إستخدام NAT في الشبكات المتداخلة

المحتويات

المقدمة
المتطلبات الأساسية
المتطلبات
المكونات المستخدمة
الاصطلاحات
التكوين
الرسم التخطيطي للشبكة
التكوينات
التحقق من الصحة
استكشاف الأخطاء وإصلاحها
معلومات ذات صلة

المقدمة

يوضح هذا وثيقة كيف أنت يستطيع استعملت شبكة عنوان ترجمة (NAT) لشبكات متداخلة. ينتج عن الشبكات المتداخلة عندما تقوم بتعيين عنوان IP لجهاز على شبكتك مملوك قانونيا بالفعل ومخصص لجهاز مختلف على الإنترنت أو الشبكة الخارجية. كما ينتج عن الشبكات المتداخلة عندما تقوم شركتان، وكلتاهما تستخدم عناوين RFC 1918 IP في شبكاتهما، بالدمج. تحتاج هاتان الشبكتين إلى الاتصال، ويفضل أن يكون ذلك دون الحاجة إلى إعادة ضبط جميع أجهزتهما.

المتطلبات الأساسية

المتطلبات

يعد الفهم الأساسي لعنونة IP وتوجيه IP ونظام اسم المجال (DNS) مفيدا لفهم محتويات هذا المستند.

المكونات المستخدمة

بدأ دعم NAT في برنامج Cisco IOS® نسخة 11.2. لمزيد من المعلومات عن دعم منصة العمل راجع NAT الأسئلة المتكررة.

الاصطلاحات

للحصول على مزيد من المعلومات حول اصطلاحات المستندات، ارجع إلى اصطلاحات تلميحات Cisco التقنية.

التكوين

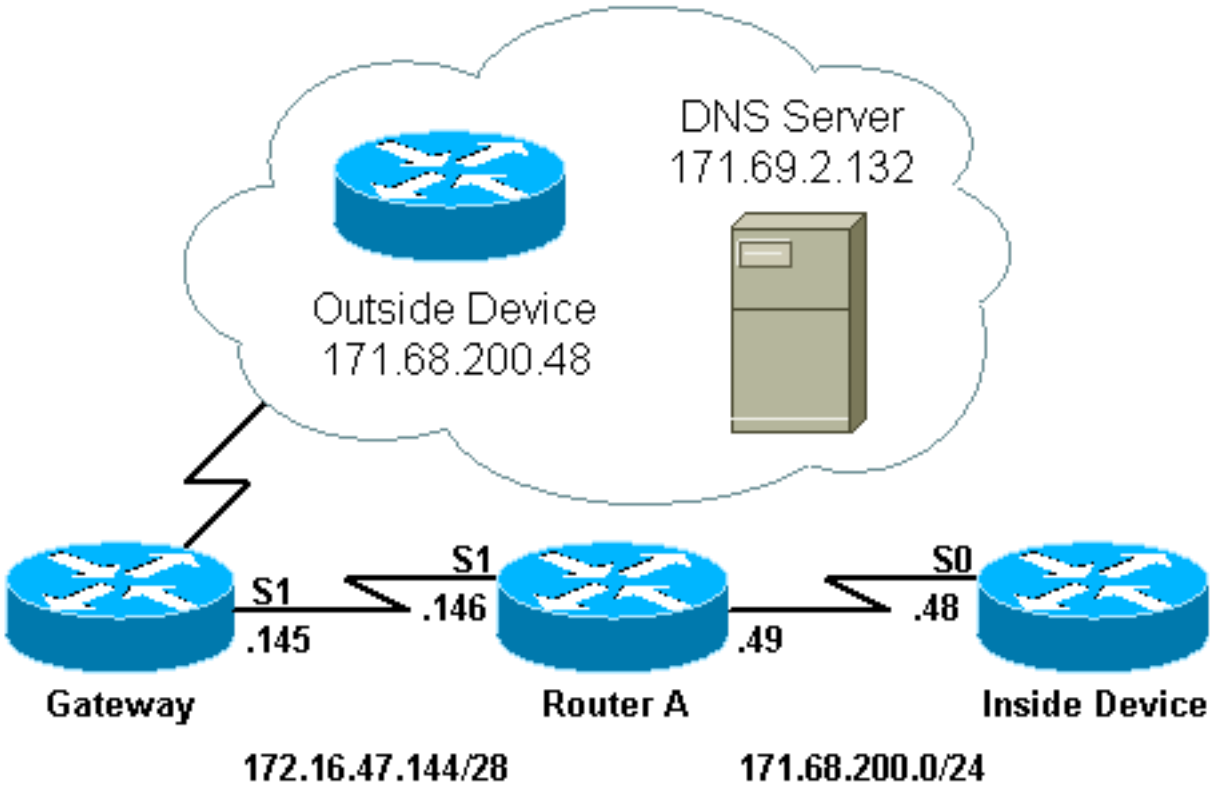
في هذا القسم، تُقدّم لك معلومات تكوين الميزات الموضحة في هذا المستند.

