Nexus 9000에서 VXLAN VRF 유출 구성 및 확인

목차

소개

이 문서에서는 VXLAN 환경에서 VRF 누설을 구성하고 확인하는 방법에 대해 설명합니다.

배경 정보

VXLAN(Virtual Extensible LAN) 환경에서 VXLAN 호스트를 패브릭의 외부 호스트에 연결하려면 VRF 누수 및 Border Leaf 디바이스를 사용해야 하는 경우가 많습니다.

VRF 유출은 네트워크 세그멘테이션 및 보안을 유지하면서 VXLAN 호스트와 외부 호스트 간의 통신을 활성화하는 데 매우 중요합니다.

Border Leaf 디바이스는 VXLAN 패브릭과 외부 네트워크 간의 게이트웨이 역할을 하며 이러한 통신을 촉진하는 데 중추적 역할을 합니다.

이 시나리오에서 VRF 유출의 중요성은 다음 설명을 통해 요약할 수 있습니다.

1. 외부 네트워크와의 상호 연결: VRF 유출을 통해 패브릭 내 VXLAN 호스트가 패브릭 외부 호스트와 통신할 수 있습니다. 이를 통해 인터넷 또는 기타 데이터 센터와 같은 외부 네트워크에서 호스팅되는 리소스, 서비스 및 애플리케이션에 액세스할 수 있습니다.

2. 네트워크 세그멘테이션 및 격리: VRF 유출은 VXLAN 패브릭 내에서 네트워크 세그멘테이션 및 격리를 유지하는 동시에 외부 네트워크와 선택적인 통신을 가능하게 합니다. 이렇게 하면 VXLAN 호스트는 VRF 할당을 기반으로 서로 격리된 상태로 유지되면서 필요에 따라 외부 리소스에 계속 액세스할 수 있습니다.

3. 정책 시행: 관리자는 VRF 누수를 통해 VXLAN 호스트와 외부 호스트 간의 트래픽 흐름에 대한 네트워크 정책 및 액세스 제어를 시행할 수 있습니다. 이를 통해 통신이 미리 정의된 보안 정책을 사용하고 중요한 리소스에 대한 무단 액세스를 방지할 수 있습니다.

4. 확장성 및 유연성: VRF 유출은 VXLAN 호스트가 외부 호스트와 원활하게 통신할 수 있도록 하여 VXLAN 구축의 확장성과 유연성을 향상시킵니다. VXLAN과 외부 네트워크 간에 리소스를 동적으로 할당 및 공유하여 기존 컨피그레이션을 중단하지 않고 변화하는 네트워크 요구 사항에 맞출 수 있습니다.

VRF(Virtual Routing and Forwarding) 유출의 경로 필터링은 네트워크 보안을 유지하고 라우팅 효율성을 최적화하며 의도하지 않은 데이터 유출을 방지하는 데 매우 중요합니다. VRF 누수는 가상 네트워크를 논리적으로 분리하면서 가상 네트워크 간의 통신을 가능하게 합니다.

VRF 누출 시 경로 필터링의 중요성은 다음 내용을 통해 요약할 수 있습니다.

1. 보안: 경로를 필터링하면 특정 경로만 VRF 인스턴스 간에 유출되므로 무단 액세스나 데이터 유출의 위험이 줄어듭니다. 관리자는 어떤 경로가 VRF 경계를 넘도록 허용되는지를 제어하여 보안 정책을 시행하고 중요한 정보가 무단 엔티티에 노출되지 않도록 할 수 있습니다.

2. 격리: VRF는 네트워크 세그멘테이션 및 격리를 제공하도록 설계되어 서로 다른 테넌트 또는 부서가 동일한 물리적 인프라 내에서 독립적으로 작동할 수 있도록 합니다. VRF 누수의 경로 필터링은 VRF 인스턴스 간의 경로 전파 범위를 제한하여 의도하지 않은 통신 및 잠재적 보안

취약성을 방지함으로써 이러한 격리를 유지하는 데 도움이 됩니다.

