为TLOC扩展配置静态NAT以实现与对称NAT的互操作性

目录

简介

本文档介绍如何使用NAT过载在TLOC扩展路由器上配置静态NAT，以便与对称NAT后面的对等体配合工作。

建议

Cisco 建议您了解以下主题：

- Cisco Catalyst软件定义的广域网(SD-WAN)
- 网络地址转换 (NAT)
- TLOC扩展

使用的组件

本文档中的信息基于以下软件和硬件版本。

- C8000V版本17.15.1a

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。

问题

Cisco Catalyst SD-WAN Design Guide重点介绍某些类型的网络地址转换(NAT)可能会影响控制连接和BFD隧道的形成。

不协同工作的两种类型NAT是Port/Address Restricted NAT和Symmetric NAT。这些NAT类型要求从内部网络发起会话，以允许每个端口上的流量。这意味着外部流量在未收到内部请求的情况下无法发起到内部网络的连接。

对称NAT后面的站点在与对等站点建立BFD会话时经常遇到困难。当使用NAT过载（也称为端口/地址受限NAT）后的TLOC扩展与站点对等时，这尤其具有挑战性。

拓扑

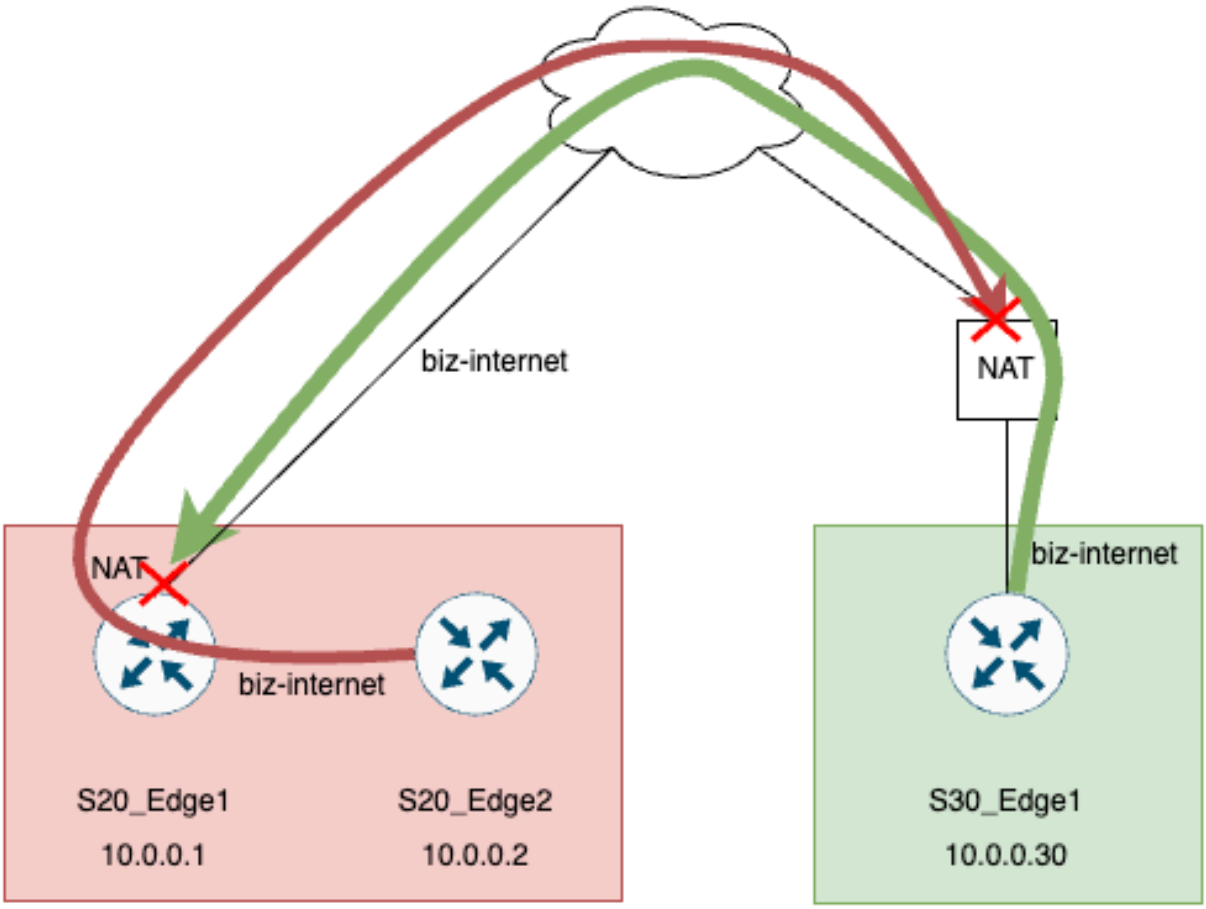
条件

1. S30_Edge1位于对称NAT之后

2. S20_Edge2位于TLOC扩展之后，其中S20_Edge1使用NAT过载(PAT)对来自Edge2的流进行NAT。

这会导致对称NAT设备和S20_Edge1上的BFD问询被丢弃，因为对等体的未知端口不存在会话。

S20_Edge1设备显示这些hello的隐式ACL丢弃，因为它们与NAT表中的任何会话都不匹配。



识别问题

步骤1.检查BFD会话

从S30_Edge1上的show sdwan bfd sessions输出中，可以看到到S20_Edge2(10.0.0.2)的BFD会话已关闭。

```
S30_Edge1#show sdwan bfd sessions
                                       SOURCE TLOC      REMOTE TLOC
SYSTEM IP        SITE ID     STATE       COLOR            COLOR            SOURCE IP
-----------------------------------------------------------------------------------------------------------
10.0.0.2         20          down        biz-internet     biz-internet     192.168.30.2
10.0.0.1         20          up          biz-internet     biz-internet     192.168.30.2
```

步骤2.检查NAT类型

在输出的底部，S30_Edge1上显示NAT类型A。这表示对称NAT。另请注意公有IP 172.16.1.34和端口31048。

```
S30_Edge1# show sdwan control local-properties



site-id                           30
domain-id                         1
protocol                          dtls
tls-port                          0
system-ip                         10.0.0.30




 NAT TYPE: E -- indicates End-point independent mapping
           A -- indicates Address-port dependent mapping
