Statische NAT für TLOC-Erweiterung für Interoperabilität mit symmetrischer NAT konfigurieren

Inhalt

Einleitung

In diesem Dokument wird die Konfiguration der statischen NAT auf einem TLOC Extension Router unter Verwendung von NAT Overload für die Zusammenarbeit mit Peers hinter der symmetrischen NAT beschrieben.

Empfehlungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Cisco Catalyst Software-Defined Wide Area Network (SD-WAN)
- Network Address Translation (NAT)
- TLOC-Erweiterung

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen.

- C8000V Version 17.15.1a

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Problem

Im Cisco Catalyst SD-WAN-Designleitfaden wird erläutert, wie bestimmte Arten der Network Address Translation (NAT) die Bildung von Steuerverbindungen und BFD-Tunneln beeinträchtigen können.

Die beiden NAT-Typen, die nicht zusammenarbeiten, sind Port/Address Restricted NAT und Symmetric NAT. Diese NAT-Typen erfordern, dass Sitzungen vom internen Netzwerk initiiert werden, um Datenverkehr auf jedem Port zuzulassen. Dies bedeutet, dass externer Datenverkehr keine Verbindung zum internen Netzwerk initiieren kann, ohne zuvor eine interne Anfrage gestellt zu haben.

Bei Standorten mit symmetrischer NAT treten häufig Schwierigkeiten beim Aufbau von BFD-Sitzungen mit Peer-Standorten auf. Dies ist besonders schwierig, wenn ein Peering mit einem Standort durchgeführt wird, der die TLOC-Erweiterung hinter NAT Overload verwendet (auch als Port/Address Restricted NAT bezeichnet).

