為TLOC擴展配置靜態NAT以實現與對稱NAT的互操作性

目錄

簡介

本文檔介紹如何使用NAT過載在TLOC擴展路由器上配置靜態NAT，以便與對稱NAT後的對等體合作。

行動

思科建議您瞭解以下主題：

- Cisco Catalyst軟體定義廣域網路(SD-WAN)
- 網路位址轉譯(NAT)
- TLOC擴展

採用元件

本文件中的資訊是以下列軟體和硬體版本為依據.

- C8000V版本17.15.1a

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

問題

Cisco Catalyst SD-WAN設計手冊強調某些型別的網路地址轉換(NAT)可能會影響控制連線和BFD隧道的形成。

兩種不協同工作的NAT型別是埠/地址受限NAT和對稱NAT。這些NAT型別要求從內部網路啟動會話，以允許每個埠上的流量。這意味著外部流量在沒有來自內部的事先請求的情況下無法啟動到內部網路的連線。

對稱NAT背後的站點在與對等站點建立BFD會話時經常遇到困難。當在NAT過載（也稱為埠/地址受限NAT）之後使用TLOC擴展與站點對等時，這尤其具有挑戰性。

拓撲

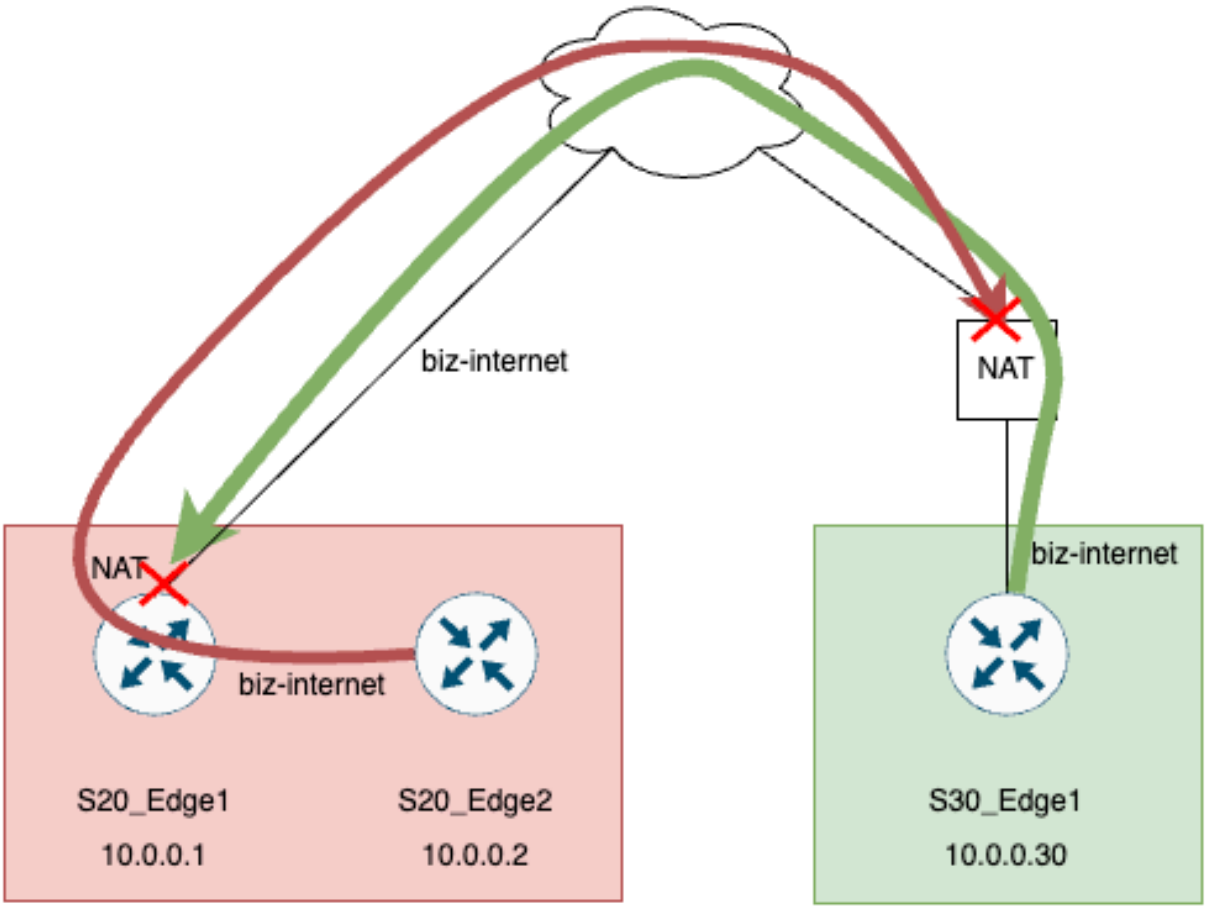
狀況

1. S30_Edge1位於對稱NAT之後

2. S20_Edge2位於TLOC擴展之後，其中S20_Edge1使用NAT過載(PAT)對來自Edge2的流進行NAT。

這會導致對稱NAT裝置和S20_Edge1上的BFD hello被丟棄，因為對等體中的未知埠不存在會話。

S20_Edge1裝置顯示這些hello的隱式ACL丟棄，因為它們與NAT表中的任何會話都不匹配。



找出問題

步驟1.檢查BFD會話

在S30_Edge1上的show sdwan bfd sessions輸出中，可以看到到S20_Edge2(10.0.0.2)的BFD會話已關閉。

```
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
```

步驟2.檢查NAT型別

在輸出的底部，在S30_Edge1上看到NAT型別A。這表示對稱NAT。另請注意公用IP 172.16.1.34和埠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    ::
