在IOS XE上配置VRF感知软件基础设施NAT

目录

简介

先决条件

- 要求
- 使用的组件

背景信息

- VASI的工作

配置

- 网络图
- 初始配置
- VASI接口配置
- NAT 配置
  - 场景1 - Vasiright上的NAT
  - 场景2 - Vasileft上的NAT

验证

故障排除

相关信息

简介

本文档介绍在运行Cisco IOS® XE的路由器上配置VRF感知软件基础设施(VASI)网络地址转换(NAT)。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档不限于特定的软件和硬件版本。本文档适用于运行Cisco IOS XE的所有Cisco路由器和交换机。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

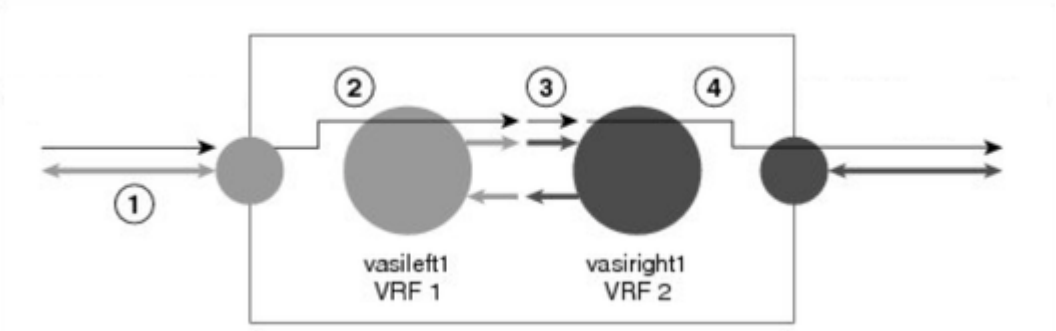
背景信息

在Cisco IOS XE上运行的设备不支持传统VRF间NAT配置，如Cisco IOS设备上的配置。通过VASI实施在Cisco IOS XE上实现VRF间NAT。

VASI能够将服务（如IPsec、防火墙和NAT）配置为在虚拟路由和转发(VRF)实例之间流动的流量。

VASI通过配置VASI对实现，其中对中的每个接口与不同的VRF实例相关联。VASI虚拟接口是需要在这两个VRF实例之间交换的任何数据包的下一跳接口。根据两个接口索引自动完成配对，以便vasrift接口自动与vasright接口配对。任何进入vasright接口的数据包都会自动转发到其配对vasright接口。

VASI的工作



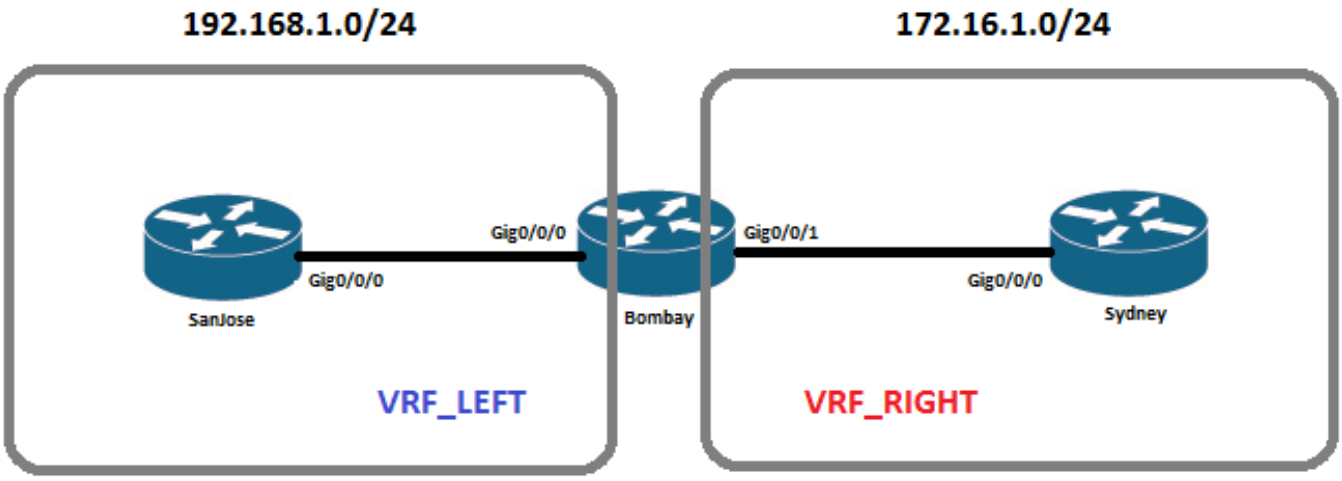
当在同一设备上配置VRF间VASI时，数据包流按以下顺序发生：

1. 数据包进入属于VRF 1的物理接口。
2. 转发数据包之前，会在VRF 1路由表中执行转发查找。选择Vasileft1作为下一跳，并且生存时间(TTL)值会从数据包中递减。通常，根据VRF中的默认路由选择转发地址。但是，转发地址也可以是静态路由或获知的路由。数据包发送到vasright1的出口路径，然后自动发送到vasright1入口路径。
3. 当数据包进入vasright1时，在VRF 2路由表中执行转发查找，TTL再次递减（此数据包需第二次递减）。
4. VRF 2将数据包转发到物理接口。

配置

这些场景描述基本的VRF间NAT配置。

网络图



初始配置

圣荷西：

```
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
```

孟买：

```
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
```

悉尼：

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

VASI接口配置

每个VASI接口与不同的VRF实例配对。

```
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 配置

在本例中，NAT将配置有以下要求：

1. 静态NAT — 将源IP 192.168.1.1转换为172.16.1.5。
2. 动态NAT — 源子网192.168.1.0/24将转换为172.16.1.5。

场景1 - Vasiright上的NAT

在大多数情况下，WAN接口将位于此拓扑中的传出VRF(VRF_RIGHT)上。在这种情况下，可在vasright和WAN接口之间配置NAT;vasright接口上从vasrift传入的流量配置为NAT内部，而WAN接口将是NAT外部接口。

在此场景中，我们将静态路由用于VRF之间的流量。指向vasright接口的VRF_LEFT上配置了一条通往目标172.16.0.0子网的静态路由，而指向vasright接口的VRF_RIGHT上配置了一条通往源子网192.168.0.0的路由。

注意：请勿将NAT配置为将源IP地址转换为WAN接口IP地址；路由器将返回流量视为发往自身，并且不会将流量转发到VASI接口。

静态 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
```

验证：

<#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
```

动态 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
```

注意：不支持将一个对的两个VASI接口都配置为outside。

验证：

<#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
```

场景2 - Vasileft上的NAT

NAT也可以只配置在左侧，即VRF_LEFT，并在流量发送到VRF_RIGHT之前进行NAT转换。VRF_LEFT上的传入接口被视为NAT内部接口，vasrift 1被配置为NAT外部接口。

在此场景中，我们将静态路由用于VRF之间的流量。指向vasright接口的VRF_LEFT上配置了一条通往目标172.16.0.0子网的静态路由，而指向vasright接口的VRF_RIGHT上配置了一条通往源NATted IP 172.16.1.5的路由。

静态 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
```

验证：

```
<#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
```

动态 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
```

验证：

<#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
```

验证

使用本部分可确认配置能否正常运行。

1. 检查是否将动态/静态路由配置为在两个VRF实例之间路由流量。
2. 检查是否已为正确的VRF配置了NAT。

故障排除

目前没有针对此配置的故障排除信息。

相关信息

- 配置VRF感知软件基础设施
- 技术支持和下载 - 思科系统公司

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。