Configuración y verificación de la fuga de VRF de VXLAN en Nexus 9000

Contenido

Introducción

Este documento describe cómo configurar y verificar la fuga de VRF en un entorno VXLAN.

Antecedentes

En un entorno VXLAN (LAN extensible virtual), la conexión de hosts VXLAN a hosts externos desde el fabric a menudo requiere el uso de dispositivos con fugas VRF y Border Leaf.

La fuga de VRF es crucial para permitir la comunicación entre los hosts VXLAN y los hosts externos, al tiempo que se mantiene la segmentación y la seguridad de la red.

El dispositivo Border Leaf sirve como una puerta de enlace entre el fabric VXLAN y las redes externas, y desempeña un papel fundamental a la hora de facilitar esta comunicación.

La importancia de la fuga de VRF en este escenario se puede resumir con las siguientes declaraciones:

1. Interconexión con redes externas: la fuga de VRF permite que los hosts VXLAN del fabric se comuniquen con los hosts externos fuera del fabric. Esto permite el acceso a recursos, servicios y aplicaciones alojados en redes externas, como Internet u otros Data Centers.

2. Segmentación y aislamiento de la red: la fuga de VRF mantiene la segmentación y el aislamiento de la red dentro del fabric VXLAN, a la vez que permite la comunicación selectiva con redes externas. Esto garantiza que los hosts VXLAN permanezcan aislados entre sí en función de sus asignaciones VRF, al tiempo que pueden acceder a los recursos externos según sea necesario.

3. Aplicación de políticas: la fuga de VRF permite a los administradores aplicar políticas de red y controles de acceso para el tráfico que fluye entre hosts VXLAN y hosts externos. Esto garantiza que la comunicación utilice políticas de seguridad predefinidas e impide el acceso no autorizado a recursos confidenciales.

4. Escalabilidad y flexibilidad: la fuga de VRF mejora la escalabilidad y flexibilidad de las implementaciones de VXLAN, ya que permite que los hosts de VXLAN se comuniquen sin problemas con los hosts externos. Permite la asignación dinámica y el uso compartido de recursos entre VXLAN y redes externas, adaptándose a los cambiantes requisitos de red sin interrumpir las configuraciones existentes.

El filtrado de rutas en la fuga de VRF (Virtual Routing and Forwarding) es crucial para mantener la seguridad de la red, optimizar la eficiencia del routing y evitar la fuga no intencionada de datos. La fuga de VRF permite la comunicación entre redes virtuales mientras se mantienen lógicamente separadas.

La importancia del filtrado de rutas en la fuga de VRF es importante y se puede resumir con las

siguientes declaraciones:

1. Seguridad: el filtrado de rutas garantiza que solo se filtran rutas específicas entre instancias de VRF, lo que reduce el riesgo de acceso no autorizado o de violaciones de datos. Al controlar qué rutas pueden cruzar los límites VRF, los administradores pueden aplicar políticas de seguridad y evitar que la información confidencial se exponga a entidades no autorizadas.

2. Aislamiento: los VRF están diseñados para proporcionar segmentación y aislamiento de la red, lo que permite a los diferentes arrendatarios o departamentos funcionar de forma independiente dentro de la misma infraestructura física. El filtrado de rutas en la fuga de VRF ayuda a mantener este aislamiento limitando el alcance de la propagación de rutas entre instancias de VRF, evitando la comunicación no intencionada y las posibles vulnerabilidades de seguridad.

3. Routing optimizado: el filtrado de rutas permite a los administradores filtrar selectivamente solo las rutas necesarias entre VRF, lo que optimiza la eficacia del routing y reduce el tráfico innecesario en la red. Al filtrar las rutas irrelevantes, los administradores pueden garantizar que el tráfico utilice las rutas más eficientes y, al mismo tiempo, minimizar la congestión y la latencia.

4. Utilización de recursos: mediante el filtrado de rutas, los administradores pueden controlar el flujo de tráfico entre instancias de VRF, lo que optimiza la utilización de recursos y la asignación de ancho de banda. Esto ayuda a evitar la congestión de la red y garantiza que los recursos críticos estén disponibles para aplicaciones o servicios prioritarios.

5. Conformidad: el filtrado de rutas en la fuga de VRF ayuda a las organizaciones a mantener el cumplimiento de los requisitos normativos y los estándares del sector. Al restringir la filtración de rutas solo a entidades autorizadas, las organizaciones pueden demostrar el cumplimiento de la normativa de protección de datos y garantizar la integridad de la información confidencial.

6. Control granular: el filtrado de rutas proporciona a los administradores un control granular sobre la comunicación entre instancias de VRF, lo que les permite definir políticas específicas basadas en sus requisitos únicos. Esta flexibilidad permite a las organizaciones adaptar sus configuraciones de red para satisfacer las necesidades de diferentes aplicaciones, usuarios o departamentos.

