Firepower Threat Defense のスタティック ルートとデフォルト ルート

この章では、Firepower Threat Defense でスタティック ルートとデフォルト ルートを設定する方法について説明します。

スタティック ルートとデフォルト ルートについて

接続されていないホストまたはネットワークにトラフィックをルーティングするには、スタティック ルーティングとダイナミック ルーティングのどちらかを使用して、ホストまたはネットワークへのルートを定義する必要があります。通常は、少なくとも 1 つのスタティック ルート、つまり、他の方法でデフォルトのネットワーク ゲートウェイにルーティングされていない、すべてのトラフィック用のデフォルト ルート（通常、ネクスト ホップ ルータ）を設定する必要があります。

デフォルト ルート

最も単純なオプションは、すべてのトラフィックを上流に位置するルータに送信するようにデフォルト ルートを設定して、トラフィックのルーティングをルータに任せることです。デフォルト ルートは、ASA が既知のルートもスタティック ルートも指定されていないすべての IP パケットを送信するゲートウェイ IP アドレスを特定します。デフォルト スタティック ルートは、宛先 IP アドレスとして 0.0.0.0/0 が指定された単純なスタティック ルートです。

スタティック ルート

次の場合は、スタティック ルートを使用します。

- ネットワークがサポート対象外のルータ ディスカバリ プロトコルを使用している。

- ネットワークが小規模でスタティック ルートを容易に管理できる。
- ルーティング プロトコルが関係するトラフィックまたは CPU のオーバーヘッドをなくす必要がある。
- 場合によっては、デフォルト ルートだけでは不十分である。デフォルトのゲートウェイでは宛先ネットワークに到達できない場合があるため、スタティック ルートをさらに詳しく設定する必要があります。たとえば、デフォルトのゲートウェイが外部の場合、デフォルト ルートは、/Firepower Threat Defense デバイス に直接接続されていない内部ネットワークにはまったくトラフィックを転送できません。
- ダイナミック ルーティング プロトコルをサポートしていない機能を使用している。

不要なトラフィックを「ブラックホール化」するためのnull0インターフェイスへのルート

アクセス ルールを使用すると、ヘッダーに含まれている情報に基づいてパケットをフィルタ処理することができます。null0 インターフェイスへのスタティック ルートは、アクセス ルールを補完するソリューションです。null0 ルートを使用して、不要なトラフィックや望ましくないトラフィックを「ブラック ホール」に転送できるため、トラフィックがドロップされます。

スタティック null0 ルートには、推奨パフォーマンス プロファイルが割り当てられます。また、スタティック null0 ルートを使用して、ルーティング ループを回避することもできます。BGP では、リモート トリガ型ブラック ホール ルーティングのためにスタティック null0 ルートを活用できます。

ルートのプライオリティ

- 特定の宛先が特定されたルートはデフォルト ルートより優先されます。
- 宛先が同じルートが複数存在する場合（スタティックまたはダイナミック）、ルートのアドミニストレーティブ ディスタンスによってプライオリティが決まります。スタティック ルートは 1 に設定されるため、通常、それらが最もプライオリティの高いルートです。
- 宛先かつアドミニストレーティブ ディスタンスが同じスタティック ルートが複数存在する場合は、ECMP ルーティングを参照してください。
- [トンネル化（Tunneled）] オプションを使用してトンネルから出力されるトラフィックの場合、このルートが他の設定済みルートまたは学習されたデフォルト ルートをすべてオーバーライドします。

トランスペアレント ファイアウォール モードおよびブリッジ グループのルート

ブリッジ グループ メンバー インターフェイスを通じて直接には接続されていないネットワークに向かう /Firepower Threat Defense デバイス で発信されるトラフィックの場合、/Firepower Threat Defense デバイス がどのブリッジ グループ メンバー インターフェイスからトラフィックを送信するかを認識するように、デフォルト ルートまたはスタティック ルートを設定する必要があります。/Firepower Threat Defense デバイス で発信されるトラフィックには、syslog サーバまたはSNMP サーバへの通信が含まれることもあります。1 つのデフォルト ルートで到達できないサーバがある場合、スタティック ルートを設定する必要があります。トランスペアレント モードの場合、ゲートウェイ インターフェイスとしてBVI を指定できません。つまり、メンバー インターフェイスのみを使用できます。ルーテッド モードのブリッジ グループの場合、スタティック ルートに BVI を指定する必要があります。つまり、メンバー インターフェイスを指定することはできません。詳細については、MAC アドレスとルート ルックアップを参照してください。

スタティック ルート トラッキング

スタティック ルートの問題の 1 つは、ルートがアップ状態なのかダウン状態なのかを判定する固有のメカニズムがないことです。スタティック ルートは、ネクスト ホップ ゲートウェイが使用できなくなった場合でも、ルーティング テーブルに保持されています。スタティック ルートは、/Firepower Threat Defense デバイス 上の関連付けられたインターフェイスがダウンした場合に限りルーティング テーブルから削除されます。

スタティック ルート トラッキング機能には、スタティック ルートの使用可能状況を追跡し、プライマリ ルートがダウンした場合のバックアップ ルートをインストールするための方式が用意されています。たとえば、ISP ゲートウェイへのデフォルト ルートを定義し、かつ、プライマリ ISP が使用できなくなった場合に備えて、セカンダリ ISP へのバックアップ デフォルト ルートを定義できます。

/Firepower Threat Defense デバイス では、/Firepower Threat Defense デバイス が ICMP エコー要求を使用してモニタする宛先ネットワーク上でモニタリング対象ホストにスタティック ルートを関連付けることでスタティック ルート トラッキングを実装します。指定された時間内にエコー応答がない場合は、そのホストはダウンしていると見なされ、関連付けられたルートはルーティング テーブルから削除されます。削除されたルートに代わって、メトリックが高い追跡対象外のバックアップ ルートが使用されます。

