MPLS/VPN ネットワークでのルートの漏洩

内容

概要

このドキュメントでは、MPLS/VPN 環境でルート リークの設定例について説明します。

前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

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、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、「シスコ テクニカル ティップスの表記法」を参照してください。

設定

このセクションでは、次の 2 つの設定例について説明します。

- グローバル ルーティング テーブルから VPN routing/forwarding instance (VRF; ルーティング/フォワーディング インスタンス) へのルートの漏洩、および VRF からグローバル ルーティング テーブルへのルートの漏洩
- 異なる VRF 間でのルートの漏洩

注：このドキュメントのコマンドに関する詳細については、Command Lookup Tool(登録ユーザ専用)を使用してください。

グローバル ルーティング テーブルから VRF へのルートの漏洩と、VRF からグローバル ルーティング テーブルへのルートの漏洩

この設定では、グローバル ルーティング テーブルから VRF へのルートの漏洩と、VRF からグローバル ルーティング テーブルへのルートの漏洩について説明します。

ネットワーク図

この設定では、次のネットワーク設定を使用します。

コンフィギュレーション

この例では、グローバル ルーティング テーブルから、VRF にあるネットワーク管理システム (NMS) ステーションにアクセスしています。provider edge (PE; プロバイダー エッジ) ルータと、プロバイダー (P) ルータは、VRF にある NMS 端末 (10.0.2.2) に netflow 情報をエクスポートする必要があります。10.0.2.2 には、PE-4 の VRF インターフェイスから到達可能です。

グローバルテーブルから10.0.2.0/30にアクセスするには、VRFインターフェイスを指す10.0.2.0/30へのスタティックルートがPE-4に導入されます。このスタティックルートは、Interior Gateway Protocol(IGP)を介してすべてのPEおよびPルータに再配布されます。これによって、すべての PE ルータと P ルータが PE-4 経由で 10.0.2.0/30 に到達できるようになります。

スタティックな VRF ルートも追加されます。スタティックな VRF ルートは、この NMS 端末にトラフィックを送信するグローバル ネットワーク内のサブネットを指します。この追加がない場合、PE-4 は、NMS ステーションから発信され VRF インターフェイスで受信されるトラフィックをドロップします。さらに、PE-4 は NMS ステーションに `ICMP:host unreachable rcv`

このセクションでは、次の設定を使用します。

- PE-4

PE-4

```
!
ip cef
!
ip vrf vpn2
rd 200:1
route-target export 200:1
route-target import 200:1
!
interface Serial1/0
ip address 10.1.2.5 255.255.255.252
no ip directed-broadcast
!
interface Serial2/0
ip vrf forwarding vpn2
ip address 10.0.2.1 255.255.255.0
no ip directed-broadcast
!
ip classless
ip route 10.0.2.0 255.255.255.252 Serial2/0
ip route vrf vpn2 10.1.2.4 255.255.255.252 Serial1/0
!
```

ここで、スタティック ルートをあらゆる IGP に再配布して、ネットワーク全体にアナウンスされるようにすることができます。VRF インターフェイスが LAN インターフェイス (イーサネットなど) の場合も、同様な設定を適用できます。 この場合の正確な設定コマンドは次のとおりです。

```
ip route 10.0.2.0 255.255.255.252 Ethernet2/0 10.0.2.2
```

注：インターフェイス名の後に設定されたIPアドレスは、解決するアドレスを知るために、アドレス解決プロトコル(ARP)でのみ使用されます。

注：4500シリーズのスイッチでは、VRFテーブル内のスタティックARPエントリを、それぞれのネクストホップアドレスに対して設定する必要があります。

注：デフォルトでは、Cisco IOS®ソフトウェアはスタティックVRFルートを設定どおりに受け入れます。このことは、異なる VRF 間でのルートの漏洩を招く場合があるため、セキュリティが危うくなる可能性があります。このようなスタティック VRF ルートの導入を防ぐには、no ip route static inter-vrf コマンドを使用します。no ip route static inter-vrf コマンドの詳細については、『MPLS バーチャル プライベート ネットワーク (VPN)』を参照してください。

