Weiterleitung in MPLS/VPN-Netzwerken

Inhalt

Einführung

Dieses Dokument enthält Beispielkonfigurationen für das Route Leaking in einer MPLS/VPN-Umgebung.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions .

Konfigurieren

Dieser Abschnitt enthält die folgenden beiden Konfigurationsbeispiele:

- Route Leaking aus einer globalen Routing-Tabelle in eine VPN-Routing/Forwarding-Instanz (VRF) und Route Leaking von einer VRF-Instanz in eine globale Routing-Tabelle
- Route Leaking zwischen verschiedenen VRFs

Hinweis: Um weitere Informationen zu den Befehlen in diesem Dokument zu erhalten, verwenden Sie das Command Lookup Tool (nur registrierte Kunden).

Route Leaking from a Global Routing Table to a VRF and Route Leaking from a VRF to a Global Routing Table

Diese Konfiguration beschreibt das Route Leaking von einer globalen Routing-Tabelle in eine VRF-Instanz und das Route Leaking von einer VRF-Instanz in eine globale Routing-Tabelle.

Netzwerkdiagramm

Diese Konfiguration verwendet die folgende Netzwerkeinrichtung:

Konfiguration

In diesem Beispiel wird auf eine Network Management System (NMS)-Station in einer VRF-Instanz von der globalen Routing-Tabelle aus zugegriffen. Die Provider Edge (PE)-Router und Provider (P)-Router müssen die NetFlow-Informationen in eine NMS-Station (10.0.2.2) in einer VRF-Instanz exportieren. 10.0.2.2 ist über eine VRF-Schnittstelle auf PE-4 erreichbar.

Um von der globalen Tabelle auf 10.0.2.0/30 zuzugreifen, wird für PE-4 eine statische Route zu 10.0.2.0/30 eingeführt, die auf die VRF-Schnittstelle verweist. Diese statische Route wird dann über Interior Gateway Protocol (IGP) an alle PE- und P-Router verteilt. Dadurch wird sichergestellt, dass alle PE- und P-Router über PE-4 10.0.2.0/30 erreichen können.

Eine statische VRF-Route wird ebenfalls hinzugefügt. Die statische VRF-Route verweist auf das Subnetz im globalen Netzwerk, das den Datenverkehr an diese NMS-Station sendet. Ohne diese Hinzufügung verwirft der PE-4 den auf der VRF-Schnittstelle empfangenen Datenverkehr von der NMS-Station. und PE-4 sendet den `ICMP: Host unreachable rcv-`Nachricht an die NMS-Station.

In diesem Abschnitt wird diese Konfiguration verwendet:

- 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
!
```

Die statischen Routen können jetzt auf jedes IGP verteilt werden, das netzwerkweit angekündigt werden soll. Das Gleiche gilt, wenn es sich bei der VRF-Schnittstelle um eine LAN-Schnittstelle handelt (z. B. Ethernet). Der genaue Konfigurationsbefehl hierfür lautet:

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

Hinweis: Die IP-Adresse, die nach dem Schnittstellennamen konfiguriert wird, wird nur vom Address Resolution Protocol (ARP) verwendet, um die Adresse zu ermitteln, die aufgelöst werden muss.

Hinweis: Bei Switches der Serie 4500 müssen Sie statische ARP-Einträge in den VRF-Tabellen für die jeweiligen Next-Hop-Adressen konfigurieren.

Hinweis: Die Cisco IOS®-Software akzeptiert standardmäßig statische VRF-Routen wie konfiguriert. Dies kann die Sicherheit gefährden, da es zu Route Leaking zwischen verschiedenen VRFs kommen kann. Sie können den Befehl **no ip route static inter-vrf** verwenden, um die Installation solcher statischen VRF-Routen zu verhindern. Weitere Informationen zum **statischen Inter-VRF-**Befehl **no ip route finden Sie unter** MPLS Virtual Private Networks (VPNs).

Überprüfen

Dieser Abschnitt enthält Informationen zur Bestätigung, dass Ihre Konfiguration ordnungsgemäß funktioniert.

Bestimmte **show**-Befehle werden vom Output Interpreter Tool unterstützt (nur registrierte Kunden), mit dem Sie eine Analyse der **show**-Befehlsausgabe anzeigen können.

- **show ip route 10.0.2.0**: Zeigt einen angegebenen IP-Adressen-Routing-Eintrag an.
- **show ip route vrf vpn2 10.1.2.4**: Zeigt einen angegebenen VRF-Routing-Eintrag für die IP-Adresse an.

```
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
```

Route Leaking zwischen verschiedenen VRFs

Diese Konfiguration beschreibt das Route Leaking zwischen verschiedenen VRFs.

Netzwerkdiagramm

Diese Konfiguration verwendet dieses Netzwerkdiagramm:

Konfiguration

Sie können nicht zwei statische Routen konfigurieren, um jedes Präfix zwischen den VRFs anzukündigen, da diese Methode nicht unterstützt wird - Pakete werden vom Router nicht weitergeleitet. Um ein Route Leaking zwischen VRFs zu erreichen, müssen Sie die Importfunktion von route-target verwenden und Border Gateway Protocol (BGP) auf dem Router aktivieren. Es ist kein BGP-Nachbar erforderlich.

In diesem Abschnitt wird diese Konfiguration verwendet:

- 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
!
```

Überprüfen

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

Bestimmte **show**-Befehle werden vom Output Interpreter Tool unterstützt (nur registrierte Kunden), mit dem Sie eine Analyse der **show**-Befehlsausgabe anzeigen können.

- **show ip bgp vpnv4 all**: Zeigt alle VPNv4-Präfixe an, die über BGP abgerufen werden.

```
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 ?
```

Hinweis: Die andere Möglichkeit, Routen zwischen VRFs zu durchlaufen, besteht darin, zwei Ethernet-Schnittstellen am PE-4-Router miteinander zu verbinden und jede Ethernet-Schnittstelle mit einer der VRFs zu verknüpfen. Sie müssen außerdem statische ARP-Einträge in den VRF-Tabellen für die jeweiligen nächsten Hop-Adressen konfigurieren. Dies ist jedoch keine empfohlene Lösung für das Route Leaking zwischen VRFs. Die oben beschriebene BGP-Technik ist die empfohlene Lösung.

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Zugehörige Informationen

- MPLS-Support-Seite
- Technischer Support und Dokumentation - Cisco Systems