Topologie

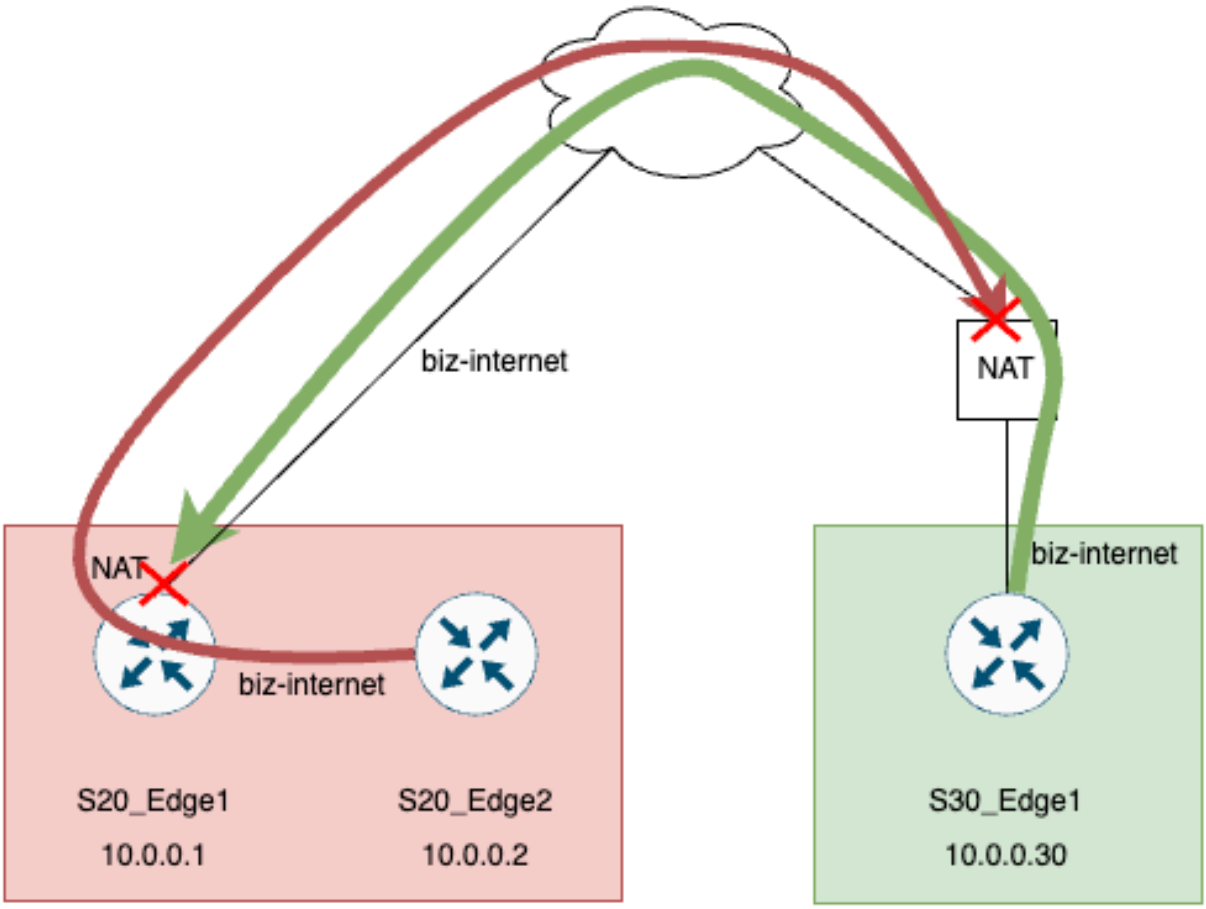
Bedingungen

1. S30_Edge1 befindet sich hinter einer symmetrischen NAT

2. S20_Edge2 befindet sich hinter der TLOC-Erweiterung, wobei S20_Edge1 NAT Overload (PAT) verwendet, um die Datenflüsse von Edge2 NAT durchzuführen.

Dies führt dazu, dass die BFD-Hellos auf dem symmetrischen NAT-Gerät und dem S20_Edge1 verworfen werden, da keine Sitzung für den unbekannten Port vom Peer vorhanden ist.

Das Gerät S20_Edge1 zeigt eine implizite ACL-Löschung für diese Hellos an, da sie keiner Sitzung in der NAT-Tabelle entsprechen.



Identifizieren des Problems

Schritt 1: BFD-Sitzungen überprüfen

Aus der Ausgabe von show sdwan bfd sessions auf S30_Edge1 wird ersichtlich, dass die BFD-Sitzung zu S20_Edge2, 10.0.0.2 ausgefallen ist.

```
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
```

Schritt 2: Überprüfen des NAT-Typs

Unten in der Ausgabe wird der NAT-Typ A auf S30_Edge1 angezeigt. Dies gibt Symmetric NAT an. Beachten Sie auch die öffentliche IP 172.16.1.34 und Port 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    ::
```

Schritt 3: Überprüfen der NAT-Konfiguration

Aus der Topologie ist bekannt, dass sich S20_Edge2 hinter der TLOC-Erweiterung befindet. An diesem Punkt können wir die PAT-Konfiguration auf dem S20_Edge1 prüfen.

NAT-Überlastungskonfiguration ist bereits auf S20_Edge1 vorhanden

```
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
```

Schritt 4: Überprüfen der öffentlichen IP-Adresse und des Ports

Aktivieren Sie show sdwan control local properties output on S20_Edge2, um die öffentliche IP und Port 172.16.1.18 und Port 5063 anzuzeigen.

```
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   ::
```

Schritt 5: Überprüfen der NAT-Übersetzungen

Überprüfen Sie nun die NAT-Übersetzungen auf dem S20_Edge1-Gerät. Es gibt nur eine NAT-Sitzung mit der angegebenen IP und dem angegebenen Port für S30_Edge1, IP 172.16.1.34 und Port 31048. Angesichts der Informationen über die symmetrische NAT ist dies nicht der Fall. Es muss sich mindestens ein Port von 31048 unterscheiden (kein Standard-SD-WAN-Port wie

12346), wenn nicht eine andere IP- UND Port-Kombination vorhanden ist.

```
 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
```

Schritt 6: FIA-Ablaufverfolgung überprüfen

Führen Sie eine FIA-Ablaufverfolgung aus, um zu überprüfen, ob Pakete auf S20_Edge1 verworfen werden. Beachten Sie, dass die IP nicht mit der angegebenen übereinstimmen muss, in diesem Fall jedoch aus Gründen der Einfachheit.

```
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)
```

Überprüfen Sie Paket 8, um festzustellen, ob es sich um das verdächtige Paket handelt.

