ECMP

この章では、ルーティングプロトコルでネットワークトラフィックの負荷分散に使用される等コストマルチパス（ECMP）ルーティングを設定する手順について説明します。

ECMP について

Firepower Threat Defense デバイスは、等コストマルチパス（ECMP）ルーティングをサポートしています。インターフェイスのグループを含むように、仮想ルータごとにトラフィックゾーンを設定できます。各ゾーンにある最大 8 つのインターフェイス間に最大 8 つの等コストのスタティックルートまたはダイナミックルートを設定できます。たとえば、次のようにゾーン内の 3 つのインターフェイ間に複数のデフォルト ルートを設定できます。

```
route for 0.0.0.0 0.0.0.0 through outside1 to 10.1.1.2
route for 0.0.0.0 0.0.0.0 through outside2 to 10.2.1.2
route for 0.0.0.0 0.0.0.0 through outside3 to 10.3.1.2
```

ECMP の注意事項と制限事項

ファイアウォール モードのガイドライン

ECMP ゾーンは、ルーテッド ファイアウォール モードでのみサポートされています。

インターフェイスのガイドライン

dVTI とループバック インターフェイスはサポートされていません。

その他のガイドライン

- デバイスには、最大 256 の ECMP ゾーンを設定できます。
- ECMP ゾーンごとに 8 つのインターフェイスのみを関連付けられます。
- 1 つのインターフェイスがメンバーになれる ECMP ゾーンは 1 つだけです。
- 等コストのスタティックルートに関連付けられているインターフェイスは、ECMP ゾーンから削除できません。
- インターフェイスに等コストのスタティックルートが関連付けられている場合、ECMP ゾーンは削除できません。
- ルーテッドインターフェイスのみを ECMP ゾーンに関連付けられます。
- 次のインターフェイスは、ECMP ゾーンに関連付けられません。
  - BVI インターフェイス。
  - EtherChannel のメンバーインターフェイス。
  - フェールオーバーまたはステート リンク インターフェイス。
  - 管理専用インターフェイスまたは管理アクセスインターフェイス。
  - クラスタ制御リンクインターフェイス。
  - VNI。
  - VLAN インターフェイス
  - SSL が有効になっているリモートアクセス VPN 設定のインターフェイス。
- ECMP ゾーン内のインターフェイスでは DHCP リレーはサポートされていません。
- デュアル ISP/WAN Firewall Threat Defense の展開：プライマリおよびセカンダリ データ インターフェイス用に単一の ECMP ゾーンを作成します。この構成により、同じメトリック値を持つ両方のインターフェイスのスタティックルートを作成できます。
- Firewall Threat Defense は、IPsec セッションでの NAT を使用した ECMP をサポートしていません。標準の IPsec 仮想プライベートネットワーク（VPN）トンネルは、IPsec パケットの提供パス内の NAT ポイントでは機能しません。

ECMP の管理ページ

[ルーティング（Routing）] ペインで [ECMP] をクリックすると、仮想ルータに対応する ECMP ページが表示されます。このページには、仮想ルータの関連インターフェイスを持つ既存の

ECMPゾーンが表示されます。このページでは、仮想ルータにECMPゾーンを追加できます。ECMP の**Edit** ( )と**Delete** ( )もできます。

次を実行します。

- ECMP ゾーンの作成 （3 ページ）
- 等コストスタティックルートの設定 （4 ページ）
- ECMP ゾーンの変更 （5 ページ）
- ECMP ゾーンの削除 （6 ページ）

ECMP ゾーンの作成

ECMP ゾーンは、仮想ルータごとに作成されるため、ECMP が作成されている仮想ルータのインターフェイスのみを ECMP に関連付けることができます。

手順

ステップ 1 **Devices** > **Device Management** を選択し、Firewall Threat Defense デバイスを編集します。

