중복 NAT 엔드포인트로 SD-WAN 허브 터널 문제 해결

목차

소개

사전 요구 사항

- 요구 사항
- 사용되는 구성 요소

배경 정보

- 컨트롤 플레인 NAT 학습
- 데이터 플레인 NAT 학습 및 VCONTROL
- 포트 보존, 포트 중첩, 포트 임의 지정

샘플 토폴로지

충돌이 발생하는 이유

- 서로 다른 vBond에서 동일한 퍼블릭 엔드포인트를 관찰할 수 있음
- 동일한 광고가 하나의 허브에 도달함
- 반복되는 브랜치 주소로 Private-as-Public 충돌
- NAT 엔드포인트 재할당

증상 및 영향

문제 진단

- 1단계. 소프트웨어 및 스포크 전송 상태 기록
- 2단계. OMP에서 중복 엔드포인트 찾기
- 3단계. 논리 TLOC를 허브 세션 소유권과 비교
- 4단계. NAT 게이트웨이가 실제로 수행하는 작업을 확인합니다.
- 5단계. Wireshark에서 VCONTROL 검사
- 6단계. 영향 받는 경로 확인 및 증거 보존

해결 방법 및 제한 사항

- 고유한 할당으로 안정적인 엔드포인트 독립적 매핑 사용
- 서로 다른 스포크 간에 포트 겹치기 사용 안 함
- 소형 제어 그룹에 대해 포트 오프셋 사용
- 소스 포트 보존 사용 안 함 또는 임의 할당 사용
- 별도의 공용 주소 또는 예약 포트 블록
- 대체 전송 및 좌표 복구 유지

관련 소프트웨어 결함

부록: IPv4 VCONTROL 트레일러 디코딩

관련 정보

소개

이 문서에서는 스포크가 하나의 공용 NAT(Network Address Translation) 엔드포인트를 공유할 때 허브 터널 장애를 식별하고 완화하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco Catalyst SD-WAN(software-defined wide area network) 아키텍처 및 제어 연결
- OMP(Overlay Management Protocol), TLOC(Transport Locator), BFD(Bidirectional Forwarding Detection) 및 IPsec(IP Security)
- MPLS(Multiprotocol Label Switching) 전송 네트워크
- NAT 매핑 및 필터 동작
- Wireshark를 통한 기본 패킷 분석

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco IOS® XE Catalyst SD-WAN 라우터
- Cisco Catalyst SD-WAN Controller(vSmart)
- Cisco Catalyst SD-WAN Validator(vBond)

Cisco IOS XE 17.18.2에서 페어와이즈 키가 작동 중인 상태로 허브 세션 소유권 오류가 재현되었습니다. 명령 가용성 및 출력 필드는 플랫폼과 릴리스에 따라 달라집니다.

예를 들어 RFC 5737에서 예약한 개인 주소 또는 문서 주소를 일반 디바이스 이름과 함께 사용합니다. CLI 발췌문이 단축되고 표준화된 식별자를 사용합니다. 인터페이스 이름 및 일부 출력 필드는 플랫폼 및 릴리스에 따라 달라집니다.

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.

⚠ 주의: 컨피그레이션 변경 및 연결 재설정으로 인해 트래픽이 중단될 수 있습니다. 승인된 유지 관리 계획을 사용합니다. 초기 진단 명령은 읽기 전용입니다.

배경 정보

대칭 NAT가 올바르게 식별되는 시나리오부터 시작합니다. 스포크 A는 vBond 1에 등록하고 스포크 B는 vBond 2에 등록합니다. NAT 게이트웨이는 대상이 서로 다를 경우 RFC 7857에서 허용하는 대로 이러한 연결에 동일한 변환된 소스 IP 주소 및 포트를 할당할 수 있습니다. 두 스포크 모두 NAT 유형 A를 보고하는 경우에도 결과적으로 공용 인터넷 TLOC에 대해 동일한 공용 엔드포인트를 광고할 수 있습니다.

샘플 토폴로지에서는 공용 인터넷 색상을 사용합니다. 동일한 시나리오는 biz-internet과 같은 다른 공용 색상과 관련될 수 있습니다. 실제 영향을 받는 전송 색상에 진단 필터를 적용합니다. 리터럴 공용 인터넷 색상은 필수 조건이 아닙니다.

참고: Cisco Catalyst SD-WAN은 동일한 공용 IP 주소 및 UDP 포트를 공통 수신 에지에 광고하는 서로 다른 사이트의 TLOC를 지원하지 않습니다. 이 충돌 조건의 수신기 동작은 예측할 수 없습니다. 대칭 NAT가 올바르게 식별된 경우에도 이 문제가 발생할 수 있습니다. 올바른 NAT 분류만으로는 알려진 끝점이 고유하지 않습니다.

컨트롤 플레인 NAT 학습

Edge는 vBond에 등록하는 동안 전용 전송 주소와 포트를 전송합니다. vBond는 해당 연결의 소스 주소와 포트를 관찰하고 관찰된 엔드포인트를 Edge로 반환합니다. Edge는 OMP를 통해 이 정보를 공용 인터넷 또는 비즈 인터넷과 같은 공용 색상이 있는 TLOC를 포함하여 TLOC의 공용 주소 및 포트 특성으로 광고할 수 있습니다.

이 관찰은 해당 vBond와의 연결을 설명합니다. 수신 종속 NAT의 경우 허브에 대한 매핑은 다를 수 있습니다. 라우터는 매핑 동작을 분류하기 위해 NAT 관찰을 비교합니다. show sdwan control local-properties에서 A는 주소와 포트에 의존하는 매핑을 의미하고, E는 엔드포인트에 독립적인 매핑을 의미합니다. 표시된 분류는 라우터의 결정을 설명합니다. nat 변환 테이블 또는 패킷 캡처는 NAT 게이트웨이의 실제 동작을 확인합니다.

예를 들어 show sdwan control local-properties를 실행하고 전송에 대한 NAT TYPE 열을 찾습니다. 이 단축 출력에서는 NAT 유형 범례 및 선택한 인터페이스 열이 정규화된 주소와 함께 유지됩니다.

<#root>

Spoke-A# show sdwan control local-properties

```
...
 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                          NAT
INTERFACE                 IPv4          PORT   IPv4           PORT    COLOR         STATE      TYPE
GigabitEthernet2          192.168.9.11   12346  192.168.9.11   12346   mpls          up         E
GigabitEthernet3          203.0.113.10   23012  192.168.11.11  12346   biz-internet  up         A
```

biz-internet transport는 A를 보고하고 203.0.113.10:23012를 공용 엔드포인트로 광고합니다. MPLS 전송은 E를 보고하며 동일한 프라이빗 및 퍼블릭 엔드포인트를 포함합니다. NAT 유형에서 분류를 읽습니다. 주소 또는 포트 일치만 NAT 유형을 식별하지 않습니다. N은 라우터가 분류를 학습하지 않았음을 의미합니다.

데이터 플레인 NAT 학습 및 VCONTROL

허브가 암호화된 BFD 패킷을 처리하려면 먼저 해당 피어 및 터널의 인바운드 IPsec SA(Security Association)를 찾아야 합니다. SA는 암호화 키 및 패킷을 인증하고 해독하는 데 필요한 기타 상태를 식별합니다. 수신기는 ESP(Encapsulating Security Payload) SPI(Security Parameters Index)와 함께 엔드포인트 정보를 사용하여 해당 상태를 찾습니다. SPI만 전역적으로 고유한 스포크 식별자가 아닙니다.

