IOS XE에서 VRF 인식 소프트웨어 인프라 NAT 구성

목차

소개

이 문서에서는 Cisco IOS® XE를 실행하는 라우터에서 VASI(VRF-Aware Software Infrastructure) NAT(Network Address Translation)의 컨피그레이션에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다. 이 문서는 Cisco IOS XE를 실행하는 모든 Cisco 라우터 및 스위치에 적용됩니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

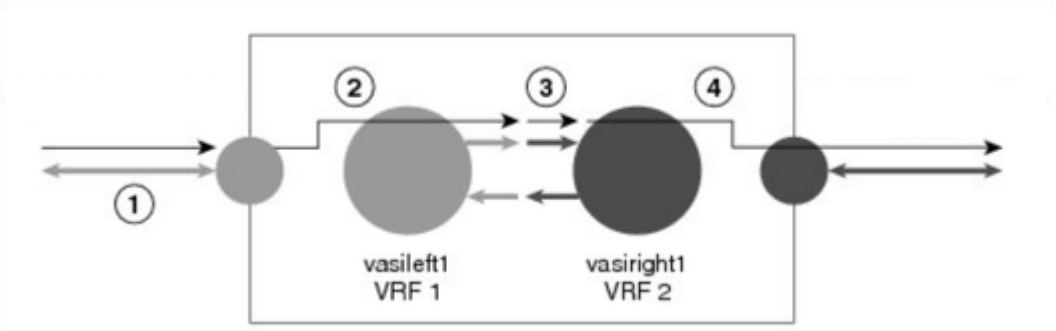
배경 정보

Cisco IOS XE에서 실행되는 디바이스는 Cisco IOS 디바이스에 있는 것과 같은 클래식 VRF 간 NAT 컨피그레이션을 지원하지 않습니다. Cisco IOS XE의 VRF 간 NAT는 VASI 구현을 통해 지원됩니다.

VASI는 VRF(virtual routing and forwarding) 인스턴스 간에 흐르는 트래픽에 대해 IPsec, 방화벽 및 NAT와 같은 서비스를 구성할 수 있는 기능을 제공합니다.

VASI는 VASI 쌍을 구성하여 구현됩니다. 여기서 쌍의 각 인터페이스는 서로 다른 VRF 인스턴스와 연결됩니다. VASI 가상 인터페이스는 이 두 VRF 인스턴스 간에 전환해야 하는 모든 패킷에 대한 next-hop 인터페이스입니다. 페어링은 vasileft 인터페이스가 vasiright 인터페이스에 자동으로 페어링되도록 2개의 인터페이스 인덱스를 기반으로 자동으로 수행됩니다. vasileft 인터페이스로 들어오는 모든 패킷은 페어링된 vasiright 인터페이스로 자동으로 전달됩니다.

VASI 작업



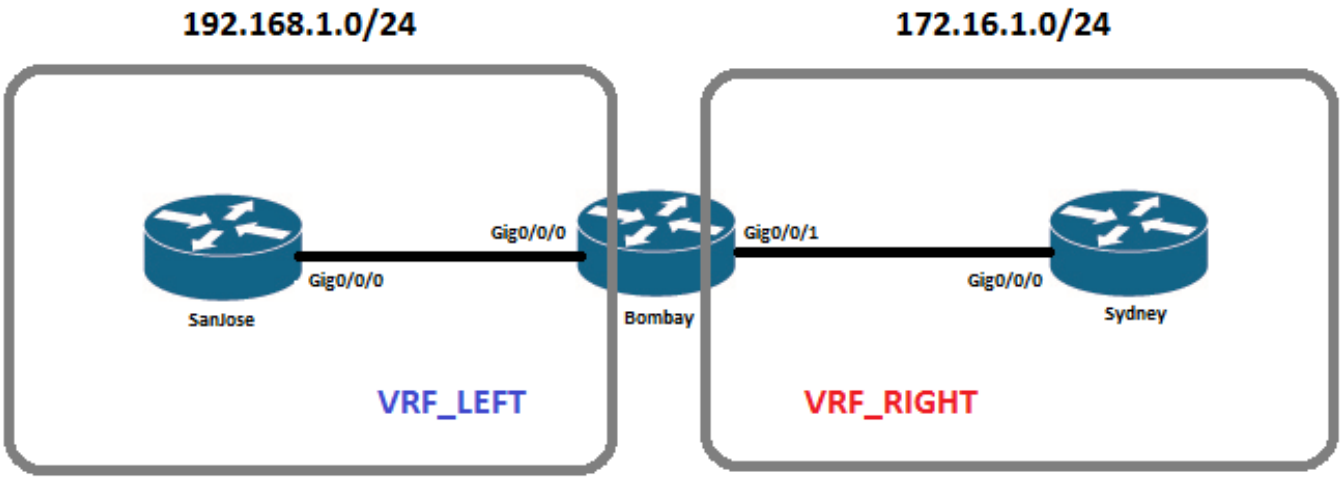
동일한 디바이스에서 VRF 간 VASI가 구성된 경우 패킷 흐름은 다음 순서로 이루어집니다.

