Problemen oplossen met SD-WAN-hubtunnels met dubbele NAT-eindpunten

Inhoud

- Inleiding
- Voorwaarden
  - Vereisten
  - Gebruikte componenten
- Achtergrondinformatie
  - Control-Plane NAT Learning
  - Data-Plane NAT Learning en VCONTROL
  - Poortbehoud, poortoverlapping en poortrandomisatie
- Voorbeeldtopologie
- Waarom de botsing plaatsvindt
  - Verschillende obligaties kunnen hetzelfde publieke eindpunt waarnemen
  - Dezelfde advertenties bereiken één hub
  - Private-as-Public-botsingen met herhaalde filiaaladressen
  - NAT-eindpunthertoewijzing
- Symptomen en impact
- Diagnose van het probleem
  - Stap 1. De status van de software en het gesproken transport vastleggen
  - Stap 2. Dubbele eindpunten zoeken in OMP
  - Stap 3. Vergelijk logische TLOC's met Hub Session Ownership
  - Stap 4. Controleer wat de NAT Gateway daadwerkelijk doet
  - Stap 5. Inspecteer VCONTROL in Wireshark
  - Stap 6. Bevestig het getroffen pad en bewaar bewijs
- Workarounds en beperkingen
  - Stabiele eindpuntonafhankelijke toewijzingen met unieke toewijzingen gebruiken
  - Overlapping van poorten tussen verschillende spaken uitschakelen
  - Poortverschuiving gebruiken voor een kleine, gecontroleerde groep
  - Behoud van bron-poort uitschakelen of Willekeurige toewijzing inschakelen
  - Afzonderlijke openbare adressen of reservepoortblokken
  - Een alternatief transport behouden en herstel coördineren
- Gerelateerde softwaredefecten
- Bijlage: De IPv4 VCONTROL-trailer decoderen
- Gerelateerde informatie

Inleiding

In dit document wordt beschreven hoe storingen in de hubtunnel kunnen worden geïdentificeerd en beperkt wanneer spokes één NAT-eindpunt (Public Network Address Translation) delen.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco Catalyst Software-Defined Wide Area Network (SD-WAN)-architectuur en besturingsverbindingen
- Overlay Management Protocol (OMP), Transport Locators (TLOC's), Bidirectional Forwarding Detection (BFD) en IP Security (IPsec)
- Multiprotocol Label Switching (MPLS)-transportnetwerken
- NAT-toewijzing en filtergedrag
- Basispakketanalyse met Wireshark

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco IOS® XE Catalyst SD-WAN-routers
- Cisco Catalyst SD-WAN-controller (vSmart)
- Cisco Catalyst SD-WAN Validator (vBond)

De hub sessie-eigendom mislukking werd gereproduceerd op Cisco IOS XE 17.18.2 met paarsgewijze sleutels operationeel. Beschikbaarheid van commando's en uitvoervelden variëren per platform en release.

Voorbeelden hiervan zijn privéadressen of documentatieadressen die zijn gereserveerd door RFC 5737, met algemene apparaatnamen. CLI-uittreksels worden ingekort en gebruiken genormaliseerde identificatoren. Interfacenamen en sommige uitvoervelden verschillen per platform en release.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

⚠ Waarschuwing: Configuratiewijzigingen en verbindingsresets kunnen het verkeer onderbreken. Gebruik een goedgekeurd onderhoudsplan. De eerste diagnostische opdrachten zijn alleen-lezen.

Achtergrondinformatie

Begin met een scenario waarin symmetrische NAT correct wordt geïdentificeerd. Spoke A registreert bij vBond 1 en Spoke B registreert bij vBond 2. De NAT-gateway kan hetzelfde vertaalde bron-IP-adres en dezelfde poort toewijzen aan deze verbindingen wanneer hun bestemmingen verschillen, zoals RFC 7857 toestaat. Beide woordvoerders kunnen bijgevolg hetzelfde publieke eindpunt voor hun publiek-internet TLOC's adverteren, zelfs wanneer beide NAT-type A rapporteren.

De sample-topologie gebruikt de public-internet-kleur. Hetzelfde scenario kan betrekking hebben op andere openbare kleuren, zoals biz-internet. Breng de diagnostische filters aan op de daadwerkelijk aangetaste transportkleur; de letterlijke publiek-internetkleur is geen vereiste voorwaarde.

✎ Opmerking: Cisco Catalyst SD-WAN ondersteunt geen TLOC's van verschillende sites die hetzelfde openbare IP-adres en UDP-poort adverteren voor een gemeenschappelijke ontvangende Edge. Het gedrag van de ontvanger onder deze botsingstoestand is onvoorspelbaar. Dit kan zelfs gebeuren wanneer symmetrische NAT correct wordt geïdentificeerd. Een correcte NAT-classificatie alleen garandeert niet dat geadverteerde eindpunten uniek zijn.

Control-Plane NAT Learning

Een Edge verzendt zijn privétransportadres en -poort tijdens registratie bij vBond. vBond observeert het bronadres en de poort op die verbinding en retourneert het waargenomen eindpunt naar de Edge. The Edge kan deze informatie via OMP adverteren als het publieke adres en poortattributen van een TLOC, inclusief een TLOC met een publieke kleur zoals openbaar internet of biz-internet.

De waarneming beschrijft de verbinding met die vBond. Met bestemmingsafhankelijke NAT kan het in kaart brengen van een hub anders zijn. De router vergelijkt NAT-waarnemingen om het kaartgedrag te classificeren. In show sdwan control local-properties, A betekent adres-en-poort-afhankelijke mapping, en E betekent eindpunt-onafhankelijke mapping. De weergegeven classificatie beschrijft de beslissing van de router; een NAT-vertaaltabel of pakketopname verifieert het werkelijke gedrag van de NAT-gateway.

