SD-WAN تاهجوم قافنأ ءاطخأ فاشكتسأ NAT ةيانهلا طاقن مادختساب اهحالصإو ةرركملا

تايوتحملا

ةمدقملا

ةيساسألا تابلطتملا

تابلطتملا

ةمدختسملا تانوكملا

ةيساسأ تامولعم

مكحتلا ىوتسمل nat ميلعت

مكحتلاو NAT تانايبلا ىوتسم ميلعت

ذفنملا ةيئاوشعو، ذفنملا لخادت، ذفنملا ظفح

ةنيعلا ايجولوبوط

مادصلا ريصيب شيل

ةماعلا ةيانهلا ةطقن سفن ةفلتخملا vBond ظحالت نأ نكمي

ةدحاو ةرص ىلا لصت تانالعالا سفن

ةرركتملا عورفلا نيوانع عم ةماعك ةصاخ تامداصت

NAT ةيانه ةطقن نييعت ةداعا

ريثأتلاو ضارعألا

ةلكشملا صيخشت

جماربلا ربع لقنلا ةلاح لجيست .1 ةوطخلا

OMP يف ةرركم ةيانه طاقن نع ثحبلا .2 ةوطخلا

زكرملا لمع ةسلج ةيكلمو ةيقطنملا تالماعملا نيب نراق .3 ةوطخلا

لعفلاب NAT ةرابع هب موقت ام نم ققحت .4 ةوطخلا

Wireshark يف vControl صحف .5 ةوطخلا

ةلدألا ظفحو رثأتملا راسملا ديكأت .6 ةوطخلا

دويقلاو لولحلا

ةديرف صيصخت تايلمع عم ةيانهلا طاقن ىلع ةدمتعم ريغ ةتباث تانييعت مادختسا

ةفلتخملا عورفلا ربع ذفنملا لخادت ليطعت

ةطوبضم ةريغص ةعومجمل ذفنملا ةحازا مادختسا

يئاوشعلا عيزوتلا نيكمت وأ ردصملا ذفنمب ظافتحالا ليطعت

ذفنملا لتك زجح وأ ةلصفنملا ةماعلا نيوانعلا

دادرتسالا قيسنتو ةليدب لقن ةيلمعب ظافتحالا

ةلصلا تاذ جماربلا بويع

IPv4 vControl ةروطقملا ريفشت كف :قحلملا

ةلص تاذ تامولعم

المقدمة

يوضح هذا المستند كيفية تحديد حالات فشل نفق المحور والتخفيف من حدتها عندما تتشارك الخوادم نقطة نهاية واحدة لترجمة عنوان الشبكة (NAT).

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- بنية شبكة المنطقة الواسعة (SD-WAN) المعرفة من Cisco Catalyst واتصالات التحكم
- بروتوكول إدارة التضمين (OMP)، محددات موقع النقل (TLOCs)، اكتشاف إعادة التوجيه ثنائي الإتجاه (BFD)، أمان IP (IPsec)
- شبكات نقل تحويل التسمية متعدد البروتوكولات (MPLS)
- تعيين NAT وسلوك المرشح
- تحليل أساسي للحزم باستخدام Wireshark

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- موجهات Cisco IOS® XE Catalyst SD-WAN
- وحدة التحكم Cisco Catalyst SD-WAN (vSmart)
- أداة التحقق من الصحة Cisco Catalyst SD-WAN (vBond)

تم نسخ فشل مكيفة جلسة عمل الموزع على Cisco IOS XE 17.18.2 مع تشغيل Pairwise Keys. تختلف حقول توفر الأوامر والمخرجات حسب النظام الأساسي والإصدار.

تستخدم الأمثلة عناوين أو وثائق خاصة محجوزة بواسطة RFC 5737، مع أسماء أجهزة عامة. يتم إختصار مقتطفات CLI وتستخدم المعرفات العادية. تختلف أسماء الواجهة وبعض حقول الإخراج حسب النظام الأساسي والإصدار.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

⚠ تحذير: يمكن لتغييرات التكوين وعمليات إعادة ضبط الاتصال مقاطعة حركة المرور. إستخدام خطة صيانة معتمدة. أوامر التشخيص الأولية للقراءة فقط.

معلومات أساسية

أبدأ بسيناريو يتم فيه تعريف NAT المتماثل بشكل صحيح. تحدثت A بالسجلات مع vBond 1، والسجلات B ذات vBond 2. يمكن لبوابة NAT تعيين نفس عنوان IP المصدر والمنفذ إلى هذه الاتصالات عندما تختلف وجهات الاتصال، كما يسمح RFC 7857. المترجم وبالتالي، يمكن لكل الخادمين الإعلان عن نفس نقطة النهاية العامة لمحولاتهما العامة على الإنترنت، حتى عندما يقدم كل منهما تقريرا عن نوع NAT.

تستخدم عينة طوبولوجيا اللون العام للإنترنت. نفس السيناريو يمكن أن يتضمن ألوان عامة أخرى، مثل biz-internet. تطبيق عوامل التصفية التشخيصية على لون النقل الفعلي المتأثر؛ اللون الحرفي للإنترنت العام ليس شرطا مطلوبا.

✎ ملاحظة: الا يدعم Cisco Catalyst SD-WAN وحدات التحكم في الوصول (TLOC) من مواقع مختلفة التي تعلن عن نفس عنوان IP العام ومنفذ UDP نحو حافة إستقبال مشتركة. لا يمكن التنبؤ بسلوك المستلم في ظل حالة التصادم هذه. يمكن أن يحدث ذلك حتى عند تحديد NAT المتماثل بشكل صحيح. لا يضمن تصنيف NAT الصحيح وحده أن نقاط النهاية المعلن عنها فريدة.

تعليم nat لمستوى التحكم

يراقب vBond. يرسل Edge عنوان النقل الخاص والمنفذ الخاص به أثناء التسجيل مع vBond. يعيد vBond عنوان المصدر والمنفذ على ذلك الاتصال ويعيد نقطة النهاية المرفوعة إلى الحافة. يمكن أن يعلن الحافة هذه المعلومات من خلال OMP كعنوان عام وخصائص منفذ TLOC، بما في ذلك TLOC بلون عام مثل عام-الإنترنت أو biz-internet.

تصف الملاحظة الصلة بذلك vBond. مع غياية baser nat، التخطيط نحو صرة يستطيع كنت صنفت التشكيل سلوك. في show sdwan control local-properties، و E يعني تعيين معتمد على العنوان والمنفذ، و A يعني تعيين مستقل عن النقطة النهائية. يصف التصنيف المعروض قرار الموجه؛ NAT ترجمة طواقة أو ربط التقاط يتحقق السلوك الفعلي من ال nat مدخل.