```

步驟3.檢查NAT配置

從拓撲中可以得知，S20_Edge2位於TLOC擴展的後面。此時，我們可以檢查S20_Edge1上的PAT配置。

S20_Edge1上已經存在NAT過載配置

```
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
```

步驟4.檢查公共IP和埠

檢查S20_Edge2上的show sdwan control local properties輸出，檢視公共IP和埠172.16.1.18以及埠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   ::
```

步驟5.檢查NAT轉換

現在檢查S20_Edge1裝置上的NAT轉換。對於S30_Edge1、IP 172.16.1.34和埠31048，只有到通告的IP和埠的NAT會話。考慮到我們對對稱NAT的瞭解，情況並非如此。必須至少有一個與31048不同的埠(不是像12346這樣的標準SD-WAN埠)，如果不是不同的IP和埠組合。

```
 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
```

步驟6.檢查FIA跟蹤

運行FIA跟蹤，只是為了檢查資料包是否在S20_Edge1上被丟棄。請記住，IP可能與通告的IP不同，但為了簡便起見，IP可能不同。

```
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)
```

檢查資料包8，檢視此資料包是否為可疑資料包。

```
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
```

這似乎的確是來自S30_Edge1的封包。

在步驟6中再次檢查NAT表，我們可以看到沒有此資料包的會話。這就是股市下跌的原因。

步驟7.檢查BFD計數器

來自S20_Edge2的BFD資料包不會在S30_Edge1上看到，因為這些資料包將被丟棄到裝置之外（在NAT裝置上）。可以通過show sdwan tunnel statistics命令檢查BFD Tx/Rx計數器。