Voer bijvoorbeeld show sdwan control local-properties uit en zoek de NAT TYPE kolom voor het transport. Deze verkorte uitvoer behoudt de legende van het NAT-type en de gekozen interfacekolommen, met genormaliseerde adressen:

<#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
```

De biz-internet transport rapporteert A en adverteert 203.0.113.10:23012 als het publieke eindpunt. De MPLS transport rapporteert E en heeft gelijke private en publieke eindpunten. Lees de classificatie van het NAT-TYPE; adres of havengelijkheid alleen identificeert het NAT-type niet. N betekent dat de router geen classificatie heeft geleerd.

Data-Plane NAT Learning en VCONTROL

Voordat een hub een gecodeerd BFD-pakket kan verwerken, moet deze de inkomende IPsec-beveiligingsassociatie (SA) vinden voor de bijbehorende peer en tunnel. De SA identificeert de cryptografische sleutel en andere staat die nodig is om het pakket te verifiëren en te decoderen. De ontvanger gebruikt eindpuntinformatie samen met de ESP-beveiligingsparameterindex (ESP) om die toestand te lokaliseren. De SPI alleen is geen wereldwijd unieke spraakherkenning.

Een spaak achter symmetrische NAT initieert normaal gesproken het verkeer naar een bereikbare hub. Dit creëert een mapping voor die specifieke bestemming. Het bronadres of de poort die door de hub wordt gezien, kan verschillen van het openbare eindpunt dat eerder via vBond is geleerd en in OMP is geadverteerd. Als gevolg hiervan komen de ontvangen buitenste headers niet altijd overeen met het eindpunt in de geïnstalleerde tunnelstatus. De hub heeft een manier nodig om dit nieuwe on-wire eindpunt te associëren met de bekende externe TLOC en de IPsec-status voordat het BFD kan decoderen.

Voor het hier besproken IPv4 BFD-over-IPsec-formaat plaatst SD-WAN eindpuntinformatie in een zichtbare VCONTROL-trailer aan het einde van de UDP-payload, buiten de versleutelde BFD-payload. De hub kan deze informatie lezen voordat deze wordt gedecodeerd. VCONTROL draagt eindpuntinformatie, geen coderingssleutels, en stelt zelf geen peer-identiteit vast.

Bijvoorbeeld, tijdens de eerste tunnelinstelling, voordat het leren van het dataplane voltooid is:

```
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
```

De ontvanger probeert eerst het normale eindpunt/SPI-opzoeken. Als die opzoeking geen SA vindt, biedt het VCONTROL-broneindpunt een fallback. In dit voorbeeld kan de hub gebruikmaken van de 203.0.113.10:12346, samen met de lokale bestemmingscontext en de SPI, om de inkomende SA te vinden die is gekoppeld aan de bekende externe TLOC, ook al komt het pakket uit 203.0.113.10:45678.

De gekozen SA biedt de receive-key context. De SPI kiest de toepasselijke sleutelgeneratie binnen die context. De hub voert vervolgens IPsec-verificatie en -decodering uit; alleen een pakket dat de vereiste controles doorstaat, is beschikbaar voor BFD-verwerking. Een leesbare trailer of een succesvolle opzoeking alleen is niet bewezen succesvolle authenticatie, decryptie of BFD-ontvangst.

Het verschil tussen de waargenomen en gedragen bronpoorten kan daarom normaal zijn met symmetrische NAT. Om de peer-relatie te laten werken, moet de hub het pakket koppelen aan de juiste tunnel en sleutelstatus en het daadwerkelijke retoureindpunt leren kennen. In dit voorbeeld laat succesvol leren de hub retourverkeer verzenden naar 203.0.113.10:45678. Dit staat los van control-plane learning via vBond.

VCONTROL dwingt de ontvanger niet om een bestaand eindpunt/SPI-match te overschrijven. Als de dubbele eindpuntstatus een pakket koppelt aan de verkeerde peer- of sleutelgeneratie, garandeert de trailer geen herstel. Het biedt een opzoekhint; het kan geen onderscheid maken tussen twee leeftijdsgenoten die hetzelfde eindpunt dragen zonder de juiste omliggende tunnel en cryptografische staat.

VCONTROL is ook aanwezig op toepasselijke BFD-pakketten wanneer NAT-type E wordt gerapporteerd. De aanwezigheid ervan is geen symmetrische NAT-vlag en is niet opgenomen in elk gewoon IPsec-gegevenspakket. Voor het hier beschreven IPv4 BFD-formaat wordt de publiek-TLOC-informatie weggelaten tussen twee privékleuren.

Het peer-specifieke eindpunt dat via het gegevensvlak wordt geleerd, betekent niet dat de spaak zijn OMP-advertentie moet vervangen door een nieuw eindpunt voor elke bestemming. Verschillende geleerde mappings zijn een verwacht onderdeel van symmetrische NAT-traversal.

Zodra een tunnel omhoog is, kan een afzender die zijn eigen vertaalde eindpunt voor die tunnel heeft geleerd, dat eindpunt als broninformatie dragen. Dit is het publieke eindpunt per tunnel van

de afzender, niet het externe eindpunt of een nieuwe wereldwijde OMP-advertentie. Vergelijk altijd het pakket, de OMP-advertentie en de sessiestatus uit dezelfde observatieperiode.

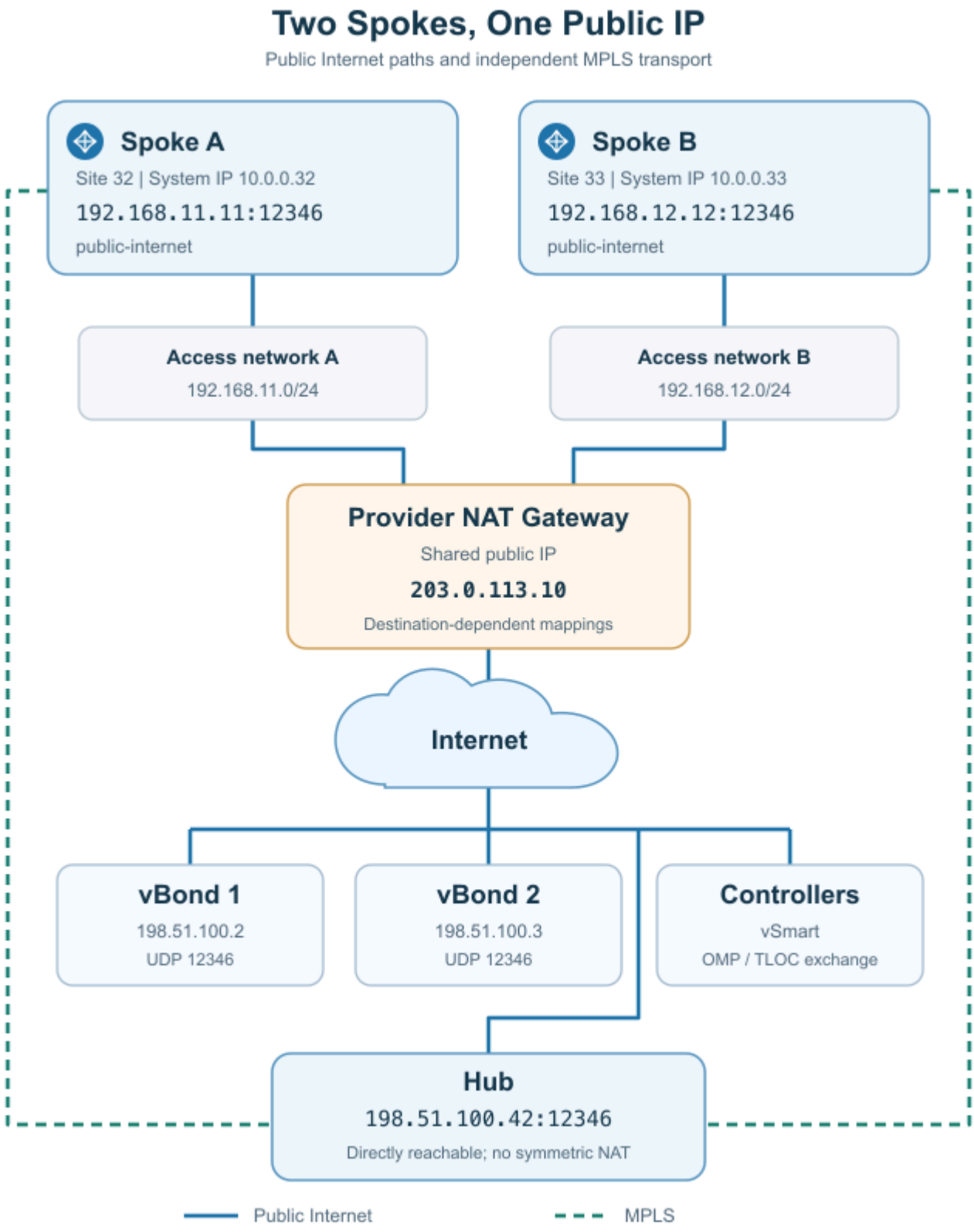
Poortbehoud, poortoverlapping en poortrandomisatie

Dit zijn verschillende gedragingen:

gedrag	Betekenis
Behoud van bron-poort	De NAT-gateway probeert de oorspronkelijke UDP-bronpoort van de spaak te behouden, bijvoorbeeld 12346, als de vertaalde bronpoort.
Poortoverlapping tussen bestemmingen	De NAT-gateway hergebruikt één vertaalde IP: poort voor verschillende interne eindpunten die communiceren met verschillende externe bestemmingen.