Prerequisites

Entorno VXLAN existente con un router de borde

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Plataforma NXOS

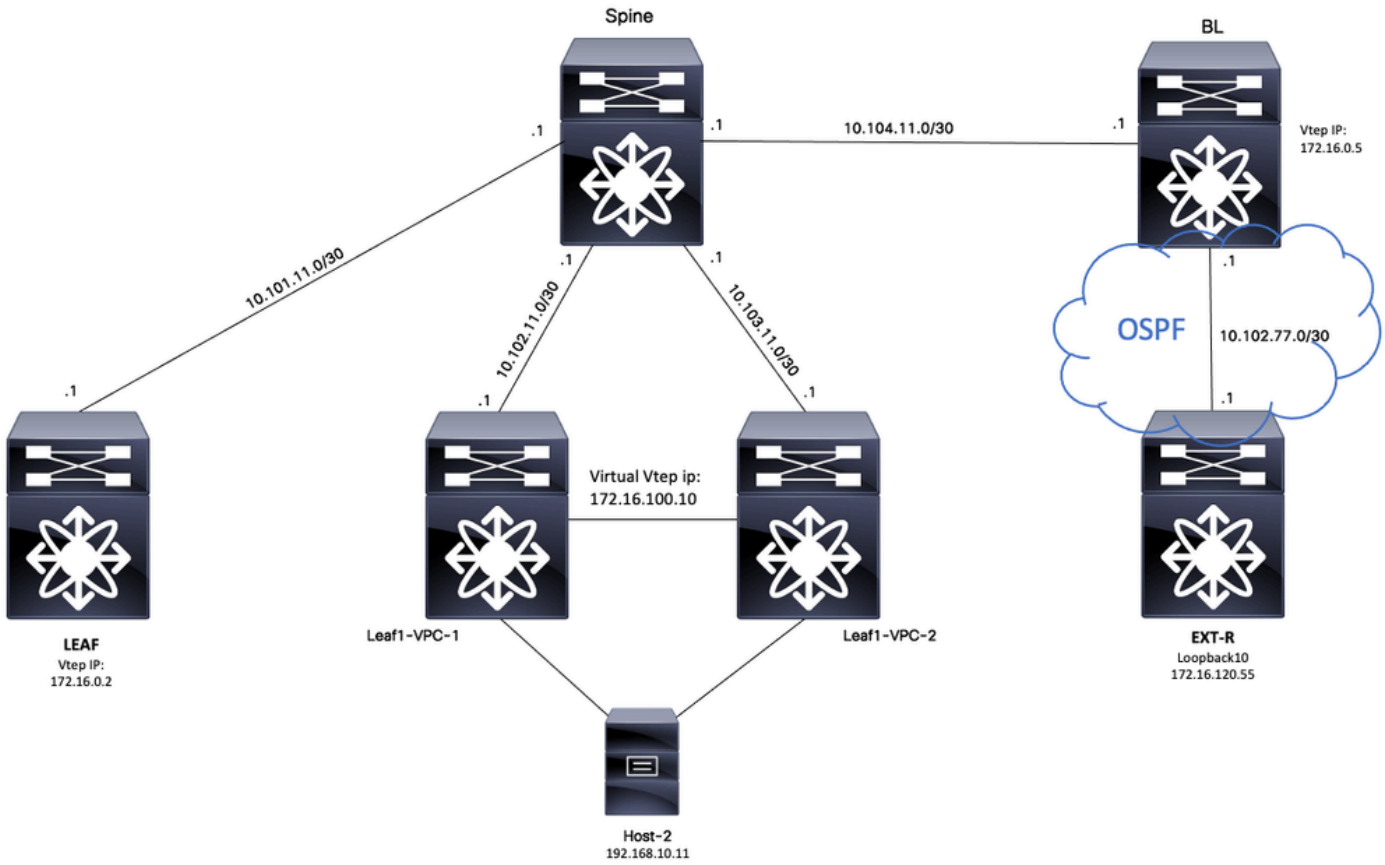
- VXLAN
- VRF
- BGP

Componentes Utilizados

Nombre	Platform	Versión
HOST-2	N9K-C92160YC-X	9.3(6)
Leaf-VPC-1	N9K-C93180YC-EX	9.3(9)
Leaf-VPC-2	N9K-C93108TC-EX	9.3(9)
HOJA	N9K-C9332D-GX2B	10.2(6)
BL	N9K-C934D-GX2A	10.2(5)
EXT-R	N9K-C934D-GX2A	10.2(3)
COLUMNA VERTEBRAL	N9K-C93108TC-FX3P	10.1(1)

"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 su red está activa, asegúrese de comprender el impacto potencial de cualquier comando".