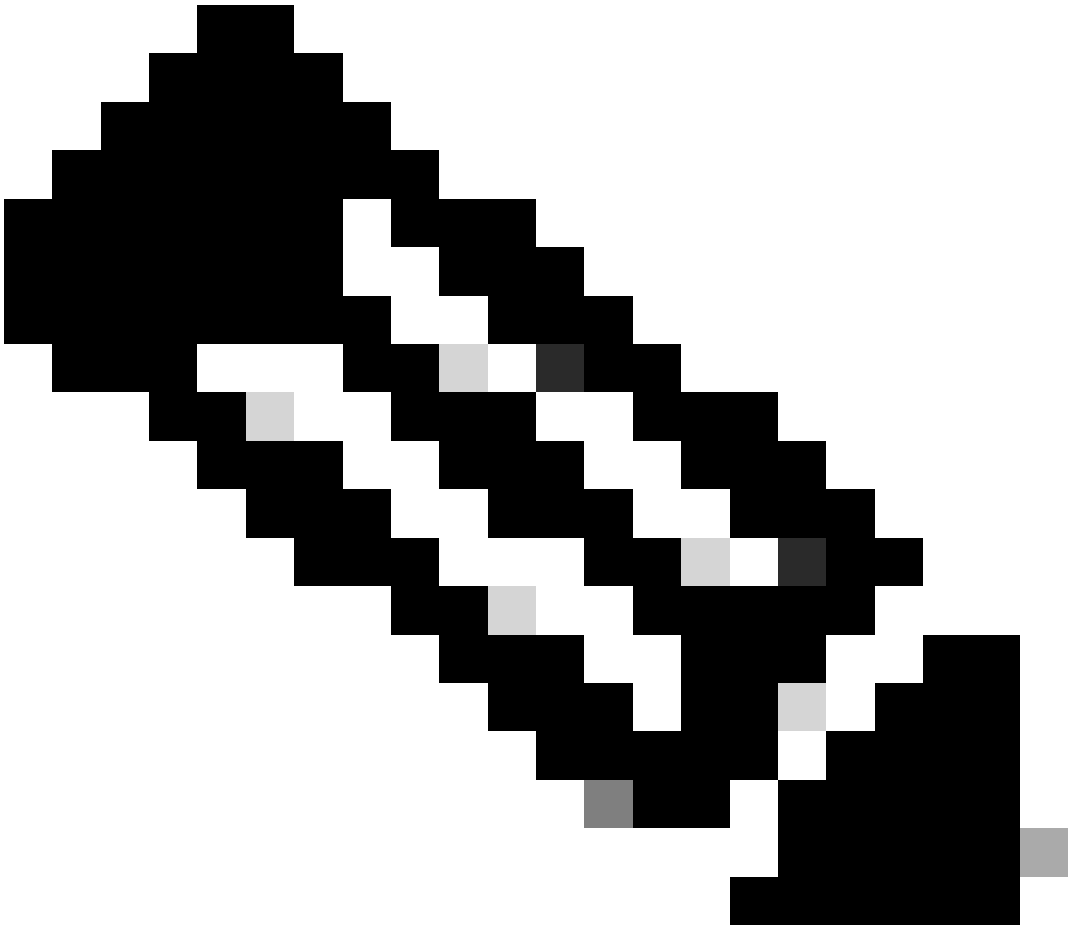
```
S30_Edge1#show sdwan tunnel statistics
tunnel stats ipsec 192.168.30.2 172.16.1.18 12346 12347
 system-ip            10.0.0.2
 local-color          biz-internet
 remote-color         biz-internet
 tunnel-mtu           1438
 tx_pkts              10
 tx_octets            1060
 rx_pkts              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
```

