تكوين شبكة خاصة إلى خاصة لنفق IPsec ثابت و NAT باستخدام للموجه

المحتويات

المقدمة

يوضح هذا النموذج من التكوين كيفية:

- تشفير حركة المرور بين شبكتين خاصتين (x.10.1.1 و x.172.16.1).
- عينت عنوان ساكن إستاتيكي (عنوان خارجي 200.1.1.25) إلى شبكة أداة في 10.1.1.3.

أنت تستخدم قوائم التحكم في الوصول (ACLs) أن يخبر المسحاج تخديد ألا يقوم ترجمة عنوان الشبكة (NAT) إلى حركة مرور الشبكة من الخاص إلى الخاص، والتي يتم بعد ذلك تشفيرها ووضعها على النفق أثناء خروجه من الموجه. هناك أيضا NAT ساكن إستاتيكي لخادم داخلي على شبكة x.10.1.1 في هذا عينة تشكيل. يستخدم هذا التكوين العينة خيار خريطة المسار على الأمر nat لمنع كونه NAT إذا كانت حركة مرور له موجهة أيضا عبر النفق المشفر.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

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

- برنامج Cisco IOS® الإصدار 12.3(14)T من Cisco
- موجهات Cisco

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

الاصطلاحات

راجع اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.

لماذا تحدد عبارة الرفض في قائمة التحكم في الوصول حركة مرور NAT؟

أنت تقوم بشكل مفاهيمي باستبدال شبكة بنفق عندما تستخدم cisco IOS IPsec أو VPN. يمكنك إستبدال سحابة الإنترنت بنفق Cisco IOS IPsec الذي يتراوح من 200.1.1.1 إلى 100.1.1.1 في هذا المخطط. أجعل هذه الشبكة شفافة من وجهة نظر شبكتي LAN الخاصتين اللتين يتم ربطهما معا بواسطة النفق. أنت عادة لا تريد أن يستعمل NAT لحركة المرور أن يذهب من واحد خاص lan إلى البعيد خاص lan لهذا السبب. أنت تريد أن يرى الربط أن يأتي من المسحاج تخديد 2 شبكة مع مصدر عنوان من ال 24/10.1.1.0 شبكة instead of 200.1.1.1 عندما الربط يصل إلى الداخل مسحاج تخديد 3 شبكة.

أحلت nat ترتيب العملية ل كثير معلومة على كيف أن يشكل nat. يبدي هذا وثيقة أن ال NAT يحدث قبل ال crypto فحصت عندما الربط يذهب من الداخل إلى الخارج. هذا هو السبب في أنه يجب تحديد هذه المعلومات في التكوين.

```
ip nat inside source list 122 interface Ethernet0/1 overload
```

```
access-list 122 deny ip 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255
access-list 122 permit ip 10.1.1.0 0.0.0.255 any
```

ملاحظة: من الممكن أيضا بناء النفق والاستمرار في إستخدام NAT. أنت تعين ال nat حركة مرور ك "حركة مرور مهم ل IPsec" (يشار إليها ب ACL 101 في قسم آخر من هذا وثيقة) في هذا سيناريو. ارجع إلى تكوين نفق IPsec بين الموجهات التي تحتوي على شبكات LAN فرعية مكررة للحصول على مزيد من المعلومات حول كيفية إنشاء نفق أثناء تنشيط NAT.

ماذا عن NAT الساكن إستاتيكي، لماذا لا أستطيع الوصول إلى ذلك العنوان عبر نفق IPsec؟

يتضمن هذا إعداد أيضا NAT ساكن إستاتيكي واحد إلى واحد لخادم في 10.1.1.3. هذا NAT إلى 200.1.1.25 بحيث يمكن لمستخدمي الإنترنت الوصول إليه. قم بإصدار هذا الأمر:

```
ip nat inside source static 10.1.1.3 200.1.1.25
```

يمنع هذا NAT الثابت المستخدمين على شبكة x.172.16.1 من الوصول إلى 10.1.1.3 عبر النفق المشفر. هذا لأنك بحاجة إلى رفض أن تكون حركة المرور المشفرة NAT d مع قائمة التحكم في الوصول (ACL 122). مهما، ال ساكن إستاتيكي nat يأخذ أمر أسبقية على ال NAT عام جملة لكل توصيل إلى ومن 10.1.1.3. لا ينكر بيان NAT الساكن إستاتيكي بشكل خاص حركة المرور المشفرة من أن يكون أيضا NAT d. الردود من 10.1.1.3 هي NAT d إلى

200.1.1.25 عندما يتصل مستخدم على شبكة x.172.16.1 ب 10.1.1.3 وبالتالي لا يرجع عبر النفق المشفر (NAT يحدث قبل التشفير).

