Fehlerbehebung bei SD-WAN Hub-Tunneln mit doppelten NAT-Endpunkten

Inhalt

Einleitung

Voraussetzungen

- Anforderungen
- Verwendete Komponenten

Hintergrundinformationen

- NAT-Lernen auf Kontrollebene
- NAT-Schulung und VCONTROL für die Datenebene
- Port-Erhaltung, Port-Überlappung und Port-Randomisierung

Beispieltopologie

Warum der Konflikt passiert

- Verschiedene vBonds können denselben öffentlichen Endpunkt beobachten
- Dieselben Anzeigen erreichen einen zentralen Punkt
- Private-as-Public-Kollisionen mit wiederholten Zweigstellenadressen
- Neuzuweisung von NAT-Endpunkten

Symptome und Auswirkungen

Diagnose des Problems

- Schritt 1: Aufzeichnen des Software- und Spoke-Transportstatus
- Schritt 2: Duplizierte Endpunkte in OMP finden
- Schritt 3: Vergleich logischer TLOCs mit dem Eigentümer der Hub-Sitzung
- Schritt 4: Überprüfen der tatsächlichen Funktionsweise des NAT-Gateways
- Schritt 5: Überprüfen von VCONTROL in Wireshark
- Schritt 6: Den betroffenen Pfad bestätigen und Beweise aufbewahren

Workarounds und Einschränkungen

- Verwendung stabiler, endpunktunabhängiger Zuordnungen mit eindeutigen Zuweisungen
- Deaktivieren von Port-Überlappungen zwischen verschiedenen Spokes
- Port-Offset für eine kleine, kontrollierte Gruppe verwenden
- Deaktivieren der Quellport-Beibehaltung oder Aktivieren der zufälligen Zuweisung
- Separate öffentliche Adressen oder Reserve-Port-Blöcke
- Beibehaltung eines alternativen Transports und koordinierte Wiederherstellung

Zugehörige Softwarefehler

Anhang: Dekodieren des IPv4 VCONTROL-Trailers

Zugehörige Informationen

Einleitung

In diesem Dokument wird beschrieben, wie Ausfälle von Hub-Tunneln erkannt und gemindert werden können, wenn sich Spokes einen öffentlichen Network Address Translation (NAT)-Endpunkt teilen.

Voraussetzungen

Anforderungen

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

- Cisco Catalyst Software-Defined Wide Area Network (SD-WAN)-Architektur und Steuerverbindungen
- Overlay Management Protocol (OMP), Transport Locators (TLOCs), Bidirectional Forwarding Detection (BFD) und IP Security (IPsec)
- Multiprotocol Label Switching (MPLS)-Transportnetzwerke
- NAT-Zuordnung und Filterverhalten
- Grundlegende Paketanalyse mit Wireshark

Verwendete Komponenten

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

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

Der Sitzungseigentumsfehler des Hubs wurde auf Cisco IOS XE 17.18.2 mit funktionierenden paarweisen Schlüsseln wiedergegeben. Die Befehlsverfügbarkeit und die Ausgabefelder variieren je nach Plattform und Version.

In den Beispielen werden private Adressen oder Dokumentationsadressen verwendet, die von RFC 5737 reserviert wurden, sowie generische Gerätenamen. CLI-Ausschnitte werden gekürzt und verwenden normalisierte Bezeichner. Schnittstellennamen und einige Ausgabefelder variieren je nach Plattform und Version.

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.

⚠ Vorsicht: Konfigurationsänderungen und Verbindungszurücksetzungen können den Datenverkehr unterbrechen. Verwenden Sie einen genehmigten Wartungsplan. Die ersten Diagnosebefehle sind schreibgeschützt.

Hintergrundinformationen

Beginnen Sie mit einem Szenario, in dem eine symmetrische NAT richtig identifiziert wird. Spoke A registriert sich bei vBond 1, und Spoke B registriert sich bei vBond 2. Das NAT-Gateway kann diesen Verbindungen die gleiche umgewandelte Quell-IP-Adresse und den gleichen umgewandelten Quell-Port zuweisen, wenn ihre Ziele sich unterscheiden, wie es RFC 7857 zulässt. Beide Stationen können daher denselben öffentlichen Endpunkt für ihre TLOCs für das öffentliche Internet ankündigen, selbst wenn beide NAT-Typ A melden.

In der Beispieltopologie wird die Farbe für das öffentliche Internet verwendet. Das gleiche Szenario kann auch andere öffentliche Farben, wie z. B. Biz-Internet. die Diagnosefilter auf die tatsächlich betroffene Transportfarbe anwenden; die Farbe des öffentlichen Internets ist keine zwingende Bedingung.

✎ Hinweis: Cisco Catalyst SD-WAN unterstützt keine TLOCs von verschiedenen Standorten, die dieselbe öffentliche IP-Adresse und denselben UDP-Port an einen gemeinsamen empfangenden Edge melden. Das Empfängerverhalten unter dieser Kollisionsbedingung ist unvorhersehbar. Dies kann selbst dann der Fall sein, wenn die symmetrische NAT richtig identifiziert wurde. Die richtige NAT-Klassifizierung allein garantiert nicht, dass die angegebenen Endpunkte eindeutig sind.

NAT-Lernen auf Kontrollebene

Ein Edge sendet während der Registrierung bei vBond seine private Transportadresse und seinen privaten Port. vBond überwacht die Quelladresse und den Port dieser Verbindung und gibt den beobachteten Endpunkt an den Edge zurück. Der Edge kann diese Informationen über OMP als öffentliche Adresse und Port-Attribute eines TLOC veröffentlichen, einschließlich eines TLOC in einer öffentlichen Farbe, wie z. B. öffentlich-Internet oder Biz-Internet.

Die Beobachtung beschreibt die Verbindung zu diesem vBond. Bei einer zielabhängigen NAT kann die Zuordnung zu einem Hub unterschiedlich sein. Der Router vergleicht NAT-Beobachtungen, um das Zuordnungsverhalten zu klassifizieren. In show sdwan control local-properties steht A für adressen- und portabhängige Zuordnung und E für endpunktunabhängige Zuordnung. Die angezeigte Klassifizierung beschreibt die Entscheidung des Routers. Eine NAT-

Übersetzungstabelle oder Paketerfassung verifiziert das tatsächliche Verhalten des NAT-Gateways.

