يتحرى IOS-XE nat يعجز متقطع أن يترجم بعض ربط

المحتويات

المقدمة

يصف هذا المستند الحزم غير المترجمة التي تتجاوز NAT على موجه Cisco IOS XE، مما قد يؤدي إلى فشل حركة مرور البيانات.

معلومات أساسية

في برمجية صيغة 12.2(33)xnd قدمت سمة يدعو شبكة عنوان ترجمة (NAT) مدخل وتمكنت افتراضيا. تم تصميم برنامج حماية البوابة عبر الشبكة (NAT) لمنع التدفقات التي لا تعتمد على NAT من إستخدام وحدة المعالجة المركزية (CPU) بشكل مفرط لإنشاء ترجمة NAT. لتحقيق ذلك، يتم إنشاء ذاكرتي تخزين مؤقت صغيرتين (واحدة من أجل إتجاه In2Out وواحدة من أجل إتجاه Out2In) استنادا إلى عنوان المصدر. يتكون كل إدخال من إدخالات ذاكرة التخزين المؤقت من عنوان مصدر ومعرف توجيه وإعادة توجيه ظاهريين (VRF) وقيمة مؤقت (تستخدم لإبطال الإدخال بعد 10 ثوان) وعداد إطارات. يوجد 256 إدخالا في الجدول الذي يشكل ذاكرة التخزين المؤقت. إن هناك يتعدد حركة مرور يتدفق من ال نفسه مصدر عنوان حيث بعض ربط يتطلب NAT وبعض لا، هو يستطيع أنتجت ربط لا يكون NAT-ed وأرسلت من خلال المسحاج تخديد غير مترجم. توصي Cisco بأن يتجنب العملاء وجود تدفقات NAT-ed وغير NAT-ed على نفس الواجهة حيثما أمكن.

ملاحظة: هذا لا علاقة له ب H.323.

الأنظمة الأساسية المتأثرة

- ISR1K
- ISR4K
- الطراز C8200
- الطراز C8300
- الطراز C8500

إثبات تجاوز NAT

يصف هذا القسم كيف يستطيع تنك تجاوزت nat واجب ال nat حارس ةمس. عجار المخطط بالتفصيل. يمكنك أن ترى هناك موجه مصدر، وجدار حماية جهاز الأمان القابل للتكييف (ASA)، و ASR1K، وموجه الوجهة.

تدفق حركة المرور إلى وجهة غير NAT-ED

1. أدب إختبار الاتصال من المصدر: المصدر: 172.17.250.201 الوجهة: 198.51.100.11.
2. تصل الحزمة إلى الواجهة الداخلية ل ASA التي تنفذ ترجمة عنوان المصدر. الطرب يتلقى الآن مصدر: 203.0.113.231 غاية: 198.51.100.11.
3. تصل الحزمة إلى ال ASR1K على ال NAT خارج إلى القارن داخلي. ال تعثر ترجمة nat على أي ترجمة لعنوان الوجهة وبالتالي يتم ملء ذاكرة التخزين المؤقت "out" الخاصة بالبوابة بعنوان المصدر 203.0.113.231.
4. تصل الحزمة إلى الوجهة. تقبل الوجهة حزمة بروتوكول رسائل التحكم في الإنترنت (ICMP) وترجع در ICMP ECHO الذي ينتج عنه نجاح إختبار الاتصال.

يحاول حركة المرور من المصدر نفسه إرسال وجهة NAT-ED

1. .تم بدء إختبار الاتصال من المصدر: المصدر: 172.17.250.201 الوجهة: 198.51.100.9.
2. تصل الحزمة إلى الواجهة الداخلية ل ASA التي تنفذ ترجمة عنوان المصدر. الطرب الآن يتلقى مصدر: 203.0.113.231 غاية: 198.51.100.9.
3. تصل الحزمة إلى ال ASR1K على ال NAT خارج إلى القارن داخلي. يبحث NAT أولا عن ترجمة للمصدر والوجهة. ولأنه ال يجد واحدة، فإنه يتحقق من ذاكرة التخزين المؤقت "للخارج" الخاصة ب "برنامج حماية البوابة" ويبحث عن عنوان المصدر 203.0.113.231. هو (أطخ) يفترض أن الطرب ال يحتاج إلى ترجمة وإما يرسل الطرب إن يتجاوز ممر للغاية أو يسقط الربط. بأي طريقة، ال يبلغ الربط الغاية المقصودة.