モニタリング対象の選択時には、その対象がICMP エコー要求に応答できることを確認してください。対象には任意のネットワーク オブジェクトを選択できますが、次のものを使用することを検討する必要があります。

- ISP ゲートウェイ アドレス（デュアル ISP サポート用）
- ネクストホップ ゲートウェイ アドレス（ゲートウェイの使用可能状況に懸念がある場合）
- /Firepower Threat Defense デバイス が通信する必要のある対象ネットワーク上のサーバ（syslog サーバなど）

- 宛先ネットワーク上の永続的なネットワーク オブジェクト

（注） 夜間にシャットダウンする PC は適しません。

スタティック ルート トラッキングは、スタティックに定義されたルートや、DHCP または PPPoE を通じて取得したデフォルト ルートに対して設定することができます。設定済みのルート トラッキングでは、複数のインターフェイス上の PPPoE クライアントだけを有効化することができます。

スタティックルートとデフォルトルートのガイドライン

ファイアウォール モードとブリッジ グループ

- トランスペアレント モードでは、スタティック ルートはブリッジ グループ メンバー インターフェイスをゲートウェイとして使用する必要があります。BVI を指定することはできません。
- ルーテッド モードでは、BVI をゲートウェイとして指定する必要があります。メンバー インターフェイスを指定することはできません。
- スタティック ルート トラッキングは、ブリッジ グループ メンバー インターフェイスまたは BVI ではサポートされません。

IPv6

- IPv6 では、スタティック ルート トラッキングはサポートされません。

クラスタリング

クラスタリングでは、スタティック ルート モニタリングはプライマリ ユニットでのみサポートされます。

スタティック ルートの追加

スタティック ルートは、特定の宛先ネットワークのトラフィックの送信先を定義します。少なくともデフォルト ルートを定義する必要があります。デフォルト ルートは、宛先 IP アドレスが 0.0.0.0/0 のスタティック ルートです。

手順

ステップ 1 **[デバイス（Devices）] > [デバイス管理（Device Management）]** を選択し、Firepower Threat Defense デバイスを編集します。

ステップ 2 [ルーティング（Routing）] タブをクリックします。

ステップ 3 コンテンツのテーブルから [スタティック ルート（Static Route）] を選択します。

ステップ 4 [ルートを追加（Add Routes）] をクリックします。

ステップ 5 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] オプション ボタンをクリックします。

ステップ 6 このスタティック ルートを適用する [インターフェイス（Interface）] を選択します。

トランスペアレント モードの場合は、ブリッジ グループのメンバー インターフェイスの名前を選択します。ブリッジ グループによるルーティング モードの場合、BVI 名として、いずれかのブリッジグループ メンバーインターフェイスを選択できます。不要なトラフィックを「ブラック ホール化」するには、**Null0** インターフェイスを選択します。

ステップ 7 [利用可能なネットワーク（Available Network）] リストで、宛先ネットワークを選択します。

デフォルト ルートを定義するには、アドレス 0.0.0.0/0 のオブジェクトを作成し、ここでそれを選択します。

ステップ 8 [ゲートウェイ（Gateway）] または [IPv6 ゲートウェイ（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 アドレスまたはネットワーク/ホスト オブジェクトを指定できます。

ステップ 9 [メトリック（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。有効値の範囲は 1 ～ 255 で、デフォルト値は 1 です。メトリックは、特定のホストが存在するネットワークへのホップ数（ホップ カウント）に基づくルートの「コスト」を示す測定値です。ホップ カウントは、ネットワーク パケットが最終的な宛先に到達するまでに通過する必要があるネットワークの数であり、宛先ネットワークも含まれます。メトリックは、複数のルーティング プロトコル間でルートを比較するために使用されます。スタティック ルートのデフォルトのアドミニストレーティブ ディスタンスは 1 で、ダイナミック ルーティング プロトコルで検出されるルートより優先されますが、直接には接続されていないルートです。OSPF で検出されるルートのデフォルトのアドミニストレーティブディスタンスは110です。スタティック ルートとダイナミック ルートのアドミニストレーティブ ディスタンスが同じ場合、スタティック ルートが優先されます。接続されているルートは常に、スタティック ルートおよびダイナミックに検出されたルートのどちらよりも優先されます。

ステップ 10 （任意）デフォルト ルートの場合は、[トンネル型（Tunneled）]チェックボックスをオンにして、VPN トラフィック用に別個のデフォルト ルートを定義します。

VPN トラフィックに非 VPN トラフィックとは別のデフォルト ルートを使用する必要がある場合は、VPN トラフィック用の別個のデフォルト ルートを定義できます。その場合、たとえばVPN接続からの着信トラフィックは内部ネットワークに転送する一方、内部ネットワークからのトラフィックは外部に転送するといった設定を簡単に行うことができます。[トンネル型（tunneled）] オプションを使用してデフォルト ルートを作成すると、デバイスに着信するトンネルからのすべてのトラフィックは、学習したルートまたはスタティック ルートを使用して

ルーティングできない場合、このルートに送信されます。設定できるデフォルトのトンネル ゲートウェイは、デバイスごとに 1 つのみです。トンネル トラフィックの ECMP はサポートされません。

ステップ 11 （IPv4 スタティック ルートのみ）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（サービス レベル契約）モニタ オブジェクトの名前を [ルート トラッキング（Route Tracking）] フィールドで入力または選択します。

SLA モニタ オブジェクトを参照してください。

ステップ 12 [OK] をクリックします。