```
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
```

Dies scheint das Paket von S30_Edge1 zu sein.

Wenn Sie sich in Schritt 6 erneut die NAT-Tabelle ansehen, sehen Sie, dass keine Sitzung für dieses Paket besteht. Das ist der Grund für den Rückgang.

Schritt 7: BFD-Zähler überprüfen

BFD-Pakete vom S20_Edge2 sind am S30_Edge1 nicht sichtbar, da sie außerhalb des Geräts auf dem NAT-Gerät verworfen werden. Die BFD-Tx/Rx-Zähler können mit dem Befehl show sdwan tunnel statistics überprüft werden.

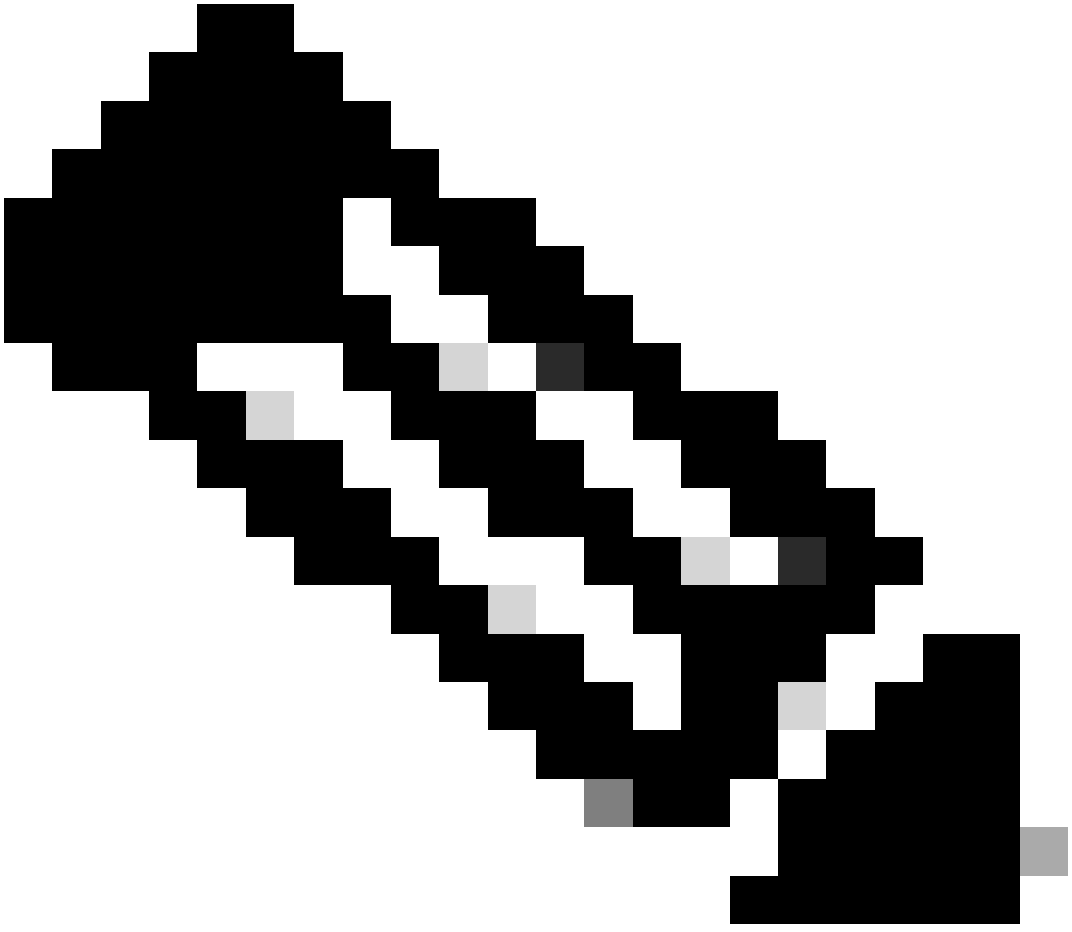
```
S30_Edge1#show sdwan tunnel statistics
tunnel stats ipsec 192.168.30.2 172.16.1.18 12346 12347
 system-ip            10.0.0.2
 local-color          biz-internet
 remote-color         biz-internet
 tunnel-mtu           1438
 tx_pkts              10
 tx_octets            1060
 rx_pkts             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

Lösung

Um dieses Problem zu beheben, kann eine statische NAT über der NAT-Überlastung (PAT) auf S20_Edge1 konfiguriert werden, um alle Steuerungs- und BFD-Pakete auf eine einzelne IP/Port-Kombination zu übertragen.