ステップ 2 [ルーティング（Routing）] をクリックします。

ステップ 3 仮想ルータの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。

グローバル仮想ルータおよびユーザー定義の仮想ルータにECMPゾーンを作成できます。仮想ルータの作成については、仮想ルータの作成を参照してください。

ステップ 4 [ECMP] をクリックします。

ステップ 5 [Add] をクリックします。

ステップ 6 [ECMPの追加（Add ECMP）] ボックスに ECMP ゾーンの名前を入力します。

（注）
ECMP 名は、ルーテッドデバイスに対して一意である必要があります。

ステップ 7 インターフェイスを関連付けるには、[使用可能なインターフェイス（Available Interfaces）] ボックスでインターフェイスを選択し、[追加（Add）] をクリックします。

次の点を忘れないでください。

- 割り当てに使用できるのは、仮想ルータに属しているインターフェイスだけです。
- 論理名を持つインターフェイスのみが [Available Interfaces] ボックスの下にリストされます。インターフェイスを編集し、[インターフェイス（Interfaces）] で論理名を指定できます。設定を有効にするには、必ず変更を保存してください。

ステップ 8 [OK] をクリックします。

[ECMP] ページに、新しく作成された ECMP が表示されます。

ステップ 9 [保存（Save）] をクリックして、設定を展開します。

ECMP ゾーンインターフェイスを等コストのスタティックルートに関連付けるには、同じ宛先とメトリック値、および異なるゲートウェイを指定してインターフェイスを定義します。

次のタスク

- 等コストスタティックルートの設定 （4 ページ）
- ECMP ゾーンの変更 （5 ページ）
- ECMP ゾーンの削除 （6 ページ）

等コストスタティックルートの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス
すべて	N/A	Firewall Threat DefenseおよびFirewall Threat Defense Virtual	任意	Admin/Network Admin/Security Approver

グローバル仮想ルータとユーザー定義仮想ルータのどちらも、そのインターフェイスをデバイスの ECMP ゾーンに割り当てることができます。

始める前に

- インターフェイスの等コストスタティックルートを設定する場合は、必ず、それを ECMP ゾーンに関連付けてください。ECMP ゾーンの作成 （3 ページ） を参照してください。
- 非 VRF 対応デバイスのすべてのルーティング設定は、グローバル仮想ルータでも使用できます。
- インターフェイスを ECMP ゾーンに関連付けずに、同じ宛先とメトリックでインターフェイスのスタティックルートを定義することはできません。

手順

ステップ 1 **Devices** > **Device Management** ページで、Firewall Threat Defense デバイスを編集します。[ルーティング（Routing）] タブをクリックします。

ステップ 2 ドロップダウンリストから、インターフェイスが ECMP ゾーンに関連付けられている仮想ルータを選択します。

ステップ 3 インターフェイスの等コストスタティックルートを設定するには、[スタティックルート（Static Route）] をクリックします。

ステップ 4 [ルートを追加（Add Route）] をクリックして新しいルートを追加するか、既存のルートの場合は **Edit** (✎) をクリックします。

ステップ 5 [インターフェイス（Interface）] ドロップダウンから、仮想ルータと ECMP ゾーンに属するインターフェイスを選択します。

ステップ 6 [使用可能なネットワーク（Available Networks）] ボックスから宛先ネットワークを選択し、[追加（Add）] をクリックします。

ステップ 7 ネットワークのゲートウェイを入力します。

ステップ 8 メトリック値を入力します。1 ～ 254 の数値を指定できます。

ステップ 9 設定を保存するには、[Save] をクリックします。

ステップ 10 等コストスタティックルーティングを設定するには、手順を繰り返して、同じ ECMP ゾーンに含まれる別のインターフェイスのスタティックルートを、同じ宛先ネットワークとメトリック値で設定します。必ず、別のゲートウェイを指定してください。

次のタスク

- ECMP ゾーンの変更 （5 ページ）
- ECMP ゾーンの削除 （6 ページ）

ECMP ゾーンの変更

手順

ステップ 1 **Devices** > **Device Management** を選択し、Firewall Threat Defense デバイスを編集します。

