGICAL NAME	STATUS	MODE	IP ADDRESS	STANDBY ADDRESS	MONITOR FOR HA	ACTIONS
> GigabitEthernet0/0	outside	<input type="checkbox"/>	Routed			Enabled	
> GigabitEthernet0/1	outside 1	<input checked="" type="checkbox"/>	Routed	10.1.1.1		Enabled	

ステップ0インターフェイスGi0/1

Edit Physical Interface ウィンドウで、次の操作を行います。

1. Interface Name を設定します。この例では、outside1 です。



2. Statusスライダを有効に設定します()。
3. IPv4 Addressタブをクリックして、IPv4アドレスを設定します。この例では、10.1.1.1/24です。
4. [OK] をクリックします。

GigabitEthernet0/1 Edit Physical Interface



Interface Name

outside1

Mode

Routed

Status



Most features work with named interfaces only, although some require unnamed interfaces.

Description

IPv4 Address

IPv6 Address

Advanced

Type

Static

IP Address and Subnet Mask

10.1.1.1

/

255.255.255.0

e.g. 192.168.5.15/17 or 192.168.5.15/255.255.128.0

Standby IP Address and Subnet Mask

/

e.g. 192.168.5.16

CANCEL

OK

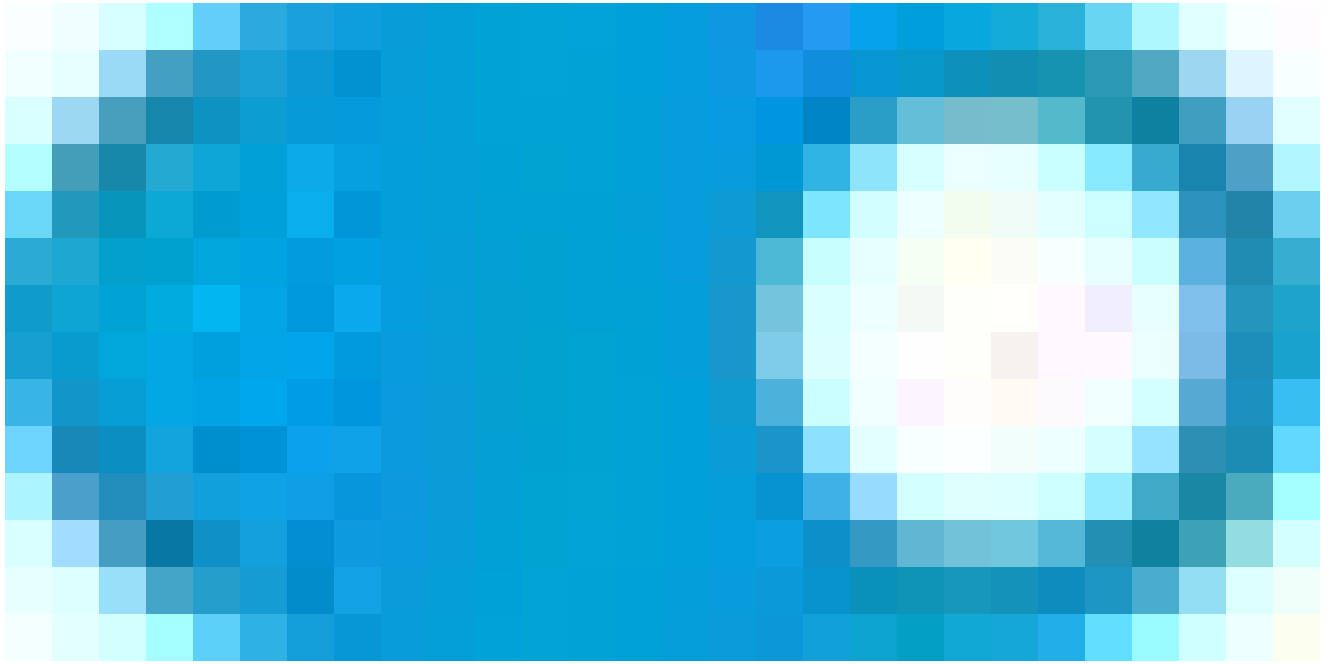
ステップ0インターフェイスGi0/1の編集



注:ECMPゾーンに関連付けることができるのは、ルーテッドインターフェイスだけです。

同様の手順を繰り返して、セカンダリISP接続のインターフェイスを設定します。この例では、物理インターフェイスはGigabitEthernet0/2です。Edit Physical Interface ウィンドウで、次の操作を行います。

1. Interface Name(この例ではoutside2)を設定します。
2. Status スライダーを有効な設定(



)に設定します。

3. IPv4 Addressタブをクリックして、IPv4アドレス(この例では10.1.2.1/24)を設定します。
4. [OK] をクリックします。

GigabitEthernet0/2 Edit Physical Interface

Interface Name:

Mode:

Status:

Most features work with named interfaces only, although some require unnamed interfaces.

Description:

IPv4 Address | IPv6 Address | Advanced

Type:

