ルーティング

システムは、ルーティング テーブルを使用して、システムに入るパケットの出力インターフェイスを決定します。ここでは、ルーティングの概要とデバイスでのルーティングの設定方法について説明します。

ルーティングの概要

次に、Firepower Threat Defenseデバイス内でルーティングがどのように動作するかを示します。ルーティングは、送信元から宛先にネットワーク経由で情報を移動する行為のことです。その間に、通常は少なくとも 1 つの中間ノードがあります。ルーティングには、最適なルーティング パスの決定と、インターネットワーク経由でのパケットの転送という 2 つの基本的なアクティビティが含まれます。

NAT がルート選択に及ぼす影響

Firepower Threat Defenseは、ルーティングを決定するために、ルーティング テーブルとネットワーク アドレス変換（NAT）XLATE（変換）テーブルの両方を使用します。宛先 IP 変換対象トラフィック、つまり、未変換のトラフィックを処理するために、システムは既存の XLATE またはスタティック変換を検索して、出力インターフェイスを選択します。

選択プロセスは、次の手順に従っています。

1. 宛先 IP 変換 XLATE がすでに存在する場合、出力インターフェイスはルーティング テーブルではなく、XLATE テーブルから決定されます。
2. 宛先 IP 変換 XLATE が存在しないが、一致するスタティック NAT 変換が存在する場合は、出力インターフェイスはスタティック NAT ルールから決定され、XLATE が作成され、ルーティング テーブルは使用されません。

3 宛先 IP 変換 XLATE が存在せず、一致するスタティック変換がない場合は、パケットの宛先 IP は変換されません。システムは、出力インターフェイスを選択するためにルートをルックアップしてこのパケットを処理し、その後、送信元 IP 変換が実行されます（必要な場合）。

正規のダイナミック アウトバウンド NAT の場合、初期発信パケットはルート テーブルを使用してルーティングされ、その後、XLATE が作成されます。着信リターン パケットは、既存の XLATE のみを使用して転送されます。スタティック NAT の場合、宛先変換済みの着信パケットは常に、既存の XLATE またはスタティック変換ルールを使用して転送されます。

出力インターフェイスの選択後、選択した出力インターフェイスに属する適切なネクスト ホップを見つけるために、追加のルートルックアップが実行されます。ルーティングテーブルに、選択したインターフェイスに明示的に属するルートがないと、異なる出力インターフェイスに属する所定の宛先ネットワークへの別のルートが存在する場合でも、パケットはドロップされ、レベル 6 診断 syslog メッセージ 110001（ホストへのルートがない）が生成されます。選択した出力インターフェイスに属するルートが見つかった場合は、パケットは対応するネクスト ホップに転送されます。

ルーティング テーブルとルートの選択

NAT XLATEs とルールによって出力インターフェイスが決定されない場合、システムはルーティング テーブルを使用してパケットのパスを決定します。

ルーティング テーブルのルートには、特定のルートに相対的な優先順位を提供する、「アドミニストレーティブ ディスタンス」と呼ばれるメトリックが含まれています。パケットが複数のルート エントリに一致する場合、ディスタンスが最小のものが使用されます。直接接続ネットワーク（インターフェイスで定義されるもの）のディスタンスは 0 であるため、常に優先されます。スタティック ルートのデフォルト ディスタンスは 1 ですが、1 ～ 254 までの任意のディスタンスでそれらを作成できます。

特定の宛先を識別するルートは、デフォルト ルート（宛先が 0.0.0.0/0 である）よりも優先されます。

転送の決定方法

転送は次のように決定されます。

- 宛先がルーティング テーブル内のエントリと一致しない場合、パケットはデフォルト ルートに指定されたインターフェイスを介して転送されます。デフォルト ルートが設定されていない場合、パケットは廃棄されます。
- 宛先がルーティングテーブル内の単一のエントリと一致する場合、パケットはそのルートに関連付けられたインターフェイスを介して転送されます。
- 宛先がルーティングテーブル内の複数のエントリに一致する場合、パケットは、ネットワーク プレフィックス長がより長いルートに関連付けられたインターフェイスから転送されます。

たとえば、192.168.32.1宛てのパケットが、ルーティングテーブル内の次のルートのインターフェイスに到達したものとします。

- 192.168.32.0/24 ゲートウェイ 10.1.1.2
- 192.168.32.0/19 ゲートウェイ 10.1.1.3

この場合、192.168.32.1は192.168.32.0/24ネットワークに含まれるため、192.168.32.1宛てのパケットは10.1.1.2にダイレクトされます。ルーティング テーブル内の他のルートにも含まれますが、192.168.32.0/24がルーティング テーブル内で最長のプレフィックスを保持しています（24ビット対19ビット）。パケットを転送する場合は、より長いプレフィックスがより短いプレフィックスより常に優先されます。

