대칭 NAT와의 상호 운용성을 위해 TLOC 확장용 고정 NAT 구성

목차

소개

이 문서에서는 대칭 NAT 뒤에 있는 피어에서 작동하도록 NAT 오버로드를 사용하여 TLOC 확장 라우터에서 고정 NAT를 구성하는 방법에 대해 설명합니다.

권장 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

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

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- C8000V 버전 17.15.1a

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.

문제

Cisco Catalyst SD-WAN 설계 가이드는 특정 유형의 NAT(Network Address Translation)가 제어 연결 및 BFD 터널의 형성에 영향을 미칠 수 있음을 강조합니다.

함께 작동하지 않는 두 가지 NAT 유형은 포트/주소 제한 NAT 및 대칭 NAT입니다. 이러한 NAT 유형을 사용하려면 각 포트의 트래픽을 허용하기 위해 내부 네트워크에서 세션을 시작해야 합니다. 이는 외부 트래픽이 내부로부터의 사전 요청 없이 내부 네트워크에 대한 연결을 시작할 수 없음을 의미합니다.

대칭 NAT 뒤에 있는 사이트에서는 피어 사이트와 BFD 세션을 설정하는 데 자주 문제가 발생합니다. 이는 NAT 오버로드(포트/주소 제한 NAT라고도 함) 뒤에 TLOC 확장을 사용하여 사이트를 피어링하는 경우 특히 어렵습니다.