IP Address and Subnet Mask: /

e.g. 192.168.5.15/17 or 192.168.5.15/255.255.128.0

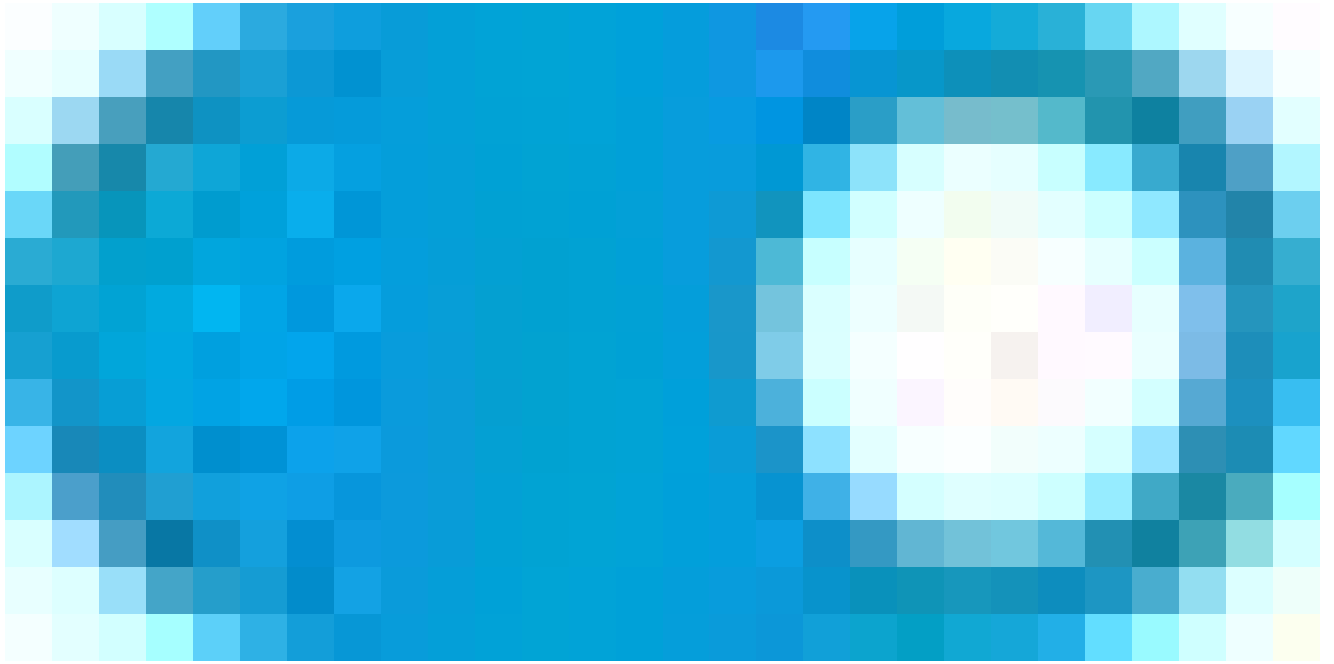
Standby IP Address and Subnet Mask: /

e.g. 192.168.5.16

ステップ0インターフェイスGi0/2の編集

同様の手順を繰り返して、内部接続のインターフェイスを設定します。この例では、物理インターフェイスはGigabitEthernet0/3です。Edit Physical Interface ウィンドウで、次の操作を行います。

1. Interface Name(この例ではinside)を設定します。
2. Status スライダを有効な設定(



)に設定します。

3. IPv4 Addressタブをクリックして、IPv4アドレス(この例では10.1.3.1/24)を設定します。
4. [OK] をクリックします。

GigabitEthernet0/3 Edit Physical Interface



Interface Name

inside

Mode

Routed

Status



Most features work with named interfaces only, although some require unnamed interfaces.

Description

IPv4 Address

IPv6 Address

Advanced

Type

Static

IP Address and Subnet Mask

10.1.3.1

/

24

e.g. 192.168.5.15/17 or 192.168.5.15/255.255.128.0

Standby IP Address and Subnet Mask

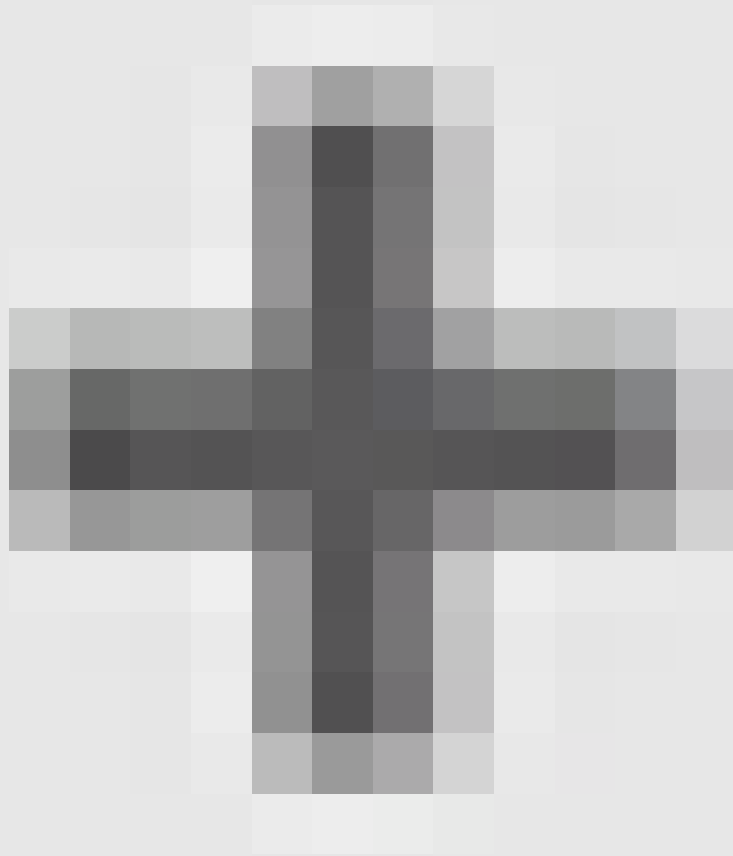
e.g. 192.168.5.16

CANCEL

OK

ステップ0インターフェイスGi0/3の編集

Objects > Object Types > Networksの順に移動し、追加アイコン(



)をクリックして新しいオブジェクトを追加します。

Firewall Device Manager Monitoring Policies **Objects** Device: firepower admin Administrator

Object Types ←
Networks
Ports
Security Zones
Application Filters
URLs
Geolocations
Syslog Servers
IKE Policies

Network Objects and Groups

8 objects Filter +

Preset filters: Default, Applied, User, Applied

#	NAME	TYPE	VALUE	ACTIONS
1	IPv4-Private-All-RFC1918	Group	IPv4-Private-10.0.0.0-8, IPv4-Private-172.16.0.0-12, IPv4-Private-192.168.0.0-16	
2	IPv4-Private-10.0.0.0-8	NETWORK	10.0.0.0/8	
3	IPv4-Private-172.16.0.0-12	NETWORK	172.16.0.0/12	
4	IPv4-Private-192.168.0.0-16	NETWORK	192.168.0.0/16	
5	any-ipv4	NETWORK	0.0.0.0/0	
6	any-ipv6	NETWORK	::/0	

ステップ0オブジェクト1

Add Network Object ウィンドウで、最初のISPゲートウェイを設定します。

1. オブジェクトのName(この例ではgw-outside1)を設定します。
2. オブジェクトのタイプ(この例ではホスト)を選択します。
3. ホスト(この例では10.1.1.2)のIPアドレスを設定します。
4. [OK] をクリックします。

Add Network Object



Name

gw-outside1

Description

Type



Network



Host



FQDN



Range

Host

10.1.1.2

e.g. 192.168.2.1 or 2001:DB8::0DB8:800:200C:417A

CANCEL

OK

ステップ0オブジェクト2

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ネットワークオブジェクトを設定します。

1. オブジェクトの名前を設定します。この例では、gw-outside2です。
2. オブジェクトのタイプ(この例ではホスト)を選択します。
3. ホスト(この例では10.1.2.2)のIPアドレスを設定します。
4. [OK] をクリックします。