Diagrama



Considerando BGP como una aplicación, BGP es la aplicación que se utiliza para realizar fugas entre VRFs

VRF predeterminado a Arrendatario-VRF

En este ejemplo, Border VTEP (BL) recibe 172.16.120.55 del dispositivo externo a través de OSFP en el VRF predeterminado que se filtrará al VRF de arrendatario.

Verificar tabla de ruteo

```
BL# sh ip route 172.16.120.55
IP Route Table for VRF "default"
'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%<string>' in via output denotes VRF <string>

172.16.120.55/32, ubest/mbest: 1/0
*via 10.105.100.2, Eth1/41.2, [110/2], 00:00:10, ospf-1, intra
```

Filtrar ruta

En NXOS se requiere un route-map como parámetro para filtrar y redistribuir rutas, para este

ejemplo se va a filtrar el prefijo 172.16.120.55/32.

Configurar

	Comando o acción	Propósito
Paso 1	BL# configure terminal Ingrese los comandos de configuración, uno por línea. Finalizar con CNTL/Z.	Ingresa en el modo de configuración.
Paso 2	BL(config)# ip prefix-list VXLAN-VRF-default-to-Tenant permit 172.16.120.55/32	Crear host coincidente de lista de prefijos.
Paso 3	BL(config)# route-map VXLAN-VRF-default-to-Tenant	Crear mapa de rutas.
Paso 4	BL(config-route-map)# match ip address prefix-list VXLAN-VRF-default-to-Tenant	Haga coincidir la lista de prefijos creada en el paso 2.

Importar ruta a BGP

Una vez que se verifica que la ruta existe en el VRF predeterminado, la ruta se debe importar al proceso BGP.

Configurar

	Comando o acción	Propósito
Paso 1	BL# configure terminal Ingrese los comandos de configuración, uno por línea. Finalizar con CNTL/Z.	Ingresa en el modo de configuración.
Paso 2	BL(config)# router bgp 65000	Ingresa en la configuración BGP.
Paso 3	BL(config-router)# address-family ipv4 unicast	Ingrese BGP address-family IPV4.

Paso 4	BL(config-router-af)# redistribute ospf 1 route-map VXLAN-VRF-default-to-Tenant	Redistribuya la ruta de OSPF a BGP mediante el route-map creado en el paso 3.

Verificar tabla BGP

```
BL(config-router-af)# show ip bgp 172.16.120.55
BGP routing table information for VRF default, address family IPv4 Unicast
BGP routing table entry for 172.16.120.55/32, version 16
Paths: (1 available, best #1)
Flags: (0x000002) (high32 00000000) on xmit-list, is not in urib

Advertised path-id 1
Path type: redist, path is valid, is best path, no labeled nexthop
AS-Path: NONE, path locally originated
0.0.0.0 (metric 0) from 0.0.0.0 (172.16.0.5)
Origin incomplete, MED 2, localpref 100, weight 32768
Extcommunity: OSPF RT:0.0.0.0:0:0
```