대칭 NAT 뒤에 있는 스포크는 일반적으로 도달 가능한 허브로 향하는 트래픽을 시작합니다. 이렇게 하면 해당 특정 대상에 대한 매핑이 생성됩니다. 허브에 표시되는 소스 주소 또는 포트는 vBond를 통해 이전에 학습하고 OMP에서 광고한 퍼블릭 엔드포인트와 다를 수 있습니다. 따라서 수신된 외부 헤더가 설치된 터널 상태의 엔드포인트와 항상 일치하지는 않습니다. 허브는 BFD를 해독하기 전에 이 새로운 온-와이어 엔드포인트를 알려진 원격 TLOC 및 해당 IPsec 상태와 연결하는 방법이 필요합니다.

여기서 설명하는 IPv4 BFD-over-IPsec 형식의 경우 SD-WAN은 엔드포인트 정보를 암호화된 BFD 페이로드 외부의 UDP 페이로드 끝에 있는 보이는 VCONTROL 트레일러에 배치합니다. 허브는 암호 해독 전에 이 정보를 읽을 수 있습니다. VCONTROL은 암호화 키가 아닌 엔드포인트 정보를 전달하며, 피어 ID를 자체적으로 설정하지 않습니다.

예를 들어 초기 터널 설정 중에 데이터 플레인 학습이 완료되기 전에 다음을 수행합니다.

```
Spoke B advertised through OMP:       203.0.113.10:12346
Spoke B observed at the hub:          203.0.113.10:45678
VCONTROL carried source endpoint:    203.0.113.10:12346
```

수신자는 먼저 일반 엔드포인트/SPI 조회를 시도합니다. 해당 조회에서 SA를 찾지 못하면 VCONTROL 소스 엔드포인트가 대안을 제공합니다. 이 예에서 허브는 패킷이 203.0.113.10:45678에서 도착하더라도 알려진 원격 TLOC와 연결된 인바운드 SA를 찾기 위해 203.0.113.10:12346을 로컬 대상 컨텍스트 및 SPI와 함께 사용할 수 있습니다.

선택한 SA는 수신 키 컨텍스트를 제공합니다. SPI는 해당 컨텍스트 내에서 적용 가능한 키 생성을 선택합니다. 그런 다음 허브는 IPsec 인증 및 암호 해독을 수행합니다. 필수 검사를 통과한 패킷만 BFD 처리에 사용할 수 있습니다. 읽기 가능한 트레일러 또는 성공적인 조회만으로는 성공적인 인증, 암호 해독 또는 BFD 수신을 입증하지 못합니다.

따라서 대칭 NAT에서는 관찰된 소스 포트와 전달된 소스 포트 간의 차이가 정상일 수 있습니다. 피어 관계가 작동하려면 허브는 패킷을 올바른 터널 및 키 상태와 연결하고 실제 반환 엔드포인트를 학습해야 합니다. 이 예에서 학습이 성공하면 허브가 반환 트래픽을 203.0.113.10:45678로 보낼 수 있습니다. 이는 vBond를 통한 컨트롤 플레인 학습과는 별개입니다.

VCONTROL은 수신자가 기존 엔드포인트/SPI 일치를 재정의하도록 강제하지 않습니다. 중복 엔드포인트 상태가 패킷을 잘못된 피어 또는 키 생성과 연결하는 경우 트레일러는 복구를 보장하지 않습니다. 조회 힌트를 제공합니다. 올바른 주변 터널 및 암호화 상태 없이 동일한 엔드포인트를 전달하는 두 피어를 구분할 수 없습니다.

VCONTROL은 NAT 유형 E가 보고될 때 적용 가능한 BFD 패킷에도 존재합니다. 이 플래그는 대칭 NAT 플래그가 아니며, 모든 일반 IPsec 데이터 패킷에 포함되지 않습니다. 여기서 설명하는 IPv4 BFD 포맷의 경우 두 가지 프라이빗 컬러 간에는 public-TLOC 정보가 생략된다.

데이터 평면을 통해 학습된 피어 특정 엔드포인트가 스포크가 모든 대상에 대해 OMP 광고를 새 엔드포인트로 교체해야 한다는 의미는 아닙니다. 다른 학습된 매핑은 대칭 NAT 통과의 예상 부분입니다.

터널이 가동되면 해당 터널에 대해 자체 변환된 엔드포인트를 학습한 발신자는 해당 엔드포인트를 소스 정보로 전달할 수 있습니다. 이는 발신자의 터널당 공용 엔드포인트이며 원격 엔드포인트나 새로운 전역 OMP 광고는 아닙니다. 항상 동일한 관찰 기간의 패킷, OMP 광고 및 세션 상태를 비교합니다.

포트 보존, 포트 중첩, 포트 임의 지정

다음은 서로 다른 동작입니다.

동작	의미
소스 포트 보존	NAT 게이트웨이는 스포크의 원래 UDP 소스 포트(예: 12346)를 변환된 소스 포트로 유지하려고 시도합니다.
대상 간에 포트 중복	NAT 게이트웨이는 하나의 변환된 IP를 재사용합니다. 서로 다른 외부 대상과 통신하는 서로 다른 내부 엔드포인트의 포트입니다.
포트 임의 지정	NAT 게이트웨이는 무작위 할당 방법을 사용하여 변환된 포트를 선택합니다.

동작	의미
엔드포인트에 구애받지 않는 매핑	하나의 내부 엔드포인트는 외부 대상 간에 동일한 변환된 엔드포인트를 유지하지만 매핑은 존재합니다.

RFC 7857, 섹션 3에서는 대상이 다를 경우 서로 다른 내부 엔드포인트에 대해 중복되는 외부 포트를 허용합니다. NAT는 5개의 튜플을 사용하여 흐름을 구분합니다. 이렇게 하면 동일한 목적지에 대해 두 개의 식별할 수 없는 UDP 플로우를 동시에 허용할 수 없습니다. 임의배분과 보존은 별개의 배분선택이다. 둘 다 엔드포인트 독립성을 설정하지 않습니다.

