Resolución de problemas de túneles de concentrador SD-WAN con terminales NAT duplicados

Contenido

- Introducción
- Prerequisites
  - Requirements
  - Componentes Utilizados
- Antecedentes
  - Aprendizaje de NAT del plano de control
  - Aprendizaje NAT de plano de datos y VCONTROL
  - Preservación de puertos, superposición de puertos y aleatorización de puertos
- Topología de ejemplo
- Por qué ocurre la colisión
  - Diferentes vBonds pueden observar el mismo terminal público
  - Los Mismos Anuncios Llegan A Un Hub
  - Colisiones de lo privado como lo público con direcciones de sucursal repetidas
  - Reasignación de extremo NAT
- Síntomas e impacto
- Diagnosticar el problema
  - Paso 1. Registro del estado de transporte de software y radio
  - Paso 2. Buscar terminales duplicados en OMP
  - Paso 3. Comparación de TLOCs Lógicos con la Propiedad de la Sesión del Hub
  - Paso 4. Verifique lo que hace realmente la puerta de enlace NAT
  - Paso 5. Inspeccione VCONTROL en Wireshark
  - Paso 6. Confirmar el trayecto afectado y conservar la evidencia
- Soluciones y limitaciones
  - Utilizar asignaciones independientes de terminales estables con asignaciones únicas
  - Deshabilitar la superposición de puertos entre diferentes radios
  - Uso del desplazamiento de puertos para un grupo pequeño y controlado
  - Desactivar conservación de puerto de origen o activar asignación aleatoria
  - Direcciones públicas separadas o bloques de puertos de reserva
  - Conservación de un transporte alternativo y recuperación de coordenadas
- Defectos de software relacionados
- Apéndice: Decodificación de la cola IPv4 VCONTROL
- Información Relacionada

Introducción

Este documento describe cómo identificar y mitigar fallas del túnel hub cuando los spokes comparten un punto final de traducción de direcciones de red (NAT) público.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Arquitectura de red de área extensa (SD-WAN) definida por software Cisco Catalyst y conexiones de control
- Overlay Management Protocol (OMP), Transport Locators (TLOC), Bidirectional Forwarding Detection (BFD) y IP Security (IPsec)
- Redes de transporte de switching de etiquetas multiprotocolo (MPLS)
- Asignación NAT y comportamiento de filtro
- Análisis básico de paquetes con Wireshark

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Routers Cisco IOS® XE Catalyst SD-WAN
- Controlador Cisco Catalyst SD-WAN (vSmart)
- Cisco Catalyst SD-WAN Validator (vBond)

La falla de propiedad de la sesión del hub se reprodujo en Cisco IOS XE 17.18.2 con claves pares operativas. La disponibilidad de los comandos y los campos de resultados varían según la plataforma y la versión.

Los ejemplos utilizan direcciones privadas o direcciones de documentación reservadas por RFC 5737, con nombres de dispositivos genéricos. Los extractos de CLI se acortan y utilizan identificadores normalizados. Los nombres de interfaz y algunos campos de salida varían según la plataforma y la versión.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente

de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

⚠ Precaución: Los cambios de configuración y los reinicios de conexión pueden interrumpir el tráfico. Utilice un plan de mantenimiento aprobado. Los comandos de diagnóstico iniciales son de sólo lectura.

Antecedentes

Comience con un escenario en el que la NAT simétrica se identifique correctamente. Spoke A se registra con vBond 1 y Spoke B se registra con vBond 2. El gateway NAT puede asignar la misma dirección IP de origen traducida y el mismo puerto a estas conexiones cuando sus destinos difieren, como permite RFC 7857. Por consiguiente, ambos spokes pueden anunciar el mismo punto final público para sus TLOC de Internet público, incluso cuando ambos informan de NAT tipo A.

La topología de ejemplo utiliza el color de Internet público. El mismo escenario puede involucrar otros colores públicos, como internet de negocios. Aplicar los filtros de diagnóstico al color de transporte real afectado; el color literal de internet pública no es una condición obligatoria.

✎ Nota: Cisco Catalyst SD-WAN no admite TLOC de diferentes sitios que anuncian la misma dirección IP pública y el mismo puerto UDP hacia un extremo de recepción común. El comportamiento del receptor en esta condición de colisión es impredecible. Esto puede ocurrir incluso cuando la NAT simétrica está identificada correctamente. La clasificación NAT correcta por sí sola no garantiza que los extremos anunciados sean únicos.

Aprendizaje de NAT del plano de control

Un extremo envía su dirección y puerto de transporte privado durante el registro con vBond. vBond observa la dirección de origen y el puerto en esa conexión y devuelve el extremo observado al extremo. El Edge puede anunciar esta información a través de OMP como la dirección pública y los atributos de puerto de un TLOC, incluido un TLOC con un color público como internet público o internet de negocios.

La observación describe la conexión con ese vBond. Con NAT dependiente del destino, la asignación hacia un hub puede ser diferente. El router compara las observaciones de NAT para clasificar el comportamiento de mapeo. En show sdwan control local-properties, A significa mapeo dependiente de la dirección y el puerto, y E significa mapeo independiente del punto final. La clasificación mostrada describe la decisión del router; una tabla de traducción NAT o captura de

paquetes verifica el comportamiento real del gateway NAT.

