WSA へトラフィックを転送するには、Cisco マルチレイヤ スイッチまたはルータでどのようにポリシーベース ルーティング（PBR）を構成しますか。

目次

質問：

WSA へトラフィックを転送するには、Cisco マルチレイヤ スイッチまたはルータでどのようにポリシーベース ルーティング（PBR）を構成しますか。

環境： Cisco Web セキュリティ アプライアンス（WSA）、透過モード- L4 スイッチ

WSA が L4 スイッチを使用して透過モードで設定されるとき、設定は WSA で必要とされません。 リダイレクションは L4 スイッチ制御されます（またはルータ）によって。

WSA に Webトラフィックをリダイレクトするのに Policy Based Routing（PBR）を使用することは可能性のあるです。 これは正しいトラフィックと（TCP ポートに基づいて）一致することおよび WSA にこのトラフィックをリダイレクトするようにルータ/スイッチに指示することによって実現します。

次の例では、WSA のデータ/プロキシ インターフェイスはマルチレイヤ スイッチ/ルータの専用 VLAN インターフェイスに（設定による M1 か P1）あります（VLAN 3）およびインターネット ルータは専用VLAN インターフェイスに同様にあります（Vlan4）。 クライアントは Vlan1 および Vlan2 にあります。

初期設定（表示される関連した部分だけ）
interface Vlan1 desc ユーザ VLAN 1 ip address 10.1.1.1 255.255.255.0 !! インターフェイス Vlan2 desc ユーザ VLAN 2 ip address 10.1.2.1 255.255.255.0 !! インターフェイス Vlan3 desc Cisco WSA 専用VLAN IP アドレス 192.168.1.1 255.255.255.252

```
!!
インターフェイス Vlan4
desc インターネットルータ 専用VLAN
IP アドレス 192.168.2.1 255.255.255.252
!!
IP ルート 0.0.0.0 0.0.0.0 192.168.2.2
```

上の 192.168.1.2 の IP アドレスを持っている例および Cisco WSA を与えられて Policy Based Routing (PBR) を設定する次のコマンドを追加します:

ステップ 1： Webトラフィックを定義して下さい

```
!! HTTPトラフィックを一致する
access-list 100 割り当て TCP 10.1.1.0 0.0.0.255 eq 80
access-list 100 割り当て TCP 10.1.2.0 0.0.0.255 eq 80
!! 一致 HTTPS トラフィック
access-list 100 割り当て TCP 10.1.1.0 0.0.0.255 eq 443
access-list 100 割り当て TCP 10.1.2.0 0.0.0.255 eq 443
```

ステップ 2： パケットがどこに出力されるか制御するためにルート マップを定義して下さい。

```
ルート マップ ForwardWeb 割り当て 10
match ip address 100
set ip next-hop 192.168.1.2
```

ステップ 3： **正しいインターフェイスにルート マップを加えて下さい。**

```
!! これがソースインターフェイス ( クライアント側 ) に適用する必要があることに注目して下さい
interface Vlan1
IP ポリシー ルート マップ ForwardWeb
!!
インターフェイス Vlan2
IP ポリシー ルート マップ ForwardWeb
```

注: トラフィック リダイレクション (PBR) のこの方式にいくつかの制限があります。 この方式における主要な問題はアプライアンスが到達可能でなくてもトラフィックが WSA に常にリダイレクトされることです (ネットワーク上の問題がたとえば原因で)。 このように、オプション上の失敗がありません。

回避策にこの不足、次のどちらかを設定することができます:

1. Ciscoルータを使用する場合の**トラッキング オプションの PBR**。 この機能がトラフィックをリダイレクトする前にネクスト ホップのアベイラビリティを確認するのに使用されています。

   次の技術情報のより多くの詳細:
   [複数のトラッキング オプション機能を使用したポリシー ベース ルーティングの設定例]
2. オプションをトラッキングして Cisco Catalyst スイッチで利用できてであってはなりません。 ただし、利用可能な高度回避策が同じ動作を実現させるためにあります。

   詳細は次の Cisco Wiki で見つけることができます:

Catalyst 3xxx スイッチ用のトラッキングの Policy Based Routing（PBR） - EEM を使用する回避策