على سبيل المثال، قم بتشغيل show sdwan control local-properties وحدد موقع عمود نوع NAT للنقل. يحتفظ هذا الإخراج المختصر بأسطوانة نوع NAT أو عمدة الواجهة المختارة، مع عناوين معيارية:

<#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
```

يبلغ نقل البيانات عبر الإنترنت (BIZ) عن نقطة النهاية العامة 203.0.113.10:23012 ويعلن عنها. ويبلغ نظام النقل المتعدد الأطراف (MPLS) (ه)، وهو يضم نقاط نهاية خاصة وعامة متساوية. قراءة التصنيف من نوع nat؛ ال يحدد تساوي العنوان أو المنفذ وحده نوع NAT. n يعني أن الموجه لم يتعلم تصنيفا.

تعليم مستوى البيانات NAT والتحكم

قبل أن يعالج صرة حزمة BFD مشفرة، يجب أن يجد وه الوارد IPsec أمن اقترانا (SA) للنظير والنفق المتوافق. تحدد SA المفتاح المشفر والحالة الأخرى المطلوبة لمصادقة الحزمة وفك تشفيرها. يستخدم المستقبل معلومات نقطة النهاية مع مؤشر معلمات أمان حمولة الأمان (ESP) لتضمين الحالة لتحديد موقع هذه الحالة. ال يعد SPI وحده معرفا متكلما فريدا بشكل عام.

عادة ما يقوم متحدث خلف NAT المتماثل بتهيئة حركة مرور البيانات نحو محور يمكن الوصول إليه. هذا يخلق تخطيط لذلك الهدف المحدد. يمكن أن يختلف عنوان المصدر أو المنفذ الذي يراه الصرة عن نقطة النهاية العامة التي تم التعرف عليها من قبل من خلال vBond والإعلان عنها في OMP. ونتيجة لذلك، ال تتطابق الرؤوس الخارجية المستلمة دائما مع نقطة النهاية في حالة النفق المثبت. يحتاج الصرة طريقة لإقران نقطة النهاية الجديدة على السلك مع TLOC البعيد المعروفة وحالة IPsec الخاصة به قبل أن يستطيع فك تشفير BFD.

بالنسبة لتنسيق IPv4 BFD-over-IPsec الذي تمت مناقشته هنا، يضع SD-WAN معلومات نقطة النهاية في مقطورة vControl مرئية في نهاية حمولة UDP، خارج حمولة BFD المشفرة. الصرة يستطيع قرأت هذا معلومة قبل فك تشفير. يحمل vControl معلومات نقطة النهاية، وليس مفاتيح التشفير، وال يقوم بإنشاء هوية النظير بنفسه.

على سبيل المثال، خلال الإنشاء الأولي للنفق، قبل اكتمال تعلم مستوى البيانات:

```
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
```

يحاول المستقبل أو البحث عن نقطة النهاية/SPI العادية الخاصة به. إذا لم يعثر هذا البحث على مطابقة، فإنه يستخدم VCONTROL كمصدر نقطة نهاية مؤقتة. في هذا المثال، يمكن أن تستخدم SA، توفر نقطة النهاية المحلية 203.0.113.10:12346، بالإضافة إلى سياق التوجيه و SPI، لتحديد الصورة المحمولة بشكل صحيح، على الرغم من أن SA تشير إلى عنوان IP الوجهة 203.0.113.10:45678.

يختار SPI الرئيسي القابل للتطبيق مفاتيح السياق المستخدمة لتوفير خدمة SA المختارة. ثم يقوم بتنفيذ مصادقة IPsec وفك تشفير هذا السياق. يتم تشفير حزمة BFD وتوفر حزمة BFD المصادقة والتشفير وتجاهل الحزمة إذا فشلت المصادقة أو التشفير.

لذلك، هناك فرق بين monitore ومحمل مصدر ميناء يستطيع كنت عادي مع متماثل nat. لكي تعمل حالة الاتصال وتعلم المفاتيح بشكل صحيح، يجب على الصورة إرفاق الحزمة بالنفق الصحيح، حتى عندما تكون حركة المرور بإسالة الخروج للمحول في هذا المثال، يسمح التعلم الناجح بإرجاع حركة المرور إلى نقطة النهاية الفعلية. وهذا منفصل من تعليم مستوى التحكم من خلال البيانات العائدة إلى 203.0.113.10:45678. vBond.

في حالة وجود SPI مطابقة/نقطة نهاية المستقبل تجاوز نقطة النهاية المكررة بإنشاء نظير وهمي بإقران حزمة بإرسال غير صحيح، فإن المقطورة تتضمن الاستيراد. فهي تقدم تلميحا للبحث؛ ولا يمكنه التمييز بين نظامين يحملان نفس نقطة النهاية دون وجود النفق المحيط بحالة التشفير الصحيحة.

كما توفر vControl على حزم BFD القابلة للتطبيق عند الإبلاغ عن نوع NAT E. يعد وجوده علامة تناظرية-NAT، ولا يتم تضمينه في كل حزمة بيانات IPsec عادية. بالنسبة لتنسيق IPv4 BFD الموضح هنا، يتم حذف معلومات TLOC العامة بين لونين خاصين.

تعني نقطة النهاية الخاصة بالنظير التي تم التعرف عليها من خلال مستوى البيانات أن نقطة النهاية الخاصة بها بنقطة OMP الخاص بها إعلان OMP أو إعلان البوابة الطرفية التي تم التحدث بها إلى نقطة النهاية الجديدة لكل وجهة. تعد التعيينات المتعلمة المختلفة جزءا متوقعا من إجراءات تماثل-nat.

وبمجرد تشغيل نفق، يمكن للمرسل الذي تعلم نقطة النهاية المترجمة الخاصة به ذلك، ولكل نقطة النهاية العامة التي تحمل نقطة النهاية تلك كمعلومات مصدرها. هذه هي نقطة النهاية العامة لكل نفق الخاصة بالمرسل، وليس نقطة النهاية البعيدة أو إعلان OMP العمومي الجديد. قارن الحزمة، إعلان OMP، وحالة الجلسة دائما من نفس فترة المراقبة.

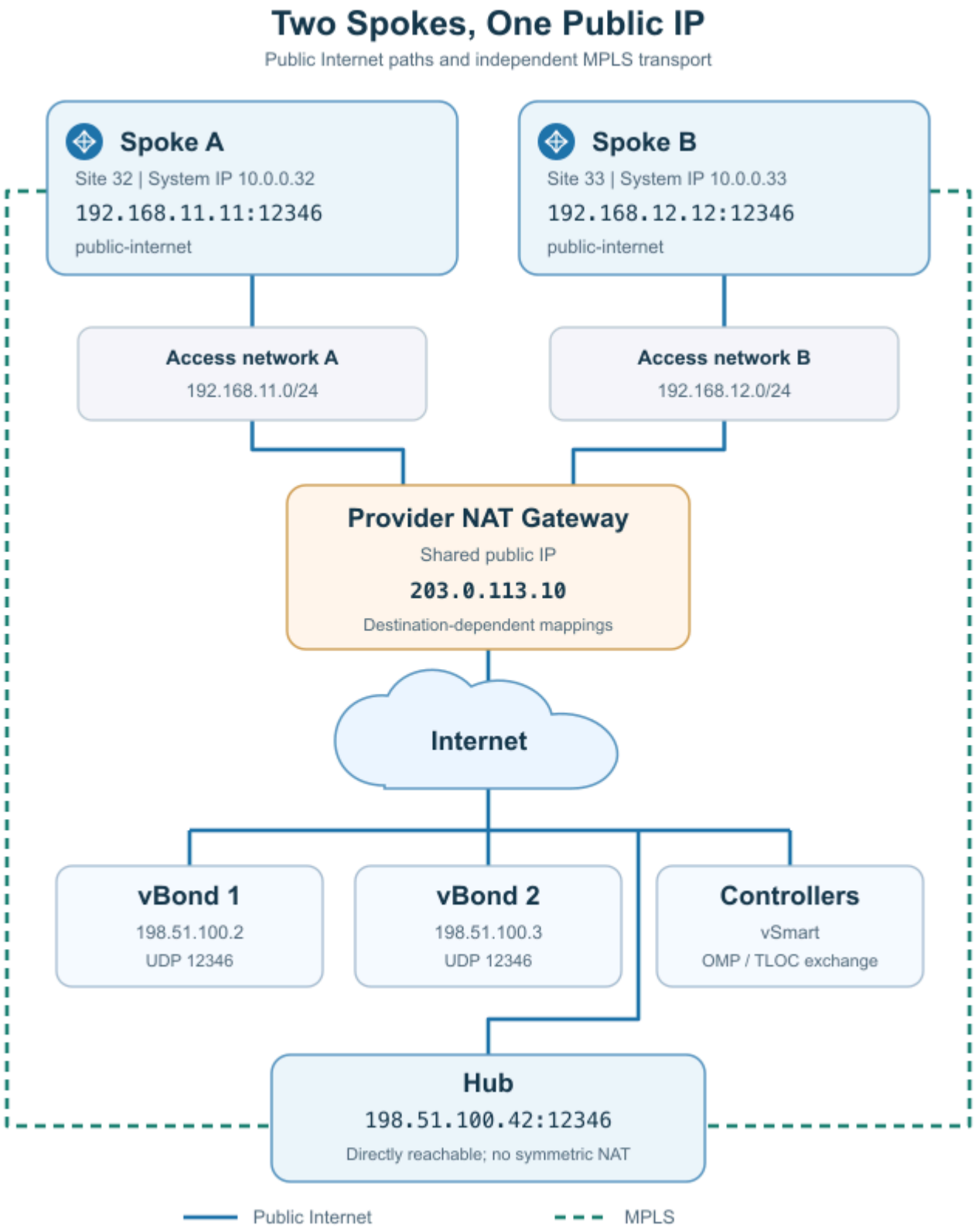
حفظ المنفذ، تداخل المنفذ، وعشوائية المنفذ

هذه هي السلوكيات المختلفة:

سلوك	المعنى
الحفاظ على المنفذ-المصدر	ال nat يحاول مدخل أن يحتفظ ال UDP أصلي مصدر ميناء من ال ميناء. يتحدث، مثلا، 12346، بما أن المصدر يترجم
تداخل المنفذ عبر الوجهات	ال nat يعيد مدخل واحد يترجم IP: منفذ لنقاط النهاية الداخلية المختلفة التي تتصل بوجهات خارجية مختلفة.
عشوائية المنفذ	ال nat يختار مدخل ميناء يترجم يستعمل طريقة توزيع عشوائي.
تعيين مستقل عن النقطة النهائية	تحتفظ نقطة نهاية داخلية بنفس نقطة النهاية المترجمة عبر الوجهات الخارجية أثناء وجود هذا التعيين.

RFC 7857، يسمح القسم 3 تداخل المنافذ الخارجية لنقاط النهاية الداخلية المختلفة عندما تختلف الوجهات. ويميز NAT بين التدفقات باستخدام خمسة رؤوس بيانات. لا يسمح هذا بتدفق UDP غير تمييزي متزامن إلى الوجهة نفسها. التوزيع العشوائي والحفظ هما خياران منفصلان للتخصيص؛ كما لا يؤسس إستقلال نقطة النهاية.

طوبولوجيا العينة



الشكل 1. بوابة NAT المشتركة وشبكات الوصول عبر الهاتف المنفصلة ونقل MPLS المستقل.

تحدث A باستخدام 192.168.11.11:12346، وتحدث B يستعمل 192.168.12.12:12346. يتشارك كلاهما العنوان العام 203.0.113.10 من خلال بوابة NAT. الصرة يتلقى عنوان يمكن الوصول إليه مباشرة ولا يكون وراء NAT متماثل. يمكن أن يعلن كل البابين عن نفس IP:port العام

.بالرغم من أختلاف نقاط نهايتهما الخاصة

ليش بيصير الصدام

يمكن أن تلاحظ vBond المختلفة نفس نقطة النهاية العامة

ضع في الاعتبار تعييناتUDP المتزامنة التالية:

نظير	مصدر خاص	مصدر مترجم	الوجهة
ج	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

ترجع الردود بشكل صحيح لأن NAT يتحقق أيضا من نقطة النهاية البعيدة. ينتمي الرد الوارد من vBond 1 إلى التعيين الخاص بـ A؛ ينتمي أحد الردود من vBond 2 إلى التعيين الخاص بـ.

كما يمكن لكل الموجهين الاتصال بـ vBond الآخر واكتشاف التخطيط المعتمد على الوجهة بشكل صحيح. على سبيل المثال، أبق مصدر الربط الخاص لكل واحد تحدث بدون تغيير واعتبر أمر الملاحظة هذا:

نظير	أول ملاحظة مقبولة عن طريق vBond	مقارنة من Other vBond	نتيجة
ج	مرتجعات vBond 1 203.0.113.10:12346	الدالة vBond 2 ترجع 203.0.113.10:40001	nat A؛ مجموعة البرامج العامة المحتفظ بها 203.0.113.10:12346
B	الدالة vBond 2 ترجع 203.0.113.10:12346	مرتجعات vBond 1 203.0.113.10:40002	nat A؛ مجموعة البرامج العامة المحتفظ بها 203.0.113.10:12346

على الرغم من ذلك، تتطابق ملاحظات vBond لكل موجه، لذلك اكتشاف nat A صحيح. تختلف الملاحظات الأولى التي تم الاحتفاظ بها عبر الموجهين. إن التصنيف (أ) الخاص بالمنفذ المصدر من هذه الملاحظات يضمن زيارة كل من الصندوقين هذا التفرد، والعمل عبر كل الفروع عاما فريدا.

يستلم كل خطاب العنوان العام والمرفأ الذي لاحظته شركة vBond في الرد على التسجيل. وتتضمن المعلومات التي يستخدمها الموجهون المحتفظ بها لتعميم خصائص النقل المحلية الخاصة بها. في سمات TLOC التي تعلن عنها الوحدة، إلى جانب نقطة النهاية الخاصة بها، تتضمن نقطة النهاية العامة البيانات التي يتم توزيعها بعد ذلك عبر OMP. وتوكول SD-WAN من خلال بروتوكول التحكم في شبكة الوحدة التي تعلن عنها؛ القوة المعمول بها لسياسة التحكم في الشبكة على الحواف الأخرى وقف وحدة التحكم في الشبكة

.OMP إعلان نفسه بإنشاء vBond

إذا احتفظ كل البابين بنفس نقطة النهاية العامة التي تم ملاحظتها، فيمكن لذلك أن يحتوي OMP على:

```
   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
```

تظل هذه المستويات مختلفة من حيث طرق TLOC المنطقية نظرا لاختلاف عناوين IP الخاصة بنظامها.

نفس الإعلانات تصل إلى صرة واحدة

الـ nat ينبغي ميزت مدخل كل فرع عندما هم يتصلون الـ نفسه صرة. أحد المخصصات المحتملة هو:

نظير	المصدر المترجم باتجاه الموزع	الوجهة
ج	203.0.113.10:12346	198.51.100.42:12346
B	203.0.113.10:45678	198.51.100.42:12346

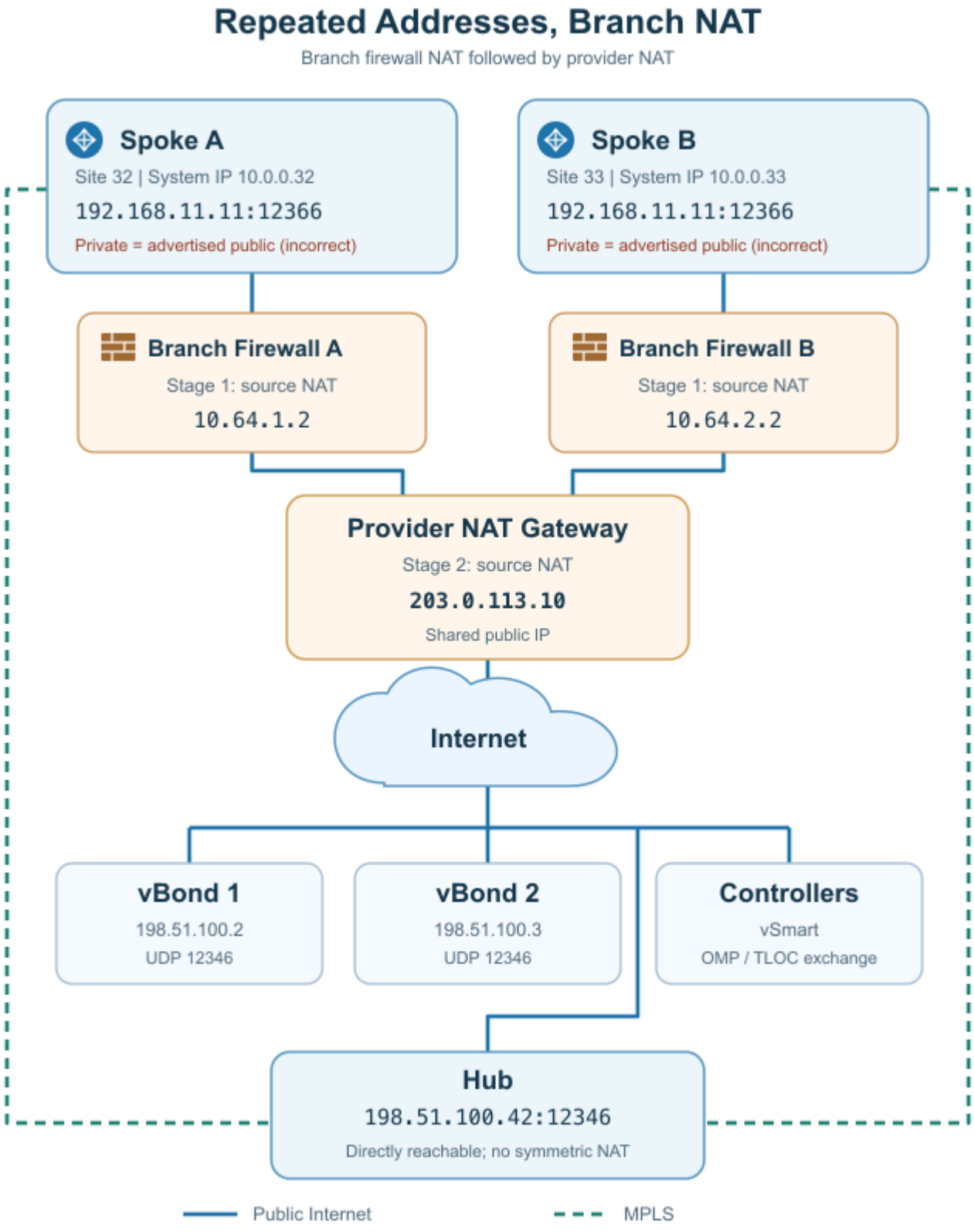
تحتوي الصرة على نظاريني منطقييني يعلنان نقطة نهاية الوجهة نفسها، بينما يمكن أن تصل الحزم من نقاط نهاية فعلية مختلفة. في العملية العادية المتماثلة-nat، يساعد تعلم مستوى البيانات على إنشاء تعييني الإرجاع.

يشأ تحديد ملكية جلسة عمل الصرة عندما يشارك أقران مختلفون حالة جلسة العمل التي تم إختيارها بواسطة مفتاح النقل هذا:

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

إذا قام كل الإعلانين باختيار نفس المفتاح، فيمكن لتحديث من نظير لاحق إستبدال معلومات الملكية في حالة المشاركة. يمكن أن يؤدي السحب أو الحذف أو الاستجمام اللاحق لجلسة عمل نظير واحد إلى اضطراب حالة IPsec/BFD للنظير الآخر. لا يضمن تعليم مستوى البيانات الاسترداد عندما تكون تلك الحالة مقترنة بالفعل بإنشاء النظير أو التدفق الخطأ.

نهاية نقطة تحمل نفس مستقل: كل البابين يمكن أن يحمل نفس نقطة نهاية ال تعد المجأ المرئي معرف نظير



شكل 2. ترجمات جدار الحماية الفرعي وموزع الخدمة nat. تحتفظ سمات TLOC العامة غير الصحيحة بنقطة النهاية الخاصة الأصلية، بينما تستخدم الحزم عناوين المصدر المترجمة.

إن واجه كل القديمين الخلل على مفتاحهم العام-الإنترنت يستعمل ال نفسه بعد-hop مصدر ميناء، الصرة يستطيع إستلمت هذا إعلان:

نظير	نقطة النهاية الخاصة بعد خطوة المنفذ	نقطة نهاية TLOC عامة غير صحيحة
ج	192.168.11.11:12366	192.168.11.11:12366
B	192.168.11.11:12366	192.168.11.11:12366

ملاحظة: لا تعد العناوين الخاصة المتكررة و NAT المزدوج متطلبات أساسية لمعرف التصحيح الأخطاء من Cisco CSCwx12986 نفسه. يتطلب التضارب الإضافي بين hub-local. لا يقوم IP الخاص نفسه مع المنافذ المعلن عنها المختلفة بإنشاء هذه التصادم.

المساواة في العناوين العامة والخاصة عادية في وسائل النقل بدون أن تكون. يعد عنوان RFC 1918 في حقل عام مثيرا للريبة فقط عندما يتعارض مع المسار المقصود والترجمة التي تمت ملاحظتها. تتجنب العناوين الخاصة للفرع الفريد تداخل المجموعات الخاصة المتكررة في هذا المثال؛ فهي لا تمنع سيناريو إعادة إستخدام المنفذ العام - المترجم - المنفصل الذي ورد وصفه سابقا.

إعادة تعيين نقطة نهاية NAT

كما يمكن إعادة تعيين نقطة نهاية إلى نقطة أخرى تم التحدث عنها بعد انتهاء صلاحية تعيين NAT بينما لا يزال الموزع يحتفظ بحالة نظير قديمة. قارن محفوظات التعيين بدورة حياة جلسة عمل الصرة لتحديد التداخل بين المالكين القدامى والجدد.

الأعراض والتأثير

تشمل المؤشرات النموذجية ما يلي:

- لا تزال إتصالات التحكم قيد التشغيل بينما مسارات BFD المتأثرة معطلة أو لا يمكن إستردادها.
- يعلن إثنان مختلف من عناوين IP الخاصة بالنظام عن نفس IP:Port العامة.
- يحتفظ الصرة بكل من TLOCs المنطقية، ولكن طريقة عرض جلسة عمل النظام مفقودة إلى نظير واحد أو تظهر معلومات IP غير متسقة للنظام أو لون بعيد أو مميز أو نفق أو SA.
- فالانسحاب من النقل أو الاستجمام لنظير ما يزعج نظير آخر له نفس نقطة النهاية.
- يمكن زيادة عمليات إسقاط إدخالات IPsec على المسار المتأثر.

يمكن أن يؤدي الفشل إلى جعل مسار النقل المتأثر غير قابل للاستخدام. إذا كان هذا هو مسار النقل الوحيد القابل للاستخدام للتكلم، فإن المحادثة تكون معزولة عن التغشية. في محور كبير، العديد من الفروع التي تتشارك عنوان NAT واحد تزيد السكان الذين

يحتاجون إلى الربط، لكن عدد المسارات المتأثرة يجب أن يتم قياسه؛ ولا يمكن إستدلال ذلك من عدد المواقع الموجودة خلف ذلك العنوان.

تشخيص المشكلة

الخطوة 1. تسجيل حالة النقل عبر البرامج

على كل حافة متأثرة من Cisco IOS XE، استبدل <الألوان المتأثرة>بلون النقل الحقيقي، على سبيل المثال biz-internet أو العامة-الإنترنت:

<#root>