Add Network Object



Name

gw-outside2

Description

Type

Network

Host

FQDN

Range

Host

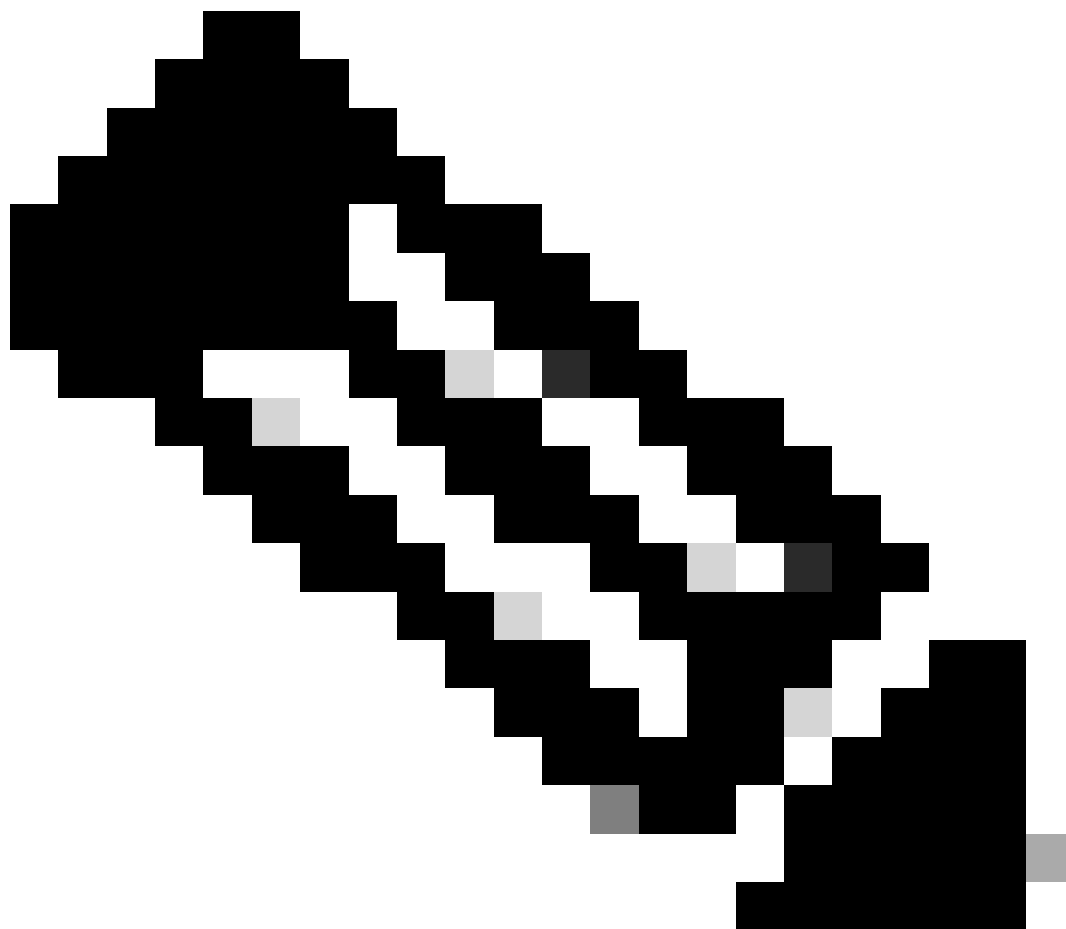
10.1.2|2

e.g. 192.168.2.1 or 2001:DB8::0DB8:800:200C:417A

CANCEL

OK


ステップ0オブジェクト3

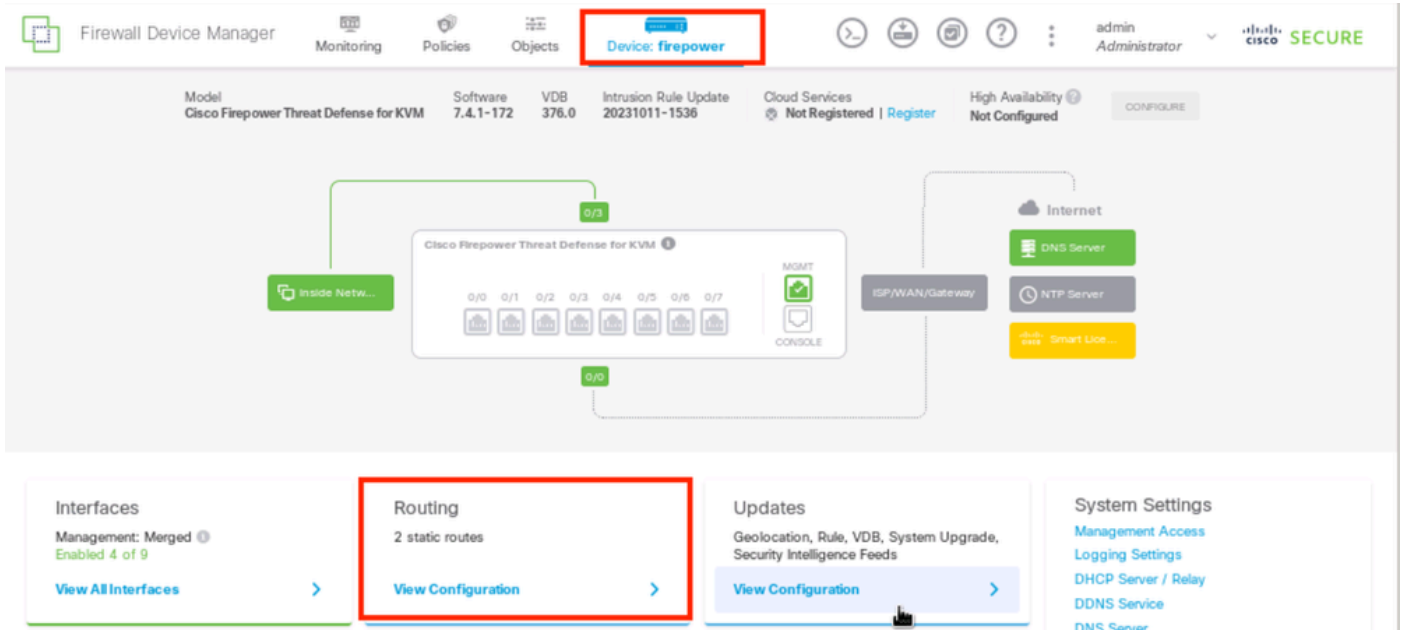


注：トラフィックを許可するには、アクセスコントロールポリシーをFTDで設定する必要があります。この部分はこのドキュメントでは扱いません。