أنت ينبغي أنكر حركة المرور المشفرة من كونها NAT d (حتى ثابت واحد إلى واحد NAT-D) مع أمر **خريطة طريق** على بيان NAT ساكن إستاتيكي.

ملاحظة: يتم دعم خيار **خريطة الطريق** على NAT الثابت فقط من برنامج Cisco IOS الإصدار 12.2(4)T والإصدارات الأحدث. راجع NAT—القدرة على إستخدام خرائط المسار مع ترجمات ثابتة للحصول على معلومات إضافية.

أنت ينبغي أصدرت هذا أمر إضافي أن يسمح مشفر منفذ إلى 10.1.1.3، ال nat'd مضيف:

```
ip nat inside source static 10.1.1.3 200.1.1.25 route-map nonat
!
access-list 150 deny   ip host 10.1.1.3 172.16.1.0 0.0.0.255
access-list 150 permit ip host 10.1.1.3 any
!
route-map nonat permit 10
match ip address 150
```

تقول هذه البيانات للموجه أن يطبق فقط NAT الثابت على حركة المرور التي تطابق قائمة التحكم في الوصول (150 ACL). تقول قائمة التحكم في الوصول (150 ACL) إنه لا يجب تطبيق NAT على حركة المرور المستمدة من 10.1.1.3 والموجهة عبر النفق المشفر إلى x.172.16.1. ومع ذلك، قم بتطبيقه على جميع حركة المرور الأخرى المستمدة من 10.1.1.3 (حركة المرور المستندة إلى الإنترنت).

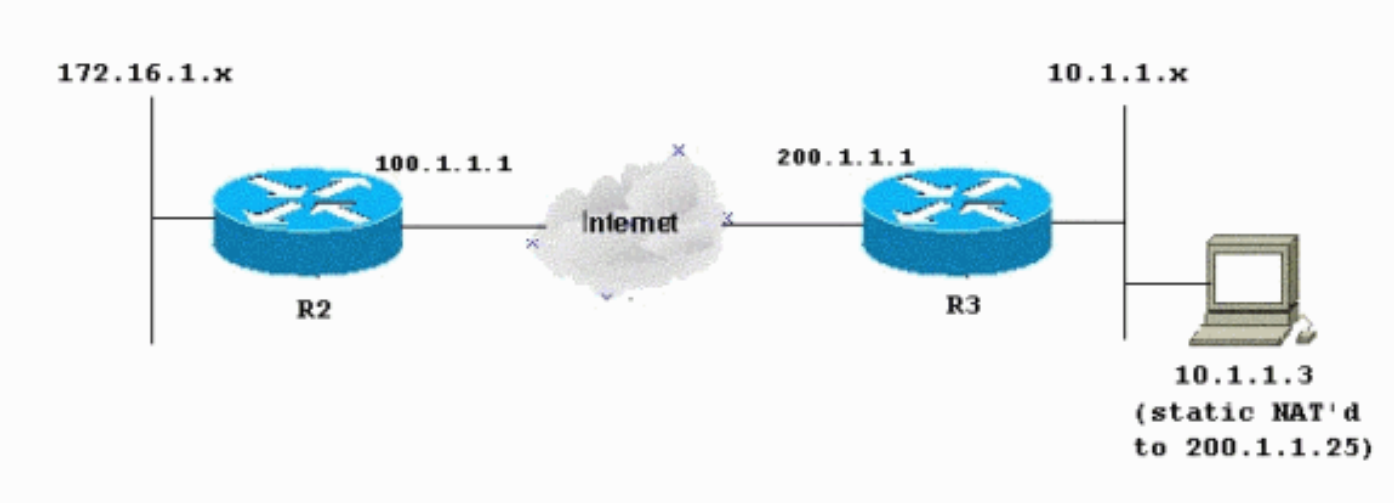
التكوين

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

ملاحظة: أستخدم أداة بحث الأوامر (للعملاء المسجلين فقط) للعثور على مزيد من المعلومات حول الأوامر المستخدمة في هذا المستند.

