فهم NAT لتمكين اتصال نظير إلى نظير على موجهات IOS و IOS XE

المحتويات

المقدمة

يصف هذا وثيقة الحاجة إلى جلسة عمل منفعة لنادل NAT (STUN)، النوع من شبكة عنوان ترجمة (NAT) فيما يتعلق بخوادم STUN، كيف NAT يسبب مشكلة في هذا إعداد والحل.

معلومات أساسية

الغرض الأساسي من أجهزة NAT هو السماح للأجهزة ذات عناوين IP الخاصة في شبكة منطقة محلية (LAN) بالاتصال بالأجهزة في مساحات العناوين العامة، مثل الإنترنت. ومع ذلك، على الرغم من أنه من المفترض أن تسمح أجهزة NAT للمضيفين الداخليين بالاتصال بالمساحة العامة، إلا أن NAT يوفر صعوبة في إنشاء إتصالات UDP هذه عندما يتعلق الأمر بتطبيقات من نقطة إلى نقطة (P2P) مثل VoIP والألعاب و WebRTC ومشاركة الملفات حيث يحتاج المستخدمون النهائيون إلى العمل كعميل وخادم على حد سواء للحفاظ على الاتصال من نقطة إلى نقطة، فإن NAT يوفر صعوبة في إنشاء إتصالات UDP هذه. تكون تقنيات إجتياز NAT مطلوبة بشكل نموذجي لجعل هذه التطبيقات تعمل.

الحاجة إلى إجتياز NAT

الاتصال بالصوت والفيديو في الوقت الفعلي على الإنترنت هو يار سائد اليوم مع العديد من المراسلات الفورية (IM) الشائعة التي تدعم مكالمات VoIP. إحدى العقبات الكبيرة التي واجهت تبني بروتوكول VoIP في بادئ الأمر هي أن معظم أجهزة الكمبيوتر الأجهزة الأخرى تقع خلف جدران الحماية وتستخدم عناوين IP الخاصة. تم تعيين عناوين خاصة متعددة (عنوان IP ومنفذ) في الشبكة إلى عنوان عام واحد بواسطة جدار حماية مع nat. ولكن الجهاز الطرفي لا يعرف عنوانه العام، وبالتالي لا يمكنه تلقي حركة مرور الصوت من الطرف البعيد على العنوان الخاص الذي أعلن عنه في اتصال VoIP الخاص به.

انفرادي عمليات الإصلاح الذاتي للعنوان (UNSAF) هي عمليات تحاول فيها بعض نقاط النهاية النشطة تحديد أو إصلاح العنوان (والمنفذ) الذي تعرف به لنقطة نهاية أخرى - على سبيل المثال، لتكون قادرة على استخدام بيانات العنوان في تبادل البروتوكول أو للإعلان عن عنوان عام والذي تستلم منه الاتصالات.

ومن ثم، فإن إتصالات P2P قيد المناقشة هي عمليات UNSAF. تعمل تطبيقات P2P إحدى

الطرق الشائعة على إنشاء جلسات للتجميع والتي لا تزال مناسبة لـ NAT وهي عندما يستخدمون خادم تناسخ قابل للتوجيه بشكل عام لأغراض التسجيل واكتشاف الأجهزة النظيرة.

أدوات مساعدة تبادل الجلسات لـ NAT

وفقا لمعيار RFC 5389، يوفر بروتوكول الشجرة المتفرعة (STUN) أداة تتعامل مع بطاقات واجهة الشبكة (NAT). وهو بروتوكول نقطة نهاية أن يحدد العنوان ومنفذ يعين بـ nat أداة أن يماثل وهو عنوان ومنفذ خاص. كما يوفر طريقة لنقطة نهاية لإبقاء ربط NAT حيا.

أنواع عمليات تنفيذ NAT

ولوحظ أن معاملة NAT لمخطط التنميط المستدامة تختلف فيما بين عمليات التنفيذ. العلاجات الأربعة التي لوحظت في عمليات التنفيذ هي:

مخروط كامل: NAT مخروط كامل واحد حيث كل طلب من النفس داخلي عنوان ومنفذ عينت إلى النفس عنوان ومنفذ خارجي. علاوة على ذلك، يمكن لأي مضيف خارجي إرسال حزمة إلى المضيف الداخلي، ويرسل حزمة إلى العنوان الخارجي الذي تم تعيينه.

مخروط مقيد: NAT مخروط مقيد وهو واحد حيث كل الطلبات من النفس داخلي عنوان ومنفذ عينت إلى النفس خارجي عنوان ومنفذ. بخلاف NAT مخروط كامل، مضيف خارجي (مع عنوان x) يستطيع أرسلت ربط إلى المضيف داخلي فقط إن المضيف داخلي كان سابقا أرسلت ربط إلى عنوان x.

المخروط المقيد للمنفذ: يشبه NAT المخروط المقيد مخروط، غير أن القيد يتضمن أرقام المنافذ. وعلى وجه الخصوص، يمكن للمضيف الخارجي إرسال حزمة، مع مصدر عنوان X ومصدر منفذ P، إلى المضيف الداخلي فقط إذا كان المضيف الداخلي قد أرسل حزمة من قبل إلى عنوان IP X ومنفذ P.