샘플 토폴로지

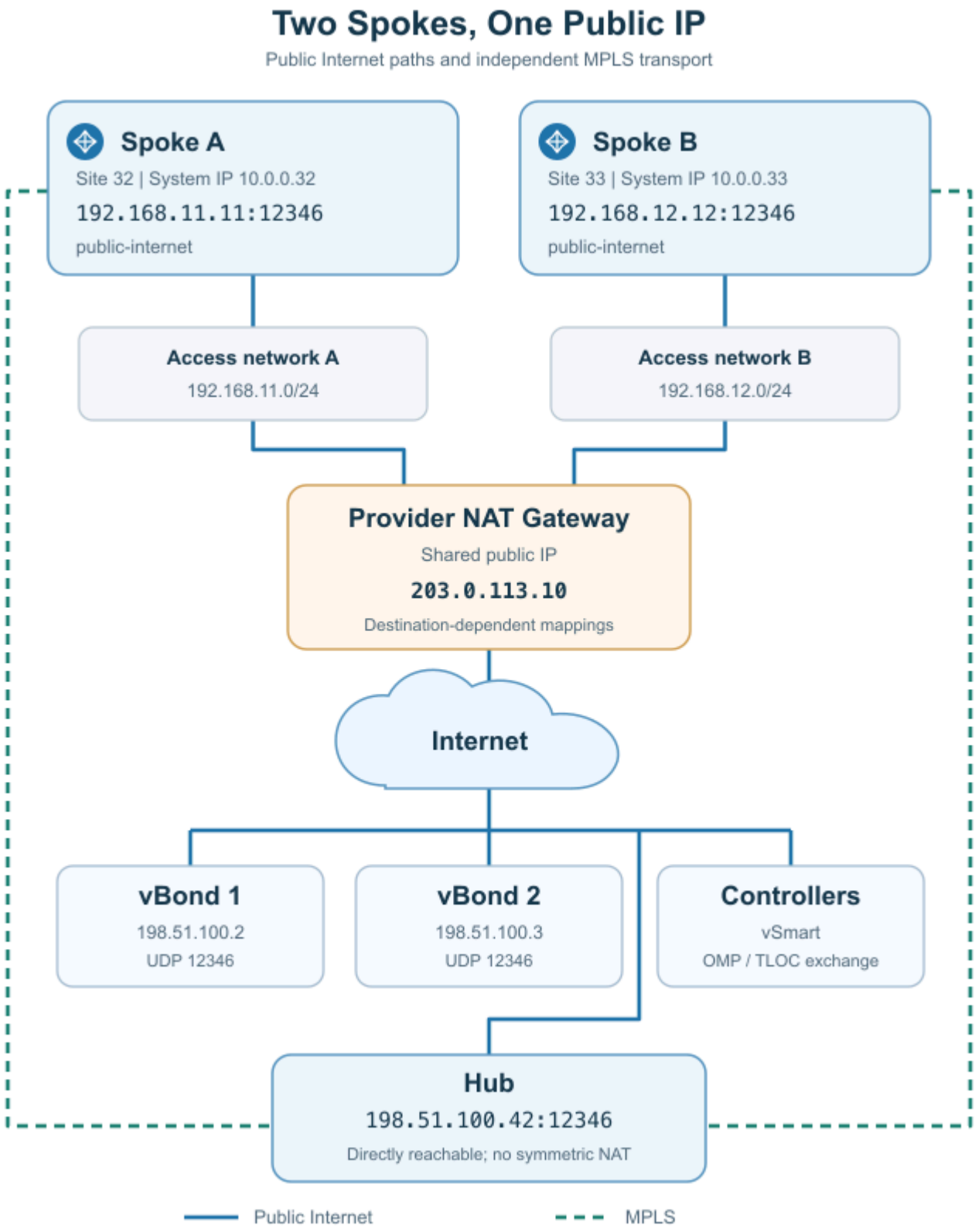

그림 1. 공유 NAT 게이트웨이, 별도의 스포크 액세스 네트워크 및 독립적인 MPLS 전송

스포크 A는 192.168.11.11:12346을 사용하고 스포크 B는 192.168.12.12:12346을 사용합니다. 둘 다 NAT 게이트웨이를 통해 공용 주소 203.0.113.10을 공유합니다. 허브는 직접 연결 가능한 주소를 가지며 대칭 NAT 뒤에 있지 않습니다. 두 스포크는 프라이빗 엔드포인트가 다르더라도 동일한 퍼블릭 IP:포트를 광고할 수 있습니다.

충돌이 발생하는 이유

서로 다른 vBond에서 동일한 퍼블릭 엔드포인트를 관찰할 수 있음

다음과 같은 동시 UDP 매핑을 고려하십시오.

피어	개인 소스	변환된 소스	대상
A	192.168.11.11:12346	203.0.113.10:12346	vBond 1, 198.51.100.2:12346
B	192.168.12.12:12346	203.0.113.10:12346	vBond 2, 198.51.100.3:12346

NAT가 원격 엔드포인트도 확인하기 때문에 회신이 올바르게 반환됩니다. vBond 1의 회신은 A에 대한 매핑에 속합니다. vBond 2의 회신은 B에 대한 매핑에 속합니다.

두 라우터 모두 다른 vBond에 연결하여 대상에 따른 매핑을 올바르게 탐지할 수 있습니다. 예를 들어, 각 스포크에 대한 프라이빗 소스 튜플을 변경하지 않고 다음과 같은 관찰 순서를 고려합니다.

피어	첫 번째로 수락된 vBond 관찰	다른 vBond와 비교	결과
A	vBond 1은 203.0.113.10:12346을 반환합니다.	vBond 2는 203.0.113.10:40001을 반환합니다.	NAT A; 유지된 공용 튜플 203.0.113.10:12346
B	vBond 2는 203.0.113.10:12346을 반환합니다.	vBond 1은 203.0.113.10:40002을 반환합니다.	NAT A; 유지된 공용 튜플 203.0.113.10:12346

vBond 관찰은 라우터마다 다르므로 NAT A를 탐지하는 것이 정확합니다. 보존된 첫 번째 관찰은 두 라우터에서 일치합니다. 분류 A는 모든 스포크에 고유한 공용 포트를 할당하지 않으며, 두 vBond를 모두 방문한다고 해서 고유성이 보장되는 것은 아닙니다.

각 스포크는 등록 회신에서 vBond에 의해 관찰된 공용 주소 및 포트를 수신하고 보존된 관찰을 사용하여 로컬 전송 속성을 채웁니다. 스포크는 OMP를 통해 SD-WAN 컨트롤러에 광고하는 TLOC 특성에 공용 엔드포인트와 사설 엔드포인트를 포함합니다. 그런 다음 컨트롤러는 해당 제어 정책에 따라 TLOC를 다른 에지에 배포합니다. vBond 자체는 OMP 광고를 시작하지 않습니다.

두 스포크가 모두 관찰된 동일한 퍼블릭 엔드포인트를 유지하는 경우 OMP는 다음을 포함할 수 있습니다.

```
TLOC system IP   Color            Public endpoint        Private endpoint
10.0.0.32        public-internet  203.0.113.10:12346     192.168.11.11:12346
10.0.0.33        public-internet  203.0.113.10:12346     192.168.12.12:12346
```

시스템 IP가 다르기 때문에 이러한 TLOC는 서로 다른 논리적 TLOC으로 유지됩니다.

동일한 광고가 하나의 허브에 도달함

NAT 게이트웨이는 동일한 허브에 연결할 때 두 스포크를 구분해야 합니다. 한 가지 가능한 할당은 다음과 같습니다.

피어	Hub로 소스 변환	대상
A	203.0.113.10:12346	198.51.100.42:12346
B	203.0.113.10:45678	198.51.100.42:12346

허브에는 동일한 대상 엔드포인트를 알리는 두 개의 논리적 피어가 있으며, 패킷은 서로 다른 실제 엔드포인트에서 전송될 수 있습니다. 일반적인 대칭 NAT 작업 하에서 데이터 평면 학습은 반환 매핑을 설정하는 데 도움이 됩니다.

허브 세션 소유권 제한은 서로 다른 피어가 이 전송 키로 선택한 세션 상태를 공유할 때 발생합니다.

```
Hub-local IP + hub-local port + remote IP + remote port + protocol
```

두 광고 모두 동일한 키를 선택하는 경우, 이후 피어의 업데이트가 공유 상태의 소유권 정보를 대체할 수 있습니다. 한 피어에 대한 세션을 이후에 취소, 삭제 또는 재생성하는 경우 다른 피어에 대한 IPsec/BFD 상태가 방해될 수 있습니다. 데이터 플레인 학습은 해당 상태가 잘못된 피어 또는 플로우 생성과 이미 연결되어 있는 경우 복구를 보장하지 않습니다.

표시된 트레일러는 독립적인 피어 식별자가 아닙니다. 두 스포크는 동일한 소스 엔드포인트를 전달할 수 있습니다. 허브가 잘못된 피어 또는 키 생성에 속하는 기존 IPsec 상태를 선택하면 패킷이 허브에 도달하더라도 인증 및 학습이 실패할 수 있습니다. 특정 패킷에 대해 해당 시퀀스를 설정하려면 Cisco TAC(Technical Assistance Center)에서 선택한 SA를 해당 피어 및 생성과 연계해야 합니다. 패킷 트레일러만으로는 이를 입증할 수 없습니다.