1. 패킷이 VRF 1에 속하는 물리적 인터페이스로 들어갑니다.
2. 패킷을 전달하기 전에 VRF 1 라우팅 테이블에서 전달 조회가 수행됩니다. Vasileft1이 다음 홉으로 선택되고 TTL(Time to Live) 값이 패킷에서 감소합니다. 일반적으로 포워딩 주소는 VRF의 기본 경로를 기준으로 선택됩니다. 그러나 전달 주소는 고정 경로 또는 학습된 경로일 수도 있습니다. 패킷은 vasileft1의 이그레스 경로로 전송된 다음 vasiright1 인그레스 경로로 자동으로 전송됩니다.
3. 패킷이 vasiright1로 들어가면 VRF 2 라우팅 테이블에서 포워딩 조회가 수행되고 TTL이 다시 감소됩니다(이 패킷의 두 번째 시간).
4. VRF 2는 패킷을 물리적 인터페이스에 전달합니다.

구성

이러한 시나리오에서는 기본 VRF 간 NAT 컨피그레이션에 대해 설명합니다.

네트워크 다이어그램



초기 컨피그레이션

산호세:

```
interface GigabitEthernet0/0/0
 ip address 192.168.1.1 255.255.255.0

ip route 0.0.0.0 0.0.0.0 192.168.1.2
```

뭄바이:

```
vrf definition VRF_LEFT
 rd 1:1
 !
 address-family ipv4
 exit-address-family

vrf definition VRF_RIGHT
 rd 2:2
 !
 address-family ipv4
 exit-address-family
```

```
interface GigabitEthernet0/0/0
  vrf forwarding VRF_LEFT
  ip address 192.168.1.2 255.255.255.0

interface GigabitEthernet0/0/1
 vrf forwarding VRF_RIGHT
 ip address 172.16.1.2 255.255.255.0
```

시드니:

```
interface GigabitEthernet0/0/0
 ip address 172.16.1.1 255.255.255.0
```

VASI 인터페이스 컨피그레이션

각 VASI 인터페이스는 다른 VRF 인스턴스와 쌍을 이룹니다.

```
interface vasileft1
 vrf forwarding VRF_LEFT
 ip address 10.1.1.1 255.255.255.252

interface vasiright1
 vrf forwarding VRF_RIGHT
 ip address 10.1.1.2 255.255.255.252
```

NAT 컨피그레이션

이 예에서 NAT는 다음 요구 사항으로 구성됩니다.

1. 고정 NAT - 192.168.1.1의 소스 IP는 172.16.1.5로 변환됩니다.
2. 동적 NAT - 192.168.1.0/24의 소스 서브넷은 172.16.1.5로 변환됩니다.