ステップ 2 [ルーティング（Routing）] をクリックします。

ステップ 3 [ECMP] をクリックします。

ECMP ゾーンおよび関連付けられたインターフェイスが [ECMP] ページに表示されます。

ステップ 4 ECMP を変更するには、目的の ECMP に対する **Edit** (✎) をクリックします。[ECMPの編集（Edit ECMP）] ボックスでは、次のことができます。

- [ECMP名（ECMP Name）]：変更された名前がデバイスに対して一意であることを確認します。
- [インターフェイス（Interfaces）]：インターフェイスを追加または削除できます。すでに別の ECMP に関連付けられているインターフェイスを含めることはできません。また、等コストのスタティックルートに関連付けられているインターフェイスは削除できません。

ステップ 5 [OK] をクリックします。

ステップ 6 変更を保存するには、[Save] をクリックします。

次のタスク

- 等コストスタティックルートの設定 （4 ページ）
- ECMP ゾーンの削除 （6 ページ）

ECMP ゾーンの削除

手順

ステップ 1 **Devices** > **Device Management** を選択し、Firewall Threat Defense デバイスを編集します。

ステップ 2 [ルーティング（Routing）] をクリックします。

ステップ 3 [ECMP] をクリックします。

ECMP ゾーンおよび関連付けられたインターフェイスが [ECMP] ページに表示されます。

ステップ 4 ECMP ゾーンを削除するには、その ECMP ゾーンに対する **Delete** ( ) をクリックします。

インターフェイスのいずれかが等コストのスタティックルートに関連付けられている場合、ECMP ゾーンは削除できません。

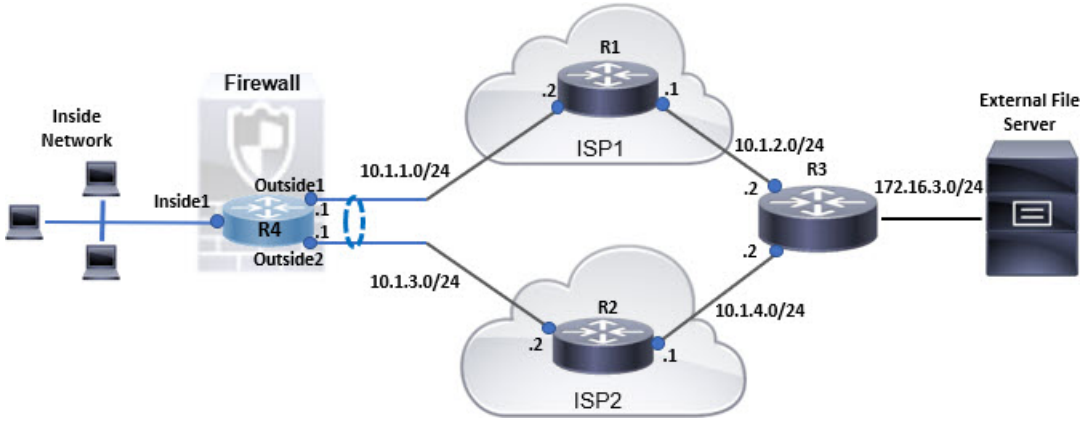
ステップ 5 確認メッセージで [削除（Delete）] をクリックします。

ステップ 6 変更を保存するには、[Save] をクリックします。

ECMP の設定例

この例では、Firewall Management Center を使用して、デバイスを通過するトラフィックが効率的に処理されるように Firewall Threat Defense の ECMP ゾーンを設定する方法を示しています。ECMP が設定されていると、Firewall Threat Defense ではゾーンごとにルーティングテーブルが維持されるため、可能な限り最良のルートでパケットを再ルーティングできます。そのため、ECMP は非対称ルーティング、負荷分散をサポートし、トラフィックの損失をシームレスに処理します。この例では、R4 は外部ファイルサーバーに到達する 2 つのパスを記録します。