```
show clock detail

show version | include Cisco IOS XE Software

show sdwan control local-properties

show sdwan control connections | include

show sdwan omp peers
```

قم بتسجيل العنوان الخاص/العام والمنفذ والواجهة واللون ونوع NAT ومعرف الموقع وحالة التحكم. بعد أول عينة خصائص محلية كاملة، أستخدم عامل التصفية المضغوط هذا للاحتفاظ برؤوس الواجهة وصف النقل المحدد. استبدل TenGigabitEthernet0/1/0.10 بالواجهة المتأثرة:

<#root>

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

للسيناريو الأساسي، يمكن أن تقرأ الحقول ذات الصلة على كلا البابين. هذا ملخص حقل، وليس تخطيط العمود الأصلي:

```
                    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
```

راسم نم قحتي ال وهو .هذه مكحتلا ةدحو ةقالع نم "ىلعأل" مكحتلا رصنع لاصتا قحتي BFD الخاص بالتحدث إلى مركز أو من تفرد نقطة النهاية العامة.

الخطوة 2. البحث عن نقاط نهاية مكررة في OMP

على لوحة وصل Cisco IOS XE:

<#root>

```
show clock detail
```

```
show sdwan omp tlocs table | include 203.0.113.10
```

على وحدة التحكم في SD-WAN (vSmart):

<#root>

```
show clock
```

```
show omp tlocs | tab | include 203.0.113.10
```

يستخدم إخراج وحدة التحكم هذه معرفات معيارية. تم حذف أعمدة IPv6 والمنطقة:

<#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
```

مقارنة IP لنظام TLOC، واللون، والتضمين، و IP العام، والمنفذ العام. المسارات المتعددة إلى نفس TLOC المنطقي من وحدات تحكم مختلفة هي عادية. مرشح التصادم هو هويتين نظيرتين مختلفتين بنفس نقطة النهاية الفعالة.

كرر الأمر الذي تمت تصفيته بعد 30-60 ثانية والاحتفاظ بكل من الطوابع الزمنية. والتداخل المستمر دليل مفيد؛ ال يلزم توفر أوامر متزامنة تمامًا. للحصول على فترة انتقالية قصيرة، قم بتجميع أحداث OMP وسجلات دورة حياة الجلسة المقابلة باستخدام TAC.