إستعادة حركة مرور NAT-ED

1. بعد 10 ثوان، خرج إدخال عنوان المصدر 203.0.113.231 مرة في ذاكرة التخزين المؤقت ل "برنامج حماية البوابة".

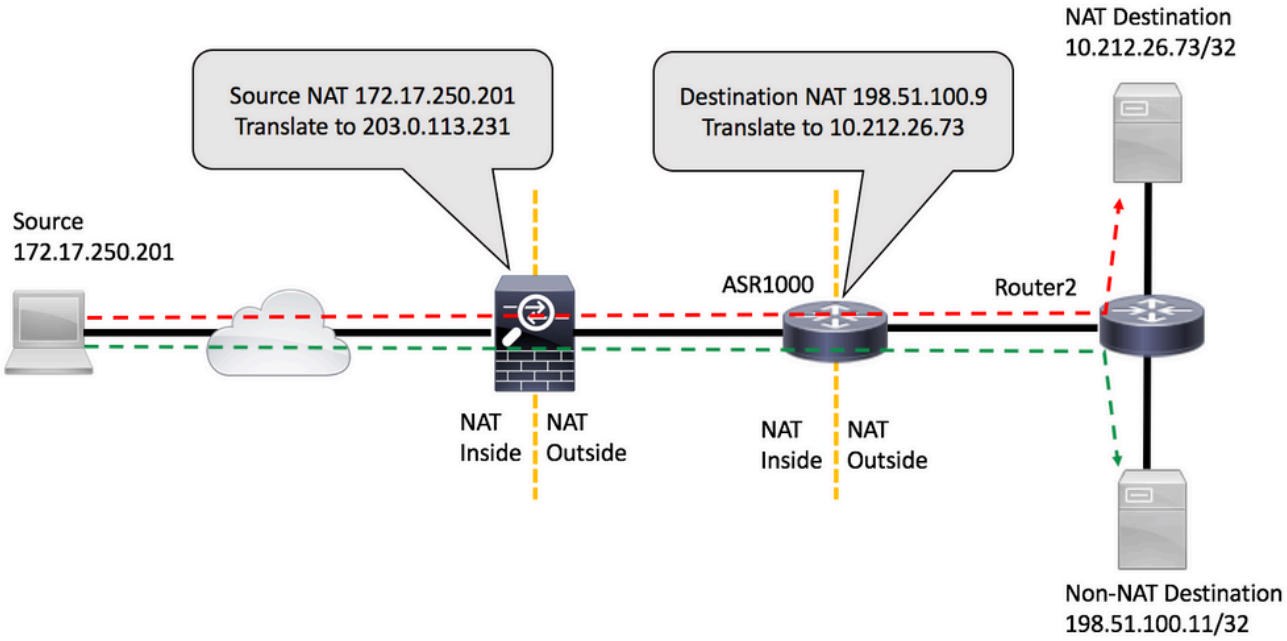
✎ ملاحظة: ال يزال الإدخال موجودا فعليا في ذاكرة التخزين المؤقت، ولكن نظرا النتهاء صالحيته، فإنه ال يتم إستخدامه.

---

2. الآن إن ال نفسه مصدر 172.17.250.201 يرسل إلى NAT-ed غاية 198.51.100.9. عندما

تصل الحزمة إلى واجهة out2in على ASR1K، لم يتم العثور على ترجمة. عندما تقوم بالتحقق من ذاكرة التخزين المؤقت الخاصة ببرنامج حماية البوابة، لا يمكنك العثور على إدخال نشط حتى تقوم بإنشاء الترجمة للوجهة وتدفق الحزم كما هو متوقع.

3. تستمر حركة المرور في هذا التدفق طالما لم يتم انتهاء مهلة الترجمات بسبب عدم النشاط. إن، في غضون ذلك، يرسل المصدر مرة أخرى حركة مرور إلى غاية غير NAT-ED، أي يسبب آخر مدخل أن يكون زودت في البوابة من ذاكرة التخزين المؤقت، وه لا يأثر وه مع موصل جلسة غير أن هناك 10 ثاني فيها جلسة جديد من أن نفسه مصدر إلى NAT-ed غاية يفشل.