Poortrandomisatie	De NAT-gateway kiest vertaalde poorten met behulp van een gerandomiseerde toewijzingsmethode.
Endpoint-independent mapping	Eén intern eindpunt behoudt hetzelfde vertaalde eindpunt voor externe bestemmingen, terwijl die toewijzing bestaat.

RFC 7857, afdeling 3, staat overlappende externe poorten toe voor verschillende interne eindpunten wanneer de bestemmingen verschillen. De NAT onderscheidt de stromen met behulp van hun vijf-tuples. Dit staat niet toe dat twee niet-onderscheidbare UDP-stromen tegelijkertijd naar dezelfde bestemming stromen. Willekeurige toewijzing en bewaring zijn afzonderlijke toewijzingskeuzes; geen van beide stelt eindpuntonafhankelijkheid vast.

Voorbeeldtopologie



Afbeelding 1. Gedeelde NAT-gateway, aparte spaaktoegangsnetwerken en onafhankelijk MPLS-transport.

Gesproken A gebruikt 192.168.11.11:12346, en Gesproken B gebruikt 192.168.12.12:12346. Beide delen het publieke adres 203.0.113.10 via de NAT-gateway. De hub heeft een direct bereikbaar adres en zit niet achter symmetrische NAT. De twee spaken kunnen dezelfde publieke

IP-poort adverteren, ook al verschillen hun privé-eindpunten.

Waarom de botsing plaatsvindt

Verschillende obligaties kunnen hetzelfde publieke eindpunt waarnemen

Overweeg deze gelijktijdige UDP-mappings:

peer	particuliere bron	Vertaalde bron	Bestemming
A	192.168.11.11:12346	203.0.113.10:12346	vBond 1, 198 51 100 2 12 346
B	192.168.12.12:12346	203.0.113.10:12346	vBond 2, 198 51 100 3 12 346

Antwoorden geven correct terug omdat de NAT ook het externe eindpunt controleert. Een antwoord van vBond 1 behoort tot de mapping voor A; een antwoord van vBond 2 behoort tot de mapping voor B.

Beide routers kunnen ook contact opnemen met de andere vBond en doelafhankelijke mapping correct detecteren. Houd bijvoorbeeld de prive-brontupel voor elke spaak ongewijzigd en overweeg deze observatievolgorde:

peer	Eerste aanvaarde vBond-waarneming	Vergelijking met de andere vBond	resultaat
A	vBond 1 geeft 203.0.113.10:12346 terug	vBond 2 geeft 203.0.113.10:40001 terug	NATA; bewaarde openbare tupel 203.0.113.10:12346
B	vBond 2 geeft 203.0.113.10:12346 terug	vBond 1 geeft 203.0.113.10:40002 terug	NATA; bewaarde openbare tupel 203.0.113.10:12346

De vBond-waarnemingen verschillen voor elke router, dus het detecteren van NATA is correct. De bewaarde eerste waarnemingen komen niettemin overeen tussen de twee routers. Classificatie A kent geen unieke openbare haven toe aan alle spaken, en het bezoeken van beide vBonds garandeert die uniciteit niet.

Elke spreker ontvangt het openbare adres en de haven die vBond in het registratieantwoord heeft waargenomen en gebruikt de bewaarde waarneming om zijn lokale transporteigenschappen te bevolken. De spaak omvat dat publieke eindpunt, samen met zijn privé-eindpunt, in de TLOC-attributen die het via OMP aan de SD-WAN-controller adverteert. De

Verwerkingsverantwoordelijke distribueert de TLOC vervolgens naar andere Edges volgens het toepasselijke controlebeleid; vBond zelf is niet de bron van de OMP-advertentie.

Als beide spaken hetzelfde waargenomen publieke eindpunt behouden, kan OMP daarom het volgende bevatten:

```
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
```

Deze blijven verschillende logische TLOC's omdat hun systeem-IP's verschillen.

Dezelfde advertenties bereiken één hub

De NAT-gateway moet beide spaken onderscheiden wanneer ze contact maken met dezelfde hub. Een mogelijke toewijzing is:

peer	Vertaalde bron naar Hub	Bestemming
A	203.0.113.10:12346	198.51.100.42:12346
B	203.0.113.10:45678	198.51.100.42:12346

De hub heeft twee logische peers die hetzelfde eindpunt van de bestemming adverteren, terwijl pakketten kunnen aankomen van verschillende werkelijke eindpunten. Onder normale symmetrische NAT-werking helpt data-plane learning de terugkeertoewijzingen vast te stellen.

De beperking van het eigendom van de hub-sessie ontstaat wanneer verschillende peers de sessiestatus delen die door deze transportsleutel is gekozen:

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

Als beide advertenties dezelfde sleutel kiezen, kan een update van een latere peer eigendomsinformatie in gedeelde staat vervangen. Een volgende intrekking, verwijdering of herhaling van de sessie voor de ene peer kan de IPsec / BFD-status voor de andere peer verstoren. Data-plane learning garandeert geen herstel wanneer die toestand al is geassocieerd met de verkeerde peer- of flow-generatie.

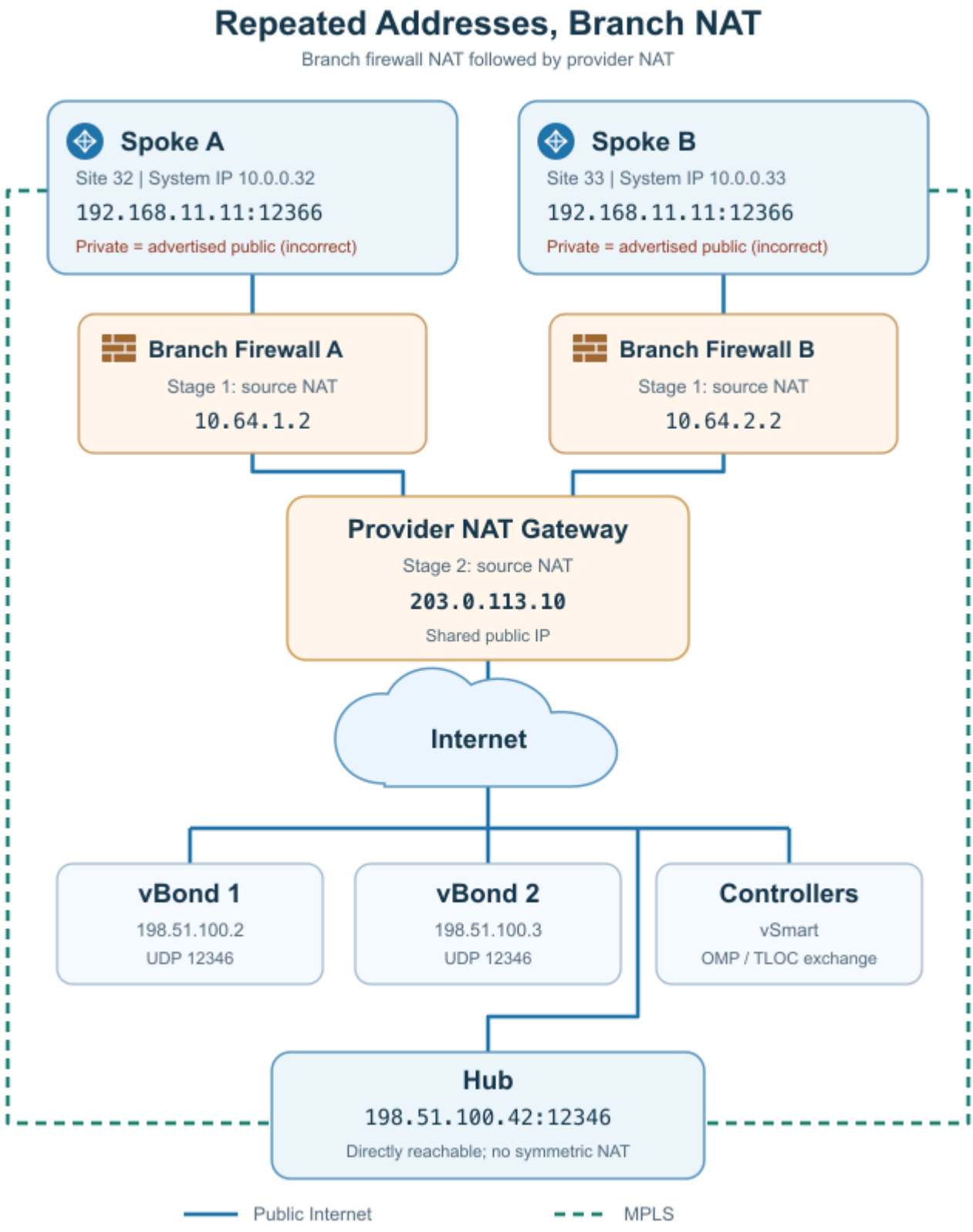
De zichtbare trailer is geen onafhankelijke peer identifier: beide spaken kunnen hetzelfde bron eindpunt dragen. Als de hub een bestaande IPsec-status kiest die tot de verkeerde peer- of sleutelgeneratie behoort, kunnen verificatie en leren mislukken, ook al bereiken pakketten de hub. Om die volgorde voor een bepaald pakket vast te stellen, moet het Cisco Technical Assistance Center (TAC) de gekozen SA correleren met zijn peer en generatie. De trailer alleen kan het niet bewijzen.

Hetzelfde publieke IP alleen veroorzaakt geen botsing. Verschillende externe poorten produceren normaal gesproken verschillende transportsleutels. Controleer ook het gekozen hub-lokale adres, de lokale poort en het protocol. Als een derde peer hetzelfde eindpunt adverteert, kan het ook concurreren om die sleutel; het mislukkingspatroon hangt af van de volgorde van de gebeurtenis.

Private-as-Public-botsingen met herhaalde filiaaladressen

Cisco bug ID CSCwx12986 kan ervoor zorgen dat een Edge een private RFC 1918-tupel adverteert in zijn publieke TLOC-attributen na een automatische bron-poort hop tijdens NAT-vergelijking. Als verschillende filialen hetzelfde privéadres en dezelfde poort hergebruiken, kunnen die onjuiste openbare kenmerken overeenkomen met die van andere filialen en het probleem van het eigendom van de hub-sessie blootleggen.

Beide spaken kunnen bijvoorbeeld 192.168.11.11 gebruiken achter afzonderlijke filiaalfirewalls. Elke firewall houdt zijn filiaalnetwerk gescheiden en vertaalt het bronadres. Als een upstream provider NAT-gateway het opnieuw vertaalt, heeft het pad twee NAT-fasen, of dubbele NAT. Separate Virtual Routing and Forwarding (VRF) contexten zijn een andere manier om overlappende filiaaladressen geïsoleerd te houden.



Afbeelding 2. Branch firewall en provider NAT vertalingen. De onjuiste openbare TLOC-attributen behouden het oorspronkelijke privé-eindpunt, terwijl pakketten de vertaalde bronadressen gebruiken.

Als beide woordvoerders het defect op hun TLOC's op het openbare internet tegenkomen en dezelfde post-hopbronpoort gebruiken, kan de hub deze advertenties ontvangen:

peer	Privé-eindpunt na Port Hop	Onjuist publiek TLOC-eindpunt
A	192.168.11.11:12366	192.168.11.11:12366
B	192.168.11.11:12366	192.168.11.11:12366

Opmerking: herhaalde privéadressen en dubbele NAT zijn geen vereisten voor Cisco bug ID CSCwx12986 zelf. De extra cross-peer botsing vereist matching geadverteerde IP: poort waarden en dezelfde hub-lokale adres, poort en protocol. Hetzelfde privé-IP met verschillende geadverteerde poorten brengt deze botsing niet tot stand.

Openbare en particuliere adresgelijkheid is normaal op een transport zonder NAT. Een RFC 1918-adres in een openbaar veld is alleen verdacht als het in tegenspraak is met het beoogde pad en de waargenomen vertaling. Unieke privé-adressen van filialen vermijden de herhaalde overlapping tussen privé en tuple in dit voorbeeld; ze voorkomen niet dat het hierboven beschreven scenario voor het hergebruik van afzonderlijke vertaalde openbare poorten wordt hergebruikt.

NAT-eindpunthertoewijzing

Een eindpunt kan ook opnieuw worden toegewezen aan een andere spaak nadat een NAT-toewijzing is verlopen terwijl de hub nog steeds de oude peer state behoudt. Vergelijk de kaartgeschiedenis met de levenscyclus van de hub-sessie om overlapping tussen de oude en nieuwe eigenaren te identificeren.

Symptomen en impact

Typische indicatoren zijn:

- Controleverbindingen blijven omhoog terwijl de betreffende BFD-paden zijn uitgeschakeld of niet kunnen worden hersteld.
- Twee verschillende systeem-IP's adverteren hetzelfde openbare IP: poort.
- De hub behoudt beide logische TLOC's, maar een gefilterde platformsessieweergave mist één peer of toont inconsistente systeem-IP-, externe kleur-, discriminator-, tunnel- of SA-informatie.
- Een transport terugtrekking of recreatie voor een peer verstoort een andere peer met hetzelfde eindpunt.
- Invoerdruppels van de IPsec kunnen toenemen op het betreffende pad.

De storing kan het getroffen transportpad onbruikbaar maken. Als dit het enige bruikbare transportpad is voor een spaak, is de spaak geïsoleerd van de overlay. Op een grote hub

verhogen veel spaken die één NAT-adres delen de populatie die correlatie vereist, maar het aantal getroffen paden moet worden gemeten; het kan niet worden afgeleid uit het aantal sites achter dat adres.

Diagnose van het probleem

Stap 1. De status van de software en het gesproken transport vastleggen

Vervang op elke getroffen Cisco IOS XE Edge **<**affected-color**>** door de werkelijke transportkleur, bijvoorbeeld biz-internet of public-internet:

<#root>

show clock detail

show version | include Cisco IOS XE Software

show sdwan control local-properties

show sdwan control connections | include <affected-color>

show sdwan omp peers

Noteer het privé-/openbare adres en de poort, interface, kleur, NAT-type, site-ID en controlestatus. Na de eerste volledige lokale eigenschappen monster, gebruik deze compacte filter om de interface koppen en de gekozen transport rij te behouden. Vervang TenGigabit Ethernet0/1/0.10 door de betreffende interface:

<#root>

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

Voor het primaire scenario kunnen de relevante velden op beide spaken worden gelezen. Dit is een veldsamenvatting, niet de oorspronkelijke kolomlay-out:

```
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
```

Met een controleverbinding omhoog wordt de relatie met de controller geverifieerd. Het verifieert geen spaak-naar-hub BFD-pad of uniciteit van het publieke eindpunt.

Stap 2. Dubbele eindpunten zoeken in OMP

Op de Cisco IOS XE-hub:

<#root>

show clock detail

show sdwan omp tlocs table | include 203.0.113.10

Op de SD-WAN-controller (vSmart):

<#root>

show clock

show omp tlocs | tab | include 203.0.113.10

Deze Controller-uitvoer maakt gebruik van genormaliseerde id's. IPv6- en regiokolommen worden weggelaten:

<#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
```

Vergelijk het TLOC-systeem IP, kleur, inkapseling, openbaar IP en openbare poort. Meerdere paden naar dezelfde logische TLOC van verschillende controllers zijn normaal. De botsingskandidaat is twee verschillende peer identiteiten met hetzelfde effectieve eindpunt.

Herhaal de gefilterde opdracht na 30-60 seconden en behoud beide tijdstempels. Aanhoudende overlap is nuttig bewijs; perfect gelijktijdige opdrachten zijn niet vereist. Verzamel OMP-gebeurtenissen en bijbehorende sessielevenscyclusrecords met TAC voor een korte overgangsperiode.

Voor twee verdachte leeftijdsgenoten, behouden hun individuele TLOC tabel vermeldingen:

<#root>

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

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

Gebruik dit filter voor een compacte weergave van de IPv4 TLOC-gegevens op Cisco IOS XE. Vervang het IP-adres van het systeem door de onderzochte peer en behoud de aanhalingstekens rond de ip <system-IP> selector:

<#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|::
```

Vergelijk de publieke en private adres / poort attributen voor beide peers. In het filter worden de overeenkomende lijnen unset, zero-valued, default en IPv6 uit deze weergave weggelaten.

Stap 3. Vergelijk logische TLOC's met Hub Session Ownership

Controleer de TLOC-status die aan FTM is geleverd. Vergelijk de systeem-IP's, kleuren, openbare IP-adressen en openbare UDP-poorten van beide peers.

<#root>

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

Voer deze opdrachten uit om Forwarding Table Manager (FTM), BFD en platformsessierecords te vergelijken:

<#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
```

Dit voorbeeld toont het patroon met genormaliseerde identificatiecodes. Kolomlabels worden toegevoegd aan de gefilterde FTM-rijen voor meer duidelijkheid; ze maken geen deel uit van de gefilterde opdrachtuitvoer:

<#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 en FTM behouden beide logische peer-identiteiten, terwijl deze sessie-zoekopdracht alleen Spoke A voor de gedeelde bestemming toont. Spoke A heeft ook een Down FTM-status; aanwezigheid in de platformsessietabel geeft geen gezond pad aan. De FTM TLOC-index verschilt van de BFD lokale discriminator (BFD-LD) in de sessietabel. Dit patroon is een reden om eigenaarschap tussen lagen te onderzoeken. Een ontbrekende CLI-rij alleen stelt geen pakketverlies vast.

In deze tabel vertegenwoordigt Kleur het lokale transport; gebruik Kleur op afstand in de gedetailleerde weergave om de externe TLOC te identificeren. Vergelijk ook DstIp en DPubIp: een aangeleerde werkelijke bestemming kan verschillen van het openbare eindpunt dat aan de sessie is gekoppeld. Gebruik de peer-specifieke weergave als een doelfilter niet meer overeenkomt met het aangeleerde adres.

Een Ongeldige volgende hop, SA-identificatiecode van 0 of In HW: FALSE levert extra bewijs in plaats van een unieke handtekening. Deze velden kunnen ook optreden tijdens de normale installatie of ondergrondse storing.

Stap 4. Controleer wat de NAT Gateway daadwerkelijk doet

Vraag de NAT- of serviceprovider-operator naar gelijktijdige UDP-vertaalrecords met deze velden:

```
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
```

Dit is een illustratieve vertaaltabel. Gebruik de equivalente diagnostische opdracht voor uw NAT-platform. Op een Cisco IOS XE NAT-gateway begint u met:

<#root>

show ip nat translations | include 203.0.113.10

Bewaar zowel de binnenkant van de bron- als de bestemmingskolommen. Een lijst met alleen de

vertaalde bron kan niet weergeven waarom hergebruik geldig is voor verschillende vBonds of welke spaak eigenaar is van de hub mapping.

Leg de getroffen UDP-stromen vast voor en na NAT voor zowel vBonds als de hub. Bewaar de volledige pakketlengte zodat de VCONTROL-trailer niet wordt ingekort. Maak gebruik van een met TAC overeengekomen verzameling van omsloten switched port analyzer (SPAN) of embedded packet capture (EPC). Vergelijk dezelfde stroom over opnamepunten; maak geen onderscheid tussen latentie en niet-gesynchroniseerde opnameklokken.

Stap 5. Inspecteer VCONTROL in Wireshark

Gebruik de Lua-decoder in de bijlage voor de hier beschreven IPv4 BFD/VCONTROL-indeling. Sla de code op als sdwan_vctrl.lua in dezelfde map als uw opname. Deze diagnostische decoder geeft zichtbare velden weer; hij decodeert ESP niet en verifieert de verificatie niet. Het bereik is compleet, niet-geneste IPv4 / UDP-pakketten met de verwachte BFD / VCONTROL-vlag en aanhangwagenstructuur.

Voer de Wireshark-opdracht uit vanuit de map die de decoder en de opname bevat:

<#root>

```
wireshark -n \

  -X lua_script:sdwan_vctrl.lua \

  -d udp.port==12346,sdwan_vctrl \

  -d udp.port==45678,sdwan_vctrl \

  -r hub.pcap
```

Vervang de voorbeeldpoorten door de voorbeeldpoorten in de opname. Gebruik in Windows of macOS het volledige pad naar het uitvoerbare bestand Wireshark als het niet in PATH staat.