동일한 공용 IP만으로는 충돌이 발생하지 않습니다. 일반적으로 원격 포트마다 다른 전송 키가 생성됩니다. 선택한 허브-로컬 주소, 로컬 포트 및 프로토콜도 확인합니다. 세 번째 피어가 동일한 엔드

포인트를 광고하는 경우에도 해당 키를 두고 경쟁할 수 있습니다. 실패 패턴은 이벤트 순서에 따라 달라집니다.

반복되는 브랜치 주소로 Private-as-Public 충돌

Cisco 버그 ID CSCwx12986은 Edge가 NAT 비교 중에 자동 소스-포트 홉 후에 공용 TLOC 특성에서 사설 RFC 1918 튜플을 광고하도록 할 수 있습니다. 서로 다른 브랜치가 동일한 개인 주소 및 포트를 재사용하는 경우 잘못된 공용 특성이 피어 간에 일치할 수 있으며 허브 세션 소유권 문제가 발생할 수 있습니다.

예를 들어, 두 스포크 모두 별도의 브랜치 방화벽 뒤에서 192.168.11.11을 사용할 수 있습니다. 각 방화벽은 브랜치 네트워크를 별도로 유지하고 소스 주소를 변환합니다. 업스트림 제공자 NAT 게이트웨이가 이를 다시 변환하는 경우 경로에는 두 개의 NAT 단계 또는 이중 NAT가 있습니다. 별도의 VRF(Virtual Routing and Forwarding) 컨텍스트도 중복되는 브랜치 주소를 격리시키는 또 다른 방법입니다.

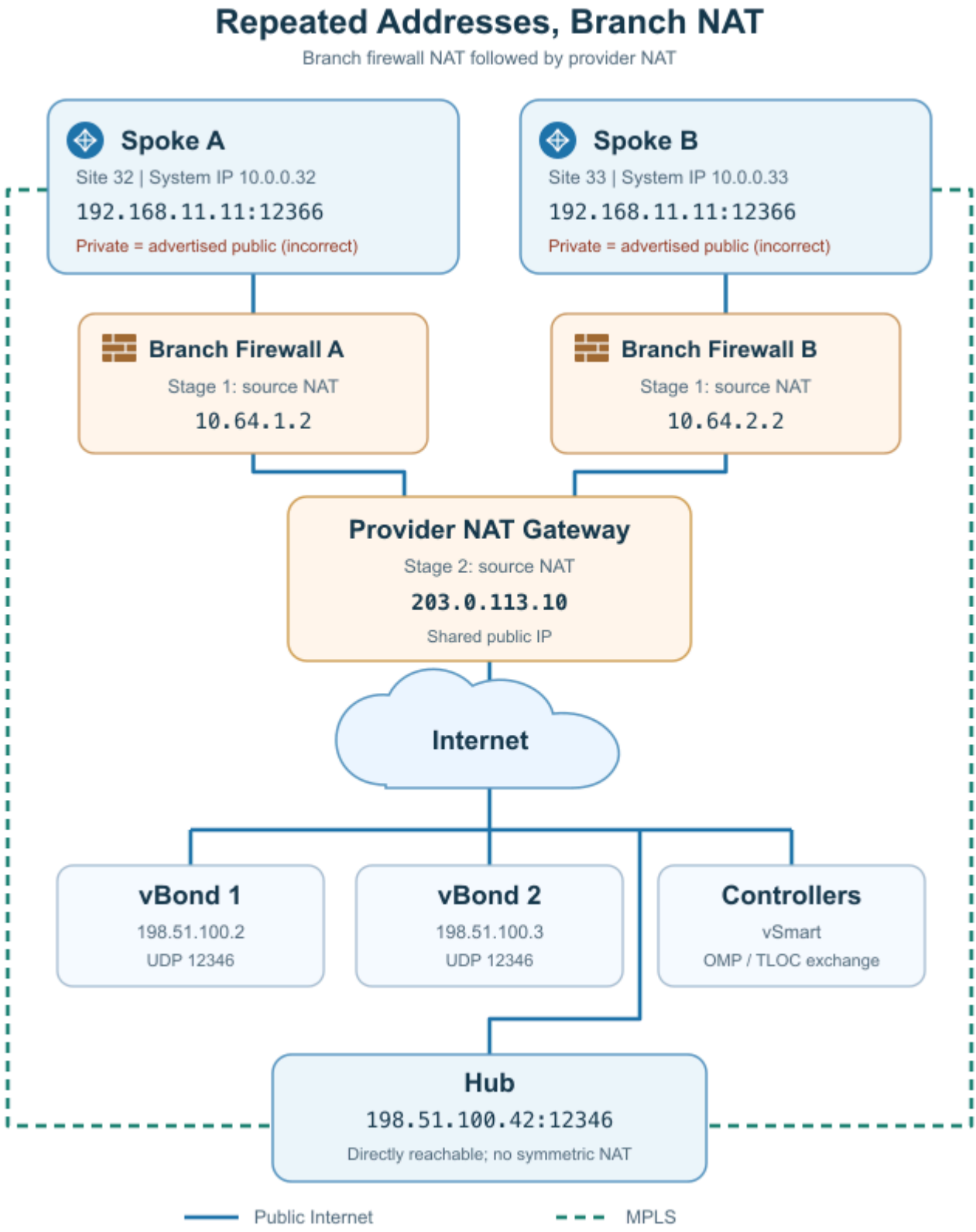

그림 2. 브랜치 방화벽 및 사업자 NAT 변환 잘못된 공용 TLOC 특성은 원래의 개인 엔드포인트를 유지하는 반면, 패킷은 변환된 소스 주소를 사용합니다.

두 스포크에 공용 인터넷 TLOC의 결함이 발생하고 동일한 포스트 홉 소스 포트를 사용하는 경우, 허브는 다음 광고를 수신할 수 있습니다.

피어	포트 홉 후 개인 엔드포인트	잘못된 공용 TLOC 끝점
A	192.168.11.11:12366	192.168.11.11:12366
B	192.168.11.11:12366	192.168.11.11:12366

참고: 반복되는 개인 주소와 이중 NAT는 Cisco 버그 ID CSCwx12986 자체에 대한 전제 조건은 아닙니다. 추가 교차 피어 충돌에는 알려진 IP:포트 값과 동일한 허브-로컬 주소, 포트 및 프로토콜이 일치해야 합니다. 서로 다른 알려진 포트를 가진 동일한 프라이빗 IP는 이 충돌을 설정하지 않습니다.

NAT가 없는 전송에서는 공용 및 사설 주소 평등이 일반적입니다. 공용 필드의 RFC 1918 주소는 의도된 경로 및 관찰된 변환과 모순되는 경우에만 의심스럽습니다. 고유 브랜치 전용 주소는 이 예에서 반복되는 프라이빗-튜플 중복을 방지합니다. 앞서 설명한 별도의 translated-public port-reuse 시나리오를 방지하지 않습니다.

NAT 엔드포인트 재할당

허브가 이전 피어 상태를 유지하는 동안 NAT 매핑이 만료된 후 엔드포인트를 다른 스포크에 재할당할 수도 있습니다. 기존 소유자와 새 소유자 간의 중복을 식별하기 위해 매핑 기록을 허브 세션 주기와 비교합니다.

증상 및 영향

일반적인 지표는 다음과 같습니다.