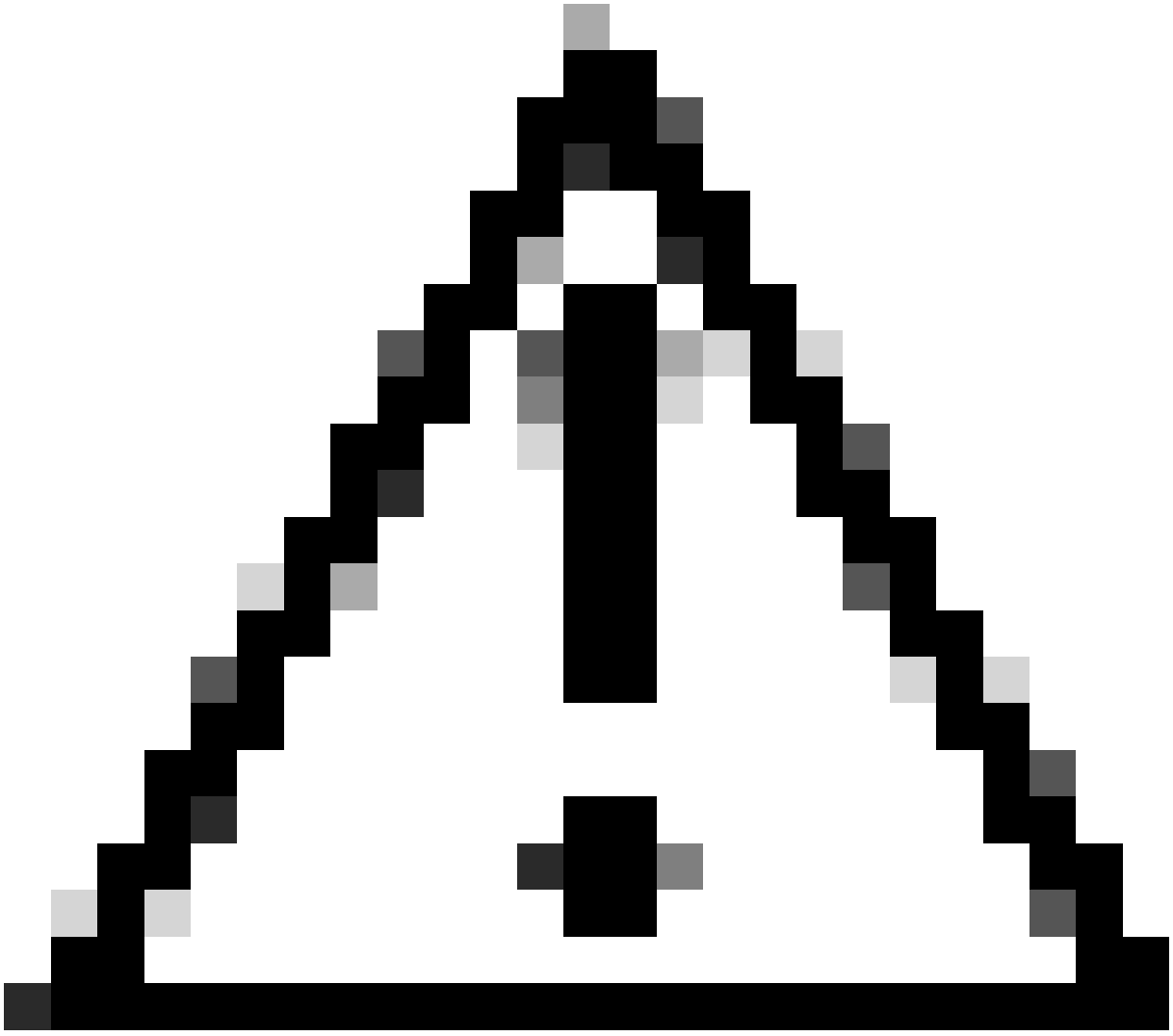
Importar ruta a VRF de arrendatario

Una vez que la ruta se importa a BGP, la ruta ahora se puede importar a VRF de destino (tenant-a).

Configurar

	Comando o acción	Propósito
Paso 1	BL(config)# vrf context tenant-a	Introduce la configuración VRF.
Paso 2	BL(config-vrf)# address-family ipv4 unicast	Introduce la familia de direcciones IPV4.
Paso 3	BL(config-vrf-af-ipv4)# import vrf default map VXLAN-VRF-default-to-Tenant advertise-vpn	Importar ruta de VRF predeterminada a arrendatario

		VRF anunciando VPN



Precaución: Por defecto, el número máximo de prefijos IP que se pueden importar desde el VRF por defecto a un VRF no por defecto es 1000 rutas. Este valor se puede cambiar con el comando VRF address-family IPV4: import vrf <number of prefixes> default map <route-map name> advertise-vpn.

Pasos de resumen

1. configure terminal
2. ip prefix-list VXLAN-VRF-default-to-Tenant permit 172.16.120.55/32
3. route-map VXLAN-VRF-default-to-Tenant
4. match ip address prefix-list VXLAN-VRF-default-to-Tenant
5. router bgp 65000
6. address-family ipv4 unicast

7. redistribute ospf 1 route-map VXLAN-VRF-default-to-Tenant
8. vrf context tenant-a
9. address-family ipv4 unicast
10. import vrf default map VXLAN-VRF-default-to-Tenant advertise-vpn

Verificación

Verifique que la ruta se importe a L2VPN.

```
BL# sh bgp l2vpn evpn 172.16.120.55
BGP routing table information for VRF default, address family L2VPN EVPN
Route Distinguisher: 172.16.0.5:3 (L3VNI 303030)
BGP routing table entry for [5]:[0]:[0]:[32]:[172.16.120.55]/224, version 38
Paths: (1 available, best #1)
Flags: (0x000002) (high32 00000000) on xmit-list, is not in l2rib/evpn
Multipath: Mixed

Advertised path-id 1
Path type: local, path is valid, is best path, no labeled nexthop
Gateway IP: 0.0.0.0
AS-Path: NONE, path locally originated
172.16.0.5 (metric 0) from 0.0.0.0 (172.16.0.5)
Origin incomplete, MED 2, localpref 100, weight 32768
Received label 303030
Extcommunity: RT:65000:303030 ENCAP:8 Router MAC:20cf.ae54.fa3b
OSPF RT:0.0.0.0:0:0

Path-id 1 advertised to peers:
10.104.11.1
```

Verificar que la ruta se importe al VRF de arrendatario

```
BL# sh ip route 172.16.120.55 vrf tenant-a
IP Route Table for VRF "tenant-a"
'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%<string>' in via output denotes VRF <string>

172.16.120.55/32, ubest/mbest: 1/0
*via 172.16.0.5%default, [200/2], 00:02:47, bgp-65000, internal, tag 65000, segid: 303030 tunnelid: 0xa
```

Arrendatario-VRF a VRF predeterminado

Para este ejemplo, Border VTEP (BL) recibe la ruta 192.168.10.11 a través de VXLAN en un VRF de arrendatario que se filtrará al VRF predeterminado.