متماثل: NAT متماثل واحد حيث كل طلب من النفس داخلي عنوان ومنفذ إلى غاية خاص عنوان ومنفذ، عينت إلى النفس خارجي عنوان ومنفذ. إن يرسل النفس مضيف ربط مع النفس مصدر عنوان ومنفذ، غير أن إلى غاية مختلف، يخطط مختلف استعملت. علاوة على ذلك، يمكن فقط للمضيف الخارجي الذي يستلم حزمة إرسال حزمة UDP مرة أخرى إلى المضيف الداخلي.

ضع في الاعتبار مخطط حيث يتصل المصدر (A، PA) (حيث A هو عنوان IP، و PA هو المنفذ المصدر) بالوجهة (B، Pb) و(C، PC) من خلال جهاز nat.

نوع تنفيذ NAT	عام المصدر عندما إلى (ب، ب ب)	المصدر العام عندما تم تعيينه إلى (C، كمبيوتر شخصي)	يمكن الوجهة (على سبيل المثال: (ب، ب ب) إرسال حركة مرور إلى (A، PA)؟
مخروط كامل	(x1،px1)	(x1،px1)	نعم
مخروط مقيد	(X1،px1)	(X1،px1)	فقط إذا (A، Pa) أرسلت الحركة إلى B مرة لأول
مخروط مقيد للمنفذ	(X1،px1)	(X1،px1)	فقط إذا كانت (A، PA) قد أرسلت الحركة لأول مرة إلى (B، Pb)
تناظري	(X1،px1)	(x2،px2)	فقط إذا كانت (A، PA) قد أرسلت الحركة لأول مرة إلى (B، Pb)

المشاكل مع NAT Traversal و Symmetric NAT

تستجيب خوادم STUN لطلبات ربط STUN التي يرسلها عملاء STUN وتوفر منفذ IP/العميل العام. الآن، هذا العنوان/المنفذ يتم إستخدام المجموعة من قبل عميل STUN في اتصال نظير إلى نظير الخاص به لإرسال الإشارات. ومع ذلك، والآن بعد مضيف داخلي يستخدم نفس العنوان/المنفذ الخاص (بعد ان فتح أن يصبح إلى IP/المنفذ العام تزود في ال STUN إستجابة) ال nat يترجم هو إلى ال نفسه ip غير أن ميناء مختلف إن متماثل nat نقشأنانترميز مستخدمة. يؤدي ذلك إلى قطع اتصال UDP لأن إرسال الإشارات قد أسس الاتصال استنادا إلى pميناء زاجح.

برنامج Cisco IOS® الموجهات nat نقشأنانترميز عندما يقوم موقع بتنفيذ برض يكون متماثل بشكل افتراضي. THERهأمامي، من المتوقع أن ترى مشاكل اتصال UDP مع هذه الموجهات التي تعمل nat.

مهما، ال cisco IOS-XE مسجاح تخديد nat تنفيذ عندما ينجز برض سيل متماثل. عندما لسرت إثنين مختلفين تيار مع ال نفسه مصدر ip ومنفذ غير أن إلى غاية مختلف، المصدر يحصل NATs إلى ال نفسه داخل لماش ip ومنفذ.

حل المسألة

من هذا الوصف، من الواضح أن يمكن حل المشكلة إذا قمت بتنفيذها مستقل عن نقطة النهاية مسر الخرائط.

حسب مركبات الكربون الكلورية فلورية 4787: مع تخطيط غير مستقل عن النقطة النهائية (EIM)، يعيد NAT تخطيط المنفذ للحزم التالية المرسلة من نفس عنوان IP الداخلي والمنفذ (X:X) إلى أي عنوان IP ومنفذ خارجي.

من عميل، عندما يركض المضيف الداخلي الأمر **nc -p 23456 10.0.0.4 4000** و**nc -p 23456 10.0.0.5 5000**، على إثنان محطة طرفية مختلف نافذة، هنا نتائج ترجمات nat إن يستعمل أنت EIM:

```
Pro Inside global       Inside local            Outside local       Outside global

tcp 10.0.0.1:23456   192.168.0.2:23456  10.0.0.4:40000 10.0.0.4:40000

tcp 10.0.0.1:23456   192.168.0.2:23456  10.0.0.5:50000 10.0.0.5:50000
```

هنا أنت يستطيع رأيت أن مختلف حركة رور يتدفق أن يتلقى ال نفسه مصدر عنوان ومنفذ يحصل ترجمت إلى ال نفسه عنوان/ميناء regardless of الغاية ميناء/عنوان.

على موجهات Cisco IOS، يمكنك تمكين تخصيص المنفذ المجمع لنقطة النهاية باستخدام الأمر **ip nat service enable-sym-المنفذ.**

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_nat/configuration/15-mt/nat-15-mt-book/iadnat-fpg-port-alloc.html

ملخص

يكون تنفيذ Cisco IOS NAT متماثل بشكل افتراضي عندما يستعمل أنت أيسر عنوان ترجمة (برض) وهو يستطيع تتسبب إصدار عندما هو يمر p2P udp حركة رور أن يتطلب لدان مثل STUN لمرور nat. تحتاج إلى تكوين EIM بشكل صريح على جهاز NAT لجعل هذا العمل.

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).