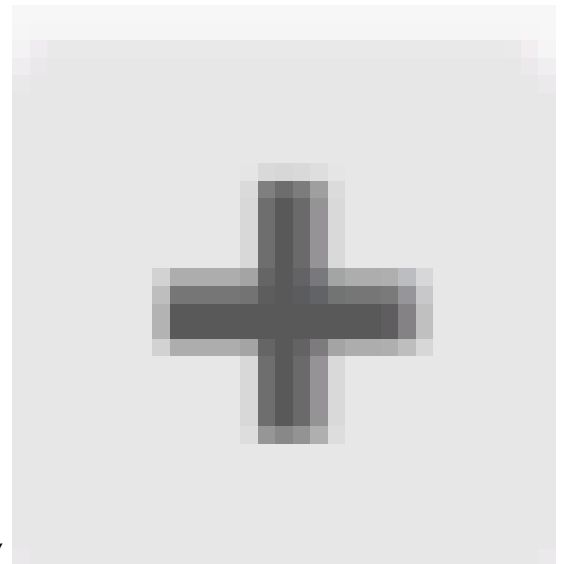
ステップ 1：ECMPゾーンの設定

Device に移動し、Routing の概要にあるリンクをクリックします。

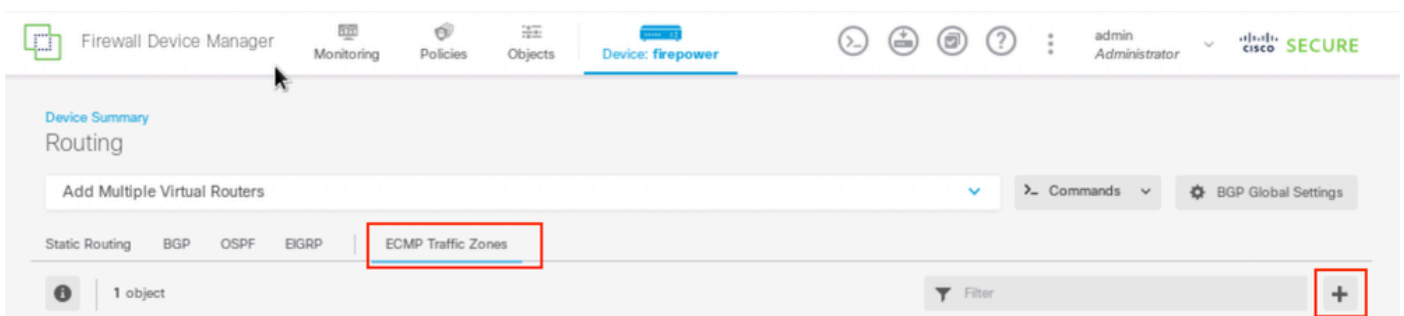
仮想ルータを有効にした場合、スタティックルートを設定するルータの表示アイコン()をクリックします。この場合、仮想ルータは有効になっていません。



ステップ1 ECMPゾーン1



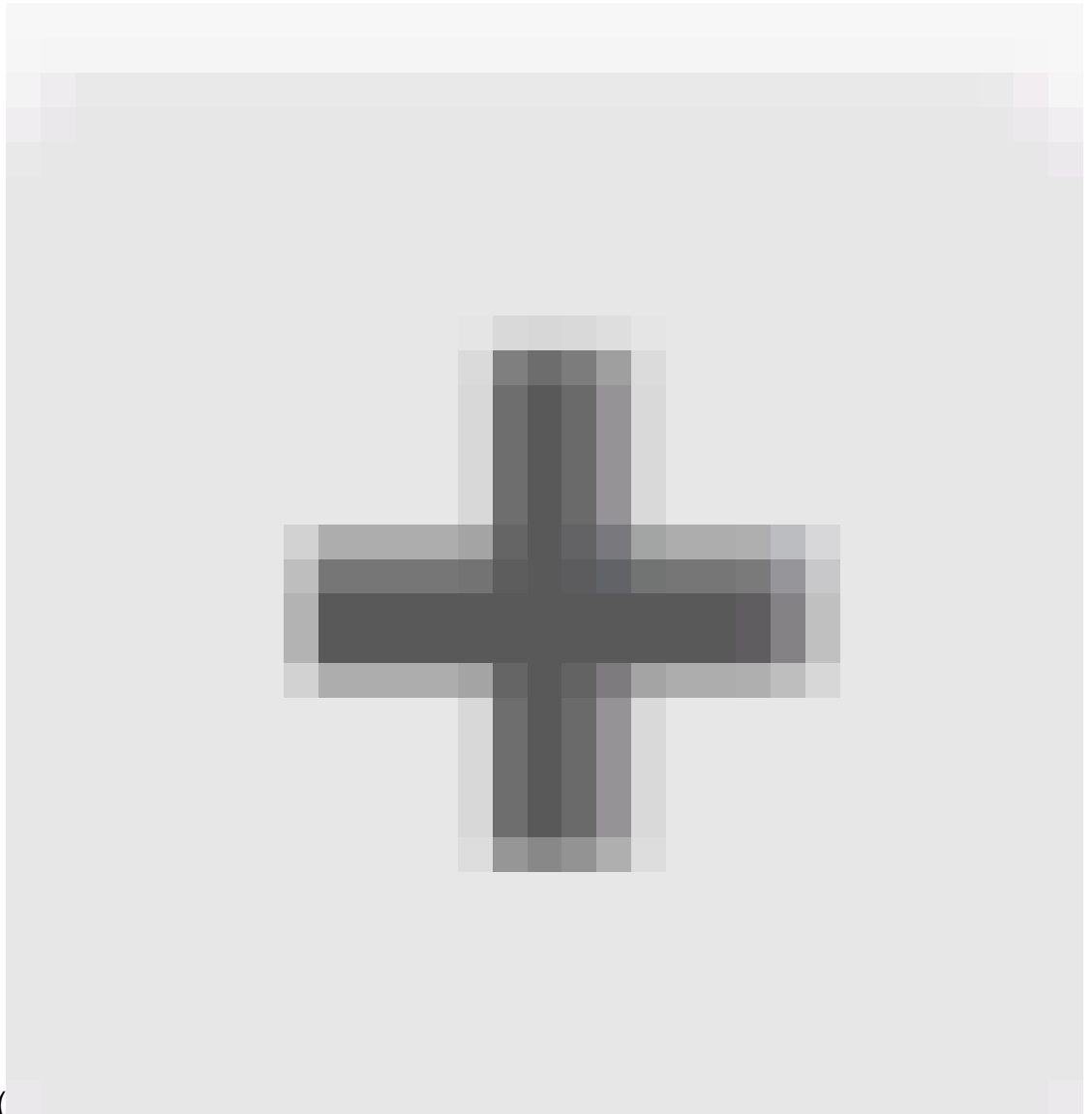
ECMP Traffic Zonesタブをクリックし、次に追加アイコン(+)をクリックして新しいゾーンを追加します。