토폴로지

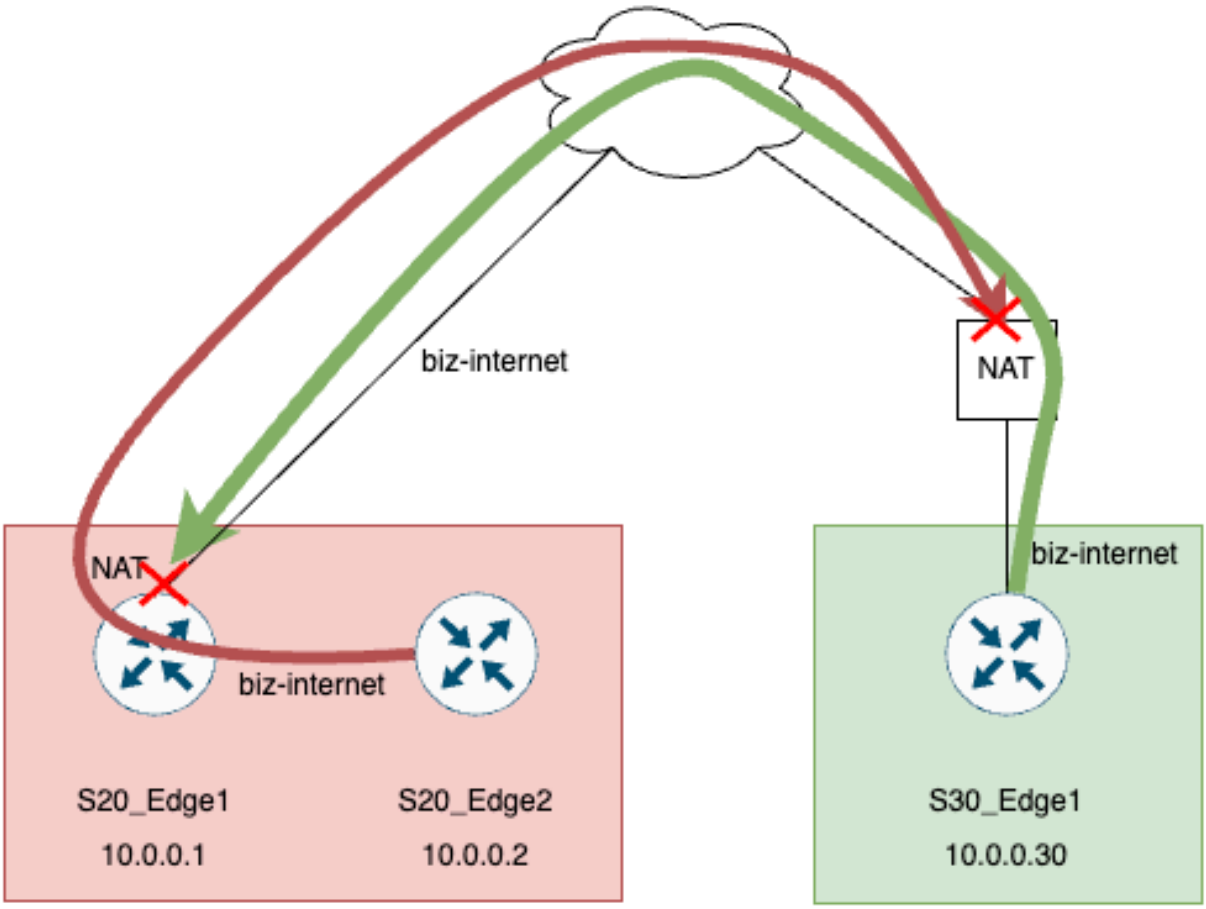
조건

1. S30_Edge1이 대칭 NAT 뒤에 있음

2. S20_Edge2는 S20_Edge1이 NAT 오버로드(PAT)를 사용하여 Edge2의 플로우를 NAT하는 TLOC 확장 뒤에 있습니다.

그러면 피어의 알 수 없는 포트에 대한 세션이 없기 때문에 대칭 NAT 디바이스에서 BFD Hello가 삭제되고 S20_Edge1이 삭제됩니다.

S20_Edge1 디바이스는 NAT 테이블의 어떤 세션과도 일치하지 않기 때문에 이러한 Hello에 대한 암시적 ACL 삭제를 표시합니다.



문제 파악

1단계. BFD 세션 확인

S30_Edge1의 show sdwan bfd 세션 출력에서 S20_Edge2에 대한 BFD 세션 10.0.0.2가 다운되었음을 알 수 있습니다.

```
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
```

2단계. NAT 유형 확인

출력의 맨 아래에 S30_Edge1에 NAT 유형 A가 표시됩니다. 이는 대칭 NAT를 나타냅니다. 또한 퍼블릭 IP 172.16.1.34 및 포트 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    ::
```

3단계. NAT 컨피그레이션을 확인합니다

토폴로지에서는 S20_Edge2가 TLOC 확장의 뒤에 있는 것으로 알려져 있습니다. 이제 S20_Edge1에서 PAT 컨피그레이션을 확인할 수 있습니다.

NAT 오버로드 컨피그레이션이 S20_Edge1에 이미 있습니다.

```
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
```

4단계. 공용 IP 및 포트 확인

공용 IP 및 포트 172.16.1.18 및 포트 5063을 보려면 S20_Edge2의 show sdwan control local properties output(sdwan 제어 로컬 속성 출력 표시)을 선택합니다

```
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   ::
```

5단계. NAT 변환 확인

이제 S20_Edge1 디바이스에서 NAT 변환을 확인합니다. S30_Edge1, IP 172.16.1.34 및 포트 31048에 대한 알려진 IP 및 포트에 대한 NAT 세션만 있습니다. 대칭 NAT에 대해 알고 있는 사항을 고려하면 그렇지 않습니다. 다른 IP AND 포트 조합이 아니면 31048과 다른 포트가 하나 이상 있어야 합니다(12346 같은 표준 SD-WAN 포트가 아님).

```
 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
```

6단계. FIA 추적 확인

S20_Edge1에서 패킷이 삭제되는지 확인하기 위해 FIA 추적을 실행합니다. IP가 알려진 IP와 동일하지 않을 수 있지만, 이 경우 간소화를 위해 삭제됩니다.

```
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)
```

패킷 8을 선택하여 의심스러운 패킷인지 확인합니다.