시나리오 1 - NAT on Vasiright

대부분의 경우 WAN 인터페이스는 이 토폴로지의 발신 VRF, VRF_RIGHT에 있습니다. 이 경우 NAT는 VASIRIGHT와 WAN 인터페이스 간에 구성할 수 있습니다. vasileft에서 vasiright 인터페이스로 들어오는 트래픽은 NAT inside로 구성되며, WAN 인터페이스는 NAT outside 인터페이스가 됩니다.

이 시나리오에서는 VRF 간 트래픽에 대한 고정 경로를 사용합니다. 대상 172.16.0.0 서브넷에 대한 고정 경로는 vasileft 인터페이스를 가리키는 VRF_LEFT에 구성되며, 소스 서브넷 192.168.0.0에 대한 다른 경로는 vasiright 인터페이스를 가리키는 VRF_RIGHT에 구성됩니다.

참고: 소스 IP 주소를 WAN 인터페이스 IP 주소로 변환하도록 NAT를 구성하지 마십시오. 라우터는 반환 트래픽을 자신에게 보내는 것으로 처리하며 트래픽을 VASI 인터페이스로 전달하지 않습니다.

고정 NAT:

```
!--- Interface configuration

interface vasiright1
 vrf forwarding VRF_RIGHT
 ip address 10.1.1.2 255.255.255.252
 ip nat inside

interface GigabitEthernet0/0/1
 vrf forwarding VRF_RIGHT
 ip address 172.16.1.2 255.255.255.0
 ip nat outside


!--- Static route configuration

ip route vrf VRF_LEFT 172.16.0.0 255.255.0.0 vasileft1 10.1.1.2
ip route vrf VRF_RIGHT 192.168.0.0 255.255.0.0 vasiright1 10.1.1.1


!--- NAT configuration

ip nat inside source static 192.168.1.1 172.16.1.5 vrf VRF_RIGHT
```

확인:

```
<#root>

Bombay#

sh ip nat translations vrf VRF_RIGHT


Pro         Inside global     Inside local       Outside local    Outside global
---         172.16.1.5        192.168.1.1        ---              ---
icmp        172.16.1.5:8      192.168.1.1:8      172.16.1.1:8     172.16.1.1:8
tcp         172.16.1.5:47491  192.168.1.1:47491  172.16.1.1:23    172.16.1.1:23
Total number of translations: 3
```

동적 NAT:

```
!--- Interface configuration

interface vasiright1
 vrf forwarding VRF_RIGHT
 ip address 10.1.1.2 255.255.255.252
 ip nat inside

interface GigabitEthernet0/0/1
 vrf forwarding VRF_RIGHT
 ip address 172.16.1.2 255.255.255.0
 ip nat outside


!--- Static route configuration

ip route vrf VRF_LEFT 172.16.0.0 255.255.0.0 vasileft1 10.1.1.2
ip route vrf VRF_RIGHT 192.168.0.0 255.255.0.0 vasiright1 10.1.1.1


!--- Access-list configuration
Extended IP access list 100
 10 permit tcp 192.168.1.0 0.0.0.255 host 172.16.1.1
 20 permit udp 192.168.1.0 0.0.0.255 host 172.16.1.1
 30 permit icmp 192.168.1.0 0.0.0.255 host 172.16.1.1


!--- NAT configuration

ip nat pool POOL 172.16.1.5 172.16.1.5 prefix-length 24
ip nat inside source list 100 pool POOL vrf VRF_RIGHT overload
```

참고: 쌍의 두 VASI 인터페이스를 모두 외부로 구성하는 것은 지원되지 않습니다.

확인:

<#root>

```
Bombay#

sh ip nat translations


Pro      Inside global      Inside local         Outside local      Outside global
icmp     172.16.1.5:1       192.168.1.1:15       172.16.1.1:15      172.16.1.1:1
tcp      172.16.1.5:1024    192.168.1.1:58166    172.16.1.1:23      172.16.1.1:23
Total number of translations: 2
```

시나리오 2 - Vasileft의 NAT

NAT는 VRF_LEFT인 vasileft 측에서만 구성할 수 있으며 VRF_RIGHT로 전송되기 전에 트래픽 NATted를 가질 수 있습니다. VRF_LEFT의 수신 인터페이스는 NAT 내부 인터페이스로 간주되며, vasileft 1은 NAT 외부 인터페이스로 구성됩니다.