3. 최적화된 라우팅: 경로를 필터링하면 관리자가 VRF 간에 필요한 경로만 선택적으로 유출하여 라우팅 효율성을 최적화하고 네트워크 전체에서 불필요한 트래픽을 줄일 수 있습니다. 관리자는 관련이 없는 경로를 필터링하여 트래픽이 가장 효율적인 경로를 사용하도록 하는 동시에 혼잡과 레이턴시를 최소화할 수 있습니다.

4. 리소스 사용률: 관리자는 경로를 필터링하여 VRF 인스턴스 간의 트래픽 흐름을 제어하고 리소스 사용률 및 대역폭 할당을 최적화할 수 있습니다. 이를 통해 네트워크 혼잡을 방지하고 중요한 리소스를 우선 순위 애플리케이션 또는 서비스에 사용할 수 있습니다.

5. 규정 준수: VRF 유출의 경로를 필터링하면 조직이 규정 요구 사항 및 업계 표준을 준수할 수 있습니다. 승인된 기업으로만 경로 유출을 제한함으로써 데이터 보호 규정 준수를 입증하고 중요한 정보의 무결성을 보장할 수 있습니다.

6. 세분화된 제어: 필터링 경로를 통해 관리자는 VRF 인스턴스 간의 통신을 세부적으로 제어할 수 있으므로 고유한 요구 사항에 따라 특정 정책을 정의할 수 있습니다. 이러한 유연성을 통해 조직은 다양한 애플리케이션, 사용자 또는 부서의 요구 사항을 충족하도록 네트워크 구성을 맞춤화할 수 있습니다.