ステップ1 ECMPゾーン2

Add ECMP Traffic Zone ウィンドウで、次の操作を行います。

1. ECMPゾーンの名前 (オプション) と説明 (オプション) を設定します。



2. 追加アイコン()をクリックして、ゾーンに含める最大8つのインターフェイスを選択します。この例では、ECMP名はOutsideであり、インターフェイスoutside1とoutside2がゾーンに追加されます。
3. [OK] をクリックします。

Add ECMP Traffic Zone



i Keep the member interfaces of a ECMP traffic zone in the same security zone to prevent different access rules being applied to those interfaces.

Name

Outside

Description

Interfaces



- > inside (GigabitEthernet0/3)
- > management (Management0/0)
- > outside (GigabitEthernet0/0)
- > outside1 (GigabitEthernet0/1)
- > outside2 (GigabitEthernet0/2)

2 item(s) selected

Create new Subinterface

CANCEL

OK

CANCEL

OK

NETWORK

INSIDE HOST

ADD ECMP TRAFFIC ZONE

ステップ1 ECMPゾーン3

インターフェイスoutside1 と outside2 の両方がECMPゾーン outside に正常に追加されました。

Device Summary
Routing

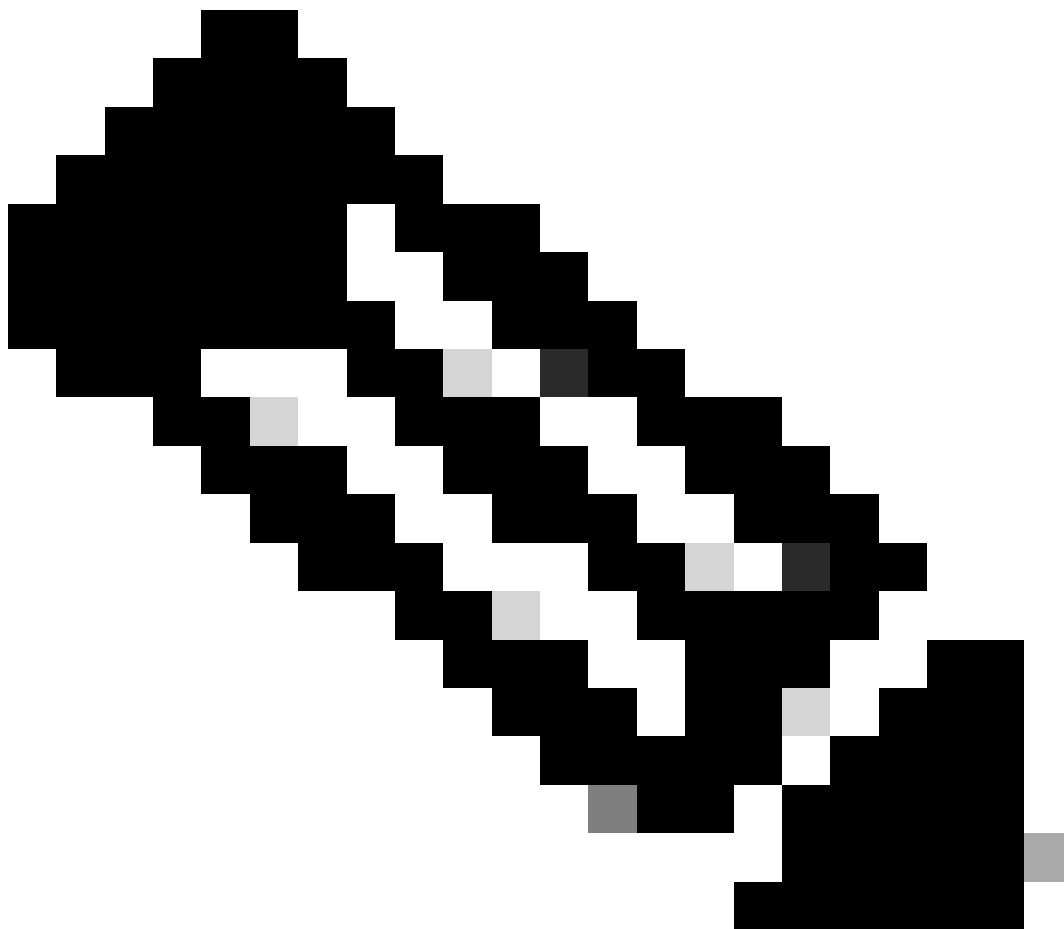
Add Multiple Virtual Routers ▼ Commands BGP Global Settings

Static Routing BGP OSPF EIGRP | ECMP Traffic Zones

1 object Filter +

#	NAME	INTERFACES	ACTIONS
1	Outside	outside1 (GigabitEthernet0/1) outside2 (GigabitEthernet0/2)	

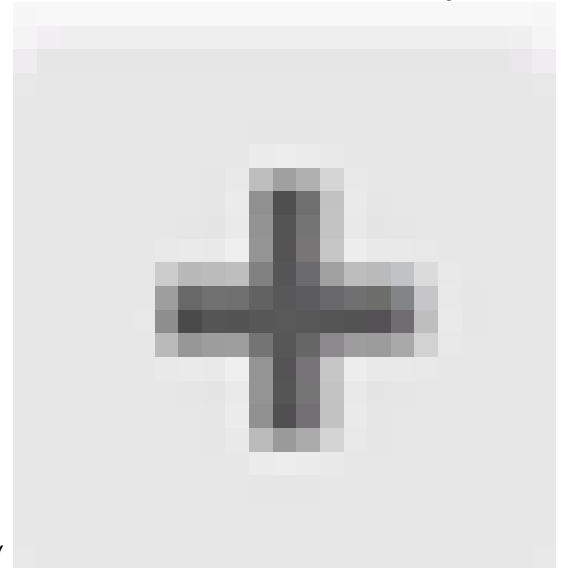
ステップ1 ECMPゾーン4



注:ECMPルーティングトラフィックゾーンは、セキュリティゾーンとは無関係です。outside1およびoutside2インターフェイスを含むセキュリティゾーンを作成しても、ECMPルーティングの目的でトラフィックゾーンは実装されません。