- 제어 연결은 영향받는 BFD 경로가 다운되거나 복구되지 않는 동안 Up 상태를 유지합니다.
- 서로 다른 두 시스템 IP는 동일한 공용 IP:포트를 광고합니다.
- 허브는 논리적 TLOC를 모두 보유하지만 필터링된 플랫폼 세션 보기에 피어가 하나 없거나 일관되지 않은 시스템 IP, 원격 색상, 판별자, 터널 또는 SA 정보가 표시됩니다.
- 한 피어에 대한 전송 철회 또는 레크리에이션은 동일한 엔드포인트를 사용하는 다른 피어를 방해합니다.
- IPsec 입력 삭제는 영향을 받는 경로에서 증가할 수 있습니다.

장애가 발생하면 영향을 받는 전송 경로를 사용할 수 없게 될 수 있습니다. 스포크에 사용할 수 있는 유일한 전송 경로인 경우 스포크는 오버레이에서 격리됩니다. 대규모 허브에서는 하나의 NAT 주소를 공유하는 여러 스포크가 상관관계가 필요한 인구를 증가시키지만, 영향을 받는 경로의 수를 측정해야 합니다. 그 주소 뒤에 있는 사이트 수에서는 유추할 수 없다.

문제 진단

1단계. 소프트웨어 및 스포크 전송 상태 기록

영향을 받는 각 Cisco IOS XE Edge에서 <affected-color>를 실제 전송 색상(예: biz-internet 또는 public-internet)으로 교체합니다.

<#root>

show clock detail

show version | include Cisco IOS XE Software

show sdwan control local-properties

show sdwan control connections | include

show sdwan omp peers

사설/공용 주소 및 포트, 인터페이스, 색상, NAT 유형, 사이트 ID 및 제어 상태를 기록합니다. 첫 번째 전체 local-properties 샘플 후에는 이 압축 필터를 사용하여 인터페이스 머리글 및 선택한 전송 행을 유지합니다. TenGigabitEthernet0/1/0.10을 영향을 받는 인터페이스로 교체합니다.

<#root>

show sdwan control local-properties "wan-interface-list" | include INTERFACE|PUBLIC|TenGigabitEthernet0/

기본 시나리오의 경우 두 스포크 모두에서 관련 필드를 읽을 수 있습니다. 이는 기본 열 레이아웃이 아니라 필드 요약입니다.

Field	Spoke A	Spoke B
System IP	10.0.0.32	10.0.0.33
Color	public-internet	public-internet
Private endpoint	192.168.11.11:12346	192.168.12.12:12346
Public endpoint	203.0.113.10:12346	203.0.113.10:12346

```
NAT type                       A                     A
vSmart controls on transport   Up                    Up
```

Up 제어 연결은 컨트롤러 관계를 확인합니다. 공용 엔드포인트의 Spoke-to-Hub BFD 경로 또는 고유성을 확인하지 않습니다.

2단계. OMP에서 중복 엔드포인트 찾기

Cisco IOS XE 허브에서 다음을 수행합니다.

<#root>

show clock detail

show sdwan omp tlocs table | include 203.0.113.10

SD-WAN 컨트롤러(vSmart)에서 다음을 수행합니다.

<#root>

show clock

show omp tlocs | tab | include 203.0.113.10

이 컨트롤러 출력에서는 정규화된 식별자를 사용합니다. IPv6 및 지역 열은 생략됩니다.

<#root>

vSmart# show omp tlocs | tab | include 203.0.113.10

```
TLOC IP     COLOR            ENCAP FROM PEER  STATUS KEY PUBLIC IP     PORT  PRIVATE IP     PORT
10.0.0.32   public-internet ipsec 10.0.0.5   C,R    1   203.0.113.10 12346 192.168.11.11 12346
                              10.0.0.32  C,I,R  1   203.0.113.10 12346 192.168.11.11 12346
10.0.0.33   public-internet ipsec 10.0.0.5   C,R    1   203.0.113.10 12346 192.168.12.12 12346
                              10.0.0.33  C,I,R  1   203.0.113.10 12346 192.168.12.12 12346
```

TLOC 시스템 IP, 색상, 캡슐화, 공용 IP 및 공용 포트를 비교합니다. 서로 다른 컨트롤러에서 동일한

논리적 TLOC에 대한 다중 경로는 정상입니다. 충돌 후보는 동일한 유효 엔드포인트를 가진 서로 다른 두 피어 ID입니다.

30-60초 후에 필터링된 명령을 반복하고 두 타임스탬프를 모두 유지합니다. 지속적인 중복은 유용한 증거입니다. 완벽하게 동시에 실행되는 명령은 필요하지 않습니다. 잠시 동안 TAC에서 OMP 이벤트 및 해당 세션 라이프사이클 레코드를 수집합니다.

두 개의 의심되는 피어에 대해 개별 TLOC 테이블 항목을 보존합니다.

<#root>

```
show sdwan omp tlocs table | include 10.0.0.32
```

```
show sdwan omp tlocs table | include 10.0.0.33
```

Cisco IOS XE의 IPv4 TLOC 세부사항을 간단하게 보려면 이 필터를 사용하십시오. 시스템 IP를 조사 중인 피어로 교체하고 ip <system-IP> 선택기에 따옴표를 유지합니다.

<#root>

```
show sdwan omp tlocs "ip 10.0.0.32" | exclude not set| 0|None|efault|::
```

```
show sdwan omp tlocs "ip 10.0.0.33" | exclude not set| 0|None|efault|::
```

두 피어의 공용 및 사설 주소/포트 특성을 비교합니다. 이 보기에서는 일치하는 unset, 0 값, 기본값 및 IPv6 행을 생략합니다.

3단계. 논리 TLOC를 허브 세션 소유권과 비교

FTM에 전달된 TLOC 상태를 검사합니다. 두 피어의 시스템 IP, 색상, 공용 IP 주소 및 공용 UDP 포트를 비교합니다.

<#root>

```
show platform software sdwan ttmd tlocs
```

FTM(Forwarding Table Manager), BFD 및 플랫폼 세션 레코드를 비교하려면 다음 명령을 실행합니다.

<#root>

show sdwan ftm bfd tloc | include 10.0.0.32

show sdwan ftm bfd tloc | include 10.0.0.33

show sdwan bfd sessions | include 10.0.0.32

show sdwan bfd sessions | include 10.0.0.33

show platform software sdwan session dstip 203.0.113.10

show platform software sdwan session remote-sysip 10.0.0.32 detail

show platform software sdwan session remote-sysip 10.0.0.33 detail

이 예에서는 정규화된 식별자를 사용하는 패턴을 보여 줍니다. 명확성을 위해 열 레이블이 필터링된 FTM 행에 추가됩니다. 필터링된 명령 출력의 일부가 아닙니다.

<#root>

Hub# show sdwan ftm bfd tloc | include 10.0.0.32

```
System IP  Remote color     Encap  TLOC index  State
10.0.0.32  public-internet  IPSEC  32827       DOWN
```

Hub# show sdwan ftm bfd tloc | include 10.0.0.33

```
System IP  Remote color     Encap  TLOC index  State
10.0.0.33  public-internet  IPSEC  32828       DOWN
```

Hub# show platform software sdwan session dstip 203.0.113.10

```
RemoteSysIP Color        Proto SrcIp         SPort DstIp        DPort DPubIp       PPort BFD-LD TUN-ID
10.0.0.32   mpls         IPSEC 192.168.9.42  12346 203.0.113.10 12346 203.0.113.10 12346 20184  798
10.0.0.32   biz-internet IPSEC 192.168.10.42 12346 203.0.113.10 12346 203.0.113.10 12346 20183  799
```

OMP 및 FTM은 두 논리적 피어 ID를 모두 유지하는 반면, 이 세션 조회는 공유 대상에 대한 스포크 A만 표시합니다. 스포크 A는 또한 다운 FTM 상태를 가지고 있습니다. 플랫폼 세션 테이블에 있는 상태가 정상 경로를 나타내지 않습니다. FTM TLOC 인덱스는 세션 테이블의 BFD 로컬 판별기(BFD-LD)와 구별된다. 이러한 패턴은 여러 레이어에서 소유권을 조사해야 하는 이유입니다. 누락된 CLI 행만으로는 패킷 손실이 발생하지 않습니다.