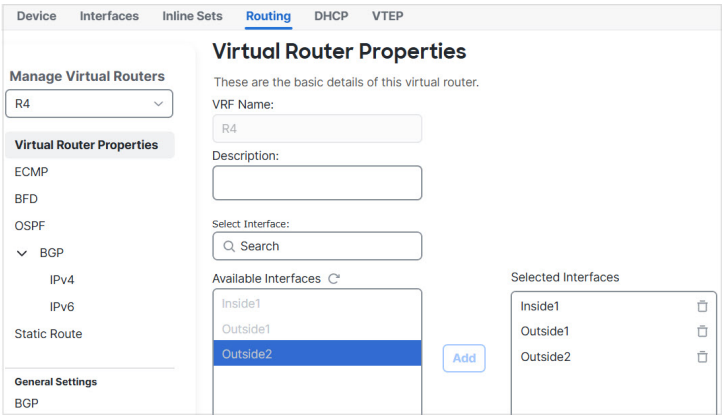
図 *1* : *ECMP* の設定例



手順

ステップ 1 仮想ルータを作成します（*Inside1*、*Outside1*、*Outside2* インターフェイスを備えた *R4*）。

図 *2* : *R4* 仮想ルータの設定



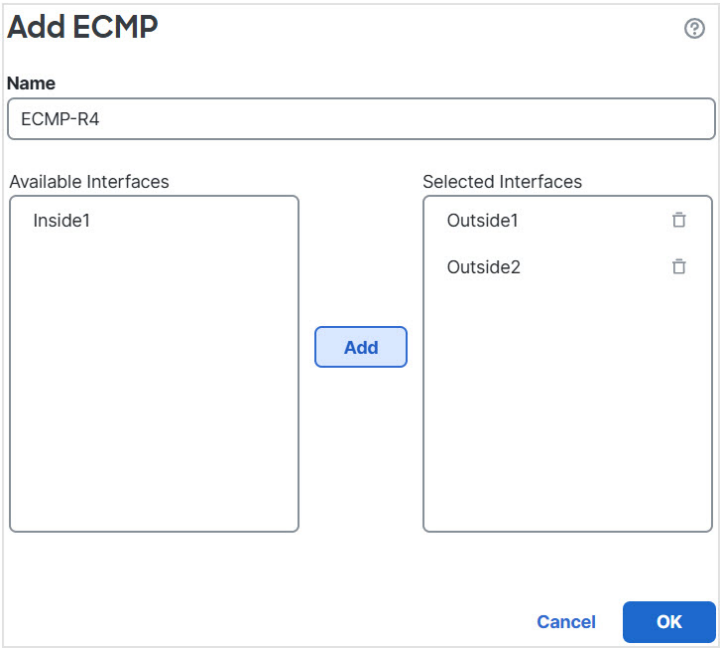
ステップ 2 ECMP ゾーンを作成します。

a) [ルーティング（Routing）] タブで、ユーザー定義の R4 仮想ルータを選択し、[ECMP] をクリックします。

b) [追加（Add）] をクリックします。

c) ECMP 名を入力し、[利用可能なインターフェイス（Available Interfaces）] リストから [Outside1] および [Outside2] を選択します。