Por ejemplo, ejecute show sdwan control local-properties y busque la columna NAT TYPE para el transporte. Este resultado abreviado conserva la leyenda de tipo NAT y las columnas de interfaz elegidas, con direcciones normalizadas:

<#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
```

El transporte biz-internet informa A y anuncia 203.0.113.10:23012 como su punto final público. El transporte MPLS informa E y tiene extremos privados y públicos iguales. Lea la clasificación de NAT TYPE; la dirección o la igualdad de puerto por sí solas no identifican el tipo de NAT. N significa que el router no ha aprendido una clasificación.

Aprendizaje NAT de plano de datos y VCONTROL

Antes de que un hub pueda procesar un paquete BFD cifrado, debe encontrar la asociación de seguridad (SA) IPsec entrante para el par y el túnel correspondientes. La SA identifica la clave criptográfica y otros estados requeridos para autenticar y descifrar el paquete. El receptor utiliza la información del terminal junto con el Índice de parámetros de seguridad (SPI) de carga de seguridad de encapsulación (ESP) para localizar ese estado. El SPI por sí solo no es un identificador de radio único global.

Un radio detrás de NAT simétrica normalmente inicia el tráfico hacia un hub alcanzable. Esto crea una asignación para ese destino en particular. La dirección o el puerto de origen que ve el hub pueden diferir del terminal público que se conocía anteriormente a través de vBond y que se anunciaba en OMP. Como resultado, los encabezados de los routers recibidos no siempre coinciden con el punto final en el estado de túnel instalado. El hub necesita una manera de asociar este nuevo punto final en el cable con el TLOC remoto conocido y su estado IPsec antes de poder descifrar BFD.

Para el formato IPv4 BFD-over-IPsec aquí descrito, SD-WAN coloca la información del terminal

en una cola VCONTROL visible al final de la carga útil UDP, fuera de la carga útil BFD cifrada. El hub puede leer esta información antes del descifrado. VCONTROL transporta información de terminal, no claves de cifrado, y no establece la identidad de peer por sí mismo.

Por ejemplo, durante el establecimiento inicial del túnel, antes de que finalice el aprendizaje del plano de datos:

```
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
```

El receptor primero intenta su búsqueda normal de terminal/SPI. Si esa búsqueda no encuentra una SA, el extremo de origen de VCONTROL proporciona una reserva. En este ejemplo, el hub puede utilizar el 203.0.113.10:12346 transportado, junto con su contexto de destino local y el SPI, para localizar la SA entrante asociada con el TLOC remoto conocido, aunque el paquete llegue desde 203.0.113.10:45678.

La SA elegida proporciona el contexto de la clave de recepción. El SPI elige la generación de claves aplicable en ese contexto. A continuación, el hub realiza la autenticación y el descifrado de IPsec; sólo un paquete que pasa las comprobaciones requeridas está disponible para el procesamiento BFD. Una cola legible o una búsqueda exitosa por sí sola no prueban una autenticación, descifrado o recepción BFD exitosos.

Por lo tanto, la diferencia entre los puertos de origen observados y transportados puede ser normal con NAT simétrica. Para que la relación de pares funcione, el hub debe asociar el paquete con el túnel y el estado de clave correctos y aprender el punto final de retorno real. En este ejemplo, el aprendizaje correcto permite que el hub envíe tráfico de retorno a 203.0.113.10:45678. Esto es independiente del aprendizaje del plano de control a través de vBond.

VCONTROL no fuerza al receptor a invalidar una coincidencia existente de terminal/SPI. Si el estado de punto final duplicado asocia un paquete con el par o la generación de clave incorrectos, la cola no garantiza la recuperación. Proporciona una pista de búsqueda; no puede distinguir dos peers que transportan el mismo punto final sin el túnel circundante y el estado criptográfico correctos.

VCONTROL también está presente en los paquetes BFD aplicables cuando se informa del tipo E de NAT. Su presencia no es un indicador NAT simétrico y no se incluye en todos los paquetes de datos IPsec ordinarios. Para el formato BFD IPv4 descrito aquí, la información de TLOC pública se omite entre dos colores privados.

El punto final específico del peer aprendido a través del plano de datos no significa que el spoke

deba reemplazar su anuncio de OMP con un nuevo punto final para cada destino. Diferentes mapeos aprendidos son una parte esperada de NAT simétrica traversal.

Una vez que un túnel está activo, un remitente que ha aprendido su propio punto final traducido para ese túnel puede transportar ese punto final como su información de origen. Este es el punto final público por túnel del remitente, no el punto final remoto o un nuevo anuncio de OMP global. Compare siempre el paquete, el anuncio de OMP y el estado de sesión del mismo período de observación.

Preservación de puertos, superposición de puertos y aleatorización de puertos

Estos son diferentes comportamientos:

Comportamiento	Significado
Preservación del puerto de origen	El gateway NAT intenta conservar el puerto de origen UDP original del spoke, por ejemplo, 12346, como puerto de origen traducido.
Superposición de puertos entre destinos	El gateway NAT reutiliza una IP traducida: puerto para diferentes terminales internos que se comunican con diferentes destinos externos.
Aleatorización de puertos	El gateway NAT elige los puertos traducidos mediante un método de asignación aleatoria.
Asignación independiente del terminal	Un terminal interno conserva el mismo terminal traducido en los destinos externos mientras exista esa asignación.

RFC 7857, Sección 3 permite la superposición de puertos externos para diferentes terminales internos cuando los destinos difieren. La NAT distingue los flujos usando sus cinco tuplas. Esto no permite dos flujos simultáneos indistinguibles de UDP al mismo destino. La asignación aleatoria y la conservación son opciones de asignación separadas; ninguna de las dos establece independencia de punto final.

Topología de ejemplo

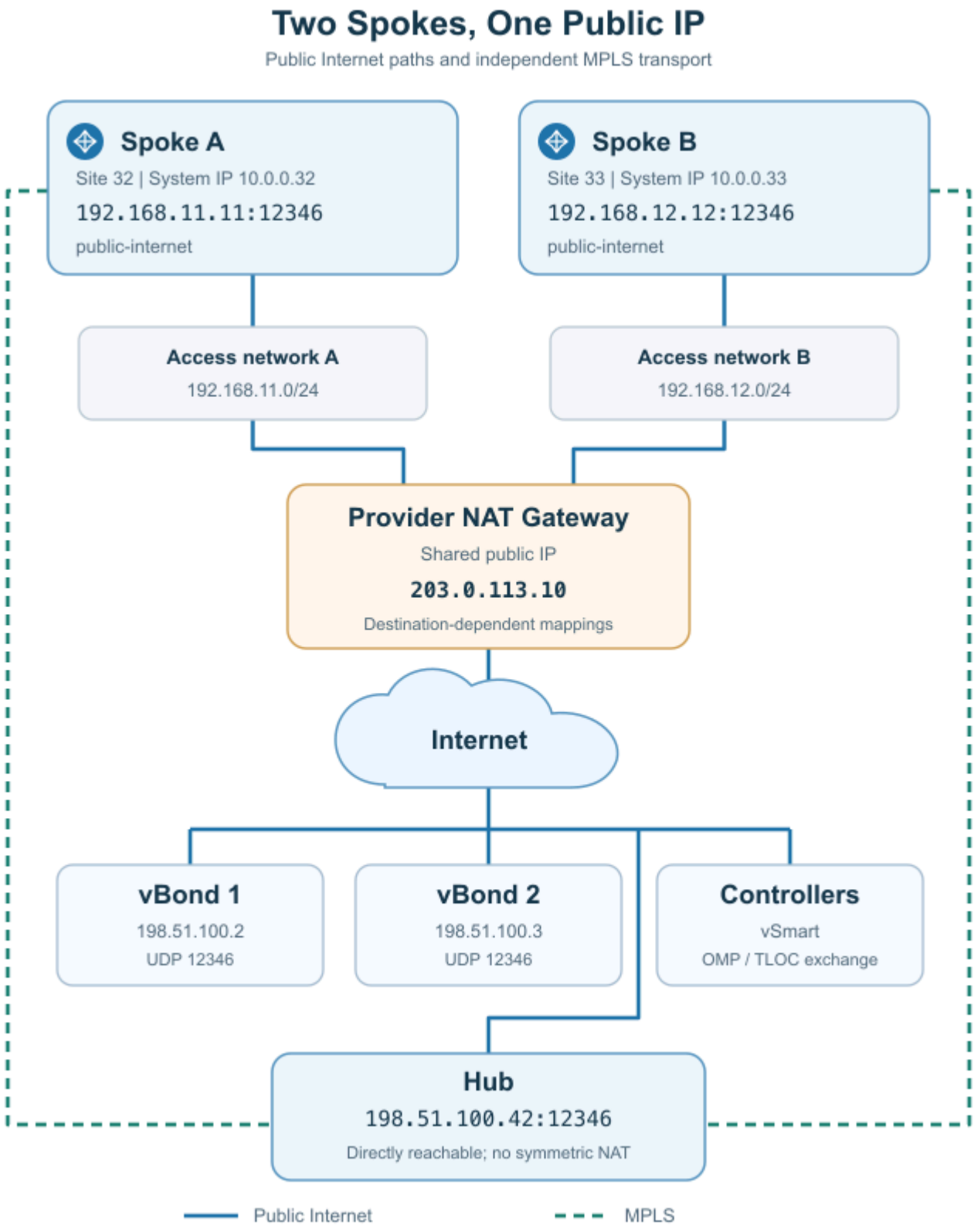

Figura 1. Gateway NAT compartido, redes de acceso de radio independientes y transporte MPLS independiente.

El Spoke A utiliza 192.168.11.11:12346, y el Spoke B utiliza 192.168.12.12:12346. Ambos comparten la dirección pública 203.0.113.10 a través del gateway NAT. El hub tiene una dirección directamente alcanzable y no está detrás de NAT simétrica. Los dos spokes pueden anunciar la

misma IP:puerto pública aunque sus terminales privados difieran.

Por qué ocurre la colisión

Diferentes vBonds pueden observar el mismo terminal público

Considere estos mapeos UDP simultáneos:

Entidad par	Origen privado	Origen traducido	Destino
R	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

Las respuestas se devuelven correctamente porque la NAT también comprueba el extremo remoto. Una respuesta de vBond 1 pertenece a la asignación para A; una respuesta de vBond 2 pertenece a la asignación para B.

Ambos routers también pueden ponerse en contacto con el otro vBond y detectar correctamente la asignación dependiente del destino. Por ejemplo, mantenga la tupla de fuente privada para cada radio sin cambios y considere este orden de observación:

Entidad par	Primera observación vBond aceptada	Comparación con otros vBond	Resultado
R	vBond 1 devuelve 203.0.113.10:12346	vBond 2 devuelve 203.0.113.10:40001	NAT A; tupla pública retenida 203.0.113.10:12346
B	vBond 2 devuelve 203.0.113.10:12346	vBond 1 devuelve 203.0.113.10:40002	NAT A; tupla pública retenida 203.0.113.10:12346

Las observaciones de vBond difieren para cada router, por lo que la detección de NAT A es correcta. Sin embargo, las primeras observaciones retenidas coinciden entre los dos routers. La clasificación A no asigna un puerto público único a todos los radios y la visita de ambos vBonds no garantiza esa exclusividad.

Cada radio recibe la dirección pública y el puerto observados por vBond en la respuesta de registro y utiliza la observación conservada para poblar sus propiedades de transporte local. El spoke incluye ese terminal público, junto con su terminal privado, en los atributos TLOC que anuncia al controlador SD-WAN a través de OMP. A continuación, el controlador distribuye el

TLOC a otras aristas de acuerdo con la política de control aplicable; vBond en sí no origina el anuncio OMP.

Si ambos radios conservan el mismo punto final público observado, el OMP puede contener:

```
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
```

Éstos siguen siendo diferentes TLOC lógicos porque sus IP del sistema difieren.

Los Mismos Anuncios Llegan A Un Hub

El gateway NAT debe distinguir ambos radios cuando entran en contacto con el mismo hub. Una posible asignación es:

Entidad par	Traducción del origen al hub	Destino
R	203.0.113.10:12346	198.51.100.42:12346
B	203.0.113.10:45678	198.51.100.42:12346

El hub tiene dos pares lógicos que anuncian el mismo punto final de destino, mientras que los paquetes pueden llegar desde diferentes puntos finales reales. En el funcionamiento normal de NAT simétrica, el aprendizaje del plano de datos ayuda a establecer las asignaciones de retorno.

La limitación de propiedad de sesión de hub surge cuando diferentes peers comparten el estado de sesión elegido por esta clave de transporte:

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

Si ambos anuncios eligen la misma clave, una actualización de un par posterior puede reemplazar la información de propiedad en estado compartido. Una retirada, eliminación o recreación subsiguiente de la sesión para un par puede perturbar el estado IPsec/BFD para el otro par. El aprendizaje del plano de datos no garantiza la recuperación cuando ese estado ya está asociado con el par o la generación de flujo incorrectos.

La cola visible no es un identificador de peer independiente: ambos spokes pueden llevar el

mismo punto final de origen. Si el hub elige un estado IPsec existente que pertenece al peer o a la generación de claves incorrecta, la autenticación y el aprendizaje pueden fallar aunque los paquetes lleguen al hub. Para establecer esa secuencia para un paquete determinado, el Cisco Technical Assistance Center (TAC) debe correlacionar la SA elegida con su par y su generación. El trailer del paquete por sí solo no puede probarlo.

La misma IP pública por sí sola no establece una colisión. Los diferentes puertos remotos normalmente producen diferentes claves de transporte. Compruebe también la dirección local del hub, el puerto local y el protocolo seleccionados. Si un tercer par anuncia el mismo punto final, también puede competir por esa clave; el patrón de error depende del orden de los eventos.

Colisiones de lo privado como lo público con direcciones de sucursal repetidas

El ID de bug de Cisco CSCwx12986 puede hacer que un Edge anuncie una tupla RFC 1918 privada en sus atributos TLOC públicos después de un salto de puerto de origen automático durante la comparación NAT. Si diferentes sucursales reutilizan la misma dirección privada y el mismo puerto, esos atributos públicos incorrectos pueden coincidir entre pares y exponer el problema de propiedad de la sesión del hub.

Por ejemplo, ambos radios pueden utilizar 192.168.11.11 detrás de firewalls de sucursal separados. Cada firewall mantiene su red de sucursal separada y traduce la dirección de origen. Si un gateway NAT de proveedor ascendente lo traduce nuevamente, la trayectoria tiene dos etapas NAT, o NAT doble. Los contextos de reenvío y routing virtuales (VRF) independientes son otra forma de mantener aisladas las direcciones de sucursal superpuestas.

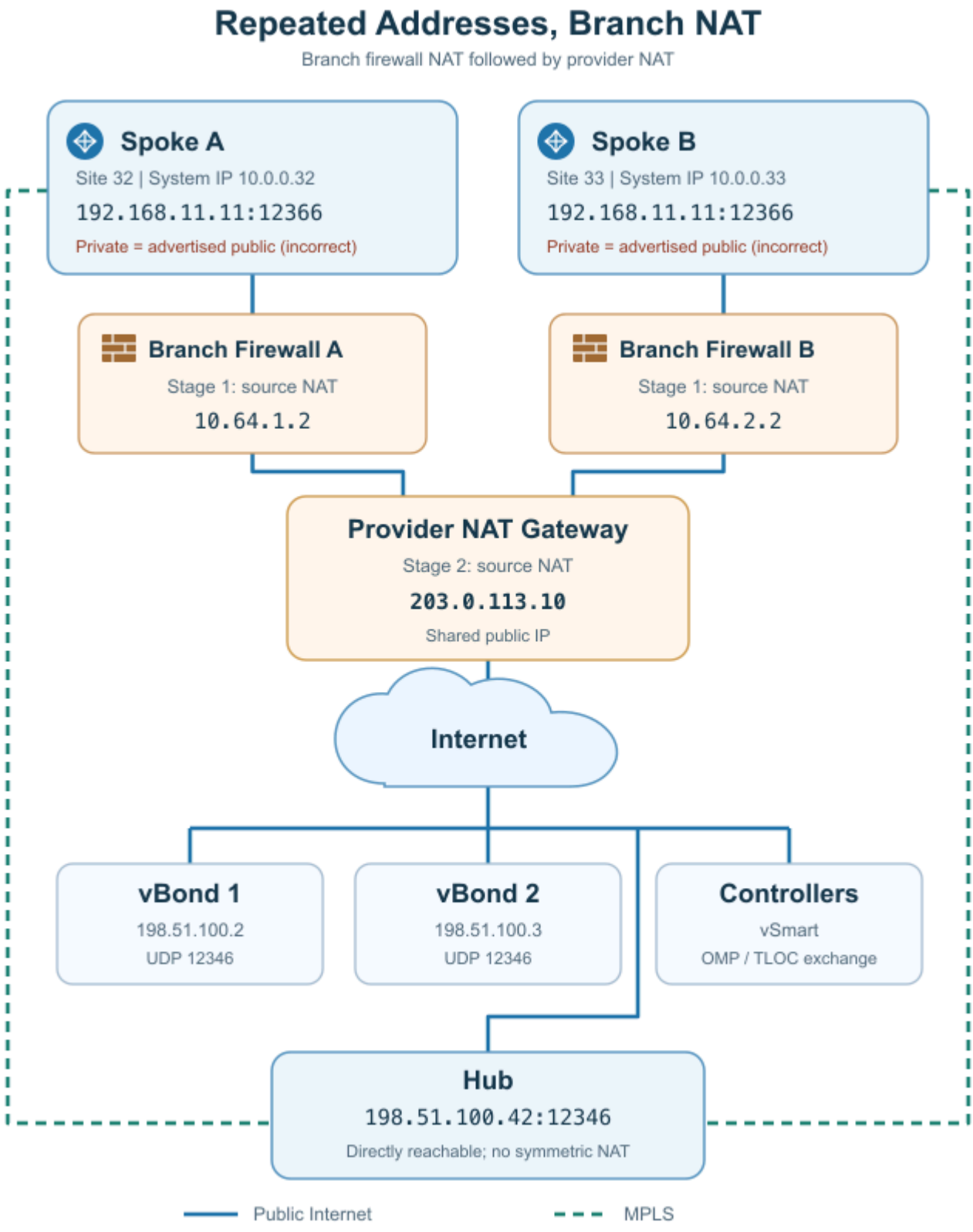

Figura 2. Firewall de sucursal y traducciones de NAT de proveedor. Los atributos TLOC públicos incorrectos conservan el terminal privado original, mientras que los paquetes utilizan las direcciones de origen traducidas.