Verificar tabla de ruteo

```
BL# sh ip route 192.168.10.11 vrf tenant-a
IP Route Table for VRF "tenant-a"
'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%<string>' in via output denotes VRF <string>

192.168.10.11/32, ubest/mbest: 1/0
*via 172.16.100.10%default, [200/0], 01:15:04, bgp-65000, internal, tag 65000, segid: 303030 tunnelid:
```

Filtrar ruta

En NXOS se requiere un route-map como parámetro para filtrar y redistribuir rutas, por este ejemplo se va a filtrar el prefijo 172.16.120.55/32.

Configurar

	Comando o acción	Propósito
Paso 1	BL# configure terminal Ingrese los comandos de configuración, uno por línea. Finalizar con CNTL/Z.	Ingresa en el modo de configuración.
Paso 2	BL(config)# ip prefix-list VXLAN-VRF-Tenant-to-default permit 192.168.10.11/32	Crear host coincidente de lista de prefijos.
Paso 3	BL(config)# route-map VXLAN-VRF-Tenant-to-default	Crear mapa de rutas.
Paso 4	BL(config-route-map)# match ip address prefix-list VXLAN-VRF-Tenant-to-default	Haga coincidir la lista de prefijos creada en el paso 2.

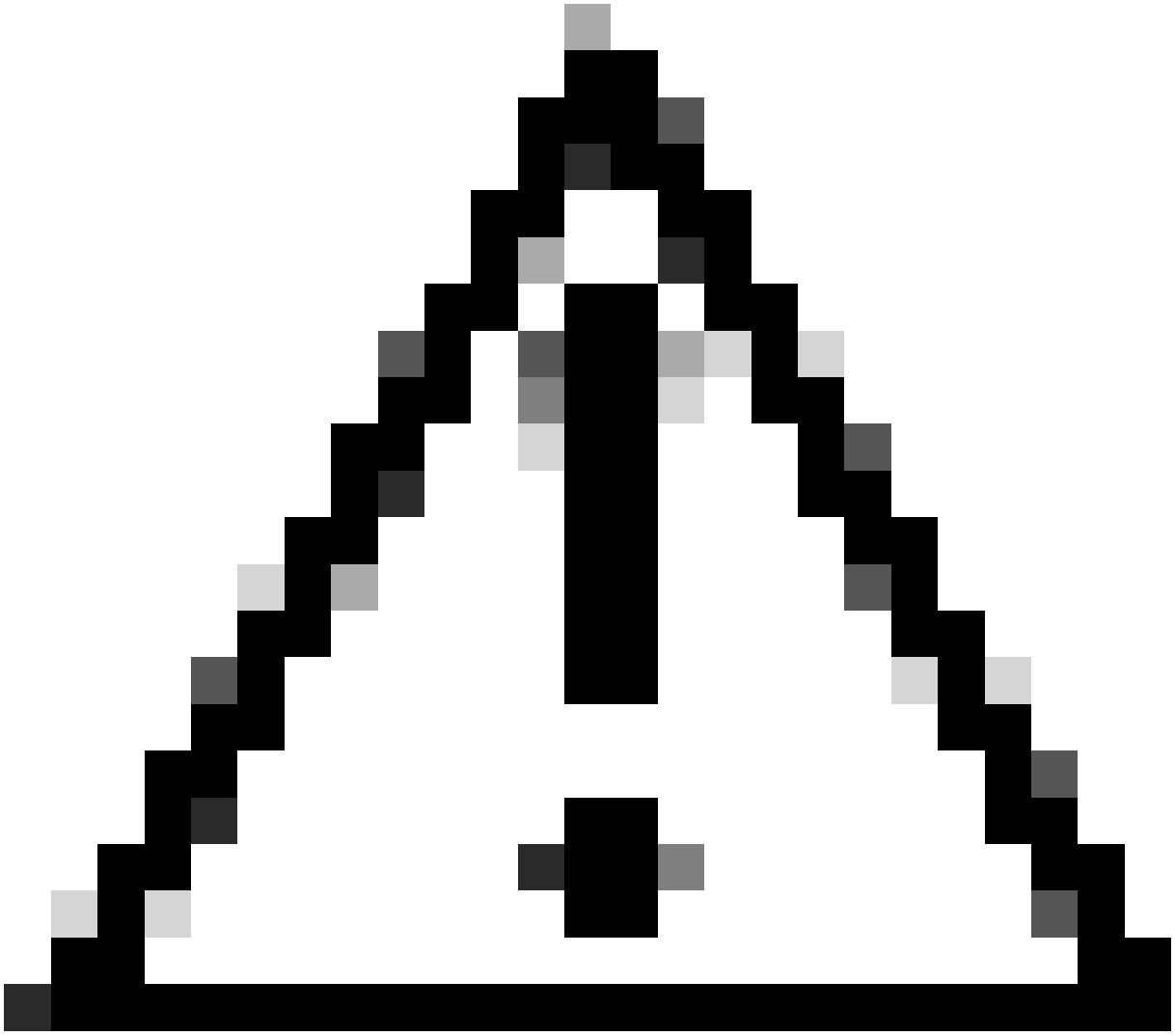
Exportar ruta a VRF predeterminado desde VRF de arrendatario a