이 표에서 Color는 로컬 전송을 나타냅니다. 원격 TLOC를 식별하려면 세부 보기에서 원격 색상을 사용합니다. DstIp와 DPubIp도 비교합니다. 학습된 실제 대상은 세션과 연결된 공용 엔드포인트와 다를 수 있습니다. 목적지 전용 필터가 더 이상 학습된 주소와 일치하지 않는 경우 피어별 보기를 사용합니다.

유효하지 않은 다음 홉, SA 식별자 0 또는 HW: FALSE는 고유한 시그니처가 아닌 추가 증거를 제공합니다. 이러한 필드는 일반 설정 또는 언더레이 실패 중에도 발생할 수 있습니다.

4단계. NAT 게이트웨이가 실제로 수행하는 작업을 확인합니다.

NAT 또는 서비스 공급자 운영자에게 다음 필드가 있는 동시 UDP 변환 레코드를 요청합니다.

```
Spoke           Inside source       Translated source    External destination
A               192.168.11.11:12346 203.0.113.10:12346   198.51.100.2:12346
B               192.168.12.12:12346 203.0.113.10:12346   198.51.100.3:12346
A               192.168.11.11:12346 203.0.113.10:12346   198.51.100.42:12346
B               192.168.12.12:12346 203.0.113.10:45678   198.51.100.42:12346
```

이것은 예시적인 변환 테이블입니다. NAT 플랫폼에 해당하는 diagnostic 명령을 사용합니다. Cisco IOS XE NAT 게이트웨이에서 다음으로 시작합니다.

<#root>

show ip nat translations | include 203.0.113.10

내부 소스 및 대상 열을 모두 유지합니다. 변환된 소스만 포함된 목록에서는 다른 vBond에 대해 재사용이 유효한 이유나 허브 매핑을 소유한 스포크를 표시할 수 없습니다.

vBonds 및 허브에 대해 NAT 전후의 영향을 받는 UDP 흐름을 캡처합니다. VCONTROL 트레일러가 잘리지 않도록 전체 패킷 길이를 보존합니다. TAC와 합의된 SPAN(Switched Port Analyzer) 또는 EPC(Embedded Packet Capture) 컬렉션을 사용합니다. 여러 캡처 지점에서 동일한 흐름을 비교합니다. 동기화되지 않은 캡처 클럭에서 레이턴시를 유추하지 마십시오.

5단계. Wireshark에서 VCONTROL 검사

여기에 설명된 IPv4 BFD/VCONTROL 형식에 대해서는 부록의 Lua 디코더를 사용합니다. 캡처와 같은 폴더에 sdwan_vctrl.lua로 코드를 저장합니다. 이 진단 디코더는 표시되는 필드를 표시합니다. ESP를 해독하거나 인증을 확인하지 않습니다. 그 범위는 완전한 비중첩 IPv4/UDP 패킷이며, 예상되는 BFD/VCONTROL 플래그 및 트레일러 구조입니다.

디코더와 캡처가 포함된 폴더에서 Wireshark 명령을 실행합니다.

<#root>

```
wireshark -n \

  -X lua_script:sdwan_vctrl.lua \

  -d udp.port==12346,sdwan_vctrl \

  -d udp.port==45678,sdwan_vctrl \

  -r hub.pcap
```

예제 포트를 캡처에 있는 포트로 바꿉니다. Windows 또는 macOS에서 Wireshark 실행 파일이 PATH에 없는 경우 해당 실행 파일의 전체 경로를 사용합니다.

또는 Wireshark 시작 시 Lua 스크립트를 로드하고 관련 UDP 패킷을 선택한 다음 Analyze > Decode As로 이동합니다. 적용 가능한 소스 및 대상 UDP 포트 항목을 SDWAN_VCTRL / SD-WAN VCTRL(IPv4)에 할당합니다. 다른 포트의 명시적 UDPENCAP 항목이 이 디코더보다 우선할 수 있습니다. 이 분석 세션에 변경 사항을 적용합니다.

이 표시 필터를 적용합니다.

```
sdwan_vctrl && ip.addr == 203.0.113.10
```

SD-WAN VCTRL > Visible VCONTROL 트레일러를 확장하고 다음을 비교합니다.

```
Outer IPv4 source:       203.0.113.10
```

```
Outer UDP source port:   45678
Carried source IPv4:     203.0.113.10
Carried source UDP port: 12346
Carried destination:     198.51.100.42:12346
```

이 예시적인 값은 데이터 평면 학습이 완료되기 전에 초기 터널 설정을 설명합니다. 여기에는 전달된 엔드포인트와 함께 B에 대한 실제 허브 매핑이 표시됩니다. NAT는 외부 헤더를 수정합니다. 이 트레일러 내부의 엔드포인트 정보는 재작성되지 않습니다. 이러한 불일치만 있다고 해서 결함이 표시되는 것은 아닙니다.

컴팩트 내보내기를 위해 TShark 명령을 실행합니다.

<#root>

```
tshark -n -X lua_script:sdwan_vctrl.lua \

  -d udp.port==12346,sdwan_vctrl \

  -d udp.port==45678,sdwan_vctrl \

  -r hub.pcap -Y sdwan_vctrl -T fields \

  -e frame.number -e ip.src -e udp.srcport -e ip.dst -e udp.dstport \

  -e sdwan_vctrl.spi \

  -e sdwan_vctrl.src_ip -e sdwan_vctrl.src_port \

  -e sdwan_vctrl.dst_ip -e sdwan_vctrl.dst_port
```

사용자 지정 디코더가 없으면 여기에 설명된 IPv4 형식은 UDP 페이로드의 끝에 이 17바이트 TLV(type-length-value) 트레일러를 갖습니다. 링크 레이어 패딩이 UDP 페이로드 외부에 있음:

```
81 00 0f cb 00 71 0a 30 3a c6 33 64 2a 30 3a 00 11
|  |     |           |     |           |     |
|  |     |           |     |           |     +-- Complete trailer length: 17
|  |     |           |     |           +-------- Destination port: 12346
|  |     |           |     +-------------------- Destination: 198.51.100.42
|  |     |           +-------------------------- Source port: 12346
|  |     +-------------------------------------- Source: 203.0.113.10
|  +-------------------------------------------- TLV length: 15
```

```
+---------------------------------------------- Type: 0x81
```

이 고정 레이아웃을 IPv6, 기타 제어 형식, 잘린 패킷 또는 임의의 암호화된 데이터에 적용하지 마십시오. 디코더 필터가 비어 있으면 패킷이 지원되는 형식을 벗어났음을 의미할 수 있습니다. 읽기 가능한 소스 엔드포인트는 인증된 시스템 IP 레이블도 아닙니다.

참고: Wireshark의 일반 ESP 시퀀스 경고는 라우터 재전송 방지 진단이 아닙니다. 인증 또는 소유권 결론을 내리기 전에 패킷을 라우터 카운터 및 로그와 상호 연결합니다.