図 *3 : ECMP* ゾーンの作成



d) [OK]、[保存（Save）] の順にクリックします。

ステップ 3 ゾーンインターフェイスのスタティックルートを作成します。

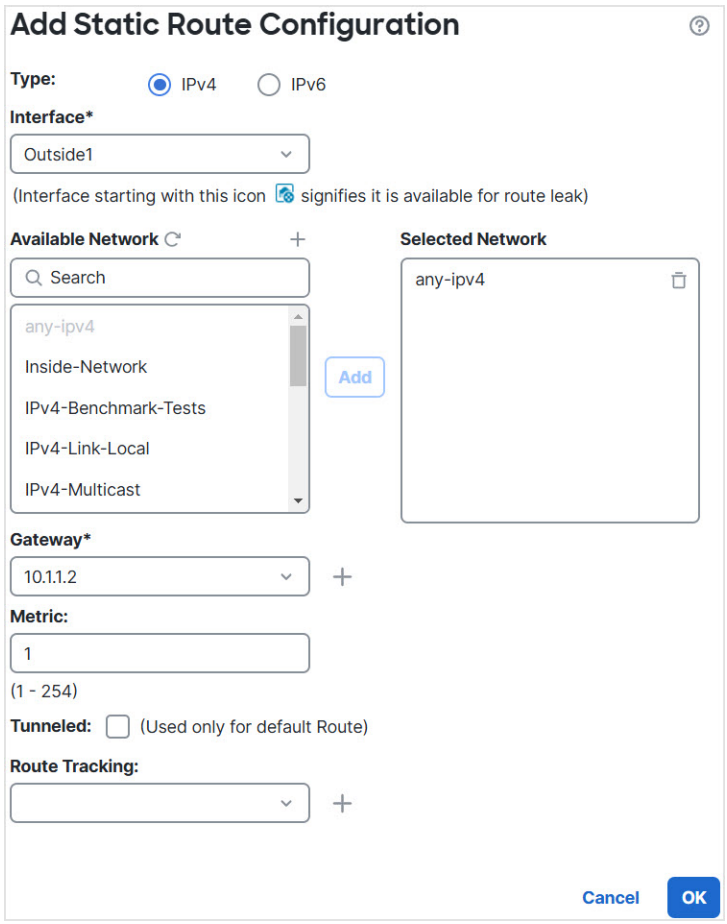
a) [ルーティング（Routing）] タブで、[スタティックルート（Static Route）] をクリックします。

b) [インターフェイス（Interface）] ドロップダウンリストから、[Outside1] を選択します。

c) [利用可能なネットワーク（Available Network）] で、any-ipv4 を選択し、[追加（Add）] をクリックします。

d) [ゲートウェイ（Gateway）] フィールドにネクストホップアドレス 10.1.1.2 を指定します。

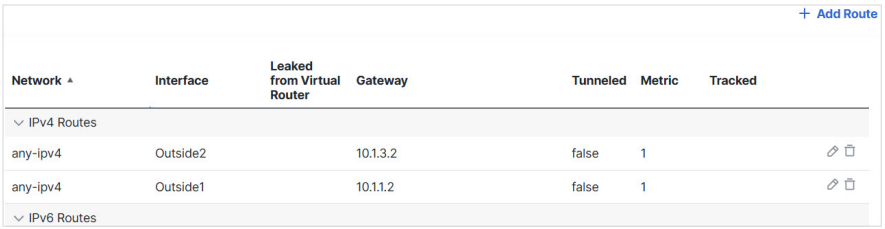
図 *4 : Outside1* のスタティックルートの設定



e) 手順 3b ～ 3d を繰り返して、Outside2 のスタティックルートを設定します。

同じメトリックを指定しますが、スタティックルートには異なるゲートウェイを指定します。

図 *5 : ECMP* ゾーンインターフェイスの設定済みスタティックルート



ステップ 4 [保存（Save）]、[展開（Deploy）] の順にクリックします。

ネットワークパケットは、ECMP アルゴリズムに基づいて、R4>R1>R3 または R4>R2>R3 に従って宛先 R3 に到達します。R1>R3 ルートが失われた場合、トラフィックはパケットドロップなしで R2 を通過します。同様に、*Outside1* からパケットを送信しても、R3 からの応答を

Outside2 が受信する可能性があります。さらに、ネットワークトラフィックが多い場合、R4 は 2 つのルート間でトラフィックを分散させ、負荷のバランスを取ります。

Secure Firewall Threat Defense の ECMP の履歴

機能	Minimum Firewall Management Center	Minimum Firewall Threat Defense	詳細
ルーティングポリシーとしての ECMP のサポート	7.1	任意（Any）	Secure Firewall Threat Defenseでは、以前は FlexConfig ポリシーを介して ECMP ルーティングがサポートされていました。このリリースから、インターフェイスをトラフィックゾーンにグループ化し、Secure Firewall Management Center でECMP ルーティングを設定できます。 新規/変更された画面：**[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > **[ルーティング（Routing）]** > **[ECMP]**

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。