사전 요구 사항

보더 라우터가 있는 기존 VXLAN 환경

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

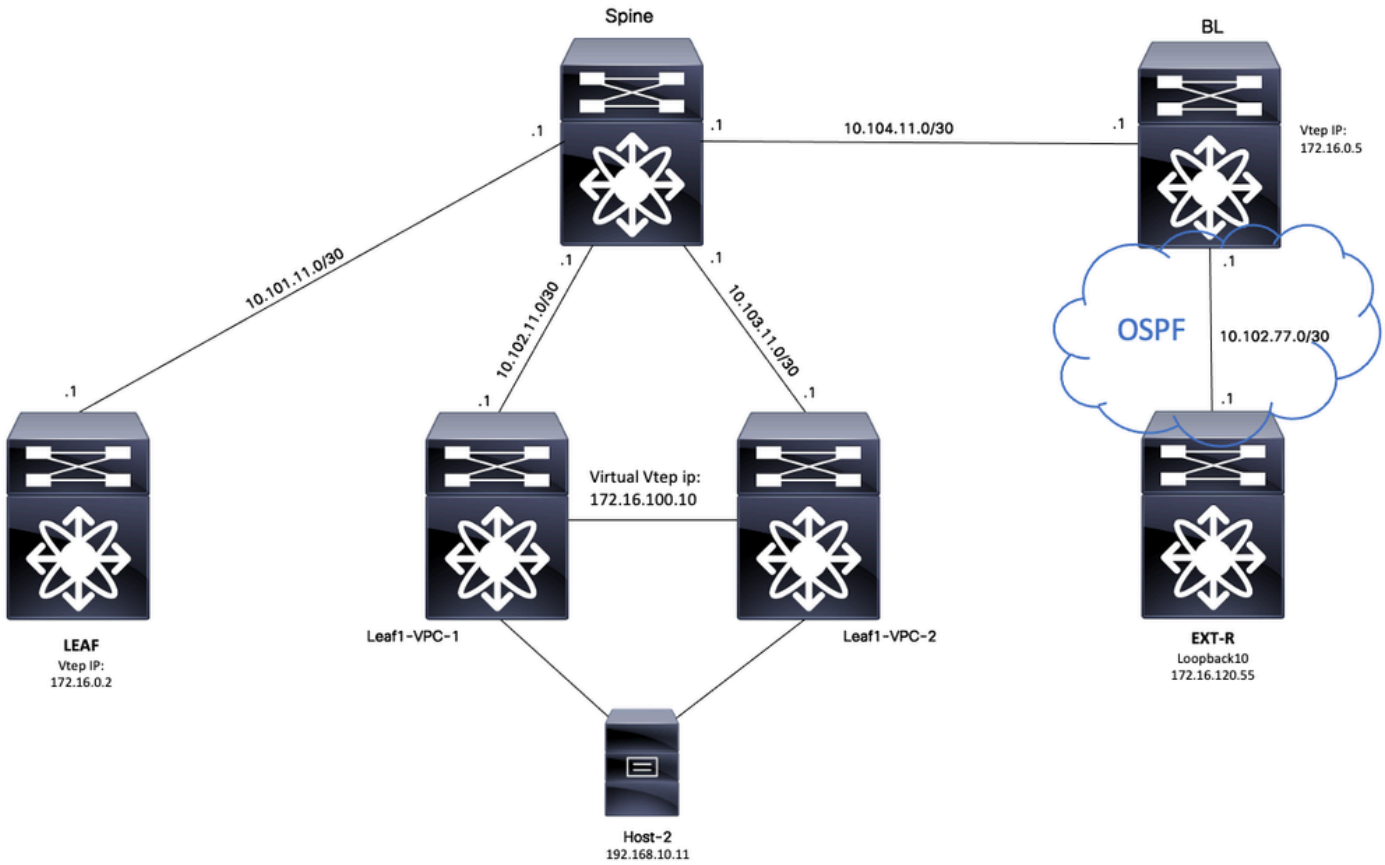
- NXOS 플랫폼
- VXLAN
- VRF
- BGP

사용되는 구성 요소

이름	플랫폼	버전
호스트-2	N9K-C92160YC-X	9.3(6)
리프-VPC-1	N9K-C93180YC-EX	9.3(9)
리프-VPC-2	N9K-C93108TC-EX	9.3(9)
리프	N9K-C9332D-GX2B	10.2(6)
비엘	N9K-C9348D-GX2A	10.2(5)
EXT-R	N9K-C9348D-GX2A	10.2(3)
등뼈	N9K-C93108TC-FX3P	10.1(1)

"이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 네트워크가 가동 중인 경우 모든 명령의 잠재적인 영향을 이해해야 합니다."

다이어그램



BGP를 애플리케이션으로 간주할 때 BGP는 VRF 간 누수를 수행하는 데 사용되는 애플리케이션입니다

기본 VRF에서 테넌트-VRF로

이 예에서 BL(Border VTEP)은 테넌트 VRF로 유출될 기본 VRF에서 OSFP를 통해 외부 장치로부터 172.16.120.55를 수신합니다.

라우팅 테이블 확인

```
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
```

경로 필터링

NXOS에서는 경로를 필터링하고 재배포하기 위한 매개변수로 경로 맵이 필요합니다. 예를 들어, 접두사 172.16.120.55/32이 필터링됩니다.

구성

	명령 또는 작업	목적
1단계	BL# 구성 터미널 한 줄에 하나씩 컨피그레이션 명령을 입력합니다. CNTL/Z로 종료합니다.	컨피그레이션 모드를 시작합니다.
2단계	BL(config)# ip prefix-list VXLAN-VRF-default-to-Tenant permit 172.16.120.55/32	접두사 목록 일치 호스트를 만듭니다.
3단계	BL(config)# 경로 맵 VXLAN-VRF-default-to-Tenant	route-map을 생성합니다.
4단계	BL(config-route-map)# match ip address prefix-list VXLAN-VRF-default-to-Tenant(BL(config-route-map)# ip 주소 접두사 목록 VXLAN-VRF에서 테넌트로 기본 설정)	2단계에서 생성된 접두사 목록 일치

BGP로 경로 가져오기

기본 VRF에 경로가 존재하는 것이 확인되면 BGP 프로세스로 경로를 가져와야 합니다.

구성

	명령 또는 작업	목적
1단계	BL# 구성 터미널 한 줄에 하나씩 컨피그레이션 명령을 입력합니다. CNTL/Z로 종료합니다.	컨피그레이션 모드를 시작합니다.
2단계	BL(config)# 라우터 bgp 65000	BGP 컨피그레이션을 시

		작합니다.
3단계	BL(config-router)# 주소군 ipv4 유니캐스트	BGP 주소군 IPV4를 입력합니다.
4단계	BL(config-router-af)# 재배포 ospf 1 경로 맵 VXLAN-VRF-default-to-Tenant	3단계에서 생성한 경로 맵을 사용하여 OSPF에서 BGP로 경로를 재배포합니다.