1. Zuerst muss Port-Hopping auf dieser Farbe oder systemweit auf S20_Edge2 deaktiviert werden.

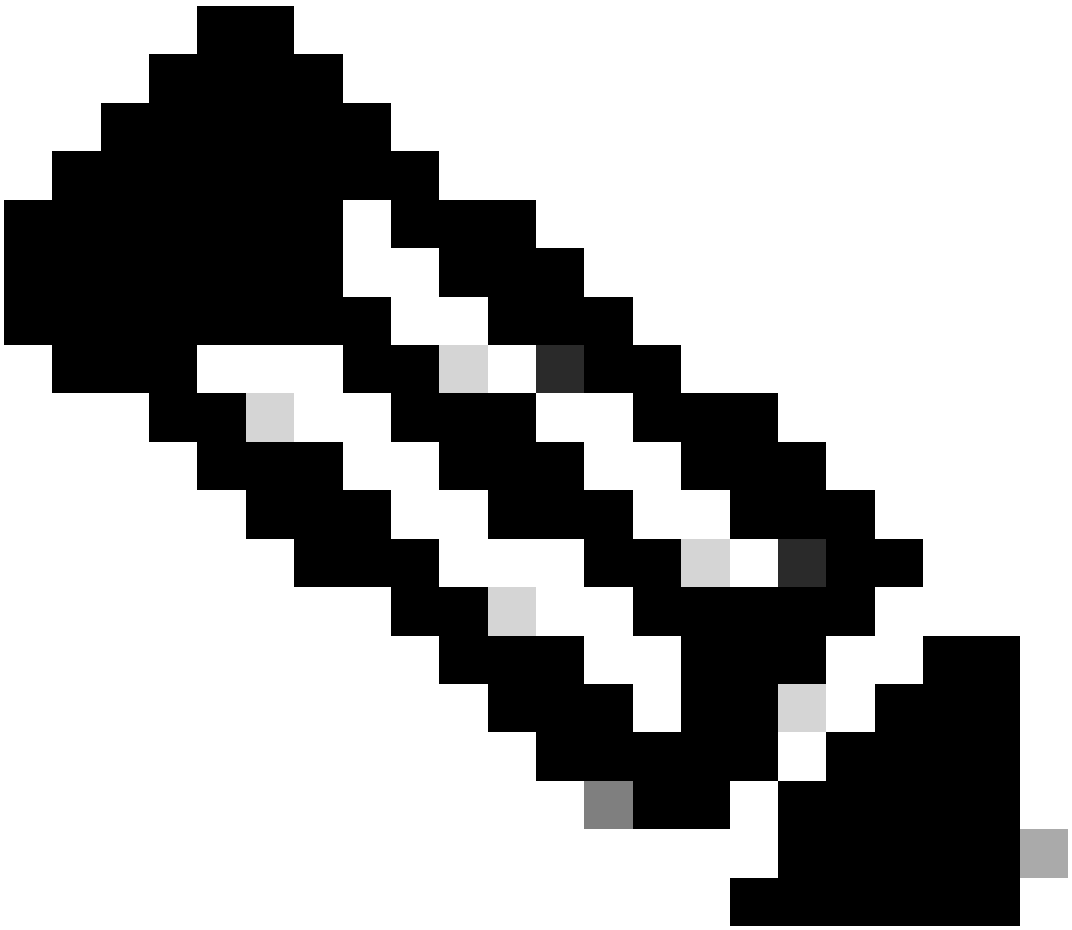
Ein Port-Offset wird auch als Best Practice für S20_Edge2 hinzugefügt, sodass S20_Edge1 und S10_Edge2 nicht denselben Quell-Port für Steuerverbindungen oder BFD-Tunnel verwenden.



> Anmerkung: Diese Konfiguration kann über die Router-CLI oder eine Add-On-Vorlage für vManage CLI vorgenommen werden.

```
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
```



> Anmerkung: Stellen Sie sicher, dass S20_Edge2 nach dieser Konfiguration den Basisport 12347 verwendet, indem Sie show sdwan control local-properties überprüfen. Wenn der Basisport nicht verwendet wird, setzen Sie den Befehl clear sdwan control port-index zurück auf den Basisport. Dadurch wird verhindert, dass sich der Port ändert, wenn er auf einem höheren Port ausgeführt wurde, und später neu gestartet wird. Mit dem Befehl clear werden Steuerverbindungen und bfd-Tunnel zurückgesetzt.

---

2. Konfigurieren Sie die statische NAT auf S20_Edge1.

```
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. Löschen Sie die NAT-Übersetzungen auf S20_Edge1.

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

Verifizierung

1. Überprüfen Sie die BFD-Sitzungen eines Peers.

```
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. Überprüfen Sie die NAT-Sitzungen auf S20_Edge1.

```
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
```

Nun wird deutlich, dass alle Steuerverbindungen und BFD-Tunnel NAT zu der konfigurierten IP und Port sind, 192.168.20.2:12347. Auch die Verbindung zu 172.16.1.34 ist zu einem völlig anderen Port als vSmart durch S30_Edge1 angekündigt. Siehe Port 50890.

3. Beachten Sie in der Ausgabe von show sdwan control local properties von S30_Edge1, dass die angegebene IP und der angegebene Port 172.16.1.34 und Port 60506 sind.

```
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    ::
```

Referenzen

[Cisco Catalyst SD-WAN - Designleitfaden]

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.