           N -- indicates Not learned
           Note: Requires minimum two vbonds to learn the NAT type

                           PUBLIC          PUBLIC PRIVATE         PRIVATE
INTERFACE                  IPv4            PORT   IPv4            IPv6

-------------------------------------------------------------------------------------------------------------
GigabitEthernet1              172.16.1.34     31048  192.168.30.2    ::
```

步骤3.检查NAT配置

从拓扑中可以知道，S20_Edge2位于TLOC扩展的后面。此时，我们可以检查S20_Edge1上的PAT配置。

S20_Edge1上已存在NAT过载配置

```
S20_Edge1#sh run int gi1
interface GigabitEthernet1
 description biz-internet
 ip dhcp client default-router distance 1
 ip address 192.168.20.2 255.255.255.0
 no ip redirects
 ip nat outside
 load-interval 30
 negotiation auto
 arp timeout 1200
end


S20_Edge1#sh run | i nat
```

```
ip nat inside source list nat-dia-vpn-hop-access-list interface GigabitEthernet1 overload
```

步骤4.检查公共IP和端口

检查S20_Edge2上的show sdwan control local properties输出，以查看公共IP和端口172.16.1.18以及端口5063

```
S20_Edge2#show sdwan control local-properties
```

```
site-id                           20
domain-id                         1
protocol                          dtls
tls-port                          0
system-ip                         10.0.0.2
```

```
 NAT TYPE: E -- indicates End-point independent mapping
           A -- indicates Address-port dependent mapping
           N -- indicates Not learned
           Note: Requires minimum two vbonds to learn the NAT type

                           PUBLIC          PUBLIC PRIVATE         PRIVATE
INTERFACE                  IPv4            PORT   IPv4            IPv6

-------------------------------------------------------------------------------------------------------------
GigabitEthernet2.100          172.16.1.18     5063   192.168.100.2   ::
```