Si ambos radios encuentran el defecto en sus TLOC de Internet pública y utilizan el mismo puerto de origen post-salto, el hub puede recibir estos anuncios:

Entidad par	Terminal privado después de salto de puerto	Terminal TLOC público incorrecto
R	192.168.11.11:12366	192.168.11.11:12366
B	192.168.11.11:12366	192.168.11.11:12366

Nota: Las direcciones privadas repetidas y la NAT doble no son requisitos previos para el ID de bug Cisco CSCwx12986 en sí. La colisión entre pares adicional requiere que coincidan los valores de IP:port anunciados y la misma dirección local del hub, puerto y protocolo. La misma IP privada con diferentes puertos anunciados no establece esta colisión.

La igualdad de direcciones públicas y privadas es normal en un transporte sin NAT. Una dirección RFC 1918 en un campo público es sospechosa solamente cuando contradice la trayectoria deseada y la traducción observada. Las direcciones privadas de sucursal únicas evitan el solapamiento repetido-privado-tupla en este ejemplo; no impiden el escenario de reutilización de puertos públicos traducidos descrito anteriormente.

Reasignación de extremo NAT

Un terminal también se puede reasignar a otro spoke después de que venza una asignación NAT mientras el hub aún conserva el estado de peer anterior. Compare el historial de asignaciones con el ciclo de vida de la sesión del hub para identificar el solapamiento entre los propietarios antiguos y los nuevos.

Síntomas e impacto

Los indicadores típicos incluyen:

- Las conexiones de control permanecen activas mientras las trayectorias BFD afectadas están inactivas o no se recuperan.
- Dos IP de sistema diferentes anuncian la misma IP:puerto pública.
- El hub conserva ambas TLOC lógicas, pero a una vista de sesión de plataforma filtrada le falta un par o muestra información incoherente de la IP del sistema, color remoto, discriminador, túnel o SA.
- Una retirada o recreación de transporte para un par perturba a otro par con el mismo punto final.
- Las caídas de entrada de IPSec pueden aumentar en la trayectoria afectada.

La falla puede hacer que la trayectoria de transporte afectada sea inutilizable. Si ésta es la única trayectoria de transporte utilizable para un spoke, el spoke se aísla de la superposición. En un

hub grande, muchos spokes que comparten una dirección NAT aumentan la población que requiere correlación, pero se debe medir el número de trayectos afectados; no puede deducirse del número de sitios detrás de esa dirección.

Diagnosticar el problema

Paso 1. Registro del estado de transporte de software y radio

En cada Cisco IOS XE Edge afectado, reemplace **<**impact-color**>** por el color de transporte real, por ejemplo biz-internet o 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

Registre la dirección privada/pública y el puerto, la interfaz, el color, el tipo de NAT, la ID de sitio y el estado de control. Después del primer ejemplo completo de propiedades locales, utilice este filtro compacto para conservar los encabezados de la interfaz y la fila de transporte elegida. Reemplace TenGigabitEthernet0/1/0.10 con la interfaz afectada:

<#root>

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

Para el escenario principal, los campos relevantes se pueden leer en ambos radios. Este es un resumen de campo, no el diseño de columna nativo:

```
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
```

Una conexión de control Up verifica esa relación de controlador. No verifica una trayectoria BFD de spoke a hub ni la exclusividad del punto final público.

Paso 2. Buscar terminales duplicados en OMP

En el hub Cisco IOS XE:

<#root>

show clock detail

show sdwan omp tlocs table | include 203.0.113.10

En el controlador SD-WAN (vSmart):

<#root>

show clock

show omp tlocs | tab | include 203.0.113.10

Este resultado de Controller utiliza identificadores normalizados. Se omiten las columnas IPv6 y de región:

<#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
```

Compare la IP del sistema TLOC, el color, la encapsulación, la IP pública y el puerto público. Es normal que existan varias trayectorias al mismo TLOC lógico desde diferentes controladores. El candidato de colisión son dos identidades de peer diferentes con el mismo terminal efectivo.

Repita el comando filtrado después de 30-60 segundos y conserve ambas marcas de tiempo. La superposición persistente es una prueba útil; no se requieren comandos perfectamente simultáneos. Para un período transitorio breve, recopile los eventos OMP y los registros del ciclo de vida de la sesión correspondientes con el TAC.

Para dos peers sospechosos, conserve sus entradas individuales de la tabla TLOC:

<#root>

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

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

Para obtener una vista compacta de los detalles de TLOC de IPv4 en Cisco IOS XE, utilice este filtro. Reemplace la IP del sistema con el peer bajo investigación y mantenga las comillas alrededor del selector ip <system-IP>:

<#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|::
```

Compare los atributos de puerto/dirección pública y privada para ambos pares. El filtro omite las líneas coincidentes no establecidas, de valor cero, predeterminadas e IPv6 de esta vista.

Paso 3. Comparación de TLOCs Lógicos con la Propiedad de la Sesión del Hub

Inspeccione el estado TLOC enviado a FTM. Compare las IP del sistema, los colores, las direcciones IP públicas y los puertos UDP públicos de ambos pares.

<#root>

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

Ejecute estos comandos para comparar los registros de sesión del Administrador de tablas de reenvío (FTM), BFD y la plataforma:

<#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
```

Este ejemplo muestra el patrón con identificadores normalizados. Los rótulos de columna se añaden a las filas FTM filtradas para mayor claridad; no forman parte del resultado del comando filtrado:

<#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 y FTM conservan ambas identidades de peer lógicas, mientras que esta búsqueda de sesión solo muestra el spoke A para el destino compartido. El radio A también tiene un estado FTM inactivo; la presencia en la tabla de sesión de plataforma no indica una ruta correcta. El índice FTM TLOC es distinto del discriminador local BFD (BFD-LD) en la tabla de sesión. Este patrón es una razón para investigar la propiedad en las capas. Una fila CLI que falta por sí sola no establece la pérdida de paquetes.

En esta tabla, Color representa el transporte local; utilice Color remoto en la vista detallada para identificar el TLOC remoto. Compare también DstIp y DPubIp: un destino real aprendido puede diferir del punto final público asociado a la sesión. Utilice la vista específica del par si un filtro solo de destino ya no coincide con la dirección aprendida.

Un Next Hop Inválido, un identificador SA de 0 o En HW: FALSE proporciona evidencia adicional en lugar de una firma única. Estos campos también pueden aparecer durante una configuración normal o un error subyacente.

Paso 4. Verifique lo que hace realmente la puerta de enlace NAT

Pida al operador de NAT o proveedor de servicios registros de traducción UDP concurrentes con estos campos:

```
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
```

Esta es una tabla de traducción ilustrativa. Utilice el comando de diagnóstico equivalente para su plataforma NAT. En un gateway NAT de Cisco IOS XE, comience por:

<#root>

show ip nat translations | include 203.0.113.10

Conservar las columnas de origen y destino internas. Una lista que contenga sólo el origen

traducido no puede mostrar por qué la reutilización es válida para diferentes vBonds o qué spoke posee la asignación de hub.

Capture los flujos UDP afectados antes y después de NAT para vBonds y el hub. Preserve las longitudes completas de los paquetes para que la cola VCONTROL no se trunca. Utilice una recopilación de analizador de puerto conmutado (SPAN) o captura de paquetes integrados (EPC) limitada y acordada con el TAC. Comparar el mismo flujo entre los puntos de captura; no inferir latencia de relojes de captura no sincronizados.

Paso 5. Inspeccione VCONTROL en Wireshark

Utilice el decodificador Lua del apéndice para el formato BFD/VCONTROL IPv4 que se describe a continuación. Guarde el código como sdwan_vctrl.lua en la misma carpeta que la captura. Este descodificador de diagnóstico muestra campos visibles; no descifra ESP ni verifica la autenticación. Su alcance es completo, paquetes IPv4/UDP no anidados con el indicador BFD/VCONTROL y la estructura de cola esperados.

Ejecute el comando Wireshark desde la carpeta que contiene el decodificador y su captura:

<#root>

```
wireshark -n \

  -X lua_script:sdwan_vctrl.lua \

  -d udp.port==12346,sdwan_vctrl \

  -d udp.port==45678,sdwan_vctrl \

  -r hub.pcap
```

Reemplace los puertos de ejemplo por los de la captura. En Windows o macOS, utilice la ruta completa al ejecutable de Wireshark si no está en PATH.

Como alternativa, cargue el script Lua en el inicio de Wireshark, elija un paquete UDP relevante y navegue hasta Analizar > Decodificar como. Asigne las entradas de puerto UDP de origen y destino aplicables a SDWAN_VCTRL / SD-WAN VCTRL (IPv4). Una entrada UDPENCAP explícita en el otro puerto puede tener prioridad sobre este decodificador. Aplicar el cambio a esta sesión de análisis.