BGP 테이블 확인

```
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
```

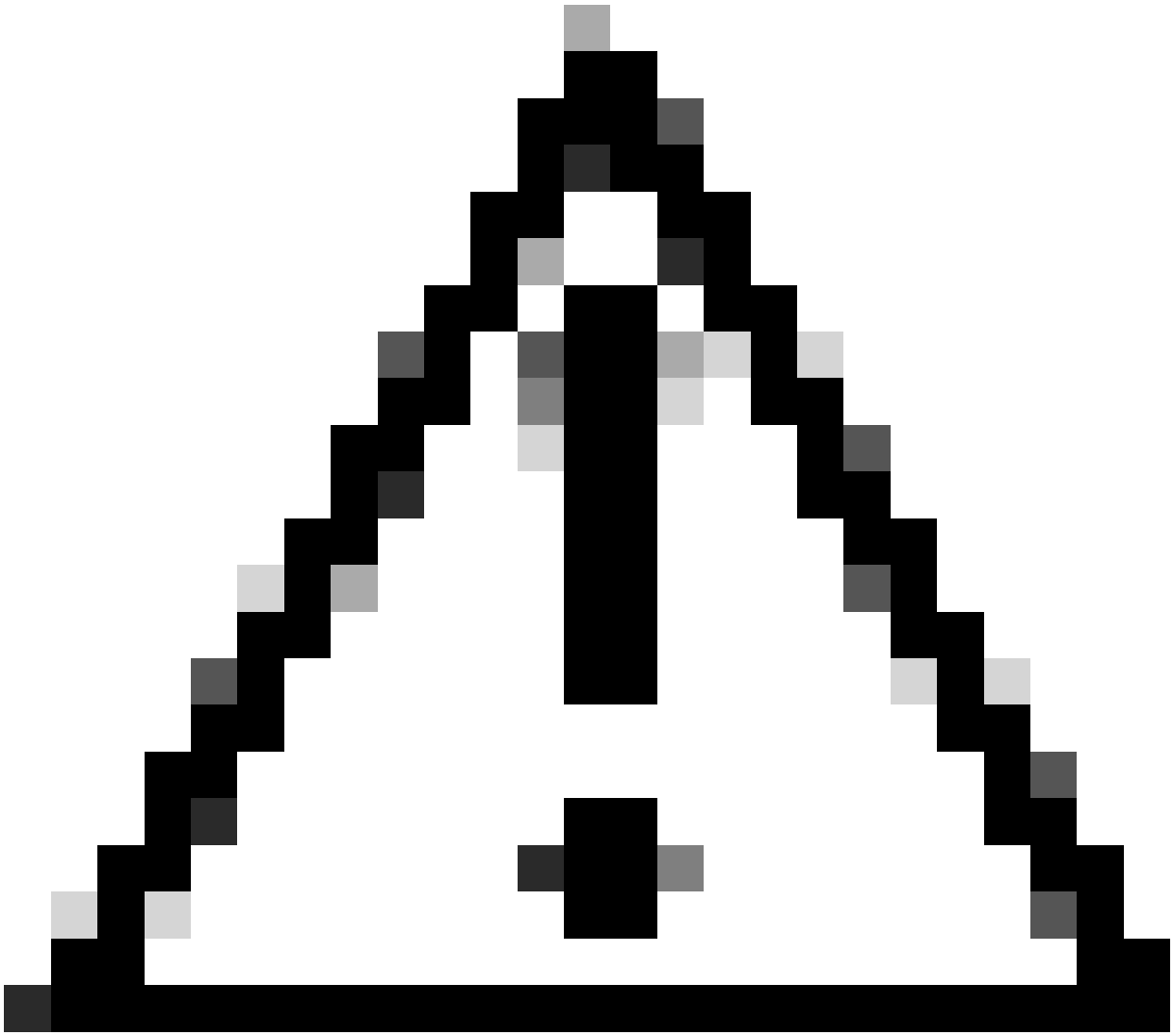
테넌트 VRF로 경로 가져오기

경로를 BGP로 가져오면 이제 경로를 대상 VRF(tenant-a)로 가져올 수 있습니다.