步骤5.检查NAT转换

现在检查S20_Edge1设备上的NAT转换。对于S30_Edge1、IP 172.16.1.34和端口31048，只有到通告的IP和端口的NAT会话。考虑到我们所了解的对称NAT的情况，情况并非如此。至少必须有一个不同于31048的端口(不是像12346这样的标准SD-WAN端口)，如果不是不同的IP和端口组合。

```
 S20_Edge1#sh ip nat translations
Pro  Inside global         Inside local          Outside local         Outside global
udp  192.168.20.2:5063     192.168.100.2:12346   172.16.1.69:12346     172.16.1.69:12346
udp  192.168.20.2:5063     192.168.100.2:12346   172.16.0.102:12446    172.16.0.102:12446
udp  192.168.20.2:5063     192.168.100.2:12346   172.16.1.50:12346     172.16.1.50:12346
udp  192.168.20.2:5063     192.168.100.2:12346   172.16.0.202:12346    172.16.0.202:12346
udp  192.168.20.2:5063     192.168.100.2:12346   172.16.1.82:12346     172.16.1.82:12346
udp  192.168.20.2:5063     192.168.100.2:12346   172.16.1.34:31048     172.16.1.34:31048
udp  192.168.20.2:5063     192.168.100.2:12346   172.16.0.201:12346    172.16.0.201:12346
udp  192.168.20.2:5063     192.168.100.2:12346   172.16.0.101:12446    172.16.0.101:12446
udp  192.168.20.2:5063     192.168.100.2:12346   172.16.1.98:12346     172.16.1.98:12346
```

步骤6.检查FIA跟踪

运行FIA跟踪，仅检查数据包是否在S20_Edge1上丢弃。请记住，IP可能与通告的IP不同，但在本例中为了简单起见，IP与通告的IP不同。

```
S20_Edge1#debug platform condition ipv4 172.16.1.34/32 both
S20_Edge1#debug platform condition start
S20_Edge1#debug platform packet packet 1024 fia
S20_Edge1#debug platform packet packet 1024 fia-trace
S20_Edge1#show platform packet summary
Pkt   Input                     Output                    State  Reason
0     Gi2.100                   Gi1                       FWD
1     internal0/0/recycle:0     Gi1                       FWD
2     Gi2.100                   Gi1                       FWD
3     internal0/0/recycle:0     Gi1                       FWD
4     Gi2.100                   Gi1                       FWD
5     internal0/0/recycle:0     Gi1                       FWD
6     Gi2.100                   Gi1                       FWD
7     internal0/0/recycle:0     Gi1                       FWD
8     Gi1                       Gi1                       DROP   479 (SdwanImplicitAclDrop)
```

检查数据包8，查看此数据包是否为可疑数据包。

```
S20_Edge1#show platform packet packet 8
Packet: 8           CBUG ID: 482
Summary
  Input     : GigabitEthernet1
  Output    : GigabitEthernet1
  State     : DROP 479 (SdwanImplicitAclDrop)
  Timestamp
    Start   : 6120860350139 ns (04/18/2025 02:35:03.873687 UTC)
    Stop    : 6120860374021 ns (04/18/2025 02:35:03.873710 UTC)
Path Trace
  Feature: IPV4(Input)
    Input       : GigabitEthernet1
    Output      :
```

```
    Source      : 172.16.1.34
    Destination : 192.168.20.2
    Protocol    : 17 (UDP)
      SrcPort   : 3618
      DstPort   : 12346
```

这似乎确实是来自S30_Edge1的数据包。

在步骤6中再次检查NAT表，我们可以看到此数据包没有会话。这就是股市下跌的原因。

步骤7.检查BFD计数器

来自S20_Edge2的BFD数据包不会在S30_Edge1上看到，因为它们将被丢弃到设备外部，即NAT设备上。可以通过show sdwan tunnel statistics命令检查BFD Tx/Rx计数器。