بالنسبة لاثنين من النظراء المشتبه بهم، احتفظ بإدخالات جدول TLOC الفردية الخاصة بهم:

<#root>

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

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

للحصول على عرض مضغوط لتفاصيل وحدة التحكم في الوصول إلى شبكة IPv4 على Cisco IOS XE، أستخدم عامل التصفية هذا. استبدلت النظام IP مع النظير قيد التحقيق واستبقيت علامات الاقتباس حول محدد <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|::
```

قارن خصائص العنوان/المنفذ العامة والخاصة لكل من الأقران. يتجاهل عامل التصفية بنود IPv6 غير المضبوطة، صفرية القيمة، الافتراضية، وغير المضبوطة من طريقة العرض هذه.

الخطوة 3. قارن بين المعاملات المنطقية وملكية جلسة عمل المركز

فحص حالة TLOC التي تم تسليمها إلى FTM. قارنت النظام IPs، الألوان، عناوين IP العامة، ومنافذ UDP العامة لكل من الأجهزة النظيرة.

<#root>

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

قم بتشغيل هذه الأوامر لمقارنة سجلات جلسات عمل مدير جدول إعادة التوجيه (FTM) و BFD:

<#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
```

يوضح هذا المثال النموذج باستخدام معرفات معيارية. تتم إضافة تسميات الأعمدة إلى صفوف FTM التي تمت تصفيتها من أجل الوضوح؛ ليسوا جزءا من إخراج الأمر الذي تمت تصفيته:

<#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
```

يحتفظ كل من OMP و FTM بكل من هويات النظير المنطقية، بينما يظهر البحث في جلسة العمل هذه Talk A فقط للوجهة المشتركة. للمحادثة A أيضا حالة أسفل FTM؛ ال يشير التواجد في جدول جلسة عمل النظام الأساسي إلى مسار سليم. يكون فهرس FTM مميزا من مميز BFD المحلي (BFD-LD) في جدول جلسة العمل. هذا النموذج هو سبب للتحقق من الملكية عبر الطبقات. ال يقوم صف واجهة سطر الأوامر (CLI) المفقود وحده بإنشاء فقدان الحزمة.

في هذا الجدول، يمثل اللون النقل المحلي؛ أستخدم اللون البعيد في طريقة العرض التفصيلية لتحديد TLOC البعيد. قارن DstIP وDPubIP أيضا: يمكن أن تختلف الوجهة الفعلية التي تم التعرف عليها عن نقطة النهاية العامة المقترنة بجلسة العمل. أستخدم طريقة العرض الخاصة بالنظير إذا لم يعد عامل تصفية الوجهة فقط يطابق العنوان الذي تم التعرف عليه.

الخطوة التالية غير صالحة أو معرف SA ل 0 أو في HW: يوفر الخطأ دليلا إضافيا بدلا من توقيع فريد. يمكن أن تحدث هذه الحقول أيضا أثناء الإعداد العادي أو فشل التمهيد.

الخطوة 4. تحقق من ما تقوم به عبارة NAT بالفعل

اطلب من عامل التشغيل NAT أو موفر الخدمة سجلات ترجمة UDP المتزامنة مع هذه الحقول:

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

هذا هو توضيحي جدول الترجمة. أستخدم الأمر التشخيصي المكافئ لنظام NAT الأساسي الخاص بك. على بوابة Cisco IOS XE NAT، ابدأ ب:

<#root>

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

الاحتفاظ بكل من الأعمدة الداخلية للمصدر والوجهة. ال يمكن للقائمة التي تحتوي على المصدر المترجم فقط إظهار سبب صلاحية إعادة الاستخدام ل vBonds مختلف أو الذي يتحدث

.روحملا نييعت يملك

لاوطأب ظافتحالا .لوحملاو vBonds نم لكل NAT دعبو لبق ةرثأتملا UDP تاقفدتلا طاقتلا
لوحملا ذفنم للحم ةعومجم مدختسأ .vControl ةروطقم عطقم يتح ال ةملكاكلا ةمزحلا
.TAC عم اهيلع قفتملا (EPC) ةنمضملا ةمزحلا طاقتلا ةعومجم وأ (SPAN) لوحملا لولحملا
طاقتلالا تاعاس نم لوصولا نمز ىلع لدتست ال ؛طاقتلالا نقاط عبر قفدتلا سفن نارق
.ةنمازتملا ريغ

Wireshark يف vControl صحف .5 ةوطخلا

حضوملا IPv4 BFD/VCONTROL قيسنتب صاخلا لحملا يف LUA زيمرتلا فلم مادختسأ
ةزهاج ضرعي .كلذب صاخلا طاقتلالا لثمل دلجملا سفن يف sdwan_vctrl.lua مسا
.هنا .اجفظ الرمز ك
نم ققحتلا وأ ESP ريفشت بفك موقي الو ؛ةيئرملا لوحلا صيخشتلا زيمرتلا
لكيهو BFD/VCONTROL ةمزح عم IPv4/UDP مزح لخادتم ريغ ،لماك هقاطن .ةقداصملا
.ةروطقملا

طاقتلالا ةيلمعو زيمرتلا فلم يوتحي يذلا دلجملا نم Wireshark رمأ ليغشتب مق
:ةصاخلا بكلا

<#root>

```
wireshark -n \

-X lua_script:sdwan_vctrl.lua \

-d udp.port==12346,sdwan_vctrl \

-d udp.port==45678,sdwan_vctrl \

-r hub.pcap
```

.طاقتلالا يف نوكي نأ عم ءانيم لاثملا تلدبتسا .Windows وأ MacOS، مدختسأ ،راسملا
.راسملا يف نكي مل اذإ Wireshark يذفنتلا فلملا ىلإ لماكلا

UDP ةمزح رتخاو، Wireshark ليغشت ءدبع دنع LUA صن ليغشت جمانرب ليحتب مق ،كلذ نم دبلا
ةلص تاذ، وتصفح ليلحتل < فلم زيمرتلا .كلذ مق بتخصيإ تاملاخدإ UDP ردصملل
.SDWAN_VCTRL / SD-WAN VCTRL (IPv4) ىلإ ةلباقلا ةهجولاو .يمكن أن يعطي
.اذه زيمرتلا فلم كلذ ىلع ةيولوألا ىلع جمانرب ةحيرص UDPENCAP لخدإ
.هذه ليلحتلا ةسلج عم ريغيتلا ىلع

تطبيق عامل تصفية العرض هذا:

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

قم بتوسيع SD-WAN VCTRL > مقطورة vControl المرئية وقارن:

```
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
```

تصف هذه القيم التوضيحية إنشاء النفق الأولي قبل اكتمال تعلم مستوى البيانات. إنها تظهر تخطيط المحور الفعلي ل B بجانب نقطة النهاية المحملة. يعدل NAT الرؤوس الخارجية؛ إنه ال يعيد كتابة معلومات نقطة النهاية داخل هذه المقطورة. ال يظهر عدم التطابق هذا وحده خطأ.

تشغيل الأمر tsHark لتصدير مضغوط:

<#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
```

تات ةروطقوم ةذه انه ىلع هحضوم IPv4 قيسنت يتحوي ،صخلملا زيمرتلا ةادأ كف نودب ةمولح .UDP ةمولح نم ةياهن في باي ت 17 تات (TLV) ليوطلا ةمقلا خارج طابترالا ةقبطم ةحاسم :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
```

ال تقو بتطبيق هذا التخطيط الثابت على IPv6 وأ تنسيقات التحكم الأخرى وأ الحزم زيمرتلا ةادأ فك نيكمت .ةيئاوشعلا ةرشفملا تانايبلا وأ ةعوطقملا .ةدمتعملا اهتقيسنت جراخ ةمزحلا نأ غارفلا .كلذ عم نأ ةهجولا ةقطنم ةيامنلا ردصملا ةقباطملل ةعارقلل .IP ةمظنلل ةمصاخلا تاقيبطتلا ليست



ةظحلام: ال تعد تاذيرحت تاسلسل ESP ةلاعفلا في Wireshark تاصخشت مقاوم ةداعإل جاتنتسا تاقوم باسح نأ لبق تالسلسلاو تاهجوملا تادادعإ ةمزحلا طبر .أ .ةيكلملا وأ ةقداصملا

6. ةوطخلا تأكيد المسار المتأثر وحفظ الأدلة

في لوحة الوصل، خذ عينتين من عداد معالج QuantumFlow (QFP) حول الفشل الذي تم ةظحلام:

<#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

أستخدم إختلافات العداد بدلا من الإجماليات المطلقة. يمكن أن يكون إجمالي عمليات

إسقاط IPsec أسباب أخرى. قم بتأكيد وصول الحزمة إلى النقل المتأثر وربطها بالنقطة الطرفية النظير والنقطة الطرفية ومميز BFD والنفق و SA ووقت الحدث.

تزويد TAC بلقطات OMP، الخصائص وعناصر التحكم المحلية التي تم التحدث بها، تفاصيل جلسة عمل المحور لكل من الأقران، حالة BFD، سجلات الترجمة، عمليات الالتقاط المحدودة، وإصدارات البرامج. إذا كان متوفرا بالفعل، فقم بتضمين admin-techs ذات الصلة ومحفوظات الاتصال/السحب. تجنب التجميع المتكرر للجداول بأكملها في لوحة وصل كبيرة.

إختبار إمكانية الوصول إلى الخدمة بشكل منفصل وتسجيل النقل الفعلي المختار. إن الإشارة إلى إرتفاع سعر الفائدة عند مستوى الحد الأدنى (BFD) في الثانية إلى الصفر ليست التعافي المستدام.

الحلول والقيود

قم بتقييم خيارات التخفيف هذه باستخدام Cisco TAC ومشغل NAT. وتتعلق هذه القيود بتكرار نقاط النهاية المعلن عنها التي تصل إلى مركز مشترك؛ ال يعني ذلك أن Symmetric NAT، أو العناوين العامة المشتركة، أو العناوين الخاصة المتكررة غير مدعومة بشكل عام. وتتوقف إجراءات الاسترداد وفعالية التخفيف على النشر.

إستخدام تعيينات ثابتة غير معتمدة على نقاط النهاية مع عمليات تخصيص فريدة

أحد خيارات الحماية من جانب NAT للتسلسل الموضح هو إعطاء كل نقطة نهاية نقل محكية مميزة نقطة نهاية UDP مستقرة وفريدة ومترجمة عبر vBond، ووحدة التحكم، ووجهات الموزع. طلب كل من إستقلالية نقطة النهاية والتفرد عبر الفروع. دققت النتيجة في ترجمة سجل ولقطات، أيضا بعد NAT مدخل التغلب على الأعطال أو حالة الترفيه.

على سبيل المثال، يمكن أن يستخدم A بشكل ثابت 203.0.113.10:40001، بينما يستخدم B بشكل ثابت 203.0.113.10:4002. يمكن أن توفر الترجمات الثابتة أو سياسة التخصيص المناسبة هذا السلوك، خاضعا لمنصة NAT وتصميم الوصول.

ال يتطلب التعيين المستقل عن نقطة النهاية الوصول الوارد غير المقيد. الاحتفاظ بعناصر تحكم جدار الحماية المطلوبة. ال يقوم تصحيح نهج NAT تلقائيا بإزالة حالة جلسة العمل المعلن عنها أو المبرمجة مسبقا؛ تنسيق دورة اكتشاف جديدة واسترداد باستخدام TAC.

تعطيل تداخل المنفذ عبر الفروع المختلفة

SD-WAN تاطباس ربع فيد لكشب ةمجرتملا UDP ةيانمن طاقن ظفحا ،امدعوم نوكي امثيح ةصلا تاذ .ةفلتخم تاوجاتو انردجم لماعتسإ ديعت ال .اذه ةرشابم ليزي ال duple-vBond ةيامنلا ةطقن نيعت ،ةيلاتلا ةرملا يف .ةيفاضإ تاونيع بلطتي ذفانم نم ديزملا دادعإلا كلهتسي نأ نكمي .وهو ليوقم ةيامنلا ةطقن نيعت ةداعإ دعب ةيلاتلا ةلاحلا يف ،ةيامنلا ةطقن نيعت نكمي ال ،ةلاحلا هذه يف .ةيامنلا ةطقن نيعت ةداعإ دعب ةيلاتلا ةرملا يف ةيامنلا ةطقن نيعت ةداعإ دعب ةيلاتلا ةرملا يف

ةطبوضم ةريغص ةعومجمل ذفنملا ةزافحإ مادختسإ

ةيامنلا ةطقن نيعت ةداعإ دعب ةيلاتلا ةرملا يف

فريدا فقط ويتطلب بوابة NAT للحفاظ والتمييز بينها. إنه يفشل كمخطط تفرد عند إعادة إستخدام الإزاحة. أيسر الي يضيف طاقة أيسر كثير هوايات.

على سبيل المثال، الي يمكن أن تتلقى جميع الموجهات 124 إزاحات فريدة خلف عنوان مشترك واحد. يتطلب نظام الإزاحة فقط والذي يحتوي على 20 موجه على الأكثر لكل مجموعة عناوين الي مجموعات على الأقل. وهذه الحسابات ليست توصية بشأن القدرات أو بديل عامة سبع مجموعات على الأقل. nat "لشركة النقل" يمكن أن يعيد أو يتداخل ميناء يترجم يستطيع قهر للتحقق من سلوك الي يمكن أن تدخل مساحة تخديد النظام حتى مع أقل.