ملاحظة: للعثور على معلومات إضافية حول الأوامر المستخدمة في هذا المستند، أستخدم أداة بحث الأوامر (للعملاء المسجلين فقط).

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة الموضح في الرسم التخطيطي أدناه.

لاحظ أن الجهاز الداخلي له نفس عنوان IP الخاص بالجهاز الخارجي الذي يرغب في الاتصال به.



التكوينات

شكلت مسحاج تخديد A ل nat، مثل أن هو يترجم الأداة داخلي إلى عنوان من البركة "إختبار أنشوطة" والجهاز الخارجي إلى عنوان من البركة "إختبار-dns". يتبع شرح لكيفية مساعدة هذا التكوين مع التداخل جدول التكوين أدناه.

الموجه A
!
version 11.2
no service udp-small-servers
no service tcp-small-servers
!
hostname Router-A
!
!
ip domain-name cisco.com
ip name-server 171.69.2.132
!
interface Loopback0
ip address 1.1.1.1 255.0.0.0
!
interface Ethernet0
ip address 135.135.1.2 255.255.255.0
shutdown

```
!
interface Serial0
 ip address 171.68.200.49 255.255.255.0
 ip nat inside
 no ip mroute-cache
 no ip route-cache
 no fair-queue
!
interface Serial1
 ip address 172.16.47.146 255.255.255.240
 ip nat outside
 no ip mroute-cache
 no ip route-cache
!
ip nat pool test-loop 172.16.47.161 172.16.47.165
 prefix-length 28
ip nat pool test-dns 172.16.47.177 172.16.47.180 prefix-
 length 28
ip nat inside source list 7 pool test-loop
ip nat outside source list 7 pool test-dns
ip classless
ip route 0.0.0.0 0.0.0.0 172.16.47.145
access-list 7 permit 171.68.200.0 0.0.0.255
!
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 login
!
end
```

من أجل أن يساعد التكوين أعلاه في التداخل عند اتصال الجهاز الداخلي بالجهاز الخارجي، يجب أن يستخدم اسم مجال الجهاز الخارجي.

يتعذر على الجهاز الداخلي إستخدام عنوان IP الخاص بالجهاز الخارجي لأنه هو نفسه العنوان المعين له (الجهاز الداخلي). لذلك، سيقوم الجهاز الداخلي بإرسال استعلام DNS لاسم مجال الجهاز الخارجي. سيكون عنوان IP الخاص بالجهاز الداخلي هو مصدر هذا الاستعلام، وسيتم ترجمة هذا العنوان إلى عنوان من تجمع "حلقة الاختبار" لأنه تم تكوين أمر **ip nat داخل قائمة المصدر**.

يرد خادم DNS على العنوان الذي جاء من التجمع "أنشوطة الاختبار" مع عنوان IP المقترن باسم مجال الجهاز الخارجي في حمولة الحزمة. تتم ترجمة عنوان الوجهة لحزمة الرد مرة أخرى إلى عنوان الجهاز الداخلي، وبعد ذلك تتم ترجمة العنوان في حمولة حزمة الرد إلى عنوان من التجمع "test-dns" بسبب أمر **ip nat خارج قائمة المصدر**. لذلك يعلم الجهاز الداخلي أن عنوان IP الخاص بالجهاز الخارجي هو أحد العناوين من تجمع "إختباري-dns"، وسيستخدم هذا العنوان عند الاتصال بالجهاز الخارجي. يعتني الموجه الذي يشغل NAT بالترجمات في هذه النقطة.