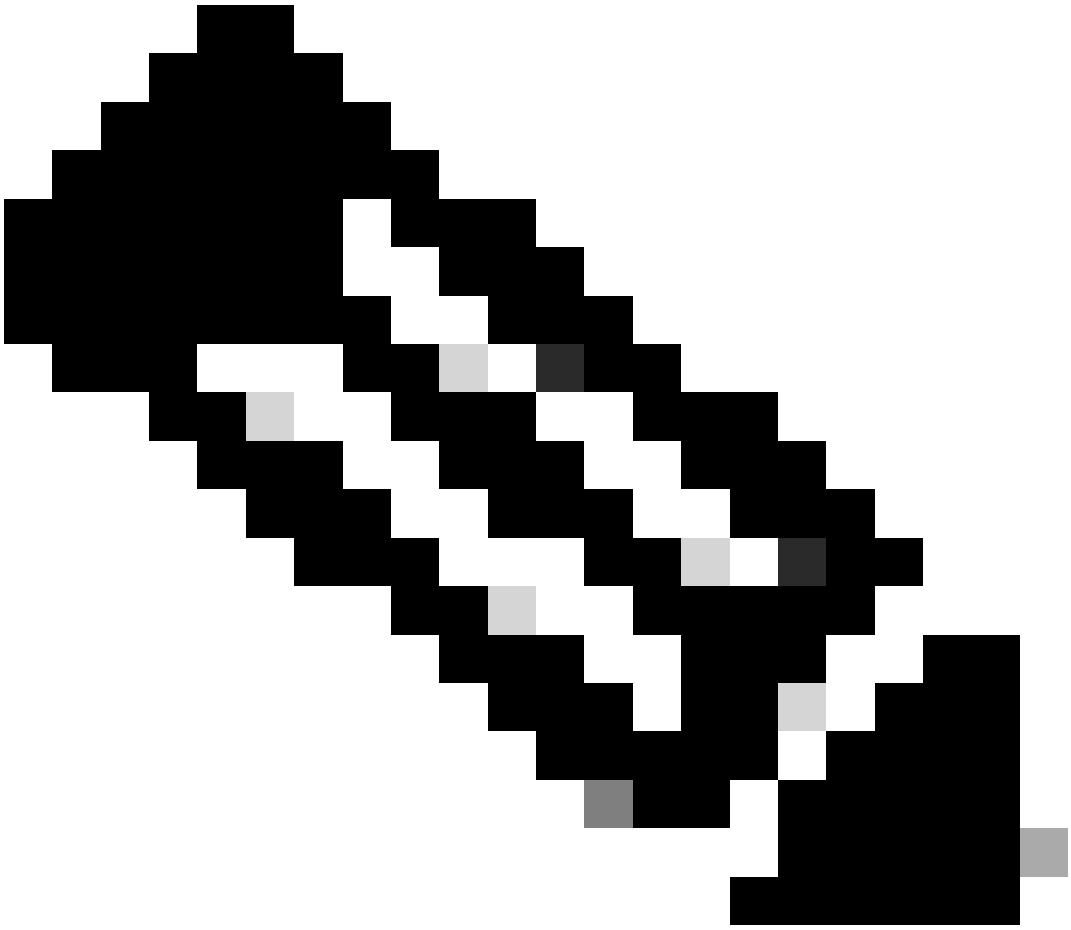
```
S30_Edge1#show sdwan tunnel statistics
tunnel stats ipsec 192.168.30.2 172.16.1.18 12346 12347
 system-ip            10.0.0.2
 local-color          biz-internet
 remote-color         biz-internet
 tunnel-mtu           1438
 tx_pkts              10
 tx_octets            1060
 rx_pkts              0   <<<<<<<<<<<<<
 rx_octets            0
 tcp-mss-adjust       1358
 ipv6_tx_pkts         0
 ipv6_tx_octets       0
 ipv6_rx_pkts         0
 ipv6_rx_octets       0
 tx_ipv4_mcast_pkts   0
 tx_ipv4_mcast_octets 0
 rx_ipv4_mcast_pkts   0
 rx_ipv4_mcast_octets 0
 tx-ipv6-mcast-pkts   0
 tx-ipv6-mcast-octets 0
 rx-ipv6-mcast-pkts   0
 rx-ipv6-mcast-octets 0
```