（注） ルートの変更のために新しい類似の接続が異なる動作をする場合でも、既存の接続は継続して確立済みのインターフェイスを使用します。

スタティック ルートの設定

スタティックルートを定義して、システムのインターフェイスに直接接続されたネットワークにバインドされていないパケットの送信先をシステムに知らせます。

少なくとも1つのスタティック ルートが必要です。ネットワークのデフォルト ルートは0.0.0.0/0です。このルートで、既存のNAT Xlates（変換）、スタティックNATルール、またはその他のスタティック ルートでは出力インターフェイスを決定できないパケットの送信先を定義します。

デフォルトゲートウェイを使用してすべてのネットワークに到達できない場合は、他のスタティックルートが必要な場合があります。たとえば、通常、デフォルトルートは外部インターフェイスの上流に位置するルータを通過します。デバイスに直接接続されていない追加の内部ネットワークがあり、デフォルト ゲートウェイを介してそれらのネットワークにアクセスできない場合、それらの各内部ネットワークのスタティック ルートが必要です。

システムインターフェイスに直接接続されているネットワークのスタティックルートは定義できません。それらのルートはシステムによって自動的に作成されます。

手順

ステップ1 デバイス、[ルーティング（Routing）] サマリでリンクをクリックします。

ステップ2 [スタティック ルーティング（Static Routing）]ページで、次のいずれかを実行します。

- 新しいルートを追加するには、[+] > [スタティック ルートの追加（Add Static Route）] をクリックします。
- 編集するルートの編集アイコン（）をクリックします。

ルートが不要になった場合は、削除するルートのごみ箱アイコンをクリックします。

ステップ 3 ルートのプロパティを設定します。

[プロトコル（Protocol）]

ルートが [IPv4]アドレス用か、[IPv6] アドレス用かを選択します。

[ゲートウェイ（Gateway）]

ゲートウェイの IP アドレスを特定するホスト 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。

[インターフェイス（Interface）]

トラフィックの送信を行う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、このインターフェイスを介してアクセスできる必要があります。

ブリッジ グループの場合、メンバー インターフェイスではなく、ブリッジ グループ インターフェイス（BVI）のルートを設定します。

[メトリック（Metric）]

ルートのアドミニストレーティブ ディスタンス（1 ~ 254）。スタティック ルートのデフォルトは 1 です。インターフェイスとゲートウェイの間に追加のルータがある場合、アドミニストレーティブ ディスタンスとしてホップの数を入力します。

アドミニストレーティブ ディスタンスは、ルートの比較に使用されるパラメータです。低い番号の方がそのルートに与えられる優先順位が高くなります。接続されたルート（デバイスのインターフェイスに直接接続されているネットワーク）は、常にスタティック ルートよりも優先されます。

[ネットワーク（Network）]

このルートのゲートウェイを使用する必要がある宛先ネットワークまたはホストを特定するネットワーク オブジェクトを選択します。

デフォルト ルートを定義するには、任意の定義済み ipv4 または ipv6 ネットワーク オブジェクトを使用するか、0.0.0.0/0（IPv4）ネットワークまたは ::/0（IPv6）ネットワークのオブジェクトを作成します。

ステップ 4 [OK]をクリックします。

ルーティングのモニタリング

ルーティングをモニタしてトラブルシュートするには、デバイスの CLI にログインして次のコマンドを使用します。

- **show route**：直接接続ネットワークのルートを含む、データ インターフェイスのルーティング テーブルが表示されます。

- **show ipv6 route**：直接接続ネットワークのルートを含む、データ インターフェイスの IPv6 ルーティング テーブルが表示されます。
- **show network**：管理ゲートウェイを含む、仮想管理インターフェイスの設定が表示されます。仮想インターフェイス経由のルーティングは、データ インターフェイスを管理ゲートウェイとして指定している場合を除き、データ インターフェイスのルーティング テーブルでは処理されません。
- **show network-static-routes**：**configure network static-routes** コマンドを使用して仮想管理インターフェイス用に設定されているスタティック ルートが表示されます。通常、ほとんどの場合のルーティングは管理ゲートウェイで管理できるため、スタティック ルートは存在しません。これらのルートはデータ インターフェイス上のトラフィックには使用できません。