مثال على المسألة

1. يبدأ إختبار الاتصال من الموجه المصدر: المصدر: 172.17.250.201 الوجهة: 198.51.100.9. يتم إصدار إختبار الاتصال مع تكرار العد إلى إثنين، أكثر من [FLOW1].
2. بعد ذلك يؤز غاية مختلف أن ال يكون NAT-ed ب ال ASR1K: مصدر: 172.17.250.201 غاية:198.51.100.11 [FLOW2].
3. ثم قم بإرسال المزيد من الحزم إلى 198.51.100.9 [Flow1]. أول حزم قليلة من هذا التدفق يتجاوز NAT كما يظهر من مطابقة قائمة الوصول على موجه الوجهة.

```
<#root>

source#

ping 198.51.100.9 source lo1 rep 2



Type escape sequence to abort.
Sending 2, 100-byte ICMP Echos to 198.51.100.9, timeout is 2 seconds:
Packet sent with a source address of 172.17.250.201
!!
Success rate is 100 percent (2/2), round-trip min/avg/max = 1/1/1 ms
source#ping 198.51.100.9 source lo1 rep 2
```

```
Type escape sequence to abort.
Sending 2, 100-byte ICMP Echos to 198.51.100.9, timeout is 2 seconds:
Packet sent with a source address of 172.17.250.201
!!
Success rate is 100 percent (2/2), round-trip min/avg/max = 1/1/1 ms
source#ping 198.51.100.11 source lo1 rep 200000

Type escape sequence to abort.
Sending 200000, 100-byte ICMP Echos to 198.51.100.11, timeout is 2 seconds:
Packet sent with a source address of 172.17.250.201
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!.
Success rate is 99 percent (3007/3008), round-trip min/avg/max = 1/1/16 ms
source#
```

ping 198.51.100.9 source lo1 rep 10

```
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 198.51.100.9, timeout is 2 seconds:
Packet sent with a source address of 172.17.250.201
...!!!!!!!
Success rate is 70 percent (7/10), round-trip min/avg/max = 1/1/1 ms
source#
```

يظهر قائمة التحكم في الوصول على موجه الواجهة الحزم الثالث التي فشلت لم تتم ترجمتها:

<#root>

Router2#

show access-list 199

```
Extended IP access list 199
    10 permit udp host 172.17.250.201 host 198.51.100.9
    20 permit udp host 172.17.250.201 host 10.212.26.73
    30 permit udp host 203.0.113.231 host 198.51.100.9
    40 permit udp host 203.0.113.231 host 10.212.26.73 (4 matches)
    50 permit icmp host 172.17.250.201 host 198.51.100.9
    60 permit icmp host 172.17.250.201 host 10.212.26.73
```

70 permit icmp host 203.0.113.231 host 198.51.100.9 (3 matches) <<<<<<<

```
    80 permit icmp host 203.0.113.231 host 10.212.26.73 (42 matches)
    90 permit udp any any log (2 matches)
    100 permit icmp any any log (4193 matches)
    110 permit ip any any (5 matches)
Router2#
```

في ال ASR1K يمكنك التحقق من إدخالات ذاكرة التخزين المؤقت ل Gatekeeper:

```
<#root>

PRIMARY#

show platform hardware qfp active feature nat datapath gatein


Gatekeeper on
sip 203.0.113.231 vrf 0 cnt 1 ts 0x17ba3f idx 74
sip 10.203.249.226 vrf 0 cnt 0 ts 0x36bab6 idx 218
sip 10.203.249.221 vrf 0 cnt 1 ts 0x367ab4 idx 229

PRIMARY#

show platform hardware qfp active feature nat datapath gateout


Gatekeeper on
sip 198.51.100.11 vrf 0 cnt 1 ts 0x36db07 idx 60
sip 10.203.249.225 vrf 0 cnt 0 ts 0x36bb7a idx 217
sip 10.203.249.222 vrf 0 cnt 1 ts 0x367b7c idx 230
```

الحل البديل/الإصلاح

في معظم البيئات، تعمل وظيفة حارس بوابة NAT بشكل جيد ولا تسبب مشاكل. ومع ذلك، إذا واجهت هذه المشكلة بالفعل، فتوجد طرق قليلة لحلها.