Debido a que la ruta ya está en el proceso L2VPN BGP, sólo necesita ser exportada al VRF

predeterminado.

Configurar

	Comando o acción	Propósito
Paso 1	BL# configure terminal Ingrese los comandos de configuración, uno por línea. Finalizar con CNTL/Z.	Ingresa en el modo de configuración.
Paso 2	BL(config)# vrf context tenant-a	Introduce la configuración VRF.
Paso 3	BL(config-vrf)# address-family ipv4 unicast	Introduzca VRF address-family IPV4.
Paso 4	BL(config-vrf-af-ipv4)# export vrf default map VXLAN-VRF-Tenant-to-default allow-vpn	Ruta de exportación desde el VRF del arrendatario al VRF predeterminado que permite VPN



Precaución: Por defecto, el número máximo de prefijos IP que se pueden exportar desde el VRF no por defecto a un VRF por defecto es 1000 rutas. Este valor se puede cambiar con el comando VRF address-family IPV4: export vrf default <number of prefixes> map <route-map name> allow-vpn.

Pasos de resumen

1. configure terminal
2. ip prefix-list VXLAN-VRF-Tenant-to-default permit 192.168.10.11/32
3. route-map VXLAN-VRF-Tenant-to-default
4. match ip address prefix-list VXLAN-VRF-Tenant-to-default
5. vrf context tenant-a
6. address-family ipv4 unicast
7. export vrf default map VXLAN-VRF-Tenant-to-default allow-vpn

Verificación

Verifique que la ruta se importe a la familia de direcciones BGP IPV4 en el VRF predeterminado

```
BL(config-router-vrf-neighbor)# sh ip bgp 192.168.10.11
BGP routing table information for VRF default, address family IPv4 Unicast
BGP routing table entry for 192.168.10.11/32, version 55
Paths: (1 available, best #1)
Flags: (0x8000001a) (high32 00000000) on xmit-list, is in urib, is best urib route, is in HW

Advertised path-id 1
Path type: internal, path is valid, is best path, no labeled nexthop, in rib
Imported from 172.16.0.5:3:192.168.10.11/32 (VRF tenant-a)
Original source: 172.16.100.1:32777:[2]:[0]:[0]:[48]:[0027.e380.6059]:[32]:[192.168.10.11]/272
AS-Path: NONE, path sourced internal to AS
172.16.100.10 (metric 45) from 10.104.11.1 (192.168.0.11)
Origin IGP, MED not set, localpref 100, weight 0
Received label 101010 303030
Extcommunity: RT:65000:101010 RT:65000:303030 SOO:172.16.100.10:0 ENCAP:8
Router MAC:70db.9855.f52f
Originator: 172.16.100.1 Cluster list: 192.168.0.11

Path-id 1 not advertised to any peer
```

Verifique que la ruta se importe a la tabla de ruteo VRF predeterminada

```
BL(config-router-vrf-neighbor)# show ip route 192.168.10.11
IP Route Table for VRF "default"
'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%<string>' in via output denotes VRF <string>

192.168.10.11/32, ubest/mbest: 1/0
*via 172.16.100.10, [200/0], 00:03:51, bgp-65000, internal, tag 65000, segid: 303030 tunnelid: 0xac1064

Tenant-VRF to Default VRF
```

Arrendatario-VRF a Arrendatario-VRF

Para este ejemplo, el Nexus LEAF está recibiendo la ruta 172.16.120.55/32 arrendatario-a que se va a filtrar al arrendatario-b VRF

Verificar tabla de ruteo

```
show ip route 172.16.120.55/32 vrf tenant-a
IP Route Table for VRF "tenant-a"
'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
```

```
'[x/y]' denotes [preference/metric]
'%<string>' in via output denotes VRF <string>

172.16.120.55/32, ubest/mbest: 1/0
*via 172.16.0.5%default, [200/2], 4d02h, bgp-65000, internal, tag 65000, segid: 303030 tunnelid: 0xac10
```

Filtrar ruta

Para filtrar rutas se necesitan dos pasos, el filtrado entre VRF se realiza mediante Destinos de ruta (RT),RT se conforma mediante <ID de proceso BGP>:L3VNI ID> y el filtrado de subredes específicas. Si no se utiliza el segundo paso, todas las rutas del VRF de origen se filtrarán al VRF de destino.