解决方案

要解决此问题，可以在S20_Edge1上的NAT过载(PAT)之上配置静态NAT，以将所有控制和BFD数据包都配置为一个IP/端口组合。

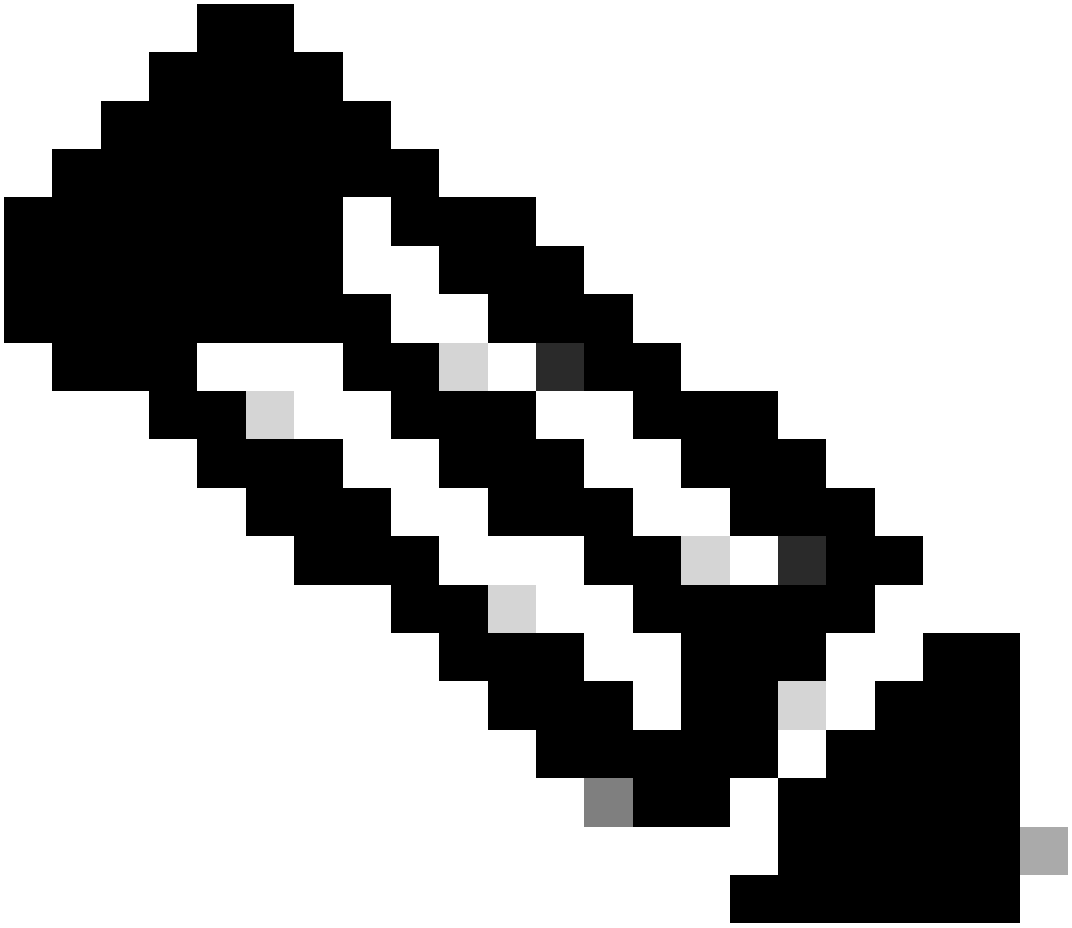
1.首先，必须在此颜色上禁用端口跳跃，或在S20_Edge2上禁用系统范围的端口跳跃。