解決方案

要解決此問題，可以在S20_Edge1上的NAT過載(PAT)之上配置靜態NAT，將所有控制和BFD資料包傳送到單個IP/埠組合。

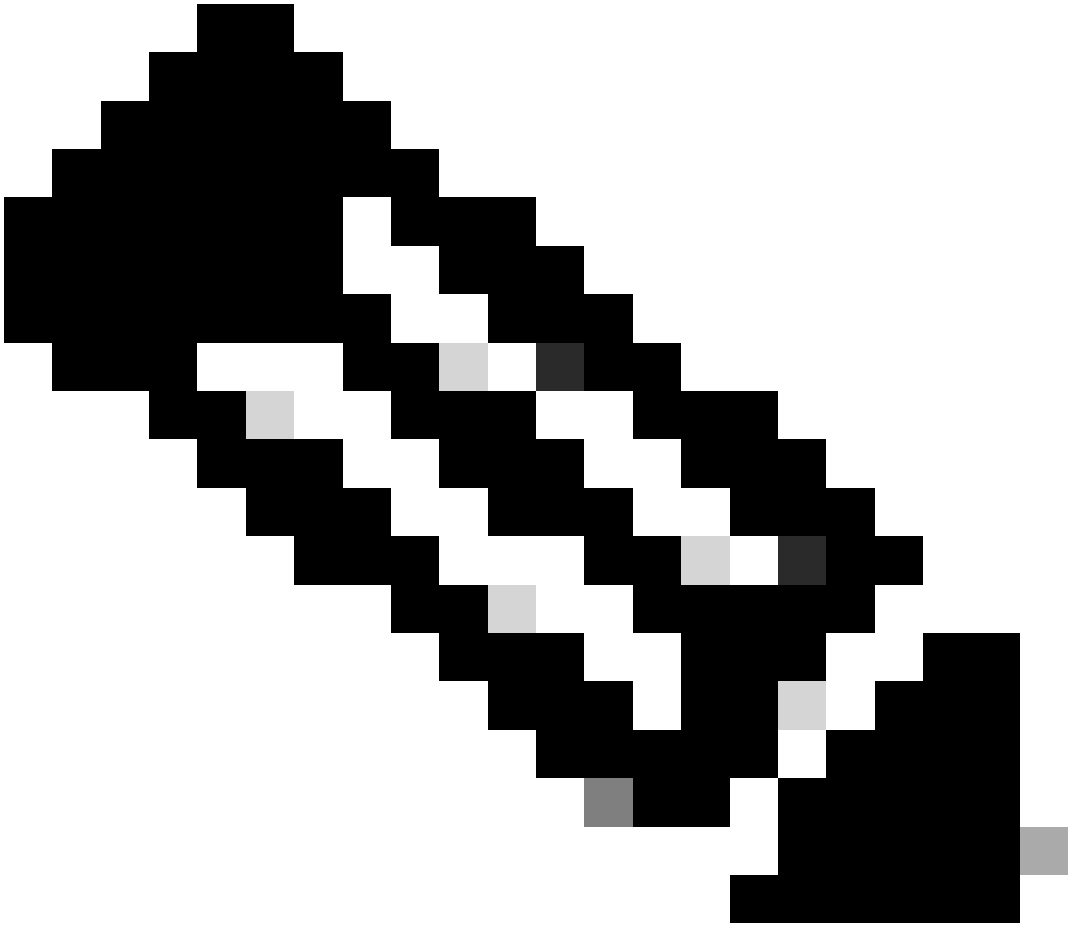
1.首先，必須在此顏色上禁用埠跳躍，或在S20_Edge2上禁用系統範圍的埠跳躍。

埠偏移也會作為S20_Edge2的最佳做法新增，因此S20_Edge1和S10_Edge2不會將相同的源埠用於控制連線或BFD隧道。



附註：此配置可以通過路由器CLI或通過vManage CLI外掛模板執行。

```
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
```



附註：通過檢查show sdwan control local-properties，確保S20_Edge12347在此配置後使用基本埠VLAN。如果未使用基本埠，請使用命令clear sdwan control port-index將埠重置回基本埠。如果連線埠在更高的連線埠上執行，且之後會重新開機，這可以防止連線埠變更。clear命令將重置控制連線和bfd隧道。

2.在S20_Edge1上配置靜態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轉換。

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

驗證

1.檢查其中一個對等體上的BFD會話。

```
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.檢查S20_Edge1上的NAT會話。

```
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
```

現在可看到，所有控制連線和BFD隧道都通過NAT連線到配置的IP和埠192.168.20.2:12347。此外，到172.16.1.34的連線與S30_Edge1向vSmart通告的連線完全不同。請參閱埠50890。

3.請注意，在S30_Edge1的show sdwan control local properties輸出中，通告的IP和埠為172.16.1.34，且埠為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    ::
```

參考資料

[Cisco Catalyst SD-WAN設計手冊]

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。