Führen Sie beispielsweise show sdwan control local-properties aus, und suchen Sie die Spalte NAT TYPE für den Transport. Diese gekürzte Ausgabe enthält die NAT-Typlegende und die ausgewählten Schnittstellenspalten mit normalisierten 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
```

Das biz-internet transport meldet A und kündigt 203.0.113.10:23012 als sein öffentliches Endgerät an. Der MPLS-Transport meldet "E" und hat identische private und öffentliche Endpunkte. Klassifizierung aus NAT TYPE lesen; Die Adressengleichheit oder die Portgleichheit allein identifiziert den NAT-Typ nicht. N bedeutet, dass der Router keine Klassifizierung gelernt hat.

NAT-Schulung und VCONTROL für die Datenebene

Bevor ein Hub ein verschlüsseltes BFD-Paket verarbeiten kann, muss er die eingehende IPsec-Sicherheitszuordnung (SA) für den entsprechenden Peer und Tunnel finden. Die SA identifiziert den kryptografischen Schlüssel und den anderen Status, der für die Authentifizierung und Entschlüsselung des Pakets erforderlich ist. Der Empfänger ermittelt diesen Zustand anhand der Endpunktinformationen und des ESP-Sicherheitsparameterindex (Encapsulating Security Payload, ESP). Der SPI allein ist keine global eindeutige Spoke-Kennung.

Ein Spoke hinter symmetrischer NAT initiiert normalerweise den Datenverkehr zu einem erreichbaren Hub. Dadurch wird eine Zuordnung für das jeweilige Ziel erstellt. Die Quelladresse oder der Port, die bzw. der vom Hub erkannt wurde, kann sich von dem öffentlichen Endpunkt unterscheiden, der zuvor über vBond ermittelt und in OMP angekündigt wurde. Daher stimmen die empfangenen äußeren Header nicht immer mit dem Endpunkt im installierten Tunnelstatus überein. Der Hub benötigt eine Möglichkeit, diesen neuen On-Wire-Endpunkt mit dem bekannten Remote-TLOC und dessen IPsec-Status zu verknüpfen, bevor BFD entschlüsselt werden kann.

Für das hier beschriebene IPv4-BFD-over-IPsec-Format platziert SD-WAN die Endpunktinformationen in einem sichtbaren VCONTROL-Trailer am Ende des UDP-Payloads, außerhalb des verschlüsselten BFD-Payloads. Der Hub kann diese Informationen vor der Entschlüsselung lesen. VCONTROL enthält Endpunktinformationen, keine Verschlüsselungsschlüssel, und stellt keine Peer-Identität selbst her.

Beispiel: Bei der erstmaligen Einrichtung des Tunnels vor Abschluss des Lernprozesses auf Datenebene:

```
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
```

Der Empfänger versucht zunächst, seine normale Endpunkt-/SPI-Suche durchzuführen. Wenn bei dieser Suche keine SA gefunden wird, bietet der VCONTROL-Quellendpunkt einen Fallback. In diesem Beispiel kann der Hub den übertragenen 203.0.113.10:12346 zusammen mit seinem lokalen Zielkontext und dem SPI verwenden, um die dem bekannten Remote-TLOC zugeordnete eingehende SA zu lokalisieren, obwohl das Paket von 203.0.113.10:45678.

Der ausgewählte SA stellt den Kontext für den Empfangsschlüssel bereit. Der SPI wählt die entsprechende Schlüsselgenerierung in diesem Kontext aus. Der Hub führt dann die IPsec-Authentifizierung und -Entschlüsselung durch. Nur ein Paket, das die erforderlichen Prüfungen besteht, ist für die BFD-Verarbeitung verfügbar. Ein lesbarer Trailer oder eine erfolgreiche Suche allein beweisen keinen erfolgreichen Authentifizierungs-, Entschlüsselungs- oder BFD-Empfang.

Der Unterschied zwischen den beobachteten und übertragenen Quellports kann daher bei symmetrischer NAT normal sein. Damit die Peer-Beziehung funktioniert, muss der Hub das Paket mit dem richtigen Tunnel- und Schlüsselstatus verknüpfen und den tatsächlichen Rückgabeendpunkt erlernen. Bei erfolgreichem Lernen kann der Hub in diesem Beispiel Datenrückverkehr an 203.0.113.10:45678 senden. Dies ist vom Lernen auf Steuerungsebene durch vBond unabhängig.

VCONTROL zwingt den Empfänger nicht, eine vorhandene Übereinstimmung zwischen Endpunkt und SPI zu überschreiben. Wenn ein doppelter Endpunktstatus ein Paket mit dem falschen Peer oder der falschen Schlüsselgenerierung verknüpft, garantiert der Trailer keine Wiederherstellung. Es gibt einen Suchhinweis; kann es nicht zwei Peers unterscheiden, die denselben Endpunkt tragen, ohne den richtigen umgebenden Tunnel und den richtigen kryptographischen Status.

VCONTROL ist auch auf entsprechenden BFD-Paketen vorhanden, wenn NAT-Typ E gemeldet wird. Es ist kein symmetrisches NAT-Flag und nicht in jedem normalen IPsec-Datenpaket enthalten. Bei dem hier beschriebenen IPv4-BFD-Format werden die Informationen für das Public-TLOC zwischen zwei Privatfarben weggelassen.

Der Peer-spezifische Endpunkt, der über die Datenebene erfasst wurde, bedeutet nicht, dass Spoke seine OMP-Werbung durch einen neuen Endpunkt für jedes Ziel ersetzen muss. Verschiedene erlernte Zuordnungen sind ein erwarteter Teil des Symmetric-NAT-Traversal.

Wenn ein Tunnel aktiv ist, kann ein Absender, der seinen eigenen übersetzten Endpunkt für diesen Tunnel gelernt hat, diesen Endpunkt als Quellinformationen übernehmen. Dies ist der öffentliche Endpunkt pro Tunnel des Absenders, nicht der Remote-Endpunkt oder eine neue globale OMP-Anzeige. Vergleichen Sie stets das Paket, die OMP-Ankündigung und den Sitzungsstatus aus demselben Beobachtungszeitraum.

Port-Erhaltung, Port-Überlappung und Port-Randomisierung

Dies sind verschiedene Verhaltensweisen:

Verhalten	Bedeutung
Erhalt des Quell-Ports	Das NAT-Gateway versucht, den ursprünglichen UDP-Quell-Port der Station (z. B. 12346) als übersetzten Quell-Port beizubehalten.
Port-Überschneidungen zwischen Zielen	Das NAT-Gateway verwendet eine übersetzte IP: Port für verschiedene interne Endpunkte, die mit verschiedenen externen Zielen kommunizieren.
Port-Randomisierung	Das NAT-Gateway wählt umgewandelte Ports mithilfe einer randomisierten Zuweisungsmethode aus.
Endgeräteunabhängige Zuordnung	Ein interner Endpunkt behält den gleichen umgewandelten Endpunkt für alle externen Ziele bei, solange diese Zuordnung vorhanden ist.

RFC 7857, Abschnitt 3 lässt überlappende externe Ports für unterschiedliche interne Endpunkte zu, wenn die Ziele unterschiedlich sind. Die NAT unterscheidet die Ströme anhand ihrer fünf Tupel. Dies lässt nicht zu, dass zwei UDP-Datenflüsse gleichzeitig an dasselbe Ziel gesendet werden, die nicht voneinander zu unterscheiden sind. Zufällige Zuteilung und Beibehaltung sind getrennte Zuteilungsoptionen. weder Endgeräteunabhängigkeit noch

Beispieltopologie

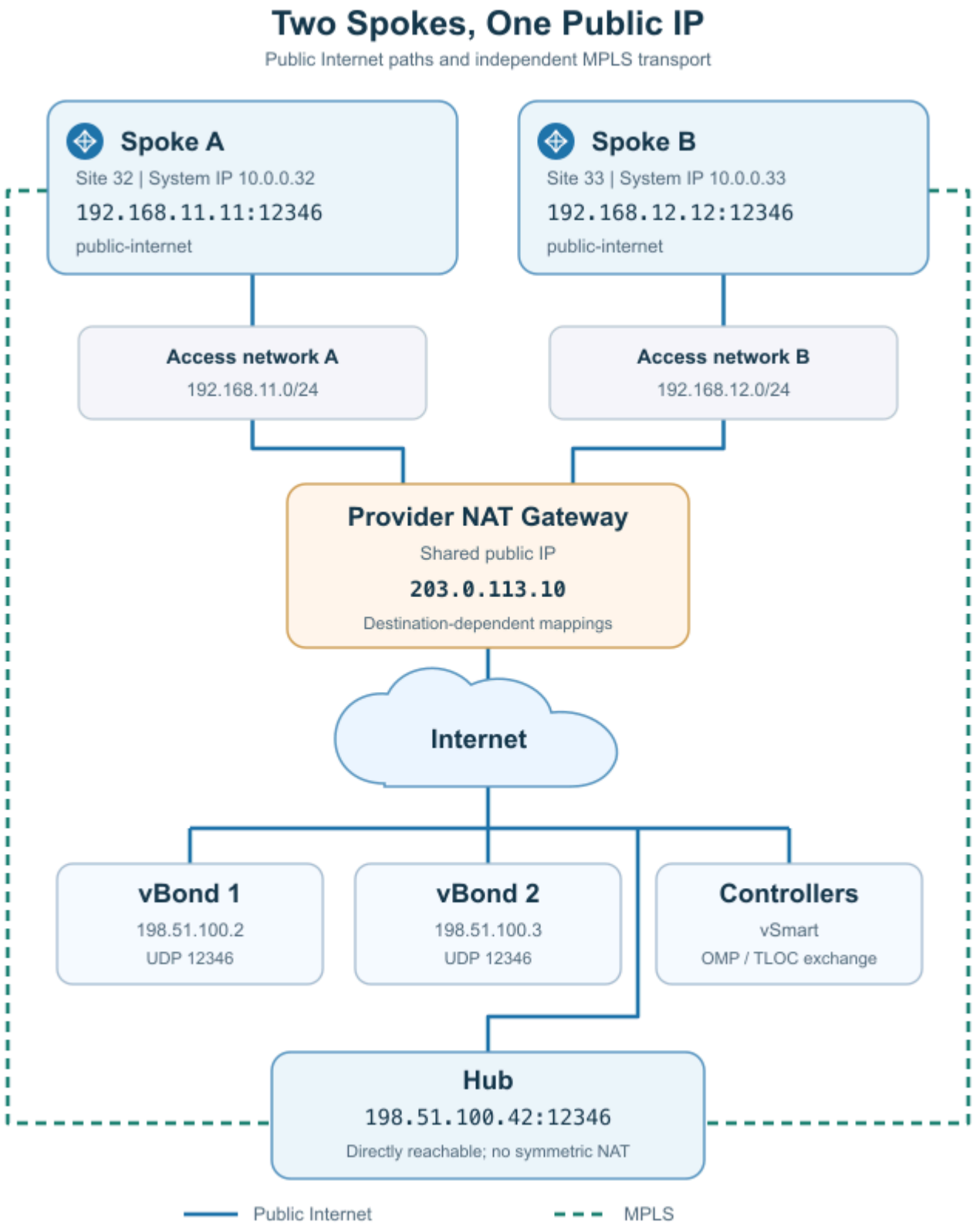

Abbildung 1: Gemeinsam genutztes NAT-Gateway, separate Spoke-Zugriffsnetzwerke und unabhängiger MPLS-Transport

Spoke A verwendet 192.168.11.11:12346 und Spoke B verwendet 192.168.12.12:12346. Beide geben die öffentliche Adresse weiter. 203.0.113.10 über das NAT-Gateway an. Der Hub hat eine direkt erreichbare Adresse und befindet sich nicht hinter symmetrischer NAT. Die beiden

Stationen können dasselbe öffentliche IP:Port ankündigen, obwohl sich ihre privaten Endpunkte unterscheiden.

Warum der Konflikt passiert

Verschiedene vBonds können denselben öffentlichen Endpunkt beobachten

Berücksichtigen Sie folgende gleichzeitige UDP-Zuordnungen:

Peer	Private Quelle	Übersetzte Quelle	Ziel
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

Die Antworten werden korrekt zurückgegeben, da die NAT auch den Remote-Endpunkt überprüft. Eine Antwort von vBond 1 gehört zur Zuordnung für A. Eine Antwort von vBond 2 gehört zur Zuordnung für B.

Beide Router können auch den anderen vBond kontaktieren und die zielabhängige Zuordnung richtig erkennen. Behalten Sie beispielsweise das private Quell-Tupel für jede Speiche unverändert bei, und beachten Sie die folgende Beobachtungsreihenfolge:

Peer	Erste akzeptierte vBond-Beobachtung	Vergleich mit der anderen vBond-Lösung	Ergebnis
A	vBond 1 gibt 203.0.113.10:12346 zurück	vBond 2 ergibt 203.0.113.10:40001	NAT A; Beibehaltenes öffentliches Tupel 203.0.113.10:12346
B	vBond 2 ergibt 203.0.113.10:12346	vBond 1 gibt 203.0.113.10:40002 zurück	NAT A; Beibehaltenes öffentliches Tupel 203.0.113.10:12346

Die vBond-Beobachtungen unterscheiden sich für jeden Router, sodass NAT A richtig erkannt werden kann. Die erhaltenen ersten Beobachtungen stimmen jedoch mit den beiden Routern überein. Klassifizierung A weist nicht allen Stationen einen eindeutigen öffentlichen Port zu, und der Besuch beider vBonds garantiert diese Einzigartigkeit nicht.

Jeder Spoke empfängt die öffentliche Adresse und den Port, die von vBond in der Registrierungsantwort beobachtet wurden, und verwendet die gespeicherte Beobachtung, um die lokalen Transporteigenschaften aufzufüllen. Das Spoke bezieht diesen öffentlichen Endpunkt

zusammen mit seinem privaten Endpunkt in die TLOC-Attribute ein, die es dem SD-WAN-Controller über OMP mitteilt. Der Controller verteilt den TLOC dann entsprechend der geltenden Kontrollrichtlinie an andere Edges. vBond selbst stammt nicht von der OMP-Werbung.

Wenn beide Speichen denselben beobachteten öffentlichen Endpunkt beibehalten, kann OMP daher Folgendes enthalten:

```
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
```

Diese bleiben unterschiedliche logische TLOCs, da sich die System-IPs unterscheiden.

Dieselben Anzeigen erreichen einen zentralen Punkt

Das NAT-Gateway muss beide Stationen unterscheiden, wenn sie denselben Hub kontaktieren. Eine mögliche Zuweisung ist:

Peer	Übersetzte Quelle zum Hub	Ziel
A	203.0.113.10:12346	198.51.100.42:12346
B	203.0.113.10:45678	198.51.100.42:12346

Der Hub verfügt über zwei logische Peers, die denselben Zielendpunkt melden, während Pakete von verschiedenen Endpunkten eintreffen können. Im normalen symmetrischen NAT-Betrieb hilft das Lernen auf Datenebene bei der Erstellung der Rückführungszuordnungen.

Die Beschränkung der Hub-Sitzungseigentumsinformationen tritt auf, wenn verschiedene Peers den durch diesen Transportschlüssel gewählten Sitzungsstatus gemeinsam nutzen:

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

Wenn beide Ankündigungen denselben Schlüssel wählen, kann ein Update eines späteren Peers die Besitzinformationen im gemeinsamen Status ersetzen. Ein anschließendes Zurückziehen, Löschen oder Neuerstellen der Sitzung für einen Peer kann den IPsec/BFD-Status für den anderen Peer stören. Das Lernen auf Datenebene garantiert keine Wiederherstellung, wenn dieser Status bereits mit dem falschen Peer oder der falschen Flow-Generierung verknüpft ist.

Der sichtbare Trailer ist keine unabhängige Peer-ID: Beide Stationen können denselben Quell-Endpunkt tragen. Wenn der Hub einen vorhandenen IPsec-Status auswählt, der zu der falschen Peer- oder Schlüsselgenerierung gehört, können Authentifizierung und Lernen fehlschlagen, obwohl die Pakete den Hub erreichen. Um diese Sequenz für ein bestimmtes Paket festzulegen, muss das Cisco Technical Assistance Center (TAC) die ausgewählte SA mit ihrem Peer und seiner Generation korrelieren. Der Packet Trailer allein kann es nicht beweisen.

Dieselbe öffentliche IP stellt allein keine Kollision her. Verschiedene Remote-Ports erzeugen normalerweise unterschiedliche Transportschlüssel. Überprüfen Sie auch die ausgewählte Hub-Local-Adresse, den lokalen Port und das Protokoll. Wenn ein dritter Peer denselben Endpunkt ankündigt, kann er auch um diesen Schlüssel konkurrieren. Das Fehlermuster hängt von der Ereignisreihenfolge ab.

Private-as-Public-Kollisionen mit wiederholten Zweigstellenadressen

Der Cisco Bug CSCwx12986 kann dazu führen, dass ein Edge während des NAT-Vergleichs ein privates RFC 1918-Tupel in seinen öffentlichen TLOC-Attributen ankündigt, nachdem ein automatischer Quell-Port-Hop ausgeführt wurde. Wenn verschiedene Zweigstellen dieselbe private Adresse und denselben Port verwenden, können diese falschen öffentlichen Attribute auf die Peers zutreffen und das Problem der Hub-Sitzungseigenschaft aufdecken.

Beispielsweise können beide Stationen 192.168.11.11 hinter separaten Firewalls verwenden. Jede Firewall trennt das Zweigstellennetzwerk und übersetzt die Quelladresse. Wenn ein Upstream-Provider-NAT-Gateway die Übersetzung erneut vornimmt, verfügt der Pfad über zwei NAT-Stufen oder eine doppelte NAT. Separate VRF-Kontexte (Virtual Routing and Forwarding) sind eine weitere Möglichkeit, um überlappende Zweigstellenadressen zu isolieren.

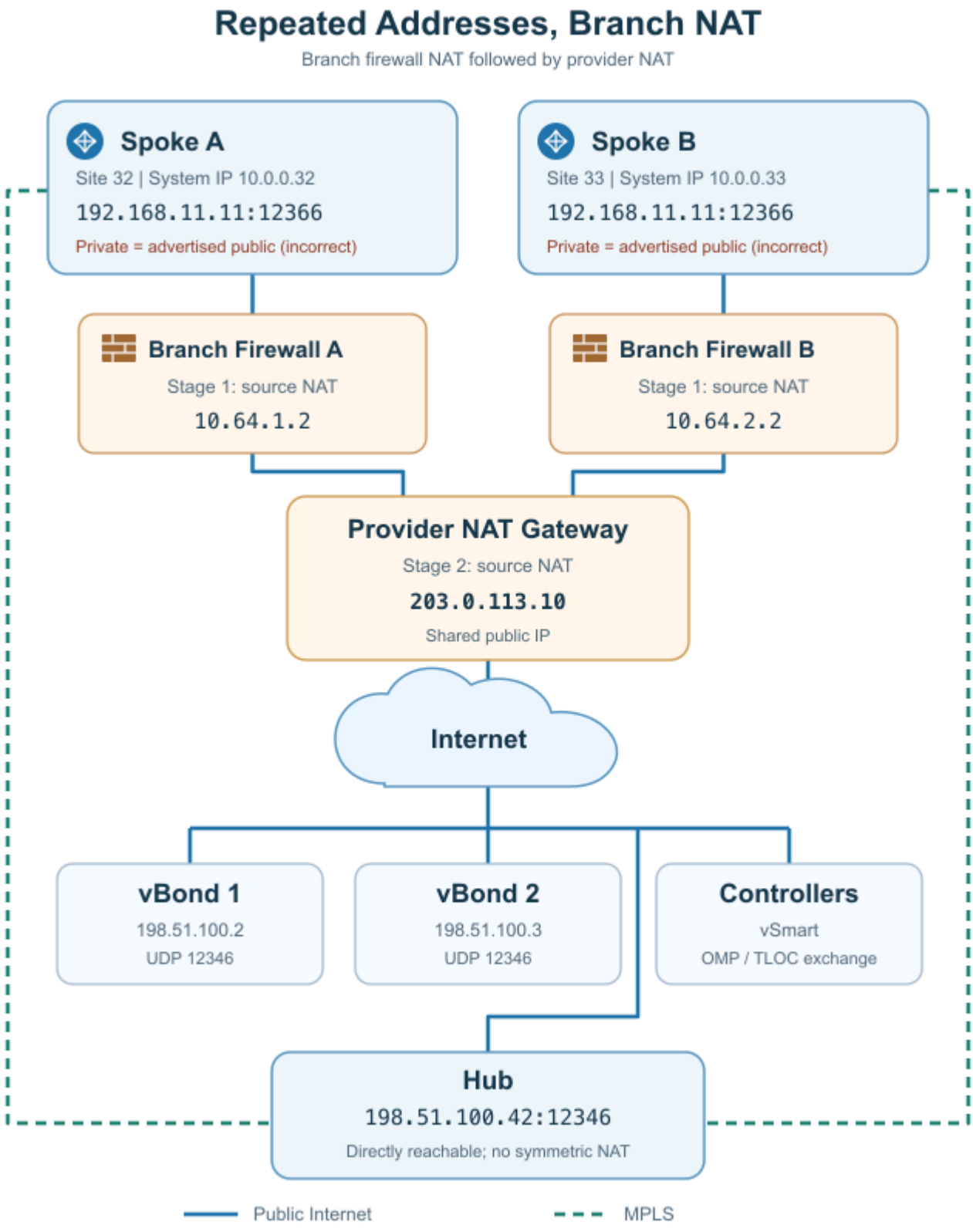

Abbildung 2: Übersetzungen von Branch Firewall und Provider NAT Die falschen öffentlichen TLOC-Attribute behalten den ursprünglichen privaten Endpunkt bei, während Pakete die umgewandelten Quelladressen verwenden.

Wenn beide Stationen auf den Defekt in ihren TLOCs für das öffentliche Internet stoßen und den gleichen Post-Hop-Quell-Port verwenden, kann der Hub folgende Meldungen empfangen:

Peer	Privater Endpunkt nach Port-Hop	Falscher öffentlicher TLOC-Endpunkt
A	192.168.11.11:12366	192.168.11.11:12366
B	192.168.11.11:12366	192.168.11.11:12366

Anmerkung: Wiederholte private Adressen und doppelte NAT sind keine Voraussetzung für die Cisco Bug-ID CSCwx12986 selbst. Für die zusätzliche Peer-übergreifende Kollision müssen die angegebenen IP:Port-Werte und die gleichen lokalen Hub-Adressen, Ports und Protokolle übereinstimmen. Dieselbe private IP-Adresse mit unterschiedlichen angekündigten Ports führt zu keiner Kollision.

Die Gleichheit öffentlicher und privater Adressen ist bei einem Transport ohne NAT normal. Eine RFC 1918-Adresse in einem öffentlichen Feld ist nur dann verdächtig, wenn sie dem beabsichtigten Pfad und der beobachteten Übersetzung widerspricht. Eindeutige Zweigstellen-Privatadressen vermeiden in diesem Beispiel die Überschneidung von wiederholten Private-Tupeln. sie verhindern nicht das zuvor beschriebene separate übersetzte-öffentliche Port-Wiederverwendungsszenario.

Neuzuweisung von NAT-Endpunkten

Ein Endpunkt kann auch nach Ablauf einer NAT-Zuordnung einer anderen Spoke zugewiesen werden, während der Hub den alten Peer-Status beibehält. Vergleichen Sie den Zuordnungsverlauf mit dem Hub-Sitzungslebenszyklus, um Überschneidungen zwischen dem alten und dem neuen Besitzer zu ermitteln.

Symptome und Auswirkungen

Typische Indikatoren sind:

- Die Steuerungsverbindungen bleiben aktiv, während die betroffenen BFD-Pfade inaktiv sind oder sich nicht erholen.
- Zwei unterschiedliche System-IPs kündigen dieselbe öffentliche IP-Adresse an: port.
- Der Hub behält beide logischen TLOCs bei, aber in einer gefilterten Plattformsitzungsansicht fehlt ein Peer oder es werden inkonsistente System-IP-, Remote-Farb-, Diskriminator-, Tunnel- oder SA-Informationen angezeigt.
- Ein Transportausfall oder eine Wiederherstellung für einen Peer stört einen anderen Peer mit demselben Endpunkt.
- IPsec-Eingabeverwerfungen können auf dem betroffenen Pfad zunehmen.

Durch den Ausfall kann der betroffene Transportpfad unbrauchbar werden. Ist dies der einzig nutzbare Transportweg für eine Speiche, so ist die Speiche von dem Overlay isoliert. In einem großen Hub, in dem sich viele Stationen eine NAT-Adresse teilen, steigt die Anzahl der betroffenen Pfade, die eine Korrelation erfordern. aus der Anzahl der Standorte hinter dieser Adresse nicht abgeleitet werden kann.

Diagnose des Problems

Schritt 1: Aufzeichnen des Software- und Spoke-Transportstatus

Ersetzen Sie an jedem betroffenen Cisco IOS XE Edge **<**die betroffene Farbe**>** durch die tatsächliche Transportfarbe, z. B. biz-internet oder 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

Notieren Sie sich die private/öffentliche Adresse, den Port, die Schnittstelle, die Farbe, den NAT-Typ, die Standort-ID und den Steuerungsstatus. Verwenden Sie nach dem ersten vollständigen Beispiel für lokale Eigenschaften diesen kompakten Filter, um die Schnittstellenüberschriften und die ausgewählte Transportzeile beizubehalten. Ersetzen Sie TenGigabitEthernet0/1/0.10 durch die betroffene Schnittstelle:

<#root>

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

Im Primärszenario können die entsprechenden Felder auf beiden Speichen gelesen werden. Dies ist eine Feldübersicht, nicht das systemeigene Spaltenlayout:

```
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
```

Eine Up-Steuerverbindung überprüft diese Controller-Beziehung. Es verifiziert weder einen Spoke-to-Hub-BFD-Pfad noch die Eindeutigkeit des öffentlichen Endpunkts.

Schritt 2: Duplizierte Endpunkte in OMP finden

Auf dem Cisco IOS XE-Hub:

<#root>

show clock detail

show sdwan omp tlocs table | include 203.0.113.10

Auf dem SD-WAN-Controller (vSmart):

<#root>

show clock

show omp tlocs | tab | include 203.0.113.10

Diese Controllerausgabe verwendet normalisierte Bezeichner. IPv6- und Regionsspalten werden weggelassen:

<#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
```

Vergleichen Sie die IP-Adresse, die Farbe, die Kapselung, die öffentliche IP-Adresse und den öffentlichen Port des TLOC-Systems. Mehrere Pfade zu demselben logischen TLOC von verschiedenen Controllern sind normal. Der Kollisionskandidat besteht aus zwei unterschiedlichen Peer-Identitäten mit demselben effektiven Endpunkt.

Wiederholen Sie den gefilterten Befehl nach 30-60 Sekunden, und behalten Sie beide Zeitstempel bei. Eine anhaltende Überschneidung ist ein nützlicher Beweis; keine gleichzeitigen Befehle erforderlich sind. Sammeln Sie für einen kurzen Übergangszeitraum OMP-Ereignisse und die entsprechenden Sitzungslebenszyklusdatensätze beim TAC.