Als alternatief kunt u het Lua-script laden bij het opstarten van Wireshark, een relevant UDP-pakket kiezen en naar Analyze > Decode As navigeren. Wijs de toepasselijke UDP-poortvermeldingen voor bron en bestemming toe aan SDWAN_VCTRL / SD-WAN VCTRL (IPv4). Een expliciete ONDERGRENS op de andere poort kan voorrang hebben op deze decoder. Pas de wijziging toe op deze analysesessie.

Dit weergavefilter toepassen:

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

Vouw SD-WAN VCTRL > Visible VCONTROL trailer uit en vergelijk:

```
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
```

Deze illustratieve waarden beschrijven de eerste tunnelinstelling voordat het leren van het dataplane is voltooid. Ze tonen de werkelijke hub mapping voor B naast het gedragen eindpunt. NAT wijzigt de buitenste headers; het herschrijft de eindpuntinformatie in deze trailer niet. Deze mismatch alleen toont geen fout aan.

Voer de TShark-opdracht uit voor een compacte export:

<#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
```

Zonder een aangepaste decoder heeft het hier beschreven IPv4-formaat deze 17-byte type-length-value (TLV) trailer aan het einde van de UDP-payload. Linklaagvulling bevindt zich buiten de UDP-payload:

```
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
```

Pas deze vaste lay-out niet toe op IPv6, andere besturingsformaten, afgekapte pakketten of willekeurige gecodeerde gegevens. Een leeg decoderfilter kan betekenen dat het pakket zich buiten het ondersteunde formaat bevindt. Een leesbaar broneindpunt is ook geen geverifieerd systeem-IP-label.

Opmerking: generieke ESP-sequentiewaarschuwingen in Wireshark zijn geen antireplay-diagnostiek voor routers. Correleer het pakket met routertellers en logs voordat u een verificatie- of eigendomsconclusie trekt.

Stap 6. Bevestig het getroffen pad en bewaar bewijs

Neem op de hub twee QuantumFlow Processor (QFP)-tegenmonsters rond de waargenomen storing:

<#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

Gebruik tegenverschillen in plaats van absolute totalen. Geaggregeerde IPsec-druppels kunnen

andere oorzaken hebben. Bevestig de aankomst van het pakket op het getroffen transport en correleer het met het peer-, endpoint-, BFD-discriminator-, tunnel-, SA- en evenementtijdstip.

Zorg voor TAC met de twee OMP-momentopnamen, sprak lokale eigenschappen en besturingselementen, hub sessie details voor beide peers, BFD staat, vertaling records, begrensd opnames, en software versies. Indien reeds beschikbaar, vermeld de relevante admin-techs en de verbindings-/terugtrekkingsgeschiedenis. Vermijd herhaalde verzameling van hele tabellen op een grote hub.

Test de bereikbaarheid van de service afzonderlijk en noteer het daadwerkelijk gekozen transport. Een BFD Up-indicatie van 0 seconden is geen blijvend herstel.

Workarounds en beperkingen

Evalueer deze mitigatiemogelijkheden met Cisco TAC en de NAT-operator. De beperking heeft betrekking op dubbele geadverteerde eindpunten die een gemeenschappelijke hub bereiken; het betekent niet dat symmetrische NAT, gedeelde openbare adressen of herhaalde privéadressen over het algemeen niet worden ondersteund. De herstelprocedures en de doeltreffendheid van de mitigatie zijn afhankelijk van de inzet.

Stabiele eindpuntonafhankelijke toewijzingen met unieke toewijzingen gebruiken

Een NAT-side preventieoptie voor de geïllustreerde reeks is om elk afzonderlijk spraaktransport-eindpunt een stabiel, uniek vertaald UDP-eindpunt te geven voor vBond-, controller- en hubbestemmingen. Verzoek zowel eindpuntonafhankelijkheid als uniekheid tussen spaken. Controleer het resultaat in vertaalrecords en -opnamen, ook na failover van NAT-gateway of statusrecreatie.

A kan bijvoorbeeld consequent 203.0.113.10:40001 gebruiken, terwijl B consequent 203.0.113.10:40002 gebruikt. Statische vertalingen of een geschikt toewijzingsbeleid kunnen dit gedrag bieden, afhankelijk van het NAT-platform en het toegangsontwerp.

Endpoint-independent mapping vereist geen onbeperkte inkomende toegang. Bewaar de vereiste firewallbesturingselementen. Een NAT-beleidscorrectie verwijdert niet automatisch de eerder geadverteerde of geprogrammeerde sessiestatus; coördineert een nieuwe ontdekkingscyclus en herstel met TAC.

Overlapping van poorten tussen verschillende spaken uitschakelen

Indien ondersteund, vertaalde reserve UDP-eindpunten op unieke wijze over de relevante SD-WAN-spaken. Hergebruik ze niet alleen omdat hun bestemmingen verschillen. Dit verwijdert direct de gelijktijdige duplicate-vBond-toewijzing die eerder is weergegeven, zelfs als de NAT-gateway een aantal bestemmingsafhankelijke gedragingen behoudt.

De instelling kan meer poorten gebruiken of extra openbare adressen vereisen. Het maakt op zichzelf niet de mapping voor elk gesproken eindpunt-onafhankelijk, en het lost geen stabiele ontvangerstaat op na latere eindpunttoewijzing.

Controleer bij meerdere NAT-fasen of redundante NAT-gateways de toewijzing die zichtbaar is aan de uiteindelijke internetgrens. Uniekheid binnen één NAT-instantie vestigt geen uniekheid in andere instanties die hetzelfde openbare adres delen.

Poortverschuiving gebruiken voor een kleine, gecontroleerde groep

De opdracht Port-offset biedt waarden van 0 tot en met 19. Spoke A kan bijvoorbeeld offset 0 behouden en Spoke B kan offset 1 gebruiken. Voer deze configuratieopdrachten uit op Spoke B:

<#root>