ステップ 2 : IP SLAオブジェクトの設定

各ゲートウェイへの接続を監視するために使用するSLAオブジェクトを定義するには、Objects >



Object Types > SLA Monitorsの順に選択し、追加アイコン(+)をクリックして、最初のISP接続の新しいSLAモニタを追加します。

Firewall Device Manager Monitoring Policies **Objects** Device: firepower admin Administrator CISCO SECURE

Object Types

- Networks
- Ports
- Security Zones
- Application Filters
- URLs
- Geolocations
- Syslog Servers
- IKE Policies
- IPSec Proposals
- Secure Client Profiles
- Identity Sources
- Users
- Certificates
- Secret Keys
- DNS Groups
- Event List Filters
- SLA Monitors**

SLA Monitors

Filter +

#	NAME	MONITORED ADDRESS	TARGET INTERFACE	ACTIONS
There are no SLA Monitors yet. Start by creating the first SLA Monitor.				

CREATE SLA MONITOR

ステップ2 IP SLA1

Add 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 (デフォルト) とオプションで説明(この例ではsla-outside1)を設定します。
2. モニタアドレス(この場合はgw-outside1) (最初のISPゲートウェイ) を設定します。
3. モニタアドレスに到達可能なターゲットインターフェイス(TUI)を設定します。この例では、outside1です。
4. さらに、Timeout と Threshold を調整することもできます。[OK] をクリックします。

Add SLA Monitor Object



Name

sla-outside1

Description

Monitor Address

gw-outside1

Target Interface

outside1 (GigabitEthernet0/1)

IP ICMP ECHO OPTIONS

i Following properties have following correlation: Threshold ≤ Timeout ≤ Frequency

Threshold

5000

milliseconds

0 - 2147483647

Timeout

5000

milliseconds

0 - 604800000

Frequency

60000

milliseconds

1000 - 604800000, multiple of 1000

Type of Service

0

0 - 255

Number of Packets

1

0 - 100

Data Size

28

0 - 16384

bytes

CANCEL

OK

同様の手順を繰り返し、2番目のISP接続に別のSLAモニタオブジェクトを設定します。Add SLA Monitor Objectウィンドウで、次の操作を実行します。

1. SLAモニタオブジェクトの名前 (デフォルト) とオプションで説明(この例ではsla-outside2)を設定します。
2. モニタアドレスを設定します。この例では、gw-outside2 (2番目のISPゲートウェイ) です。
3. モニタアドレスに到達可能なターゲットインターフェイス(TUI)を設定します。この場合はoutside2です。
4. また、Timeout とThresholdを調整することもできます。[OK] をクリックします。

Add SLA Monitor Object



Name

sla-outside2

Description

Monitor Address

gw-outside2

Target Interface

outside2 (GigabitEthernet0/2)