Achten Sie bei zwei verdächtigen Peers darauf, die einzelnen Einträge in der TLOC-Tabelle beizubehalten:

<#root>

show sdwan omp tlocs table | include 10.0.0.32

show sdwan omp tlocs table | include 10.0.0.33

Verwenden Sie diesen Filter, um eine kompakte Ansicht der IPv4-TLOC-Details in Cisco IOS XE zu erhalten. Ersetzen Sie die System-IP durch die zu untersuchende Gegenstelle, und behalten Sie die Anführungszeichen um den IP <system-IP>-Selektor bei:

<#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|::

Vergleichen Sie die Attribute für öffentliche und private Adressen/Ports für beide Peers. Der Filter lässt übereinstimmende nicht festgelegte, nullwertige, Standard- und IPv6-Zeilen in dieser Ansicht unberücksichtigt.

Schritt 3: Vergleich logischer TLOCs mit dem Eigentümer der Hub-Sitzung

Überprüfen Sie den an FTM übermittelten TLOC-Status. Vergleichen Sie die System-IPs, die Farben, die öffentlichen IP-Adressen und die öffentlichen UDP-Ports der beiden Peers.

<#root>

show platform software sdwan ttmd tlocs

Führen Sie die folgenden Befehle aus, um die Datensätze für Forwarding Table Manager (FTM), BFD und Plattformsitzungen zu vergleichen:

<#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

Dieses Beispiel zeigt das Muster mit normalisierten Bezeichnern. Spaltenbeschriftungen werden zur Verdeutlichung zu den gefilterten FTM-Zeilen hinzugefügt; Sie sind nicht Teil der gefilterten Befehlsausgabe:

<#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 und FTM behalten beide logischen Peer-Identitäten bei, während diese Sitzungssuche nur Spoke A für das gemeinsam genutzte Ziel anzeigt. Spoke A hat ebenfalls den Status "Down FTM". Presence-Status in der Plattform-Sitzungstabelle gibt keinen fehlerfreien Pfad an. Der FTM-TLOC-Index unterscheidet sich vom lokalen BFD-Diskriminator (BFD-LD) in der Sitzungstabelle. Dieses Muster ist ein Grund, das Eigentum über mehrere Ebenen hinweg zu untersuchen. Eine fehlende CLI-Zeile allein stellt keinen Paketverlust fest.

In dieser Tabelle stellt Color den lokalen Transport dar. Verwenden Sie in der Detailansicht die Remote-Farbe, um die Remote-TLOC zu identifizieren. Vergleichen Sie auch DstIp und DPubIp: Ein erlerntes tatsächliches Ziel kann sich vom öffentlichen Endpunkt unterscheiden, der mit der Sitzung verknüpft ist. Verwenden Sie die Peer-spezifische Ansicht, wenn ein reiner Zielfilter nicht mehr mit der abgefragten Adresse übereinstimmt.

Ein ungültiger nächster Hop, ein SA-Bezeichner von 0 oder in HW: FALSE liefert zusätzliche Beweise anstelle einer eindeutigen Signatur. Diese Felder können auch bei normalem Setup- oder Underlay-Ausfall auftreten.

Schritt 4: Überprüfen der tatsächlichen Funktionsweise des NAT-Gateways

Fragen Sie den NAT- oder Dienstanbieter-Operator nach gleichzeitigen UDP-Übersetzungsdatensätzen mit folgenden Feldern:

```
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
```

Dies ist eine illustrative Übersetzungstabelle. Verwenden Sie den entsprechenden Diagnosebefehl für die NAT-Plattform. Auf einem Cisco IOS XE NAT-Gateway beginnen Sie mit:

<#root>

```
show ip nat translations | include 203.0.113.10
```

Bewahren Sie die interne Quell- und Zielspalte auf. Eine Liste, die nur die übersetzte Quelle enthält, kann nicht zeigen, warum die Wiederverwendung für verschiedene vBonds zulässig ist oder welche Spoke-Adresse für die Hub-Zuordnung zuständig ist.

Erfassen Sie die betroffenen UDP-Datenflüsse vor und nach NAT für vBonds und den Hub. Vollständige Paketlängen beibehalten, damit der VCONTROL-Trailer nicht abgeschnitten wird. Nutzung einer mit dem TAC vereinbarten Sammlung von Switched Port Analyzer (SPAN) oder Embedded Packet Capture (EPC) Vergleich des gleichen Datenflusses über Erfassungspunkte hinweg leiten Sie keine Latenz von nicht synchronisierten Erfassungsuhren ab.

Schritt 5: Überprüfen von VCONTROL in Wireshark

Verwenden Sie den Lua-Decoder im Anhang für das hier beschriebene IPv4-BFD/VCONTROL-Format. Speichern Sie den Code unter sdwan_vctrl.lua im gleichen Ordner wie die Erfassung. Dieser Diagnosedecoder zeigt sichtbare Felder an. ESP wird nicht entschlüsselt, und die Authentifizierung wird nicht überprüft. Der Umfang des Pakets umfasst vollständige, nicht verschachtelte IPv4-/UDP-Pakete mit der erwarteten BFD-/VCONTROL-Flag- und -Trailer-Struktur.

Führen Sie den Befehl Wireshark aus dem Ordner aus, der den Decoder und Ihre Erfassung enthält:

<#root>

```
wireshark -n \

  -X lua_script:sdwan_vctrl.lua \

  -d udp.port==12346,sdwan_vctrl \

  -d udp.port==45678,sdwan_vctrl \

  -r hub.pcap
```

Ersetzen Sie die Beispiel-Ports durch die Ports in der Erfassung. Verwenden Sie unter Windows oder MacOS den vollständigen Pfad zur ausführbaren Wireshark-Datei, wenn diese sich nicht in

PATH befindet.

Alternativ können Sie das Lua-Skript beim Start von Wireshark laden, ein relevantes UDP-Paket auswählen und zu Analyze > Decode As (Analyse > Decode als) navigieren. Weisen Sie die entsprechenden Quell- und Ziel-UDP-Port-Einträge SDWAN_VCTRL/SD-WAN VCTRL (IPv4) zu. Ein expliziter UDPENCAP-Eintrag auf dem anderen Port kann Vorrang vor diesem Decoder haben. Die Änderung auf diese Analysesitzung anwenden.

Diesen Anzeigefilter anwenden:

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

Erweitern Sie SD-WAN VCTRL > Visible VCONTROL-Trailer, und vergleichen Sie:

```
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
```

Diese Werte beschreiben die anfängliche Tunneleinrichtung, bevor das Lernen auf Datenebene abgeschlossen ist. Sie zeigen die tatsächliche Hub-Zuordnung für B zusammen mit dem mitgeführten Endpunkt. NAT ändert die äußeren Header. die Endpunktinformationen in diesem Trailer werden nicht umgeschrieben. Diese Diskrepanz weist nicht auf einen Fehler hin.