구성

	명령 또는 작업	목적
1단계	BL(config)# vrf context tenant-a	VRF 컨피그레이션을 시작합니다.
2단계	BL(config-vrf)# 주소군 ipv4 유니캐스트	IPV4 주소군을 입력합니다.

3단계	BL(config-vrf-af-ipv4)# vrf 기본 맵 가져오기 VXLAN-VRF-default-to-Tenant advertise-vpn	VRF 기본값에서 테넌트 VRF 광고 VPN으로 경로 가져오기



주의: 기본적으로 기본 VRF에서 기본이 아닌 VRF로 가져올 수 있는 IP 접두사의 최대 수는 1000개입니다. 이 값은 VRF 주소군 IPV4: import vrf <number of prefixes> default map <route-map name> advertise-vpn의 명령으로 변경할 수 있습니다.

요약 단계

1. 터미널 구성
2. ip prefix-list VXLAN-VRF-default-to-Tenant permit 172.16.120.55/32
3. route-map VXLAN-VRF-default-to-Tenant
4. ip 주소 접두사 목록 VXLAN-VRF-default-to-Tenant 일치

5. 라우터 bgp 65000
6. 주소군 ipv4 유니캐스트
7. ospf 1 경로 맵 VXLAN-VRF-default-to-Tenant 재배포
8. vrf 컨텍스트 테넌트-a
9. 주소군 ipv4 유니캐스트
10. vrf 기본 맵 가져오기 VXLAN-VRF-default-to-Tenant advertise-vpn

다음을 확인합니다.

경로를 L2VPN으로 가져왔는지 확인합니다.

```
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
```

테넌트 VRF로 경로 가져오기 확인

```
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
```

테넌트-VRF에서 기본 VRF로

이 예에서 BL(Border VTEP)은 테넌트-a VRF에서 VXLAN을 통해 경로 192.168.10.11을 수신하는

데, 이는 기본 VRF로 유출될 것입니다.

라우팅 테이블 확인

```
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:
```

경로 필터링

NXOS에서는 경로를 필터링하고 재배포하기 위한 매개변수로 경로 맵이 필요합니다. 예를 들어, 접두사 172.16.120.55/32은 필터링됩니다.