6단계. 영향 받는 경로 확인 및 증거 보존

허브에서 관찰된 장애와 관련하여 두 개의 QFP(QuantumFlow Processor) 카운터 샘플을 가져갑니다.

<#root>

show clock detail

show platform hardware qfp active statistics drop | include Ipsec

show sdwan bfd sessions | include 10.0.0.32

show sdwan bfd sessions | include 10.0.0.33

절대 합계가 아닌 카운터 차이를 사용합니다. 집계 IPsec 삭제에는 다른 원인이 있을 수 있습니다. 영향을 받는 전송에 대한 패킷 도착을 확인하고 이를 피어, 엔드포인트, BFD 판별기, 터널, SA 및 이벤트 시간과 연계합니다.

TAC에 두 개의 OMP 스냅샷, 스포크 로컬 속성 및 컨트롤, 두 피어에 대한 허브 세션 세부사항, BFD 상태, 변환 레코드, 바운드 캡처 및 소프트웨어 버전을 제공합니다. 이미 사용 가능한 경우 관련 admin-techs 및 연결/탈퇴 기록을 포함합니다. 대형 허브에서 전체 테이블을 반복해서 수집하지 마십시오.

서비스 연결성을 별도로 테스트하고 실제 선택한 전송을 기록합니다. 0초 BFD Up 표시는 지속적인 복구가 아닙니다.

해결 방법 및 제한 사항

Cisco TAC 및 NAT 연산자를 사용하여 이러한 완화 옵션을 평가합니다. 이러한 제한은 광고된 엔드포인트가 공통 허브에 도달하는 것과 관련이 있습니다. 대칭 NAT, 공유 공용 주소 또는 반복되는 개인 주소가 일반적으로 지원되지 않는 것은 아닙니다. 복구 절차 및 완화 효과는 구축에 따라 다릅니다.

고유한 할당으로 안정적인 엔드포인트 독립적 매핑 사용

예시된 시퀀스에 대한 NAT 측 방지 옵션 중 하나는 각 개별 스포크 전송 엔드포인트에 vBond, 컨트롤러 및 허브 대상 전체에서 안정적이고 고유한 변환 UDP 엔드포인트를 제공하는 것입니다. 스포크 전반에 걸쳐 엔드포인트 독립성과 고유성을 모두 요청합니다. NAT 게이트웨이 장애 조치 또는 상태 레크리에이션 후에도 변환 레코드 및 캡처의 결과를 확인합니다.

예를 들어, A는 203.0.113.10:40001을 일관되게 사용할 수 있지만 B는 203.0.113.10:40002를 일관되게 사용합니다. 고정 변환 또는 적합한 할당 정책은 NAT 플랫폼 및 액세스 설계에 따라 이 동작을 제공할 수 있습니다.

엔드포인트 독립적 매핑에는 무제한 인바운드 액세스가 필요하지 않습니다. 필요한 방화벽 제어를 유지합니다. NAT 정책 수정은 이전에 알려졌거나 프로그래밍된 세션 상태를 자동으로 제거하지 않습니다. TAC를 통해 새로운 검색 주기 및 복구를 조정합니다.

서로 다른 스포크 간에 포트 겹치기 사용 안 함

지원되는 경우 관련 SD-WAN 스포크 전체에서 변환된 UDP 엔드포인트를 고유하게 예약합니다. 대상이 다르다는 이유만으로 재사용하지 마십시오. 이렇게 하면 NAT 게이트웨이가 일부 대상 종속 동작을 유지하는 경우에도 앞서 표시된 동시 중복 vBond 매핑이 직접 제거됩니다.

이 설정은 더 많은 포트를 사용하거나 추가 공용 주소를 요구할 수 있습니다. 각 스포크 엔드포인트에 대한 매핑은 자체로는 독립적이지 않으며, 이후 엔드포인트 재할당 후 오래된 수신기 상태를 해결하지 않습니다.

여러 NAT 스테이지 또는 이중 NAT 게이트웨이의 경우, 최종 인터넷 경계에서 할당이 표시되는지 확인합니다. 한 NAT 인스턴스 내부의 고유성은 동일한 공용 주소를 공유하는 다른 인스턴스 간의 고유성을 설정하지 않습니다.

소형 제어 그룹에 대해 포트 오프셋 사용

port-offset 명령은 0에서 19 사이의 값을 제공합니다. 예를 들어 스포크 A는 오프셋 0을 유지할 수 있으며 스포크 B는 오프셋 1을 사용할 수 있습니다. 스포크 B에서 다음 구성 명령을 실행합니다.

```
Spoke-B# config-transaction

Spoke-B(config)# system

Spoke-B(config-system)# port-offset 1

Spoke-B(config-system)# commit

Spoke-B(config-system)# end

Spoke-B# show sdwan control local-properties
```

변경 후 활성 소스 및 변환된 포트를 확인합니다. 이 시스템 설정을 변경하면 전송 간에 제어 및 데이터 연결을 다시 작성할 수 있습니다. 이는 무중단 진단 단계가 아닙니다.

20개의 오프셋은 오프셋 0을 하나의 선택으로 하여 20개의 고유한 기본 포트 그룹을 제공합니다. 하나의 공용 IP 뒤에 20개의 SD-WAN 라우터가 있는 것으로 일반적인 제한은 아닙니다. 이 특정 해결 방법은 20개의 고유한 오프셋 선택만 제공하고 NAT 게이트웨이가 이를 보존하고 구분해야 합니다. 오프셋을 재사용할 경우 고유성 체계로 실패합니다. 포트 호핑은 더 많은 오프셋 ID를 추가하지 않습니다.

예를 들어, 124개의 라우터가 모두 하나의 공유 주소 뒤에 고유한 오프셋을 수신할 수는 없습니다. 공용 주소 그룹당 최대 20개의 라우터가 있는 오프셋 전용 체계에는 최소 7개의 그룹이 필요합니다. 이 산수는 용량 권장 사항 또는 NAT 동작 확인의 대체가 아닙니다. 변환된 포트를 재작성하거나 겹치는 NAT 게이트웨이는 라우터 수가 적더라도 체계를 무력화할 수 있습니다.

소스 포트 보존 사용 안 함 또는 임의 할당 사용

보존 선호도가 없는 정책은 여러 스포크가 서로 다른 vBond에 대해 :12346을 받는 경향을 줄일 수 있습니다. 무작위 할당은 이러한 매핑을 더 큰 포트 풀로 배포할 수 있습니다.

그러나 변화만으로는 충돌 회피를 보장할 수 없습니다. 무작위 할당자는 여전히 대상 간에 포트를 재사용하거나, 허브에 대한 매핑을 변경하거나, 이전 허브 상태가 유지되는 동안 만료된 엔드포인트를 재할당할 수 있습니다. 할당이 가입자와 대상 간에 고유한지 확인합니다. 무작위 포트만으로는 고유성이 보장되지 않습니다.

운영자와 함께 NAT 게이트웨이의 소스 포트 유지 및 할당 설정을 검토합니다. 적용 가능한 컨피그레이션은 NAT 플랫폼에 따라 달라집니다. 변환 레코드 및 패킷 캡처를 사용하여 vBond 및 허브에 대한 결과 매핑을 확인합니다.

변환된 포트는 원래 SD-WAN 기본 포트 범위를 벗어날 수 있습니다. 소스 포트가 변경되었다는 이유만으로 합법적으로 변환된 트래픽을 거부하지 않도록 방화벽 규칙을 검토합니다.