الحل 1

وسيكون الخيار المفضل هو ترقية Cisco IOS® XE إلى إصدار يتضمن تحسين برنامج حماية البوابة:

ترقية معرفة تصحيح الأخطاء من Cisco CSCun06260 XE3.13 Gatekeeper

يتيح هذا التحسين ل NAT Gatekeeper أن يخزن عناوين المصدر والوجهة مؤقتا، وكذلك يجعل حجم ذاكرة التخزين المؤقت قابلا للتكوين. لتشغيل الوضع الموسع، تحتاج لزيادة حجم ذاكرة التخزين المؤقت باستخدام هذه الأوامر. يمكنك أيضا مراقبة التخزين المؤقت لترى إذا كنت تحتاج لزيادة الحجم.

```
<#root>

PRIMARY(config)#

ip nat settings gatekeeper-size 1024


PRIMARY(config)#

end
```

يمكن التحقق من الوضع الموسع بالتحقق من هذه الأوامر:

```
<#root>

PRIMARY#

show platform hardware qfp active feature nat datapath gatein


Gatekeeper on


sip 10.203.249.221 dip 10.203.249.222 vrf 0 ts 0x5c437 idx 631

PRIMARY#

show platform hardware qfp active feature nat datapath gateout


Gatekeeper on


sip 10.203.249.225 dip 10.203.249.226 vrf 0 ts 0x5eddf idx 631

PRIMARY#

show platform hardware qfp active feature nat datapath gatein active


Gatekeeper on


ext mode Size 1024

, Hits 2, Miss 4, Aged 0 Added 4 Active 1

PRIMARY#

show platform hardware qfp active feature nat datapath gateout active


Gatekeeper on


ext mode Size 1024

, Hits 0, Miss 1, Aged 1 Added 2 Active 0
```

الحل 2

بالنسبة للإصدارات التي لا تحتوي على الإصلاح لمعرف الأخطاء من Cisco CSCun06260، يكون الخيار الوحيد هو إيقاف تشغيل ميزة "حماية البوابة". التأثير السلبي الوحيد هو انخفاض طفيف في أداء حركة المرور غير المعتمدة على NAT بالإضافة إلى إستخدام أعلى لوحدة المعالجة المركزية في معالج تدفق الكم (QFP).

```
<#root>

PRIMARY(config)#

no ip nat service gatekeeper

PRIMARY(config)#

end

PRIMARY#PRIMARY#

Sh platform hardware qfp active feature nat datapath gatein

Gatekeeper off

PRIMARY#
```

يمكن مراقبة إستخدام QFP باستخدام الأوامر التالية:

```
<#root>

show platform hardware qfp active data utilization summary


show platform hardware qfp active data utilization qfp 0
```

الحل 3

افصل حركة المرور بحيث ال تصل حزم NAT وحزم غير NAT إلى الواجهة نفسها.

ملخص

تم إدخال الأمر nat Gatekeeper لتعزيز أداء الموجه للتدفقات غير NAT-ed. تحت بعض الشروط، المميزة يستطيع سبب مشكلة عندما يصل خليط من حزم NAT وغير NAT من المصدر نفسه. الحل هو إستخدام وظيفة "برنامج حماية البوابة" المحسنة، أو تعطيل ميزة "برنامج حماية البوابة" إذا لم يكن ذلك ممكنا.

المراجع

تغييرات البرامج التي سمحت بإيقاف تشغيل برنامج حماية البوابة:
Cisco Bug ID CSCty67184 ASR1k NAT CLI - Gatekeeper قيد التشغيل/إيقاف التشغيل
Cisco CSCth23984 إضافة قدرة CLI لتشغيل/إيقاف تشغيل معرف تصحيح الأخطاء من nat وظائف برنامج حماية البوابة

تحسين برنامج حماية البوابة ل NAT
تقوية معرف تصحيح الأخطاء من Cisco CSCun06260 XE3.13 Gatekeeper

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).