구성

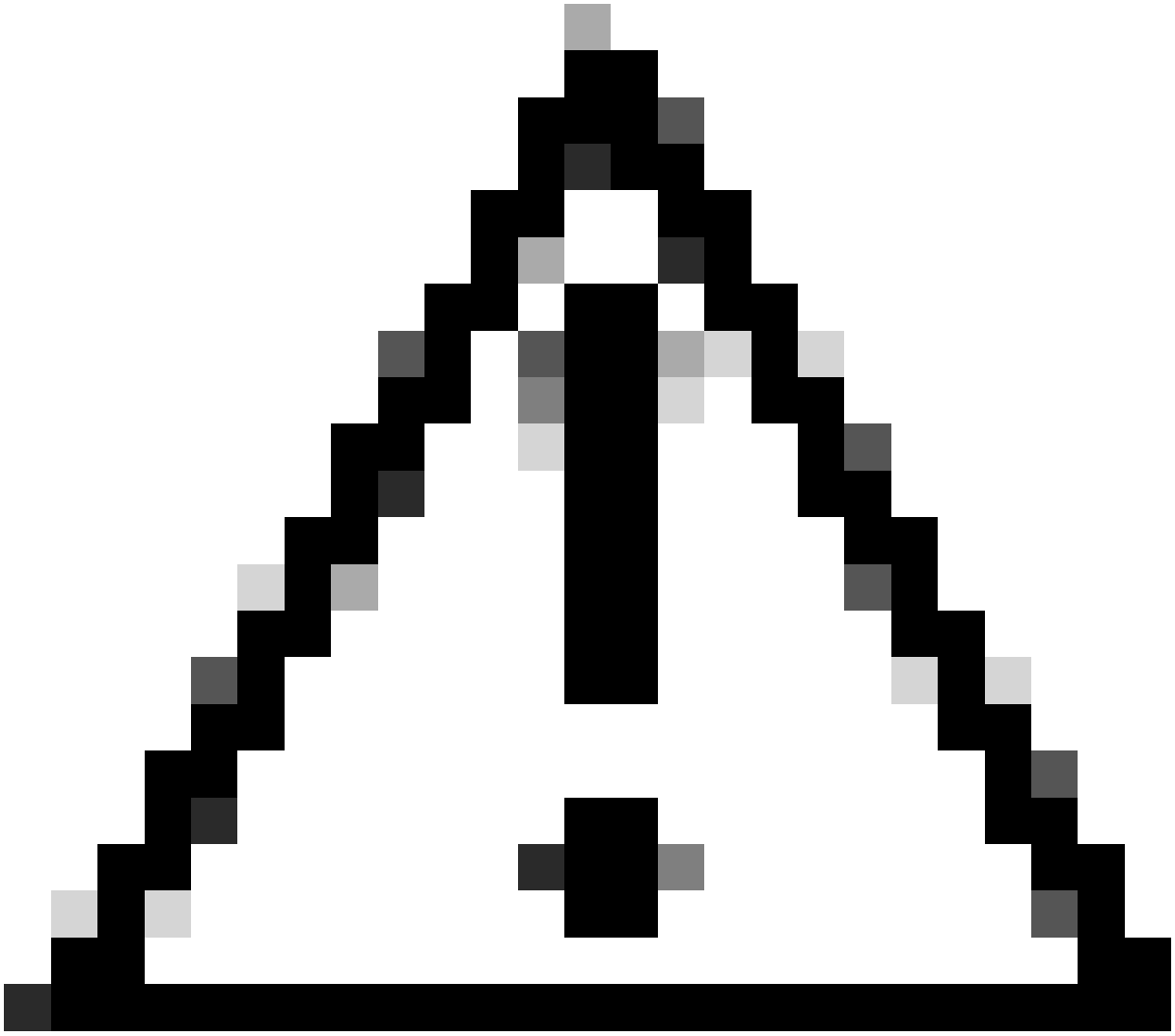
	명령 또는 작업	목적
1단계	BL# 구성 터미널 한 줄에 하나씩 컨피그레이션 명령을 입력합니다. CNTL/Z로 종료합니다.	컨피그레이션 모드를 시작합니다.
2단계	BL(config)# ip prefix-list VXLAN-VRF-Tenant-to-default permit 192.168.10.11/32	접두사 목록 일치 호스트를 만듭니다.
3단계	BL(config)# 경로 맵 VXLAN-VRF-Tenant-to-default	route-map을 생성합니다.
4단계	BL(config-route-map)# ip address prefix-list VXLAN-VRF-Tenant-to-default 매칭	2단계에서 생성된 접두사 목록 일치

테넌트-a VRF에서 기본 VRF로 경로 내보내기

경로가 이미 BGP L2VPN 프로세스에 있으므로 VRF 기본값으로 내보내기만 하면 됩니다.

구성

	명령 또는 작업	목적
1단계	BL# 구성 터미널 한 줄에 하나씩 컨피그레이션 명령을 입력합니다. CNTL/Z로 종료합니다.	컨피그레이션 모드를 시작합니다.
2단계	BL(config)# vrf context tenant-a	VRF 컨피그레이션을 시작합니다.
3단계	BL(config-vrf)# 주소군 ipv4 유니캐스트	VRF 주소군 IPV4를 입력합니다.
4단계	BL(config-vrf-af-ipv4)# export vrf default map VXLAN-VRF-Tenant-to-default allow-vpn	테넌트 VRF에서 VPN을 허용하는 기본 VRF로 경로 내보내기



주의: 기본적으로 기본값이 아닌 VRF에서 기본 VRF로 내보낼 수 있는 IP 접두사의 최대 수는 1000개입니다. 이 값은 VRF 주소군 IPV4: export vrf default <number of prefixes> map <route-map name> allow-vpn의 명령을 사용하여 변경할 수 있습니다.