Identificar destino de ruta

<#root>

```
LEAF# show nve vni
<Snipped>
Interface VNI Multicast-group State Mode Type [BD/VRF] Flags
--------- -------- ----------------- ----- ---- ------------------ -----
nve1 50500 n/a Up CP L3 [tenant-b]
nve1 101010 224.10.10.10 Up CP L2 [10]
nve1 202020 224.10.10.10 Up CP L2 [20]
nve1
```

303030

```
 n/a Up CP L3 [
```

tenant-a

```
]

LEAF# show run bgp | include ignore-case router
router bgp
```

65000

```
router-id 172.16.0.2
```

Para este ejemplo, el destino de ruta es igual a: 65000:303030 y la ruta 172.16.120.55/32 se va a filtrar.

Configurar

	Comando o acción	Propósito

Paso 1	LEAF# configure terminal Ingrese los comandos de configuración, uno por línea. Finalizar con CNTL/Z.	Ingresa en el modo de configuración.
Paso 2	LEAF(config)# ip prefix-list filter-tenant-a-to-tenant-b permit 172.16.120.55/32	Crear host coincidente de lista de prefijos.
Paso 3	LEAF(config)# route-map tenantA a tenantB	Crear mapa de rutas.
Paso 4	LEAF(config-route-map)# match ip address prefix-listfilter-tenant-a-tenant-b	Haga coincidir la lista de prefijos creada en el paso 2.

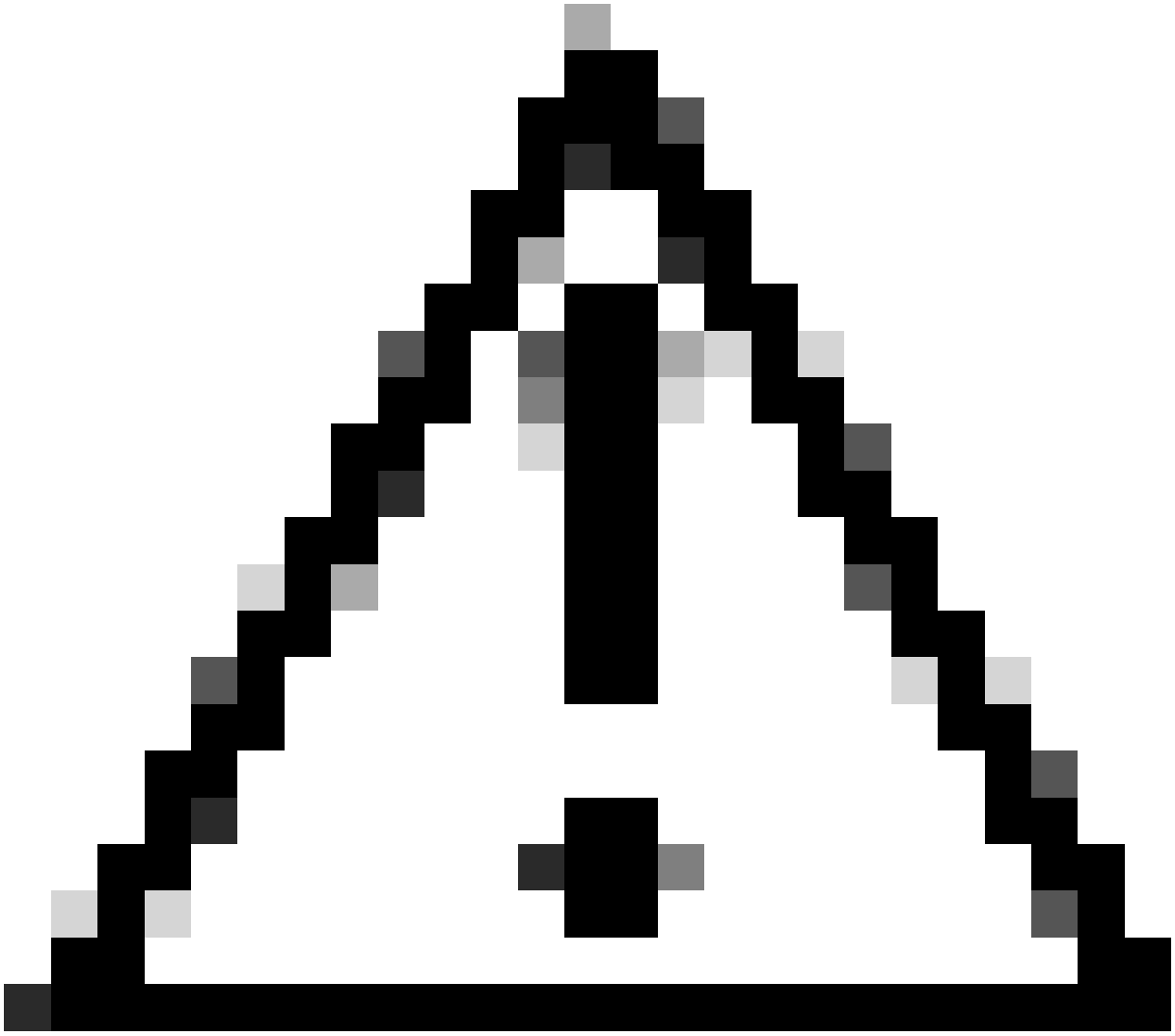
Importar ruta a VRF de arrendatario a desde VRF de arrendatario a