يمكن ملاحظة هذه العملية بالتفصيل في قسم أستكشاف الأخطاء واصلاحها. يمكن أن تتصل الأجهزة التي تستخدم عناوين متداخلة مع بعضها البعض بدون إستخدام DNS، ولكن في هذه الحالة، سيتعين تكوين NAT الثابت. وفيما يلي مثال على كيفية القيام بذلك.

الموجه A

```
!
version 11.2
no service udp-small-servers
no service tcp-small-servers
!
```

```
hostname Router-A
!
!

ip domain-name cisco.com
ip name-server 171.69.2.132
!
interface Loopback0
ip address 1.1.1.1 255.0.0.0
!
interface Ethernet0
ip address 135.135.1.2 255.255.255.0
shutdown
!
interface Serial0
ip address 171.68.200.49 255.255.255.0
ip nat inside
no ip mroute-cache
no ip route-cache
no fair-queue
!
interface Serial1
ip address 172.16.47.146 255.255.255.240
ip nat outside
no ip mroute-cache
no ip route-cache
!
ip nat pool test-loop 172.16.47.161 172.16.47.165
prefix-length 28
ip nat inside source list 7 pool test-loop
ip nat outside source static 171.68.200.48 172.16.47.177
ip classless
ip route 0.0.0.0 0.0.0.0 172.16.47.145
ip route 172.16.47.160 255.255.255.240 Serial0
 This line is necessary to make NAT work for return ---!
  traffic. !--- The router needs to have a route for the
pool to the inside !--- NAT interface so it knows that a
translation is needed. access-list 7 permit 171.68.200.0
0.0.0.255
!
!
line con 0
exec-timeout 0 0
line aux 0
line vty 0 4
login
!
end
```

مع التكوين المذكور أعلاه، عندما يريد الجهاز الداخلي الاتصال بالجهاز الخارجي، يمكن الآن إستخدام عنوان IP 172.16.47.177 و DNS في غير الضروري. كما هو موضح أعلاه، لا تزال ترجمة عنوان الجهاز الداخلي تتم بشكل ديناميكي، ما يعني أن الموجه يجب أن يحصل على الحزم من الجهاز الداخلي قبل إنشاء ترجمة. ولهذا السبب، يجب أن يبدأ الجهاز الداخلي جميع الاتصالات للاتصال بالجهاز الداخلي والجهاز الخارجي. إذا كان مطلوبا أن يبدأ الجهاز الخارجي الاتصالات بالجهاز الداخلي، فيجب أيضا تكوين عنوان الجهاز الداخلي بشكل ثابت.

التحقق من الصحة

لا يوجد حاليًا إجراء للتحقق من صحة هذا التكوين.

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

يمكن عرض العملية التي يستخدم من خلالها الجهاز الداخلي DNS للاتصال بالجهاز الخارجي، كما هو موضح أعلاه، بالتفصيل باستخدام عملية أستكشاف الأخطاء وإصلاحها التالية.

حاليا هناك ما من ترجمة في الترجمة طاولة أن يستطيع كنت رأيت مع **العرض ip nat ترجمة** أمر. تستخدم الأمثلة أدناه أوامر **debug ip packet** و**debug ip nat** بدلا من ذلك.

ملاحظة: تقوم أوامر **تصحيح الأخطاء** بإنشاء كمية كبيرة من الإخراج. يمكنك إستخدامها فقط عندما تكون حركة المرور على شبكة IP منخفضة، وبالتالي لا تتأثر الأنشطة الأخرى على النظام بشكل سلبي.

```
Router-A# show ip nat translations
Router-A# show debug
:Generic IP
(IP packet debugging is on (detailed
IP NAT debugging is on
```

عندما يرسل الجهاز الداخلي استعلام DNS الخاص به إلى خادم DNS، الموجود خارج مجال NAT، يتم ترجمة عنوان المصدر الخاص باستعلام DNS (عنوان الجهاز الداخلي) بسبب أوامر **ip nat inside**. يمكن ملاحظة ذلك في إخراج تصحيح الأخطاء أدناه.

```
[NAT: s=171.68.200.48->172.16.47.161, d=171.69.2.132 [0
IP: s=172.16.47.161 (Serial0), d=171.69.2.132 (Serial1), g=172.16.47.145, len 66, forward
UDP src=6988, dst=53
```

عندما يرسل خادم DNS ردا على DNS، تتم ترجمة حمولة رد DNS بسبب الأوامر **ip nat الخارجية**.