تعطيل الاحتفاظ بمنفذ المصدر أو تمكين التوزيع العشوائي

يمكن للسياسة التي لا تتضمن تفضيل للحفظ أن تقلل من ميل العديد من الفورع إلى تلقي 12346: توزيع تلك التوزيع العشوائي يمكن للتوزيع العشوائي إعادة إستخدام منفذ عبر الوجهات، أو تغيير تخطيط باتجاه المصدر، أو إعادة تعيين التعيينات على تجمع منافذ أكبر.

غير أن أيا من هذين التغييرين لا يضمن وحده تجنب التصادم. لا يزال بمقدور التخصيص العشوائي إعادة إستخدام منفذ عبر الوجهات، أو تغيير تخطيط باتجاه المصدر، أو إعادة تعيين نقطة نهاية منتهية الصلاحية بينما تبقى حالة المصدر القديمة. تحقق ما إذا كان التخصيص فريدا عبر المشتركين والوجهات. المنافذ العشوائية وحدها لا تؤسس للتمييز.

راجع إعدادات الحفظ والتوزيع الخاصة بالمنفذ المصدر على بوابة NAT مع المشغل الخاص بها. يعتمد التكوين القابل للتطبيق على النظام الأساسي لـ NAT؛ تحقق من التعيينات الناتجة باتجاه كل من vBonds والمحول باستخدام سجلات الترجمة والتقاط الحزم.

يمكن أن تقع المنافذ المترجمة خارج نطاق المنفذ الأساسي SD-WAN الأساسي. راجع قواعد جدار الحماية حتى لا ترفض حركة المرور الشرعية المترجمة فقط بسبب تغيير منفذ المصدر.

العناوين العامة المنفصلة أو حجز كتل المنفذ

يمكن أن توفر العناوين المترجمة المخصصة، أو كتل المنافذ غير المتداخلة المحجوزة لكل مجاثة، نطاق نهاية معلنة مميزة للخادمات النشطة المختلفة. يجب تطبيق السياسة بشكل متناسق عبر مسارات الاكتشاف والموزع وعبر عقد NAT المكررة. قد يتطلب الأمر مساحة عنوان إضافية ودعم موفر. لا تزال إعادة الاستخدام الديناميكية بعد تعيين التقاعد تتطلب إدارة دورة حياة جلسة عمل المحور الصحيحة.

الاحتفاظ بعملية نقل بديلة وتنسيق الاسترداد

يمكن أن تحتفظ خدمة MPLS التي تم التحقق منها أو أي مسار آخر مؤهل بالخدمة أثناء التحقيق في مسار الإنترنت المتأثر. توفر قائمة التحكم في الوصول الأساسية (ACL)

التي تمنع عنوان NAT المشترك الاحتواء فقط: يمكنه إزالة تكرار الإنترنت لكل شخص يتم التحدث خلف هذا العنوان ولا يقوم بسحب إعلانات OMP الخاصة به تلقائيا.

يمكن أن يقوم مسح عنصر التحكم أو إعادة تعيين الواجهة أو مسح حالة NAT أو إعادة تحميل الموزع بإعادة إنشاء الحالة مؤقتا. ولا تضمن أي منها منع التكرار. لا تقم بتنفيذ عمليات مسح واسعة كخطوة تشخيصية أولى. الحفاظ على الأدلة وتصحيح شروط التوزيع حيثما كان ذلك ممكنا، والاتفاق على أصغر إجراء إستردادمع TAC. تحقق من صحة حركة مرور بيانات BFD لأعلى وثنائية الإتجاه على المسار المستردد.

عيوب البرامج ذات الصلة

النطاق ذي الصلة بهذه المادة	معرف الخطأ من Cisco
توثيق تحديد ملكية جلسة عمل الصرة عندما يعلن النظراء المختلفون عن نفس نقطة نهاية سجل الدخول العامة. يقوم هذا السجل بتعقب تحديث الوثائق، بدلا من تصحيح البرامج.	CSCww45867
يمكن أن يترك تسلسل تعلم نقطة الوصول/nat التلقائي مجموعة نصية خاصة في حقول TLOC العامة. إذا أعادت الفروع إستخدام نفس IP:port الخاص، يمكن أن تتطابق نقاط النهاية العامة غير الصحيحة عبر الأقران. لا يمنع تصحيح عيب المنتج هذا إعادة إستخدام المنفذ المترجم-العام الصحيح.	CSCwx12986
يمكن أن يصبح تصنيف NAT E بشكل غير صحيح عندما يعود الاكتشاف إلى نفس vBond. لا يمنع التصنيف الصحيح سيناريو إعادة إستخدام منفذ vBond مختلف صالح.	CSCwx48929

لا تضمن التصحيحات الخاصة بمعرف تصحيح الأخطاء من Cisco CSCwx12986 ومعرف تصحيح الأخطاء من Cisco CSCwx48929 نقاط النهاية العامة الفريدة المعلن عنها ولا تقوم، بحد ذاتها، بالقضاء على سيناريو التصادم هذا. لا ينشئ إغلاق سجل توثيق معرف تصحيح الأخطاء من Cisco CSCww45867 تغييرا في سلوك البرنامج. أكدت التحديد والتخفيف القابل للتطبيق مع Cisco TAC.

الملحق: فك تشفير المقطورة IPv4 vControl

احفظ هذا الرمز على هيئة sdwan_vctrl.lua. لا يقوم جهاز فك الترميز التشخيصي بمصادقة الحزم أو فك تشفير الحمولات الخاصة بها. وهو يستخدم عامل تصفية عرض sdwan_vctrl ويسجل فك ترميز صريح كخيار. يبقى التقاط الحزمة بدون تغيير.

```
-- 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)
```

ةلص تاذ تامولعم

- ذفنملا لخادت كولس :3 مسقلا، RFC 7857 راعيملا
- Unicast UDP ل NAT ل ةيكولسلا تابلطتملا :RFC 4787
- قئاثولل ةزوجحملا IPv4 نيوانع لتك :RFC 5737
- Cisco Catalyst SD-WAN ميمصت ليلد
- ذفنملا ةحازا :Cisco IOS XE Catalyst SD-WAN ماظن رماوأ
- Cisco SD-WAN ذفنم ةحازا نيوكت
- Wireshark رماوأ رطس عجرم
- TShark رماوأ رطس عجرم
- Cisco Systems - تادنتسملاو ينقتلا معدلا

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).