이 시나리오에서는 VRF 간 트래픽에 대한 고정 경로를 사용합니다. 대상 172.16.0.0 서브넷에 대한 고정 경로는 vasileft 인터페이스를 가리키는 VRF_LEFT에 구성되고, 소스 NATted IP 172.16.1.5에 대한 다른 경로는 vasiright 인터페이스를 가리키는 VRF_RIGHT에 구성됩니다.

고정 NAT:

```
!--- Interface configuration

interface GigabitEthernet0/0/0
 vrf forwarding VRF_LEFT
 ip address 192.168.1.2 255.255.255.0
 ip nat inside

interface vasileft1
 vrf forwarding VRF_LEFT
 ip address 10.1.1.1 255.255.255.252
 ip nat outside


!--- Static route configuration

ip route vrf VRF_LEFT 172.16.0.0 255.255.0.0 vasileft1 10.1.1.2
ip route vrf VRF_RIGHT 172.16.1.5 255.255.255.255 vasiright1 10.1.1.1


!--- NAT configuration
ip nat inside source static 192.168.1.1 172.16.1.5 vrf VRF_LEFT
```

확인:

<#root>

```
Bombay#

sh ip nat translations vrf VRF_LEFT

Pro       Inside global        Inside local         Outside local      Outside global
---       172.16.1.5           192.168.1.1          ---                ---
icmp      172.16.1.5:5         192.168.1.1:5        172.16.1.1:5       172.16.1.1:5
tcp       172.16.1.5:35414     192.168.1.1:35414    172.16.1.1:23      172.16.1.1:23
Total number of translations: 3
```

동적 NAT:

```
!--- Interface configuration

interface GigabitEthernet0/0/0
 vrf forwarding VRF_LEFT
 ip address 192.168.1.2 255.255.255.0
 ip nat inside

interface vasileft1
 vrf forwarding VRF_LEFT
 ip address 10.1.1.1 255.255.255.252
 ip nat outside


!--- Static route configuration

ip route vrf VRF_LEFT 172.16.0.0 255.255.0.0 vasileft1 10.1.1.2
ip route vrf VRF_RIGHT 172.16.1.5 255.255.255.255 vasiright1 10.1.1.1


!--- Access-list configuration

Extended IP access list 100
 10 permit tcp 192.168.1.0 0.0.0.255 host 172.16.1.1
 20 permit udp 192.168.1.0 0.0.0.255 host 172.16.1.1
 30 permit icmp 192.168.1.0 0.0.0.255 host 172.16.1.1


!--- NAT configuration

ip nat pool POOL 172.16.1.5 172.16.1.5 prefix-length 24
ip nat inside source list 100 pool POOL vrf VRF_LEFT overload
```

확인:

<#root>

```
Bombay#

sh ip nat translations vrf VRF_LEFT


Pro      Inside global      Inside local        Outside local    Outside global
icmp     172.16.1.5:1       192.168.1.1:4       172.16.1.1:4     172.16.1.1:1
tcp      172.16.1.5:1024    192.168.1.1:27593   172.16.1.1:23    172.16.1.1:23
Total number of translations: 2
```

다음을 확인합니다.

구성이 올바르게 작동하는지 확인하려면 이 섹션을 활용하십시오.

1. 두 VRF 인스턴스 간에 트래픽을 라우팅하도록 동적/고정 경로가 구성되어 있는지 확인합니다
.
2. NAT가 올바른 VRF에 대해 구성되었는지 확인합니다.

문제 해결

현재 이 설정에 사용할 수 있는 특정 문제 해결 정보가 없습니다.

관련 정보

- VRF 인식 소프트웨어 인프라 구성
- 기술 지원 및 다운로드 - Cisco Systems

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.