요약 단계

1. 터미널 구성
2. ip prefix-list VXLAN-VRF-Tenant-to-default permit 192.168.10.11/32
3. route-map VXLAN-VRF-Tenant-to-default
4. ip 주소 접두사 목록 VXLAN-VRF-Tenant를 기본값으로 일치
5. vrf 컨텍스트 테넌트-a
6. 주소군 ipv4 유니캐스트
7. vrf 기본 맵 VXLAN-VRF-Tenant-to-default allow-vpn 내보내기

다음을 확인합니다.

기본 VRF에서 BGP IPV4 주소군으로 경로 가져오기 확인

```
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
```

경로를 기본 VRF 라우팅 테이블로 가져왔는지 확인합니다.

```
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
```

테넌트-VRF - 테넌트-VRF

이 예에서 Nexus LEAF는 VRF tenant-b로 유출될 경로 172.16.120.55/32 tenant-a를 수신합니다

라우팅 테이블 확인

```
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
```

경로 필터링

경로를 필터링하려면 두 단계를 수행해야 합니다. VRF 간의 필터링은 RT(Route Targets)를 참조하여 수행되며, RT는 <BGP Process ID>:L3VNI ID>와 필터링하여 특정 서브넷을 확인합니다. 두 번째 단계가 사용되지 않으면 소스 VRF의 모든 경로가 대상 VRF로 유출됩니다.