IP ICMP ECHO OPTIONS



Following properties have following correlation: Threshold ≤ Timeout ≤ Frequency

Threshold

5000

milliseconds

0 - 2147483647

Timeout

5000

milliseconds

0 - 604800000

Frequency

60000

milliseconds

1000 - 604800000, multiple of 1000

Type of Service

0

0 - 255

Number of Packets

1

0 - 100

Data Size

28

0 - 16384

bytes


CANCEL

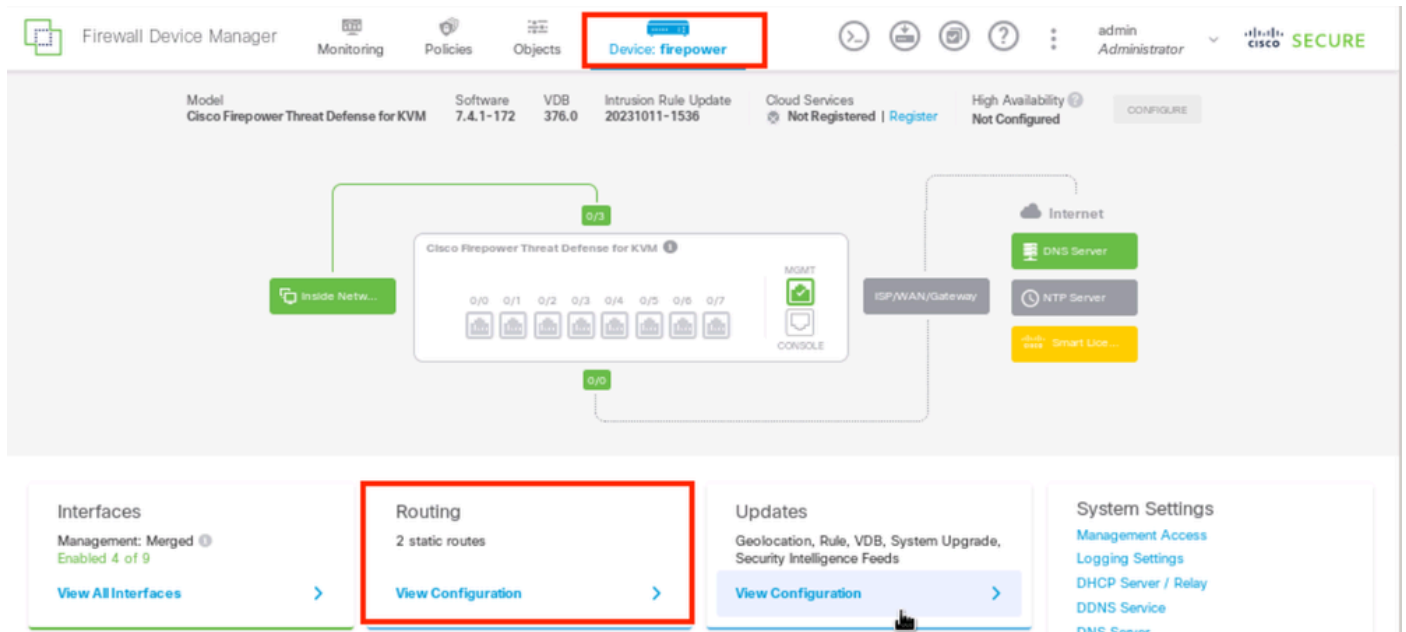
OK

ステップ2 IP SLA3

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

Device に移動し、Routing の概要にあるリンクをクリックします。

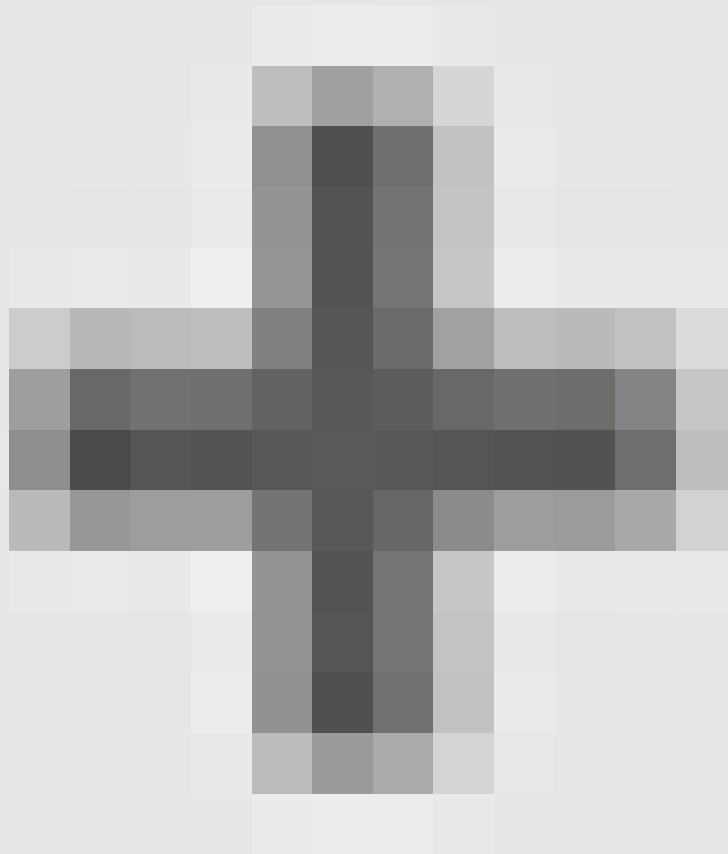
仮想ルータを有効にした場合、スタティックルートを設定するルータの表示アイコン()をクリックします。この場合、仮想ルータは有効になっていません。



The screenshot shows the Cisco Firepower Device Manager (FDM) interface. The top navigation bar includes 'Monitoring', 'Policies', 'Objects', and 'Device: firepower' (highlighted with a red box). The main dashboard displays a network diagram with a central 'Cisco Firepower Threat Defense for KVM' device. The bottom navigation bar shows 'Routing' (highlighted with a red box) and 'View Configuration' link. The 'Routing' section shows '2 static routes' and a 'View Configuration' link.

ステップ3:Route1

Static Routing ページで、addアイコン(



)をクリックして、最初のISPリンクの新しいスタティックルートを追加します。

Add Static Route ウィンドウで、次の手順を実行します。

1. ルートの名前 (オプション) と説明 (オプション) を設定します。この例では、`route_outside1`です。
2. Interfaceドロップダウンリストから、トラフィックを送信するインターフェイスを選択します。ゲートウェイアドレスは、インターフェイスを介してアクセス可能である必要があります。この例では、`outside1(GigabitEthernet0/1)`です。
3. 宛先ネットワークを識別するネットワーク、またはこのルートでゲートウェイを使用するホストを選択します。この例では、事前定義された`any-ipv4`です。
4. Gatewayドロップダウンリストから、ゲートウェイのIPアドレスを識別するネットワークオ

プロジェクトを選択します。トラフィックはこのアドレスに送信されます。この例では、gw-outside1 (最初のISPゲートウェイ) です。

5. ルートのメトリックを1 ~ 254の間で設定します。この例では、1です。
6. SLAモニタドリップダウンリストから、SLAモニタオブジェクトを選択します。この例では、sla-outside1です。
7. [OK] をクリックします。

Add Static Route



Name

route_outside1

Description

Interface

outside1 (GigabitEthernet0/1)

Protocol

IPv4 IPv6

Networks



any-ipv4

Gateway

gw-outside1

Metric

1

SLA Monitor Applicable only for IPv4 Protocol type

sla-outside1

CANCEL

OK

同様の手順を繰り返して、2番目のISP接続に別のスタティックルートを設定します(Add Static Routeウィンドウ)。

1. ルートの名前 (オプション) と説明 (オプション) を設定します。この例では、route_outside2です。
2. Interfaceドロップダウンリストから、トラフィックを送信するインターフェイスを選択します。ゲートウェイアドレスは、インターフェイスを介してアクセス可能である必要があります。この例では、outside2(GigabitEthernet0/2)です。
3. 宛先ネットワークを識別するネットワーク、またはこのルートでゲートウェイを使用するホストを選択します。この例では、事前定義されたany-ipv4です。
4. Gatewayドロップダウンリストから、ゲートウェイのIPアドレスを識別するネットワークオブジェクトを選択します。トラフィックはこのアドレスに送信されます。この例では、gw-outside2 (2番目のISPゲートウェイ) です。
5. ルートのメトリックを1 ~ 254の間で設定します。この例では、1です。
6. SLAモニタドロップダウンリストから、SLAモニタオブジェクトを選択します。このシナリオでは、sla-outside2です。
7. [OK] をクリックします。

Add Static Route



Name

route_outside2

Description

Interface

outside2 (GigabitEthernet0/2)

Protocol

IPv4

IPv6

Networks



any-ipv4

Gateway

gw-outside2

Metric

1

SLA Monitor Applicable only for IPv4 Protocol type

sla-outside2

CANCEL

OK

ルートトラックを持つoutside1 インターフェイスとoutside2 インターフェイスを経由する2つのルートがあります。



#	NAME	INTERFACE	IP TYPE	NETWORKS	GATEWAY IP	SLA MONITOR	METRIC	ACTIONS
1	route_outside1	outside1	IPv4	0.0.0.0/0	10.1.1.2	sla-outside1	1	
2	route_outside2	outside2	IPv4	0.0.0.0/0	10.1.2.2	sla-outside2	1	

ステップ3 Route4

FTDに変更を導入します。

確認

FTDのCLIにログインし、コマンド `show zone` 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 GigabitEthernet0/2
```

```
  outside1 GigabitEthernet0/1
```

`show running-config route` コマンドを実行して、ルーティング設定に関する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。