確認

このセクションでは、設定が正常に動作しているかどうかを確認するための情報について説明します。

一部の show コマンドはアウトプット インタープリタ ツールによってサポートされています (登録ユーザ専用) 。このツールを使用することによって、show コマンド出力の分析結果を表示できます。

- **show ip route 10.0.2.0：指定した IP アドレスのルーティング エントリを表示します。**
- **show ip route vrf vpn2 10.1.2.4**：指定されたIPアドレスのVRFルーティングエントリを表示します。

```
PE-4# show ip route 10.0.2.0
```

```
Routing entry for 10.0.2.0/30
Known via "static", distance 1, metric 0 (connected)
Routing Descriptor Blocks:
* directly connected, via Serial2/0
Route metric is 0, traffic share count is 1

PE-4# show ip route vrf vpn2 10.1.2.4

Routing entry for 10.1.2.4/30
Known via "static", distance 1, metric 0 (connected)
Redistributing via bgp 1
Advertised by bgp 1
Routing Descriptor Blocks:
* directly connected, via Serial1/0
Route metric is 0, traffic share count is 1
```

異なる VRF 間でのルートの漏洩

この設定では、異なる VRF 間でのルートの漏洩について説明します。

ネットワーク図

この設定では、次のネットワーク ダイアグラムを使用します。

コンフィギュレーション

この方式はサポートされていないため、パケットはルータによってルーティングされないため、VRF間で各プレフィクスをアドバタイズするように2つのスタティックルートを設定することはできません。VRF 間でのルートの漏洩を実現するには、ルートターゲットのインポート機能を使用して、ルータ上で Border Gateway Protocol（BGP; ボーダー ゲートウェイ プロトコル）を有効にする必要があります。BGP ネイバーは不要です。

このセクションでは、次の設定を使用します。

- PE-4

PE-4

```
!
ip vrf vpn1
 rd 100:1
 route-target export 100:1
 route-target import 100:1
 route-target import 200:1
!
ip vrf vpn2
 rd 200:1
```

```
 route-target export 200:1
 route-target import 200:1
 route-target import 100:1
!
interface Serial1/0
 ip vrf forwarding vpn1
 ip address 10.1.2.5 255.255.255.252
 no ip directed-broadcast
!
interface Serial2/0
 ip vrf forwarding vpn2
 ip address 10.0.2.1 255.255.255.0
 no ip directed-broadcast
router bgp 1
!
address-family ipv4 vrf vpn2
 redistribute connected
 !
address-family ipv4 vrf vpn1
 redistribute connected
!
```

確認

このセクションでは、設定のトラブルシューティングを行うための情報について説明します。

一部の show コマンドはアウトプット インタープリタ ツールによってサポートされています（登録ユーザ専用）。このツールを使用することによって、show コマンド出力の分析結果を表示できます。

- **show ip bgp vpnv4 all**:BGPで学習されたすべてのVPNv4プレフィックスを表示します。

```
PE-4# show ip bgp vpnv4 all

BGP table version is 13, local router ID is 7.0.0.4
Status codes: s suppressed, d damped, h history, * valid,
> best, i - internal, r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

Network Next Hop Metric LocPrf Weight Path
Route Distinguisher: 100:1 (default for vrf vpn1)
*> 10.0.2.0/24 0.0.0.0 0 32768 ?
*> 10.1.2.4/30 0.0.0.0 0 32768 ?
Route Distinguisher: 200:1 (default for vrf vpn2)
*> 10.0.2.0/24 0.0.0.0 0 32768 ?
*> 10.1.2.4/30 0.0.0.0 0 32768 ?
```

注：VRF間でルートを漏出する別の方法は、PE-4ルータ上の2つのイーサネットインターフェイスを接続し、各イーサネットインターフェイスをいずれかのVRFに関連付けることです。VRF テーブルでは、それぞれのネクスト ホップ アドレスに対して、スタティックな ARP エントリを設定する必要があります。ただし、これは VRF 間のルートの漏洩に対する推奨ソリューションではありません。前述の BGP の手法が推奨ソリューションです。

トラブルシュート

現在、この設定に関する特定のトラブルシューティング情報はありません。

関連情報

- MPLS に関するサポートページ
- テクニカルサポートとドキュメント - Cisco Systems