```
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
```

S30_Edge1의 패킷인 것 같습니다.

6단계에서 NAT 테이블을 다시 확인하면 이 패킷에 대한 세션이 없음을 확인할 수 있습니다. 그것이 하락의 이유입니다.

7단계. BFD 카운터 확인

S20_Edge2의 BFD 패킷은 NAT 디바이스에서 디바이스 외부로 삭제되므로 S30_Edge1에서 볼 수 없습니다. BFD Tx/Rx 카운터는 show sdwan tunnel statistics 명령을 통해 확인할 수 있습니다.

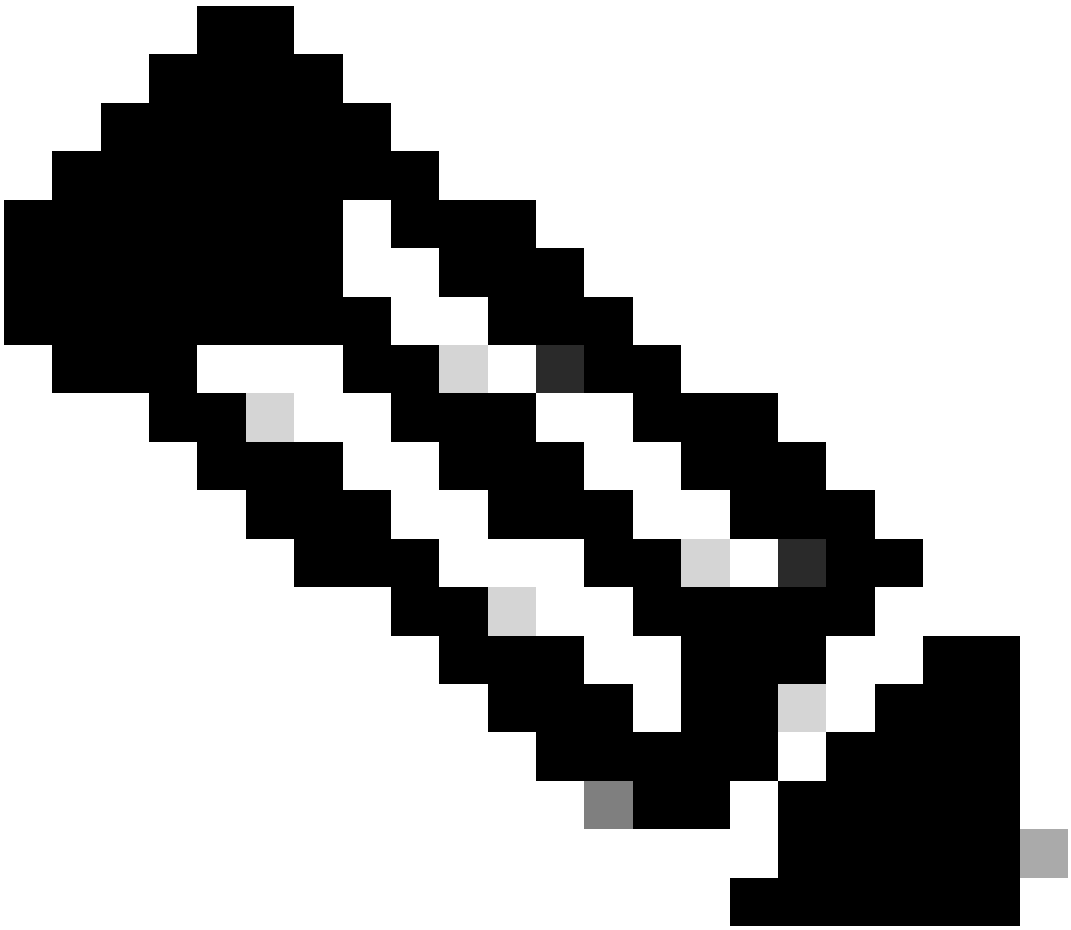
```
S30_Edge1#show sdwan tunnel statistics
tunnel stats ipsec 192.168.30.2 172.16.1.18 12346 12347
 system-ip            10.0.0.2
 local-color          biz-internet
 remote-color         biz-internet
 tunnel-mtu           1438
 tx_pkts              10
 tx_octets            1060
 rx_pkts             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

솔루션

이를 해결하기 위해 S20_Edge1의 NAT 오버로드(PAT) 위에 고정 NAT를 구성하여 모든 제어 패킷과 BFD 패킷을 단일 IP/포트 조합으로 NAT할 수 있습니다.