```
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
```

Controleer de actieve bron en de vertaalde poorten na de wijziging. Een wijziging in deze systeeminstelling kan besturings- en gegevensverbindingen tussen transporten opnieuw opbouwen. Het is geen niet-verstorende diagnostische stap.

De 20 offsets bieden 20 verschillende basispoortgroepen met offset 0 als één keuze. Ze zijn geen algemene limiet van 20 SD-WAN-routers achter één openbaar IP. Deze specifieke oplossing biedt

slechts 20 unieke offsetkeuzes en vereist de NAT-gateway om ze te behouden en te onderscheiden. Het faalt als een uniek schema wanneer compensaties worden hergebruikt. Port hopping voegt niet meer offset identiteiten toe.

124 routers kunnen bijvoorbeeld niet allemaal unieke offsets ontvangen achter één gedeeld adres. Voor een offset-only-regeling met maximaal 20 routers per groep met een openbaar adres zijn ten minste zeven groepen vereist. Deze rekenkunde is geen capaciteitsaanbeveling of vervanging voor verificatie van NAT-gedrag. Een NAT-gateway die vertaalde poorten herschrijft of overlapt, kan het schema zelfs met minder routers verslaan.

Behoud van bron-poort uitschakelen of Willekeurige toewijzing inschakelen

Een beleid zonder een conserveringsvoorkeur kan de neiging voor veel spaken verminderen om :12346 naar verschillende vBonds te ontvangen. Gerandomiseerde toewijzing kan deze toewijzingen over een grotere poortpool verdelen.

Geen van beide veranderingen alleen garandeert echter het voorkomen van botsingen. Een gerandomiseerde allocator kan nog steeds een poort hergebruiken op verschillende bestemmingen, een toewijzing naar de hub wijzigen of een verlopen eindpunt opnieuw toewijzen terwijl de oude hubstaat blijft bestaan. Controleer of de toewijzing uniek is voor abonnees en bestemmingen. Willekeurige poorten alleen vestigen geen uniekheid.

Controleer de instellingen voor bronpoortbehoud en -toewijzing op de NAT-gateway met de operator. De toepasselijke configuratie is afhankelijk van het NAT-platform; controleer de resulterende toewijzingen naar zowel vBonds als de hub met vertaalrecords en pakketopnamen.

Vertaalde poorten kunnen buiten het oorspronkelijke SD-WAN-basispoortbereik vallen. Controleer de firewallregels zodat ze niet alleen legitiem vertaald verkeer afwijzen omdat de bronpoort is gewijzigd.

Afzonderlijke openbare adressen of reservepoortblokken

Toegewezen vertaalde adressen of niet-overlappende poortblokken gereserveerd per spaak, kunnen verschillende geadverteerde eindpunten bieden voor verschillende actieve spaken. Het beleid moet consistent worden toegepast op de detectie- en hubpaden en op redundante NAT-knooppunten. Extra adresruimte en ondersteuning van de provider kan nodig zijn. Dynamisch hergebruik na het in kaart brengen van het pensioen vereist nog steeds een correct beheer van de levenscyclus van de hubsessie.

Een alternatief transport behouden en herstel coördineren

Een geverifieerde MPLS of een ander geschikt pad kan de service behouden terwijl het betreffende internetpad wordt onderzocht. Een onderliggende toegangscontrolelijst (ACL) die het gedeelde NAT-adres blokkeert, biedt alleen insluiting: deze kan internetredundantie verwijderen voor elke spaak achter dat adres en trekt hun OMP-advertenties niet automatisch in.

Een controle, clear interface reset, NAT-state clear of hub reload kan tijdelijk de status opnieuw creëren. Geen van beide garandeert preventie van herhaling. Voer geen brede wissels uit als eerste diagnostische stap. Bewaar het bewijs, corrigeer waar mogelijk de toewijzingsvoorwaarden en stem in met de kleinste herstelactie met TAC. Valideren van aanhoudende BFD Up en bidirectioneel verkeer op het herstelde pad.

Gerelateerde softwaredefecten

Cisco bug-ID	Toepassingsgebied relevant voor dit artikel
CSCww45867	Documentatie van de beperking van het eigendom van de hub-sessie wanneer verschillende collega's hetzelfde openbare TLOC-eindpunt adverteren. Dit record volgt de documentatie-update in plaats van een softwarecorrectie.
CSCwx12986	Een automatische port-hop/NAT-leersequentie kan een privé-tupel achterlaten in de openbare TLOC-velden. Als filialen dezelfde privé-IP: poort hergebruiken, kunnen de onjuiste openbare eindpunten overeenkomen met die van andere peers. Het corrigeren van dit producentendefect verhindert niet dat een geldige openbare haven wordt hergebruikt.
CSCwx48929	NAT-classificatie kan ten onrechte E worden wanneer de detectie terugkeert naar dezelfde vBond. Een correcte classificatie voorkomt het geldige hergebruikscenario van de verschillende vBond-poorten niet.

Correcties voor Cisco bug ID CSCwx12986 en Cisco bug ID CSCwx48929 garanderen geen unieke geadverteerde openbare eindpunten en elimineren dit botsingsscenario niet op zichzelf. Sluiting van de Cisco-bug-ID CSCww45867-documentatie brengt geen verandering in het softwaregedrag aan het licht. Bevestig de toepasselijke beperkingen en beperkingen met Cisco TAC.

Bijlage: De IPv4 VCONTROL-trailer decoderen

Sla deze code op als sdwan_vctrl.lua. De diagnostische decoder verifieert geen pakketten of decodeert hun payloads niet. Het maakt gebruik van de sdwan_vctrl display filter en registreert een expliciete Decode As choice. De packet capture blijft ongewijzigd.

```
-- 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)
```

Gerelateerde informatie

- RFC 7857, afdeling 3: Overlappend gedrag van poorten
- RFC 4787: NAT Behavioral Requirements for Unicast UDP
- RFC 5737: IPv4 Address Blocks Reserved for Documentation
- Cisco Catalyst SD-WAN-ontwerpgids
- Cisco IOS XE Catalyst SD-WAN-systeemopdrachten: poort-offset
- Offset-configuratie Cisco SD-WAN-poort
- Wireshark-opdrachtregelverwijzing
- TShark-opdrachtregelverwijzing
- Technische ondersteuning en documentatie – Cisco Systems

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.