Route Leaking en las redes MPLS/VPN

Contenido

Introducción

Este documento contiene ejemplo de configuraciones para la fuga de ruta en un entorno MPLS/VPN.

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Para obtener más información sobre las convenciones del documento, consulte las Convenciones de Consejos Técnicos de Cisco.

Configurar

Esto secciona contiene estos dos ejemplos de configuración:

- Fuga de rutas desde una tabla de ruteo global hacia una instancia de ruteo/reenvío (VRF) de VPN y fuga de rutas desde una instancia de VRF hacia una tabla de ruteo global
- Fuga de ruta entre diferentes VRF

Nota: Para encontrar la información adicional sobre los comandos en este documento, utilice la herramienta de búsqueda de comandos (clientes registrados solamente).

Route Leaking de una tabla de Global Routing en un VRF y Route Leaking de un VRF en una tabla de Global Routing

Esta configuración describe Route Leaking de una tabla de Global Routing en un VRF y Route Leaking de un VRF en una tabla de Global Routing.

Diagrama de la red

Esta configuración utiliza esta configuración de red:

Configuración

En este ejemplo, una estación del sistema de administración de red (NMS) situada en un VRF se accede de la tabla de Global Routing. Los routers de borde del proveedor (PE) y los routers del proveedor (P) deben exportar la información de netflow a una estación NMS (10.0.2.2) en un VRF. Se puede acceder a 10.0.2.2 a través de la interfaz VRF en PE-4.

Para acceder 10.0.2.0/30 de la tabla global, una Static ruta a 10.0.2.0/30 que señala de la interfaz VRF se introduce en el PE-4. Esta Static ruta entonces se redistribuye vía el Interior Gateway Protocol (IGP) a todo el Routers PE y P. Esto asegura que todos los routers PE y P puedan alcanzar 10.0.2.0/30 vía PE-4.

Una ruta estática VRF también se agrega. Los puntos de ruta estáticos VRF a la subred en la red global que envía el tráfico a esta estación NMS. Sin esta adición, el PE-4 cae el tráfico, de la estación NMS, que se recibe en la interfaz VRF; y el PE-4 envía el `ICMP: imposible acceder al host mensaje rcv a la` estación NMS.

Esta sección usa esta configuración:

- 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 !
```

Las Static rutas se pueden ahora redistribuir en cualquier IGP para ser network de par en par anunciado. Lo mismo se aplica si la interfaz VRF es una interfaz LAN (por ejemplo, los Ethernetes). El comando de configuración exacta para ése es:

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

Nota: La dirección IP configurada después de que el nombre de la interfaz sea utilizado solamente por el Address Resolution Protocol (ARP), para conocer qué direccionamiento para resolver.

Nota: Para los 4500 Series Switch, usted debe configurar las entradas ARP estáticas en las tablas VRF para las direcciones del salto siguiente respectivas.

Nota: Por abandono, el software de Cisco IOS® valida las rutas estáticas VRF según lo configurado. Esto pudo comprometer la Seguridad porque puede ser que introduzca Route Leaking entre diversos VRF. Usted puede utilizar el **comando no ip route static inter-vrf** de prevenir la instalación de tales rutas estáticas VRF. Para obtener más información acerca del comando no ip route static inter-vrf, consulte Redes privadas virtuales (VPN) MPLS.

Verificación

Esta sección proporciona la información para confirmar que su configuración está trabajando correctamente.

La herramienta Output Interpreter (sólo para clientes registrados) permite utilizar algunos comandos “show” y ver un análisis del resultado de estos comandos.

- **muestre la ruta de IP 10.0.2.0** — Visualiza una entrada de ruteo de la dirección IP especificada.
- **muestre el vrf vpn2 10.1.2.4 de la ruta de IP** — Visualiza una entrada de ruteo de la dirección IP especificada VRF.

```
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
```

Fuga de ruta entre diferentes VRF

Esta configuración está relacionada con las fugas de rutas entre los diferentes VRF.

Diagrama de la red

Esta configuración utiliza este diagrama de red:

Configuración

Usted no puede configurar dos Static rutas para hacer publicidad de cada prefijo entre los VRF, porque este método no se soporta — los paquetes no serán ruteados por el router. Para alcanzar Route Leaking entre los VRF, usted debe utilizar las funciones de la importación de la ruta-blanco y habilitar el Border Gateway Protocol (BGP) en el router. No se requiere a ningún vecino BGP.

Esta sección usa esta configuración:

- 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 !
```

Verificación

Esta sección proporciona la información para resolver problemas en su configuración.

La herramienta Output Interpreter (sólo para clientes registrados) permite utilizar algunos comandos “show” y ver un análisis del resultado de estos comandos.

- **muestre BGP vpnv4 todo del IP** — Visualiza todos los prefijos del VPNv4 que sean doctos vía

el BGP.

```
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 ?
```

Nota: La otra manera de escaparse las rutas entre los VRF es conectar juntas dos interfaces de Ethernet en el router PE-4 y asociar cada interfaz de Ethernet con uno de los VRF. Usted también debe configurar las entradas ARP estáticas en las tablas VRF para las direcciones del salto siguiente respectivas. Sin embargo, esto no es una solución recomendada para Route Leaking entre los VRF; la técnica previamente descrita BGP es la solución recomendada.

Troubleshooting

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Información Relacionada

- Página de soporte de MPLS
- Soporte técnico y documentación - Cisco Systems