Führen Sie den Befehl TShark für einen Compact-Export aus:

<#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
```

Ohne einen benutzerdefinierten Decoder verfügt das hier beschriebene IPv4-Format über diesen 17-Byte-TLV-Trailer (Type-Length-Value) am Ende der UDP-Nutzlast. Der Link-Layer-Padding erfolgt außerhalb der UDP-Nutzlast:

```
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
```

Wenden Sie dieses feste Layout nicht auf IPv6, andere Kontrollformate, verkürzte Pakete oder beliebige verschlüsselte Daten an. Ein leerer Decoderfilter kann bedeuten, dass sich das Paket außerhalb des unterstützten Formats befindet. Ein lesbarer Quellendpunkt ist auch kein authentifiziertes System-IP-Label.



Anmerkung: Generische ESP-Sequenzwarnungen in Wireshark stellen keine Anti-Replay-Diagnose für den Router dar. Korrelieren Sie das Paket mit den Zählern und Protokollen des Routers, bevor Sie eine Schlussfolgerung zur Authentifizierung oder zum Besitz ziehen.

Schritt 6: Den betroffenen Pfad bestätigen und Beweise aufbewahren

Nehmen Sie auf dem Hub zwei QuantumFlow Processor (QFP)-Zählerproben um den beobachteten Fehler:

<#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
```

Verwenden Sie Zählerunterschiede anstelle von absoluten Summen. Aggregierte IPsec-Drops können andere Ursachen haben. Bestätigen Sie die Ankunft des Pakets beim betroffenen Transport, und korrelieren Sie es mit dem Peer, dem Endpunkt, dem BFD-Diskriminator, dem Tunnel, der SA und der Ereigniszeit.

Stellen Sie dem TAC die beiden OMP-Snapshots, lokale Spoke-Eigenschaften und -Steuerelemente, Hub-Sitzungsdetails für beide Peers, den BFD-Status, Übersetzungsdatensätze, begrenzte Erfassungen und Softwareversionen zur Verfügung. Falls bereits verfügbar, geben Sie die entsprechenden Admin-Technik und den Anschluss-/Entzugshistorie an. Vermeiden Sie das wiederholte Sammeln ganzer Tabellen an einem großen Hub.

Testen Sie die Erreichbarkeit des Service separat, und zeichnen Sie den tatsächlich ausgewählten Transport auf. Eine BFD-Up-Anzeige von 0 Sekunden ist keine nachhaltige Erholung.

Workarounds und Einschränkungen

Evaluieren Sie diese Optionen mit dem Cisco TAC und dem NAT-Operator. Die Beschränkung betrifft doppelt angekündigte Endpunkte, die einen gemeinsamen Hub erreichen; dies bedeutet nicht, dass symmetrische NAT, gemeinsam genutzte öffentliche Adressen oder wiederholte private Adressierung im Allgemeinen nicht unterstützt werden. Wiederherstellungsverfahren und Effektivität der Risikominimierung hängen von der Bereitstellung ab.

Verwendung stabiler, endpunktunabhängiger Zuordnungen mit eindeutigen Zuweisungen

Eine NAT-seitige Präventionsoption für die abgebildete Sequenz besteht darin, jedem einzelnen Spoke-Transport-Endpunkt ein stabiles, eindeutiges umgewandeltes UDP-Endpunkt für vBond-, Controller- und Hub-Ziele zuzuweisen. Anforderung von Endgeräteunabhängigkeit und Einzigartigkeit über mehrere Stationen hinweg Überprüfen Sie das Ergebnis der Übersetzungsdatensätze und -erfassungen, auch nach NAT-Gateway-Failover oder Statuswiederherstellung.

Beispielsweise kann A 203.0.113.10:40001 konsistent verwenden, während B konsistent 203.0.113.10:40002 verwendet. Statische Übersetzungen oder eine geeignete Zuweisungsrichtlinie können dieses Verhalten bereitstellen, abhängig von der NAT-Plattform und

dem Zugriff Design.

Für die endpunktunabhängige Zuordnung ist kein uneingeschränkter eingehender Zugriff erforderlich. Bewahren Sie die erforderlichen Firewall-Kontrollmechanismen auf. Durch eine NAT-Richtlinienkorrektur wird der zuvor angekündigte oder programmierte Sitzungsstatus nicht automatisch entfernt. Koordination eines neuen Erkennungszyklus und der Wiederherstellung mit dem TAC

Deaktivieren von Port-Überlappungen zwischen verschiedenen Spokes

Reservieren Sie, sofern dies unterstützt wird, übersetzte UDP-Endpunkte auf einzigartige Weise für die relevanten SD-WAN-Stationen. Verwenden Sie sie nicht allein deshalb wieder, weil ihre Ziele unterschiedlich sind. Dadurch wird das zuvor gezeigte gleichzeitige Duplicate-vBond-Mapping direkt entfernt, selbst wenn das NAT-Gateway ein bestimmtes zielabhängiges Verhalten beibehält.

Die Einstellung kann mehr Ports belegen oder zusätzliche öffentliche Adressen erfordern. Die Zuordnung für jeden Spoke-Endpunkt wird dadurch nicht eigenständig, und der Status des veralteten Empfängers wird nach der späteren Neuzuweisung des Endpunkts nicht aufgelöst.

Bei mehreren NAT-Phasen oder redundanten NAT-Gateways überprüfen Sie die an der letzten Internetgrenze sichtbare Zuweisung. Die Eindeutigkeit innerhalb einer NAT-Instanz stellt keine Eindeutigkeit für andere Instanzen her, die dieselbe öffentliche Adresse verwenden.

Port-Offset für eine kleine, kontrollierte Gruppe verwenden

Der Befehl port-offset stellt die Werte 0 bis 19 bereit. Beispiel: Spoke A kann Offset 0 beibehalten, und Spoke B kann Offset 1 verwenden. Führen Sie folgende Konfigurationsbefehle für Spoke B aus:

<#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
```

Überprüfen Sie nach der Änderung die aktiven Quell- und umgewandelten Ports. Durch eine Änderung dieser Systemeinstellung können die Steuerungs- und Datenverbindungen zwischen den Transportnetzen wiederhergestellt werden. Es handelt sich nicht um einen unterbrechungsfreien Diagnoseschritt.

Die 20 Offsets stellen 20 verschiedene Basis-Port-Gruppen mit Offset 0 zur Verfügung. Sie stellen keine allgemeine Beschränkung von 20 SD-WAN-Routern hinter einer öffentlichen IP dar. Diese spezielle Problemumgehung bietet nur 20 verschiedene Offset-Optionen und erfordert, dass das NAT-Gateway diese beibehält und zwischen ihnen unterscheidet. Wenn Offsets wiederverwendet werden, versagt sie als Eindeutigkeitsschema. Port-Hopping fügt keine weiteren Offset-Identitäten hinzu.

So können beispielsweise 124 Router nicht alle eindeutigen Offsets hinter einer gemeinsamen Adresse empfangen. Für ein Nur-Offset-Schema mit maximal 20 Routern pro Gruppe öffentlicher Adressen sind mindestens sieben Gruppen erforderlich. Diese Arithmetik ist keine Kapazitätsempfehlung oder kein Ersatz für die Verifizierung des NAT-Verhaltens. Ein NAT-Gateway, das übersetzte Ports umschreibt oder überschneidet, kann das Schema selbst mit weniger Routern umgehen.

Deaktivieren der Quellport-Beibehaltung oder Aktivieren der zufälligen Zuweisung

Eine Richtlinie, die keine Präferenz für die Erhaltung hat, kann die Tendenz vieler Speichen, 12346 zu verschiedenen vBonds zu empfangen, verringern. Bei einer zufälligen Zuweisung können diese Zuordnungen über einen größeren Port-Pool verteilt werden.

Keine Änderung allein garantiert jedoch eine Kollisionsvermeidung. Ein randomisierter Zuweiser kann einen Port weiterhin für mehrere Ziele verwenden, eine Zuordnung zum Hub ändern oder einen abgelaufenen Endpunkt neu zuweisen, solange der alte Hub-Status erhalten bleibt. Überprüfen Sie, ob die Zuweisung für Teilnehmer und Ziele eindeutig ist. Zufällige Ports allein stellen keine Eindeutigkeit her.

Überprüfen Sie die Aufbewahrungs- und Zuweisungseinstellungen für den Quell-Port am NAT-Gateway zusammen mit dem entsprechenden Operator. Die jeweilige Konfiguration hängt von der NAT-Plattform ab. Überprüfen der resultierenden Zuordnungen zu vBonds und zum Hub mithilfe von Übersetzungsdatensätzen und Paketerfassungen

Die umgewandelten Ports können außerhalb des ursprünglichen SD-WAN-Basisportbereichs liegen. Überprüfen Sie die Firewall-Regeln, damit legitimer umgewandelter Datenverkehr nicht allein aufgrund der Änderung des Quell-Ports abgelehnt wird.

Separate öffentliche Adressen oder Reserve-Port-Blöcke

Dedizierte übersetzte Adressen oder nicht überlappende Port-Blöcke, die pro Spoke reserviert sind, können unterschiedliche angekündigte Endpunkte für verschiedene aktive Stationen bereitstellen. Die Richtlinie muss konsistent auf die Erkennungs- und Hub-Pfade sowie auf redundante NAT-Knoten angewendet werden. Zusätzlicher Adressbereich und Unterstützung durch den Anbieter können erforderlich sein. Die dynamische Wiederverwendung nach der Zuordnung erfordert weiterhin das richtige Hub-Sitzungs-Lebenszyklusmanagement.

Beibehaltung eines alternativen Transports und koordinierte Wiederherstellung

Ein verifizierter MPLS- oder anderer qualifizierter Pfad kann den Service aufrechterhalten, während der betroffene Internetpfad untersucht wird. Eine unterlagerte Zugriffskontrollliste (ACL), die die gemeinsam genutzte NAT-Adresse blockiert, ermöglicht nur die Eindämmung: Sie kann die Internetredundanz für alle Spokes hinter dieser Adresse beseitigen und zieht ihre OMP-Werbung nicht automatisch zurück.

Control Clear, Interface Reset, NAT-State Clear oder Hub Reload können den Status vorübergehend neu erstellen. Keine garantiert die Vermeidung von Wiederholungen. Führen Sie als ersten Diagnoseschritt keine großflächigen Klarstellungen durch. Bewahren Sie die Nachweise auf, korrigieren Sie die Zuteilungsbedingungen nach Möglichkeit, und vereinbaren Sie mit der TAC die kleinste Bestandserholungsmaßnahme. Validierung von nachhaltigem BFD Up- und bidirektionalem Datenverkehr auf dem wiederhergestellten Pfad

Zugehörige Softwarefehler

Cisco Bug-ID	Für diesen Artikel relevanter Anwendungsbereich
CSW45867	Dokumentation der Einschränkung des Sitzungseigentums für den Hub, wenn verschiedene Peers denselben öffentlichen TLOC-Endpunkt ankündigen. Dieser Datensatz verfolgt das Dokumentations-Update und keine Software-Korrektur.
CSCwx12986	Eine automatische Port-Hop/NAT-Lernsequenz kann ein privates Tupel in den öffentlichen TLOC-Feldern belassen. Wenn Zweigstellen denselben privaten IP:Port wiederverwenden, können die falschen öffentlichen Endpunkte mit den Peers übereinstimmen. Die Korrektur dieses Herstellerfehlers verhindert nicht die Wiederverwendung gültiger übersetzter öffentlicher Ports.

Cisco Bug-ID	Für diesen Artikel relevanter Anwendungsbereich
CSCwx48929	NAT-Klassifizierung kann fälschlicherweise zu E werden, wenn die Erkennung zu demselben vBond zurückkehrt. Die korrekte Klassifizierung verhindert nicht das gültige "different-vBond port-reuse"-Szenario.

Korrekturen für Cisco Bug-ID CSCwx12986 und Cisco Bug-ID CSCwx48929 garantieren keine eindeutigen angekündigten öffentlichen Endpunkte und beseitigen dieses Kollisionsszenario nicht für sich allein. Durch das Schließen des Dokumentationsdatensatzes mit der Cisco Bug-ID CSCww45867 wird keine Änderung des Softwareverhaltens festgestellt. Bestätigen Sie die geltenden Einschränkungen und Einschränkungen mit dem Cisco TAC.

Anhang: Dekodieren des IPv4 VCONTROL-Trailers

Speichern Sie den Code unter dem Namen sdwan_vctrl.lua. Der Diagnosedecoder authentifiziert keine Pakete und entschlüsselt deren Payloads nicht. Es verwendet den Anzeigefilter sdwan_vctrl und registriert eine explizite Decode As-Auswahl. Die Paketerfassung bleibt unverändert.

```
-- 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)
```

Zugehörige Informationen

- RFC 7857, Abschnitt 3: Port-überlappendes Verhalten
- RFC 4787: NAT-Verhaltensanforderungen für Unicast UDP
- RFC 5737: Für Dokumentation reservierte IPv4-Adressblöcke
- Cisco Catalyst SD-WAN - Designleitfaden
- Cisco IOS XE Catalyst SD-WAN-Systembefehle: Port-Offset
- Konfiguration des Cisco SD-WAN-Port-Offsets
- Wireshark-Befehlszeilenreferenz
- TShark-Befehlszeilenreferenz
- Technischer Support und Dokumentation für Cisco Systeme

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.