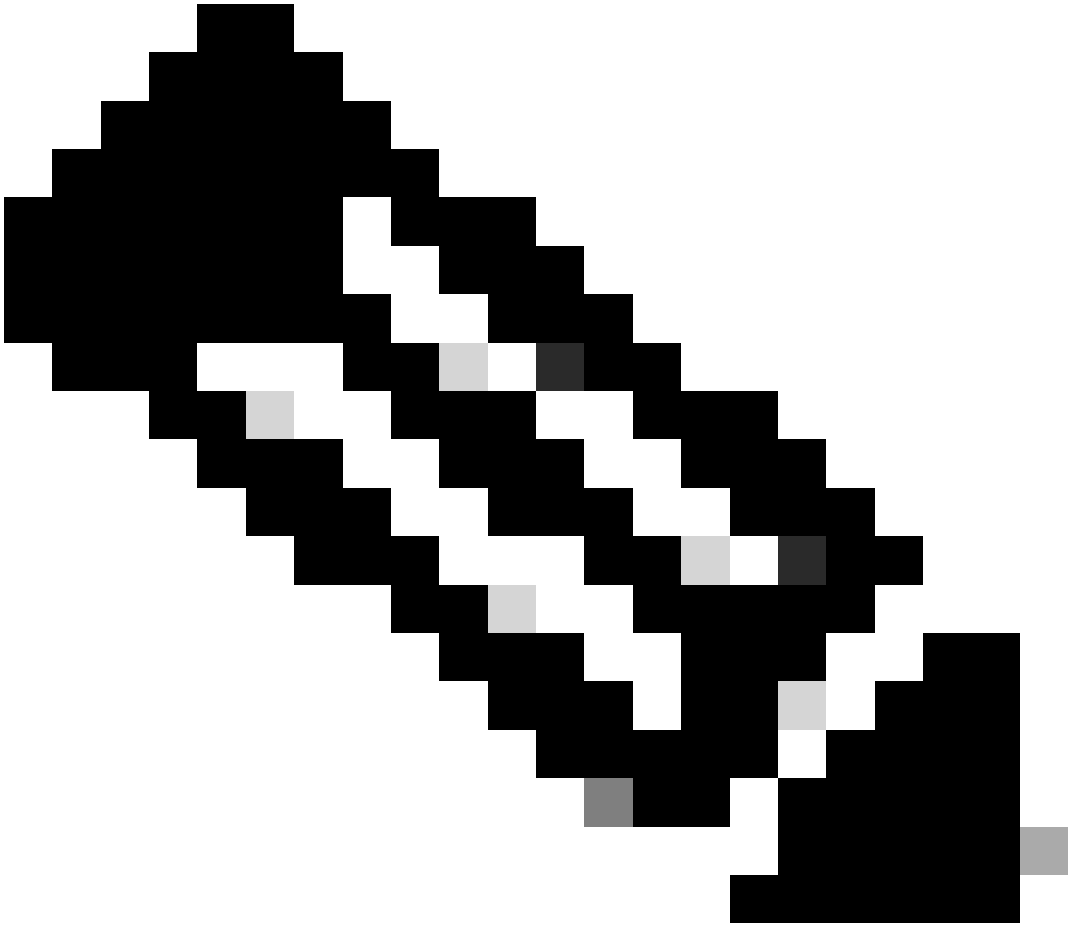
1. 먼저 이 색상에서 또는 S20_Edge2에서 시스템 전체에서 포트 호핑을 비활성화해야 합니다.

S20_Edge1과 S10_Edge2가 제어 연결 또는 BFD 터널에 동일한 소스 포트를 사용하지 않도록 S20_Edge2에 대한 모범 사례로 포트 오프셋도 추가됩니다.



참고: 이 컨피그레이션은 라우터 CLI 또는 vManage CLI 애드온 템플릿을 통해 수행할 수 있습니다.

```
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
```



참고: show sdwan control local-properties를 선택하여 S20_Edge2가 이 컨피그레이션 이후12347 기본 포트 포트를 사용하고 있는지 확인합니다. 기본 포트를 사용하지 않는 경우 clear sdwan control port-index 명령을 사용하여 포트를 다시 기본 포트로 재설정합니다. 이렇게 하면 포트가 상위 포트에서 실행 중이었다가 나중에 다시 부팅하는 경우 포트가 변경되지 않습니다. clear 명령은 제어 연결 및 bfd 터널을 재설정합니다.

---

2. S20_Edge1에서 고정 NAT를 구성합니다.

```
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. S20_Edge1에서 NAT 변환을 지웁니다.

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

확인

1. 피어 중 하나에서 BFD 세션을 확인합니다.

```
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. S20_Edge1에서 NAT 세션을 확인합니다.

```
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
```

이제 모든 제어 연결 및 BFD 터널은 구성된 IP 및 포트 192.168.20.2:12347에 대한 NAT입니다. 또한 172.16.1.34에 대한 연결은 S30_Edge1에서 vSmart에 알린 것과 완전히 다른 포트에 대한 연결입니다. 포트 50890을 참조하십시오.

3. show sdwan control local properties 출력(S30_Edge1)에서 광고된 IP 및 포트가 172.16.1.34 및 포트 60506임을 확인합니다.

```
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    ::
```

참조

[Cisco Catalyst SD-WAN 설계 가이드]

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.