Aplicar este filtro de visualización:

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

Expanda SD-WAN VCTRL > Visible VCONTROL trailer y compare:

```
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
```

Estos valores ilustrativos describen el establecimiento inicial del túnel antes de que finalice el aprendizaje del plano de datos. Muestran el mapeo del hub real para B junto con su punto final transportado. NAT modifica los encabezados externos; no reescribe la información de punto final dentro de esta cola. Esta discordancia por sí sola no demuestra una falla.

Ejecute el comando TShark para una exportación compacta:

<#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
```

Sin un descodificador personalizado, el formato IPv4 descrito aquí tiene esta cola de tipo-longitud-valor (TLV) de 17 bytes al final de la carga útil UDP. El relleno de la capa de link está fuera de la carga útil de UDP:

```
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
```

No aplique este diseño fijo a IPv6, otros formatos de control, paquetes truncados o datos cifrados arbitrarios. Un filtro decodificador vacío puede significar que el paquete está fuera de su formato soportado. Un punto final de origen legible tampoco es una etiqueta IP del sistema autenticada.

Nota: Las advertencias genéricas de la secuencia ESP en Wireshark no son diagnósticos anti-reproducción del router. Correlacione el paquete con los registros y contadores del router antes de sacar una conclusión de autenticación o propiedad.

Paso 6. Confirmar el trayecto afectado y conservar la evidencia

En el concentrador, tome dos muestras de contador del procesador QuantumFlow (QFP) alrededor del error observado:

<#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

Utilice las diferencias de los contadores en lugar de los totales absolutos. Las caídas de IPSec agregadas pueden tener otras causas. Confirme la llegada del paquete en el transporte afectado

y relaciónelo con el par, el punto final, el discriminador BFD, el túnel, la SA y la hora del evento.

Proporcione al TAC las dos instantáneas de OMP, las propiedades y los controles locales de spoke, los detalles de sesión de hub para ambos peers, el estado de BFD, los registros de traducción, las capturas delimitadas y las versiones de software. Si ya está disponible, incluya los técnicos de administración relevantes y el historial de conexiones/retiradas. Evite la recopilación repetida de tablas enteras en un concentrador grande.

Pruebe la disponibilidad del servicio por separado y registre el transporte real elegido. Una indicación de BFD Up de segundo cero no es una recuperación sostenida.

Soluciones y limitaciones

Evalúe estas opciones de mitigación con Cisco TAC y el operador NAT. La limitación se refiere a los terminales anunciados duplicados que llegan a un hub común; no significa que la NAT simétrica, las direcciones públicas compartidas o las direcciones privadas repetidas no sean compatibles en general. Los procedimientos de recuperación y la eficacia de la mitigación dependen del despliegue.

Utilizar asignaciones independientes de terminales estables con asignaciones únicas

Una opción de prevención del lado de NAT para la secuencia ilustrada es proporcionar a cada punto final de transporte de radio distinto un punto final UDP traducido único y estable a través de vBond, el controlador y los destinos de concentrador. Solicite independencia de terminal y unicidad entre radios. Verifique el resultado en las capturas y los registros de traducción, también después de la recuperación de estado o la recuperación de la recuperación de estado o la conmutación por error del gateway NAT.

Por ejemplo, A puede utilizar consistentemente 203.0.113.10:40001, mientras que B utiliza consistentemente 203.0.113.10:40002. Las traducciones estáticas o una política de asignación adecuada pueden proporcionar este comportamiento, sujeto a la plataforma NAT y al diseño de acceso.

La asignación independiente del terminal no requiere acceso entrante sin restricciones. Mantenga los controles de firewall necesarios. Una corrección de política NAT no elimina automáticamente el estado de sesión previamente anunciado o programado; coordine un nuevo ciclo de detección y recuperación con el TAC.

Deshabilitar la superposición de puertos entre diferentes radios

Siempre que sea compatible, reserve los terminales UDP traducidos de forma exclusiva a través de los radios SD-WAN relevantes. No los reutilice únicamente porque sus destinos sean diferentes. Esto elimina directamente la asignación de vBond duplicado simultáneo que se muestra anteriormente, incluso si el gateway NAT conserva algún comportamiento dependiente del destino.

La configuración puede consumir más puertos o requerir direcciones públicas adicionales. Por sí solo, no hace que la asignación para cada punto final de radio sea independiente, y no resuelve el estado del receptor obsoleto después de una reasignación de punto final posterior.

Con varias etapas NAT o gateways NAT redundantes, verifique la asignación visible en el límite final de Internet. La unicidad dentro de una instancia de NAT no establece la unicidad entre otras instancias que comparten la misma dirección pública.

Uso del desplazamiento de puertos para un grupo pequeño y controlado

El comando port-offset proporciona los valores del 0 al 19. Por ejemplo, el Spoke A puede conservar el desplazamiento 0, y el Spoke B puede utilizar el desplazamiento 1. Ejecute estos comandos de configuración en el 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
```

Verifique el origen activo y los puertos traducidos después del cambio. Un cambio en esta configuración del sistema puede reconstruir las conexiones de datos y control a través de los transportes. No es un paso de diagnóstico no disruptivo.

Los 20 desplazamientos proporcionan 20 grupos de puertos base distintos con desplazamiento 0 como opción. No son un límite general de 20 routers SD-WAN detrás de una IP pública. Esta solución alternativa en particular proporciona solamente 20 opciones de desplazamiento únicas y requiere que el gateway NAT las conserve y las distinga entre ellas. Falla como esquema de unicidad cuando se reutilizan los desvíos. El salto de puertos no agrega más identidades de desplazamiento.