ملاحظة: لا ينظر NAT إلى حمولة رد DNS ما لم تحدث الترجمة على رأس IP لحزمة الرد. راجع الأمر **ip nat خارج قائمة المصدر 7 pool** في تكوين الموجه أعلاه.

تظهر رسالة NAT الأولى في إخراج تصحيح الأخطاء أدناه أن الموجه يتعرف على الرد على DNS ويترجم عنوان IP داخل الحمولة إلى 172.16.47.177. تظهر رسالة NAT الثانية الموجه الذي يقوم بترجمة وجهة رد DNS بحيث يمكنه إعادة توجيه رد مرة أخرى إلى الجهاز الداخلي الذي قام بتنفيذ استعلام DNS الأولي. ترجمت الغاية جزء من الرأس، العنوان شامل داخلي، إلى العنوان محلي داخلي.

تمت ترجمة حمولة رد DNS:

```
NAT: DNS resource record 171.68.200.48 -> 172.16.47.177
```

تتم ترجمة جزء الوجهة من رأس IP في حزمة الرد على DNS:

```
[NAT: s=171.69.2.132, d=172.16.47.161->171.68.200.48 [65371
IP: s=171.69.2.132 (Serial1), d=171.68.200.48 (Serial0), g=171.68.200.48, len 315, forward
UDP src=53, dst=6988
```

لنلق نظرة على استعلام DNS آخر والرد عليه:

```
[NAT: s=171.68.200.48->172.16.47.161, d=171.69.2.132 [0
IP: s=172.16.47.161 (Serial0), d=171.69.2.132 (Serial1), g=172.16.47.145, len 66, forward
UDP src=7419, dst=53
```

```
                                NAT: DNS resource record 171.68.200.48 -> 172.16.47.177
                              [NAT: s=171.69.2.132, d=172.16.47.161->171.68.200.48 [65388
IP: s=171.69.2.132 (Serial1), d=171.68.200.48 (Serial0), g=171.68.200.48, len 315, forward
                                                    UDP src=53, dst=7419
```

الآن بعد ترجمة حمولة DNS، يحتوي جدول الترجمة الخاص بنا على إدخال للعناوين المحلية والعالمية الخارجية للجهاز الخارجي. مع هذه الإدخالات في الجدول، يمكننا الآن ترجمة رأس حزم ICMP المتبادلة بالكامل بين الجهاز الداخلي والجهاز الخارجي. لنلق نظرة على هذا التبادل في إخراج تصحيح الأخطاء أدناه.

يظهر الإخراج التالي عنوان المصدر (داخل عنوان الجهاز) الذي يتم ترجمته.

```
                              [NAT: s=171.68.200.48->172.16.47.161, d=172.16.47.177 [406
```

هنا، الغاية ترجمة عنوان (خارج أداة محلي خارجي عنوان).

```
                              [NAT: s=172.16.47.161, d=172.16.47.177->171.68.200.48 [406
```

بعد الترجمة، تبدو حزمة IP كما يلي:

```
IP: s=172.16.47.161 (Serial0), d=171.68.200.48 (Serial1), g=172.16.47.145, len 100, forward
                                                    ICMP type=8, code=0
```

يبدي الإنتاج التالي المصدر عنوان (خارج أداة عنوان) يكون ترجمت على الربط يرجع.

```
                              [NAT*: s=171.68.200.48->172.16.47.177, d=172.16.47.161 [16259
```

الآن ترجمت الغاية عنوان (داخل الأداة شامل عنوان) من الربط رجوع.

```
                              [NAT*: s=172.16.47.177, d=172.16.47.161->171.68.200.48 [16259
```

بعد الترجمة، تبدو حزمة الإرجاع كما يلي:

```
IP: s=172.16.47.177 (Serial1), d=171.68.200.48 (Serial0), g=171.68.200.48, len 100, forward
                                                    ICMP type=0, code=0
```