별도의 공용 주소 또는 예약 포트 블록

전용 변환 주소 또는 스포크당 예약된 비중첩 포트 블록은 서로 다른 활성 스포크에 대해 고유한 알림 엔드포인트를 제공할 수 있습니다. 정책은 검색 및 허브 경로와 중복 NAT 노드 간에 일관되게 적용되어야 합니다. 추가 주소 공간 및 공급자 지원이 필요할 수 있습니다. 매핑 종료 후 동적 재사용은 여전히 올바른 허브 세션 라이프사이클 관리를 필요로 합니다.

대체 전송 및 좌표 복구 유지

확인된 MPLS 또는 기타 적격 경로는 영향을 받은 인터넷 경로를 조사하는 동안 서비스를 유지할 수 있습니다. 공유 NAT 주소를 차단하는 언더레이 ACL(Access Control List)은 억제만 제공합니다. 해당 주소 뒤에 있는 모든 스포크에 대한 인터넷 이중화를 제거할 수 있으며 OMP 광고를 자동으로 철회하지 않습니다.

제어 지우기, 인터페이스 재설정, NAT-state 지우기 또는 허브 다시 로드는 일시적으로 상태를 재생성할 수 있습니다. 재발 방지를 보장하는 것은 없습니다. 첫 번째 진단 단계로 광범위 지우기를 수행하지 마십시오. 증거를 보존하고, 가능한 경우 할당 조건을 수정하고, TAC와 최소 복구 조치에 합의합니다. 복구된 경로의 지속적인 BFD Up 및 양방향 트래픽을 검증합니다.

관련 소프트웨어 결함

Cisco 버그 ID	이 조항과 관련된 범위
CSCw45867	서로 다른 피어가 동일한 공용 TLOC 끝점을 광고할 때의 허브 세션 소유권 제한 문서입니다. 이 레코드는 소프트웨어 수정이 아닌 문서 업데이트를 추적합니다.
CSCwx12986	자동 포트 홉/NAT 학습 시퀀스는 공용 TLOC 필드에 개인 튜플을 남길 수 있습니다. 브랜치가 동일한 프라이빗 IP:포트를 재사용하는 경우 잘못된 퍼블릭 엔드포인트가 피어 간에 매칭될 수 있습니다. 이 생산자 결함을 수정해도 유효한 변환된 공용 포트 재사용을 막을 수 없습니다.
CSCwx48929	검색이 동일한 vBond로 반환되면 NAT 분류가 E로 잘못 설정될 수 있습니다. 올바른 분류는 올바른 different-vBond 포트 재사용 시나리오를 방지하지 않습니다.

Cisco 버그 ID CSCwx12986 및 Cisco 버그 ID CSCwx48929를 수정하더라도 고유한 알려진 공용 엔드포인트가 보장되지 않으며 이 충돌 시나리오를 스스로 제거하지 않습니다. Cisco 버그 ID CSCww45867 문서 레코드를 닫아도 소프트웨어 동작의 변경 사항이 설정되지 않습니다. Cisco

TAC에 적용 가능한 제한 및 완화 사항을 확인합니다.

부록: IPv4 VCONTROL 트레일러 디코딩

이 코드를 sdwan_vctrl.lua로 저장합니다. 진단 디코더는 패킷을 인증하거나 페이로드를 해독하지 않습니다. sdwan_vctrl 디스플레이 필터를 사용하고 명시적 Decode As 선택을 등록합니다. 패킷 캡처는 변경되지 않습니다.

```
-- Cisco SD-WAN IPv4 VCONTROL trailer decoder.
-- Explicit UDP "Decode As" only; does not decrypt ESP.
-- Scope: complete ordinary IPv4/UDP packets, one IP/UDP layer.

local p = Proto("sdwan_vctrl", "SD-WAN VCTRL (IPv4)")

local f = {
    spi       = ProtoField.uint32("sdwan_vctrl.spi",
                    "Wire SPI including control flags", base.HEX),
    sequence  = ProtoField.uint32("sdwan_vctrl.sequence",
                    "ESP sequence number", base.DEC),
    type      = ProtoField.uint8("sdwan_vctrl.type",
                    "Trailer type", base.HEX),
    tlv_len   = ProtoField.uint16("sdwan_vctrl.tlv_len",
                    "TLV length", base.DEC),
    src_ip    = ProtoField.ipv4("sdwan_vctrl.src_ip",
                    "Carried source IPv4"),
    src_port  = ProtoField.uint16("sdwan_vctrl.src_port",
                    "Carried source UDP port", base.DEC),
    dst_ip    = ProtoField.ipv4("sdwan_vctrl.dst_ip",
                    "Carried destination IPv4"),
    dst_port  = ProtoField.uint16("sdwan_vctrl.dst_port",
                    "Carried destination UDP port", base.DEC),
    total_len = ProtoField.uint16("sdwan_vctrl.total_len",
                    "Complete trailer length", base.DEC)
}
p.fields = f

-- Field extractors must be created outside the dissector.
local get_udp_length = Field.new("udp.length")
local get_ip_version = Field.new("ip.version")
local get_ip_proto   = Field.new("ip.proto")

function p.dissector(tvb, pinfo, tree)
    local lengths = { get_udp_length() }
    local versions = { get_ip_version() }
    local protocols = { get_ip_proto() }

    -- Deliberately skip nested/tunnelled protocol stacks.
    if #lengths ~= 1 or #versions ~= 1 or #protocols ~= 1 then
        return 0
    end
    if tonumber(versions[1].value) ~= 4 or
       tonumber(protocols[1].value) ~= 17 then
        return 0
    end
```

```
    -- UDP length includes its 8-byte header.
    local n = tonumber(lengths[1].value) - 8

    -- Require the full declared payload, not a truncated fragment.
    if n < 25 or tvb:reported_len() ~= n or tvb:len() ~= n then
        return 0
    end

    -- Exact BFD + VCTRL control-bit combination.
    local spi = tvb(0, 4):uint()
    if math.floor(spi / 0x10000000) ~= 0xA then
        return 0
    end

    -- Trailer is at the end of UDP payload, not Ethernet frame.
    local o = n - 17

    if tvb(o, 1):uint() ~= 0x81 or
       tvb(o + 1, 2):uint() ~= 15 or
       tvb(o + 15, 2):uint() ~= 17 then
        return 0
    end

    local root = tree:add(p, tvb())
    root:add(f.spi,      tvb(0, 4))
    root:add(f.sequence, tvb(4, 4))

    local trailer = root:add(tvb(o, 17),
                             "Visible VCONTROL trailer")
    trailer:add(f.type,      tvb(o,      1))
    trailer:add(f.tlv_len,   tvb(o + 1,  2))
    trailer:add(f.src_ip,    tvb(o + 3,  4))
    trailer:add(f.src_port,  tvb(o + 7,  2))
    trailer:add(f.dst_ip,    tvb(o + 9,  4))
    trailer:add(f.dst_port,  tvb(o + 13, 2))
    trailer:add(f.total_len, tvb(o + 15, 2))

    pinfo.cols.protocol = "SDWAN-VCTRL"
    return n
end

DissectorTable.get("udp.port"):add_for_decode_as(p)
```

관련 정보

- RFC 7857, 섹션 3: 포트 중첩 동작
- RFC 4787: 유니캐스트 UDP에 대한 NAT 동작 요구 사항
- RFC 5737: 문서화를 위해 예약된 IPv4 주소 블록
- Cisco Catalyst SD-WAN 설계 가이드
- Cisco IOS XE Catalyst SD-WAN System 명령: 포트 오프셋
- Cisco SD-WAN Port Offset Configuration
- Wireshark 명령줄 참조
- TShark 명령줄 참조
- 기술 지원 및 문서 – Cisco Systems

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.