端口偏移也将作为S20_Edge2的最佳实践添加，因此S20_Edge1和S10_Edge2不会将相同的源端口用于控制连接或BFD隧道。



注意：此配置可通过路由器CLI或通过vManage CLI插件模板执行。

```
S20_Edge2#config-t
S20_Edge2(config)# system
S20_Edge2(config-system)# no port-hop
S20_Edge2(config-system)# port-offset 1
S20_Edge2(config-system)# commit
```



注意：通过选中show sdwan control local-properties，确保S20_Edge2在此配置后使用基本端口12347。如果未使用基本端口，请使用命令clear sdwan control port-index将端口重置回基本端口。如果端口在更高的端口上运行，然后重新启动，这将防止端口发生更改。clear命令将重置控制连接和bfd隧道。

2.在S20_Edge1上配置静态NAT。

```
S20_Edge1#config-t
S20_Edge1(config)# ip nat inside source static udp 192.168.100.2 12347 192.168.20.2 12347 egress-interf
S20_Edge1(config)# commit
```

3.清除S20_Edge1上的NAT转换。

```
S20_Edge1#clear ip nat translation *
```

确认

1.检查其中一个对等体上的BFD会话。

```
S30_Edge1#show sdwan bfd sessions
                                      SOURCE TLOC      REMOTE TLOC
SYSTEM IP        SITE ID     STATE       COLOR            COLOR            SOURCE IP
-------------------------------------------------------------------------------------------------
10.0.0.2         20          up          biz-internet     biz-internet     192.168.30.2
```

2.检查S20_Edge1上的NAT会话。

```
S20_Edge1#sh ip nat translations
Pro  Inside global         Inside local          Outside local         Outside global
udp  192.168.20.2:12347    192.168.100.2:12347   ---                   ---
udp  192.168.20.2:12347    192.168.100.2:12347   172.16.0.202:12346    172.16.0.202:12346
udp  192.168.20.2:12347    192.168.100.2:12347   172.16.1.50:12346     172.16.1.50:12346
udp  192.168.20.2:12347    192.168.100.2:12347   172.16.0.102:12446    172.16.0.102:12446
udp  192.168.20.2:12347    192.168.100.2:12347   172.16.1.34:50890     172.16.1.34:50890
udp  192.168.20.2:12347    192.168.100.2:12347   172.16.1.69:12346     172.16.1.69:12346
udp  192.168.20.2:12347    192.168.100.2:12347   172.16.1.98:12346     172.16.1.98:12346
udp  192.168.20.2:12347    192.168.100.2:12347   172.16.0.101:12446    172.16.0.101:12446
udp  192.168.20.2:12347    192.168.100.2:12347   172.16.0.201:12346    172.16.0.201:12346
udp  192.168.20.2:12347    192.168.100.2:12347   172.16.1.82:12346     172.16.1.82:12346
udp  192.168.20.2:12347    192.168.100.2:12347   172.16.0.1:13046      172.16.0.1:13046
Total number of translations: 11
```

现在可以看到所有控制连接和BFD隧道都通过NAT连接到配置的IP和端口192.168.20.2:12347。此外，到172.16.1.34的连接与通过S30_Edge1通告给vSmart的端口完全不同。请参阅端口50890。

3.请注意，在S30_Edge1的show sdwan control local properties输出中，通告的IP和端口为172.16.1.34，端口为60506。

```
S30_Edge1#show sdwan control local-properties

site-id                         30
domain-id                       1
protocol                        dtls
tls-port                        0
system-ip                       10.0.0.30
```

```
 NAT TYPE: E -- indicates End-point independent mapping
           A -- indicates Address-port dependent mapping
           N -- indicates Not learned
           Note: Requires minimum two vbonds to learn the NAT type

                         PUBLIC          PUBLIC PRIVATE         PRIVATE
INTERFACE                IPv4            PORT   IPv4            IPv6

-------------------------------------------------------------------------------------------------------------
GigabitEthernet1              172.16.1.34     60506  192.168.30.2    ::
```

参考

[Cisco Catalyst SD-WAN设计指南]

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）。