```
<#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
```

show route 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を介して等コストの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。

<#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
```

show sla monitor configuration コマンドを実行して、SLAモニタの設定を確認します。

<#root>

```
> show sla monitor configuration  
SA Agent, Infrastructure Engine-II  
Entry number: 1037119999  
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: 1631063762
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:

show sla monitor operational-state 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ため、ターゲットインターフェイスを経由するデフォルトルートがアクティブで、ルーティングテーブルに格納されていることを示しています。

<#root>

> show sla monitor operational-state
Entry number: 1037119999
Modification time: 04:14:32.771 UTC Tue Jan 30 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 79
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: 05:32:32.791 UTC Tue Jan 30 2024
Latest operation return code: OK
RTT Values:
RTTAvg: 1 RTTMin: 1 RTTMax: 1
NumOfRTT: 1 RTTSum: 1 RTTSum2: 1

Entry number: 1631063762
Modification time: 04:14:32.771 UTC Tue Jan 30 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 79
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: 05:32:32.791 UTC Tue Jan 30 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、Test-PC-1(10.1.3.2)とTest-PC-2(10.1.3.4)からInternet-Host(10.1.5.2)に向けてSSH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。Test-PC-1(10.1.3.2)はインターフェイスoutside1を経由し、Test-PC 2を経由します。

<#root>

```
> show conn
4 in use, 14 most used
Inspect Short:
preserve-connection: 2 enabled, 0 in effect, 12 most enabled, 0 most in effect
```

```
TCP inside 10.1.3.4:41652 outside2 10.1.5.2:22, idle 0:02:10, bytes 5276, flags UIO N1
```

```
TCP inside 10.1.3.2:57484 outside1 10.1.5.2:22, idle 0:00:04, bytes 5276, 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。

<#root>

> show sla monitor operational-state

Entry number: 1037119999

Modification time: 04:14:32.771 UTC Tue Jan 30 2024

Number of Octets Used by this Entry: 2056

Number of operations attempted: 121

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: 06:14:32.801 UTC Tue Jan 30 2024

Latest operation return code: Timeout

RTT Values:

RTTAvg: 0 RTTMin: 0 RTTMax: 0

NumOfRTT: 0 RTTSum: 0 RTTSum2: 0

Entry number: 1631063762

Modification time: 04:14:32.771 UTC Tue Jan 30 2024

Number of Octets Used by this Entry: 2056

Number of operations attempted: 121

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: 06:14:32.802 UTC Tue Jan 30 2024

Latest operation return code: OK

RTT Values:

RTTAvg: 1 RTTMin: 1 RTTMax: 1

NumOfRTT: 1 RTTSum: 1 RTTSum2: 1

show route 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。

<#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
```

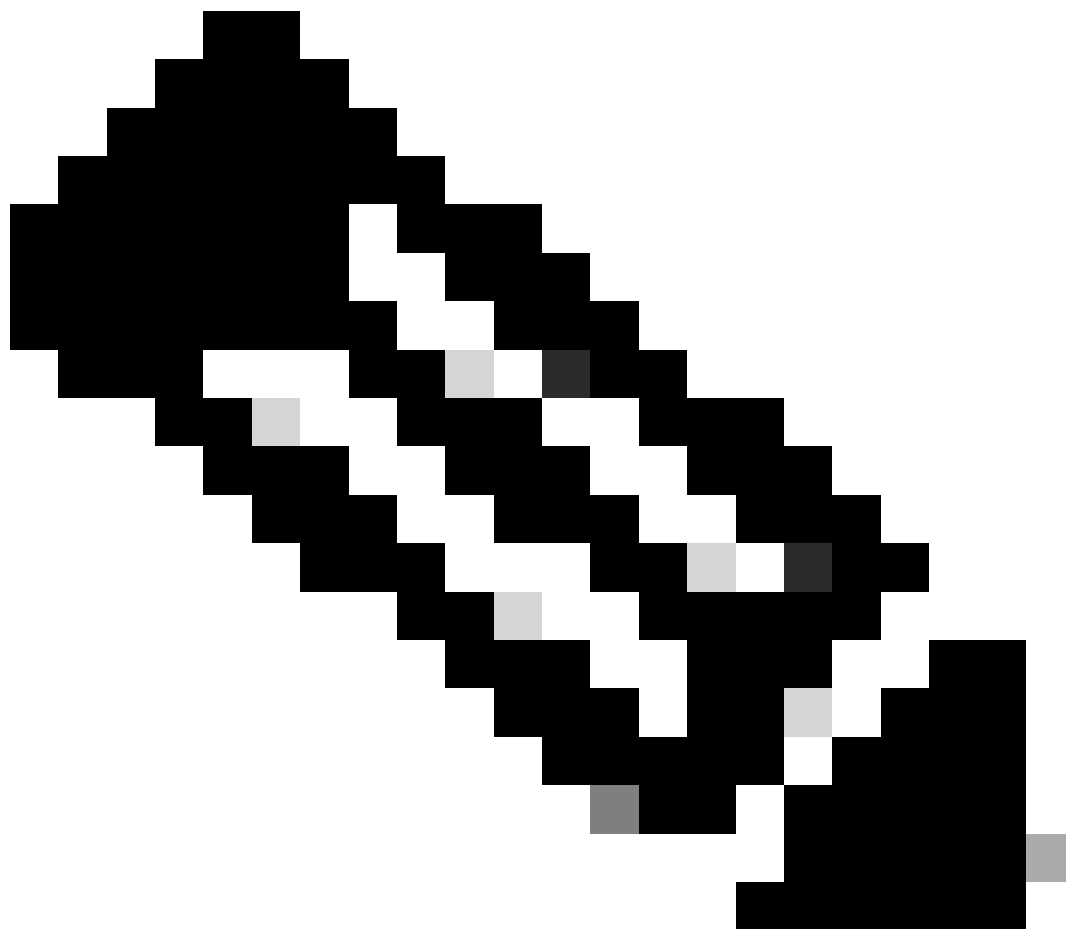
show conn コマンドを実行すると、2つの接続がまだアップしていることがわかります。SSHセッションは、中断することなく、Test-PC-1(10.1.3.2)およびTest-PC-2(10.1.3.4)でもアクティブです。

```
<#root>
```

```
> show conn  
4 in use, 14 most used  
Inspect Snort:  
preserve-connection: 2 enabled, 0 in effect, 12 most enabled, 0 most in effect
```

```
TCP inside 10.1.3.4:41652 outside2 10.1.5.2:22, idle 0:19:29, bytes 5276, flags UIO N1
```

```
TCP inside 10.1.3.2:57484 outside1 10.1.5.2:22, idle 0:17:22, bytes 5276, flags UIO N1
```



注：Test-PC-1(10.1.3.2)からのshow connの出力では、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るにもかかわらず、SSHセッションはインターフェイスoutside1を経由しています。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。Test-PC-1(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。

トラブルシューティング

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。

<#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
```

show route 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。

<#root>

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

RT(mgmt-only):

```
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
```

show route 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。

```
> 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
```

関連情報

- [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。