경로 대상 식별

<#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
```

이 예에서 Route Target은 65000:303030과 같으며 Route 172.16.120.55/32은 필터링됩니다.

구성

	명령 또는 작업	목적
1단계	LEAF# 구성 터미널 한 줄에 하나씩 컨피그레이션 명령을 입력합니다. CNTL/Z로 종료합니다.	컨피그레이션 모드를 시

		작합니다.
2단계	LEAF(config)# ip prefix-list filter-tenant-a-to-tenant-b permit 172.16.120.55/32	접두사 목록 일치 호스트를 만듭니다.
3단계	LEAF(config)# 경로 맵 tenantA-to-tenantB	route-map을 생성합니다.
4단계	LEAF(config-route-map)# match ip address prefix-listfilter-tenant-a-to-tenant-b	2단계에서 생성된 접두사 목록 일치

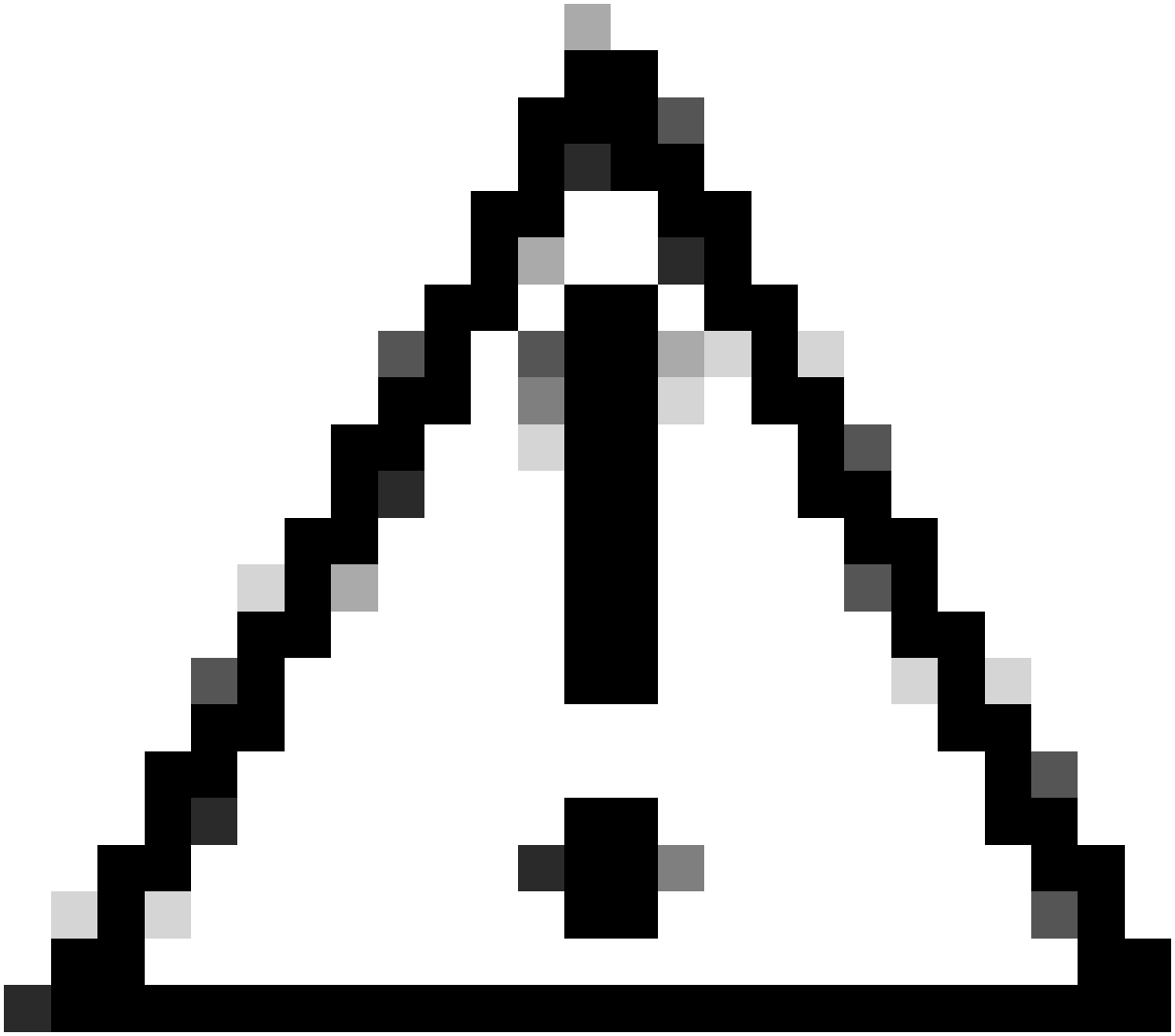
테넌트-a VRF에서 테넌트-a VRF로 경로 가져오기

RT가 식별되고 필터링이 구성되면 경로를 대상 VRF(tenant-b)로 가져올 수 있습니다.

구성

	명령 또는 작업	목적
1단계	LEAF# 구성 터미널 한 줄에 하나씩 컨피그레이션 명령을 입력합니다. CNTL/Z로 종료합니다.	컨피그레이션 모드를 시작합니다.
2단계	LEAF(config)# vrf context tenant-b	VRF 컨피그레이션을 시작합니다.
3단계	LEAF(config-vrf)# 주소군 ipv4 유니캐스트	VRF 주소군 IPV4를 입력합니다.
4단계	LEAF(config-vrf-af-ipv4)# import map tenantA-to-tenantB	경로 맵으로 필터링된 경로 가져오기
5단계	LEAF(config-vrf-af-ipv4)# route-target import 65000:303030	경로 대상 가져오기

6단계	LEAF(config-vrf-af-ipv4)# route-target import 65000:303030 evpn	경로 대상 이벤트 가져오기



주의: 가져오기 맵을 사용하지 않으면 원본 VRF의 모든 경로가 대상 VRF로 유출될 수 있습니다. 가져오기 맵을 사용하면 경로가 유출되는 것을 제어할 수 있습니다.

요약 단계

1. 터미널 구성
2. ip prefix-list filter-tenant-a-to-tenant-b permit 172.16.120.55/32
3. 경로 맵 테넌트A-to-tenantB
4. match ip address prefix-listfilter-tenant-a-to-tenant-b
5. vrf 컨텍스트 테넌트-b
6. 주소군 ipv4 유니캐스트
7. 맵 tenantA-to-tenantB 가져오기

8. route-target 가져오기 65000:303030
9. route-target import 65000:303030 evpn

다음을 확인합니다.

테넌트 b VRF의 BGP로 경로 가져오기 확인

```
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
```

테넌트-b VRF의 라우팅 테이블로 경로 가져오기 확인

```
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)
```

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.