Por ejemplo, 124 routers no pueden recibir todos los desplazamientos únicos detrás de una dirección compartida. Un esquema de solo desplazamiento con un máximo de 20 routers por grupo de direcciones públicas requiere al menos siete grupos. Esta aritmética no es una recomendación de capacidad ni un sustituto de la verificación del comportamiento de NAT. Un gateway NAT que reescribe o superpone puertos traducidos puede frustrar el esquema incluso con menos routers.

Desactivar conservación de puerto de origen o activar asignación aleatoria

Una política sin preferencia de conservación puede reducir la tendencia de muchos spokes a recibir :12346 hacia diferentes vBonds. La asignación aleatoria puede distribuir esos mapeos en un agrupamiento de puertos más grande.

Sin embargo, ninguno de los cambios garantiza por sí solo la prevención de colisiones. Un asignador aleatorio todavía puede reutilizar un puerto entre destinos, cambiar una asignación hacia el hub o reasignar un punto final caducado mientras el estado del hub antiguo permanece. Verifique si la asignación es única entre los suscriptores y los destinos. Los puertos aleatorios por sí solos no establecen exclusividad.

Revise la configuración de la preservación y asignación del puerto de origen en el gateway NAT con su operador. La configuración aplicable depende de la plataforma NAT; verifique las asignaciones resultantes hacia vBonds y el hub con registros de traducción y capturas de paquetes.

Los puertos traducidos pueden quedar fuera del intervalo de puertos base de la SD-WAN original. Revise las reglas del firewall para que no rechacen el tráfico traducido legítimo únicamente porque el puerto de origen ha cambiado.

Direcciones públicas separadas o bloques de puertos de reserva

Las direcciones traducidas dedicadas, o los bloques de puerto no solapados reservados por radio, pueden proporcionar puntos finales anunciados distintos para diferentes radios activas. La política debe aplicarse de forma uniforme en las rutas de descubrimiento y hub y en los nodos NAT redundantes. Es posible que se requiera espacio de dirección adicional y compatibilidad con

proveedores. La reutilización dinámica después de la retirada de la asignación todavía requiere una gestión correcta del ciclo de vida de la sesión del hub.

Conservación de un transporte alternativo y recuperación de coordenadas

Una MPLS verificada u otra ruta elegible puede conservar el servicio mientras se investiga la ruta de Internet afectada. Una lista de control de acceso (ACL) subyacente que bloquea la dirección NAT compartida proporciona contención únicamente: puede eliminar la redundancia de Internet para cada radio detrás de esa dirección y no retira automáticamente sus anuncios OMP.

Un comando control clear, interface reset, NAT-state clear o hub reload pueden recrear temporalmente el estado. Ninguna garantiza la prevención de la recurrencia. No realice borrados generales como primer paso de diagnóstico. Conservar las pruebas, corregir las condiciones de asignación cuando sea posible y acordar con el TAC la acción de recuperación más pequeña. Valide el tráfico sostenido BFD Up y bidireccional en la trayectoria recuperada.

Defectos de software relacionados

ID de falla de funcionamiento de Cisco	Ámbito de aplicación del presente artículo
CSCww45867	Documentación de la limitación de propiedad de sesión de hub cuando diferentes peers anuncian el mismo punto final TLOC público. Este registro realiza un seguimiento de la actualización de la documentación, en lugar de una corrección de software.
CSCwx12986	Una secuencia de aprendizaje automático de salto de puerto/NAT puede dejar una tupla privada en los campos de TLOC públicos. Si las sucursales reutilizan el mismo puerto IP:IP privado, los terminales públicos incorrectos pueden coincidir entre pares. La corrección de este defecto de productor no impide la reutilización válida de puertos públicos traducidos.
CSCwx48929	La clasificación NAT puede convertirse incorrectamente en E cuando la detección vuelve al mismo vBond. Una clasificación correcta no impide el escenario válido de reutilización de puertos de vBond diferentes.

Las correcciones para el ID de bug de Cisco CSCwx12986 y el ID de bug de Cisco CSCwx48929 no garantizan los terminales públicos anunciados únicos y, por sí solos, no eliminan este escenario de colisión. El cierre del registro de documentación del ID de bug Cisco CSCww45867 no establece un cambio en el comportamiento del software. Confirme las limitaciones y

mitigaciones aplicables con Cisco TAC.

Apéndice: Decodificación de la cola IPv4 VCONTROL

Guarde este código como sdwan_vctrl.lua. El descodificador de diagnóstico no autentica paquetes ni descifra sus cargas útiles. Utiliza el filtro de visualización sdwan_vctrl y registra una opción Decode As explícita. La captura de paquetes permanece sin cambios.

```
-- 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)
```

Información Relacionada

- RFC 7857, sección 3: Comportamiento de superposición de puertos
- RFC 4787: Requisitos de comportamiento de NAT para UDP unidifusión
- RFC 5737: Bloques de direcciones IPv4 reservados para la documentación
- Guía de diseño de SD-WAN de Cisco Catalyst
- Comandos del sistema Cisco IOS XE Catalyst SD-WAN: desplazamiento de puerto
- Configuración de la desviación de puertos SD-WAN de Cisco
- Referencia de la línea de comandos de Wireshark
- Referencia de la línea de comandos de TShark
- Soporte Técnico y Documentación - Cisco Systems

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).