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي:



التكوينات

يستخدم هذا المستند التكوينات التالية:

- الموجه 2
- الموجه 3

R2 - تكوين الموجه

```
R2#write terminal
...Building configuration
Current configuration : 1412 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R2
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
resource policy
!
clock timezone EST 0
ip subnet-zero
no ip domain lookup
!
!
crypto isakmp policy 10
authentication pre-share
!
crypto isakmp key ciscokey address 200.1.1.1
!
!
crypto ipsec transform-set myset esp-3des esp-md5-hmac
!
crypto map myvpn 10 ipsec-isakmp
set peer 200.1.1.1
set transform-set myset
Include the private-network-to-private-network ---!
traffic !--- in the encryption process: match address
101
!
!
!
interface Ethernet0/0
ip address 172.16.1.1 255.255.255.0
ip nat inside
ip virtual-reassembly
!
interface Ethernet1/0
ip address 100.1.1.1 255.255.255.0
ip nat outside
ip virtual-reassembly
crypto map myvpn
!
ip classless
ip route 0.0.0.0 0.0.0.0 100.1.1.254
```

```
!
ip http server
no ip http secure-server
!
Except the private network from the NAT process: ip ---!
nat inside source list 175 interface Ethernet1/0
overload
!
    Include the private-network-to-private-network ---!
 traffic !--- in the encryption process: access-list 101
permit ip 172.16.1.0 0.0.0.255 10.1.1.0 0.0.0.255
  Except the private network from the NAT process: ---!
access-list 175 deny   ip 172.16.1.0 0.0.0.255 10.1.1.0
0.0.0.255
access-list 175 permit ip 172.16.1.0 0.0.0.255 any
!
!
!
control-plane
!
!
line con 0
exec-timeout 0 0
line aux 0
line vty 0 4
login
!
end
```

R3 - تكوين الموجه

```
R3#write terminal
...Building configuration
Current configuration : 1630 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R3
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
resource policy
!
clock timezone EST 0
ip subnet-zero
no ip domain lookup
!
crypto isakmp policy 10
authentication pre-share
crypto isakmp key ciscokey address 100.1.1.1
!
!
crypto ipsec transform-set myset esp-3des esp-md5-hmac
!
crypto map myvpn 10 ipsec-isakmp
set peer 100.1.1.1
```

```
 set transform-set myset
 Include the private-network-to-private-network ---!
traffic !--- in the encryption process: match address
101
!
!
!
interface Ethernet0/0
 ip address 10.1.1.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly
!
interface Ethernet1/0
 ip address 200.1.1.1 255.255.255.0
 ip nat outside
 ip virtual-reassembly
 crypto map myvpn
!
!
ip classless
ip route 0.0.0.0 0.0.0.0 200.1.1.254
!
no ip http server
no ip http secure-server
!
Except the private network from the NAT process: ip ---!
nat inside source list 122 interface Ethernet1/0
overload
 Except the static-NAT traffic from the NAT process ---!
 if destined !--- over the encrypted tunnel: ip nat
inside source static 10.1.1.3 200.1.1.25 route-map nonat
!
 access-list 101 permit ip 10.1.1.0 0.0.0.255 172.16.1.0
0.0.0.255
  Except the private network from the NAT process: ---!
 access-list 122 deny   ip 10.1.1.0 0.0.0.255 172.16.1.0
0.0.0.255
 access-list 122 permit ip 10.1.1.0 0.0.0.255 any
 Except the static-NAT traffic from the NAT process ---!
 if destined !--- over the encrypted tunnel: access-list
 150 deny   ip host 10.1.1.3 172.16.1.0 0.0.0.255
 access-list 150 permit ip host 10.1.1.3 any
!
route-map nonat permit 10
 match ip address 150
!
!
!
control-plane
!
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 login
!
end
```

التحقق من الصحة

لا يوجد حاليًا إجراء للتحقق من صحة هذا التكوين.

استكشاف الأخطاء وإصلاحها

أستخدم هذا القسم لاستكشاف أخطاء التكوين وإصلاحها.

راجع أستكشاف أخطاء أمان IP وإصلاحها - فهم أوامر تصحيح الأخطاء واستخدامها للحصول على معلومات إضافية.

أوامر استكشاف الأخطاء وإصلاحها

تدعم أداة مترجم الإخراج (للعملاءالمسجلين فقط) بعض أوامر **show**. استخدم أداة مترجم الإخراج (OIT) لعرض تحليل مُخرَج الأمر **show** .

ملاحظة: ارجع إلى معلومات مهمة حول أوامر التصحيح قبل إستخدام أوامر **debug**.

- **debug crypto ipSec** —يعرض مفاوضات IPsec للمرحلة 2.
- **debug crypto isakmp sa** —راجع مفاوضات ISAKMP للمرحلة الأولى.
- **debug crypto engine** — يعرض الجلسات المشفرة.

معلومات ذات صلة

- مفاوضة IPsec/بروتوكولات IKE - أنظمة Cisco
- الدعم التقني والمستندات - 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).