يستمر تبادل الحزم بين الجهاز الداخلي والجهاز الخارجي.

```
                                [NAT: s=171.68.200.48->172.16.47.161, d=172.16.47.177 [407
                                [NAT: s=172.16.47.161, d=172.16.47.177->171.68.200.48 [407
IP: s=172.16.47.161 (Serial0), d=171.68.200.48 (Serial1), g=172.16.47.145, len 100, forward
                                                    ICMP type=8, code=0
                              [NAT*: s=171.68.200.48->172.16.47.177, d=172.16.47.161 [16262
                              [NAT*: s=172.16.47.177, d=172.16.47.161->171.68.200.48 [16262
IP: s=172.16.47.177 (Serial1), d=171.68.200.48 (Serial0), g=171.68.200.48, len 100, forward
                                                    ICMP type=0, code=0
                                [NAT: s=171.68.200.48->172.16.47.161, d=172.16.47.177 [408
                                [NAT: s=172.16.47.161, d=172.16.47.177->171.68.200.48 [408
IP: s=172.16.47.161 (Serial0), d=171.68.200.48 (Serial1), g=172.16.47.145, len 100, forward
                                                    ICMP type=8, code=0
                              [NAT*: s=171.68.200.48->172.16.47.177, d=172.16.47.161 [16267
                              [NAT*: s=172.16.47.177, d=172.16.47.161->171.68.200.48 [16267
IP: s=172.16.47.177 (Serial1), d=171.68.200.48 (Serial0), g=171.68.200.48, len 100, forward
                                                    ICMP type=0, code=0
                                [NAT: s=171.68.200.48->172.16.47.161, d=172.16.47.177 [409
                                [NAT: s=172.16.47.161, d=172.16.47.177->171.68.200.48 [409
IP: s=172.16.47.161 (Serial0), d=171.68.200.48 (Serial1), g=172.16.47.145, len 100, forward
                                                    ICMP type=8, code=0
                              [NAT*: s=171.68.200.48->172.16.47.177, d=172.16.47.161 [16273
```

```
                                [NAT*: s=172.16.47.177, d=172.16.47.161->171.68.200.48 [16273
IP: s=172.16.47.177 (Serial1), d=171.68.200.48 (Serial0), g=171.68.200.48, len 100, forward
                                                          ICMP type=0, code=0
                                  [NAT: s=171.68.200.48->172.16.47.161, d=172.16.47.177 [410
                                  [NAT: s=172.16.47.161, d=172.16.47.177->171.68.200.48 [410
IP: s=172.16.47.161 (Serial0), d=171.68.200.48 (Serial1), g=172.16.47.145, len 100, forward
                                                          ICMP type=8, code=0
                                [NAT*: s=171.68.200.48->172.16.47.177, d=172.16.47.161 [16277
                                [NAT*: s=172.16.47.177, d=172.16.47.161->171.68.200.48 [16277
IP: s=172.16.47.177 (Serial1), d=171.68.200.48 (Serial0), g=171.68.200.48, len 100, forward
                                                          ICMP type=0, code=0
```

بمجرد اكتمال تبادل الحزم بين الخارج والداخل، يمكننا النظر إلى جدول الترجمة، والذي يحتوي على ثلاثة إدخالات. تم إنشاء الإدخال الأول عندما قام الجهاز الداخلي بإرسال استعلام DNS. تم إنشاء الإدخال الثاني عند ترجمة حمولة رد DNS. تم إنشاء الإدخال الثالث عندما تم تبادل إختبار الاتصال بين الجهاز الداخلي والجهاز الخارجي. الإدخال الثالث هو ملخص للإدخالين الأولين، ويستخدم للترجمة الأكثر كفاءة.

```
                                    Router-A# show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
                ---                ---      171.68.200.48      172.16.47.161 ---
 171.68.200.48      172.16.47.177               ---                ---  ---
 171.68.200.48      172.16.47.177      171.68.200.48      172.16.47.161 ---
```

من المهم ملاحظة أنه عندما تحاول إنشاء اتصال بين شبكتين متداخلتين بتشغيل NAT ديناميكي على موجه Cisco واحد، يجب أن تستخدم DNS لإنشاء ترجمة خارجية محلية إلى خارجية عامة. إن لا يستعمل أنت DNS، موصولية يستطيع كنت أسست مع ساكن إستاتيكي nat، غير أن هو أكثر صعوبة أن يدير.

معلومات ذات صلة

- صفحة دعم ترجمة عناوين الشبكة (NAT)
- الدعم الفني - Cisco Systems

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).