Una vez que se identifica RT y se configura el filtrado, la ruta se puede importar al VRF de destino (tenant-b)

Configurar

	Comando o acción	Propósito
Paso 1	LEAF# configure terminal Ingrese los comandos de configuración, uno por línea. Finalizar con CNTL/Z.	Ingresa en el modo de configuración.
Paso 2	LEAF(config)# vrf context tenant-b	Introduce la configuración VRF.
Paso 3	LEAF(config-vrf)# address-family ipv4 unicast	Introduzca VRF address-family IPV4.
Paso 4	LEAF(config-vrf-af-ipv4)# import map tenantA-to-tenantB	Importar ruta

		filtrada con route-map
Paso 5	LEAF(config-vrf-af-ipv4)# route-target import 65000:303030	Importar destino de ruta
Paso 6	LEAF(config-vrf-af-ipv4)# route-target import 65000:303030 evpn	Importar vpn de destino de ruta



Precaución: Si no se utiliza un mapa de importación, se pueden permitir todas las rutas desde el VRF de origen que tengan fugas hacia el VRF de destino. El uso del mapa de importación puede permitir controlar las rutas que se van a filtrar.

Pasos de resumen

1. configure terminal
2. ip prefix-list filter-tenant-a-to-tenant-b permit 172.16.120.55/32
3. route-map tenantA a tenantB
4. match ip address prefix-listfilter-tenant-a-to-tenant-b
5. vrf context tenant-b
6. address-family ipv4 unicast
7. import map tenant A-to-tenant B
8. route-target import 65000:303030
9. route-target import 65000:303030 evpn

Verificación

Verifique que la ruta se importe a BGP en el VRF de arrendatario-b

```
LEAF(config-vrf-af-ipv4)# show ip bgp 172.16.120.55/32 vrf tenant-b
BGP routing table information for VRF tenant-b, address family IPv4 Unicast
BGP routing table entry for 172.16.120.55/32, version 311
Paths: (1 available, best #1)
Flags: (0x8008021a) (high32 00000000) on xmit-list, is in urib, is best urib route, is in HW
vpn: version 456, (0x00000000100002) on xmit-list

Advertised path-id 1, VPN AF advertised path-id 1
Path type: internal, path is valid, is best path, no labeled nexthop, in rib
Imported from 172.16.0.5:3:[5]:[0]:[0]:[32]:[172.16.120.55]/224
AS-Path: NONE, path sourced internal to AS
172.16.0.5 (metric 45) from 10.101.11.1 (192.168.0.11)
Origin incomplete, MED 2, localpref 100, weight 0
Received label 303030
Extcommunity: RT:65000:303030 ENCAP:8 Router MAC:20cf.ae54.fa3b
OSPF RT:0.0.0.0:0:0
Originator: 172.16.0.5 Cluster list: 192.168.0.11

VRF advertise information:
Path-id 1 not advertised to any peer

VPN AF advertise information:
Path-id 1 not advertised to any peer
```

Verifique que la ruta se importe a la tabla de ruteo en el VRF de arrendatario-b

```
LEAF# show ip route 172.16.120.55/32 vrf tenant-b
IP Route Table for VRF "tenant-b"
'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%<string>' in via output denotes VRF <string>

172.16.120.55/32, ubest/mbest: 1/0
*via 172.16.0.5%default, [200/2], 00:00:08, bgp-65000, internal, tag 65000, segid: 303030 (Asymmetric)
```

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).