IOS مجوم نيوكت لاثم ىلع NAT عم IPSec/GRE

المحتويات

المقدمة

يوضح هذا النموذج من التكوين كيفية تكوين تضمين التوجيه العام (GRE) عبر أمان IP (IPSec) حيث يمر نفق GRE/IPSec عبر جدار حماية يقوم بترجمة عنوان الشبكة (NAT).

قبل البدء

الاصطلاحات

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

المتطلبات الأساسية

يمكن إستخدام هذا النوع من التكوين لتوصيل حركة المرور وتشفيرها والتي لا تمر عادة عبر جدار حماية، مثل IPX (كما في المثال الخاص بنا هنا) أو تحديثات التوجيه. في هذا المثال، يعمل النفق بين 2621 و 3660 فقط عندما يتم إنشاء حركة مرور البيانات من الأجهزة الموجودة على مقاطع الشبكة المحلية (ليس إختبار اتصال IP/IPX موسع من موجهات IPSec). تم إختبار اتصال IP/IPX باستخدام اتصال IP/IPX بين الجهازين 2513a و 2513b.

ملاحظة: لا يعمل هذا مع ترجمة عنوان أيسر (ضرب).

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية أدناه.

- Cisco IOS®، الإصدار 12.4
- جدار حماية Cisco PIX 535
- برنامج جدار حماية PIX الإصدار x.7 من Cisco والإصدارات الأحدث

تم إنشاء المعلومات المُقدمة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كنت تعمل في شبكة مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر قبل استخدامه.

التكوين

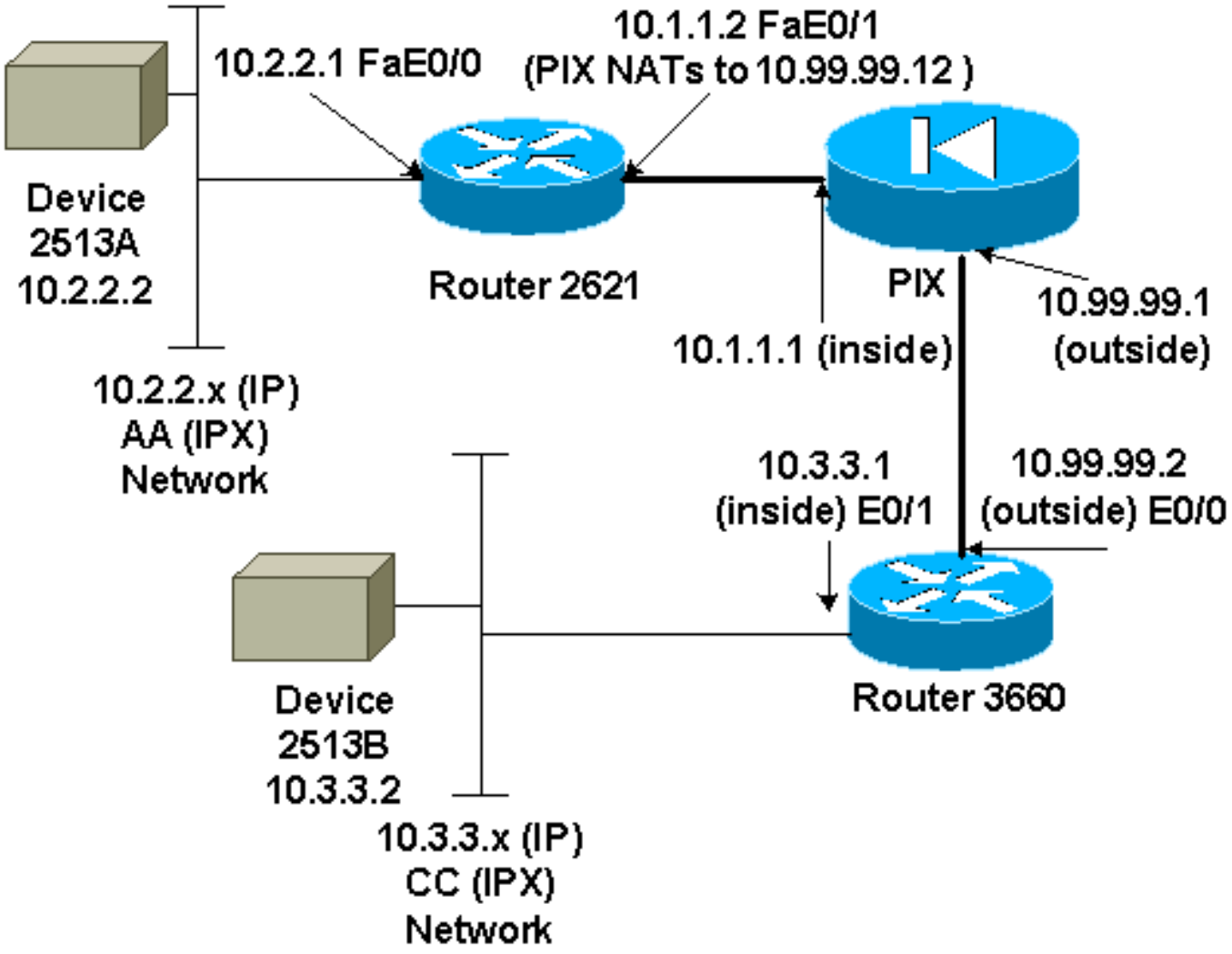
في هذا القسم، تُقدّم لك معلومات تكوين الميزات الموضحة في هذا المستند.

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

ملاحظة تكوين IOS: باستخدام برنامج Cisco IOS 12.2(13)T والرموز الأحدث (رموز t-train الأعلى ترقما، و 12.3 والرموز الأحدث) لا يلزم تطبيق "خريطة التشفير" ل IPsec التي تم تكوينها إلا على الواجهة المادية ولم يعد مطلوبا لتطبيقها على واجهة نفق GRE. لا يزال وجود "خريطة التشفير" على الواجهة المادية وواجهة النفق عند إستخدام 12.2.(13)T والرموز اللاحقة يعمل. ومع ذلك، يوصى بشدة بتطبيقه فقط على الواجهة المادية.

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة الموضح في الرسم التخطيطي أدناه.



ملاحظة: عناوين IP المستخدمة في هذا التكوين غير قابلة للتوجيه بشكل قانوني على الإنترنت. هم rfc 1918 عنوان أن يتلقى يكون استعملت في مختبر بيئة.

ملاحظات الرسم التخطيطي للشبكة

- نفق GRE من 10.2.2.1 إلى 10.3.3.1 (شبكة IPX BB)
- نفق IPSec من 10.1.1.2 (10.99.99.12) إلى 10.99.99.2

التكوينات

جهاز 2513a

```
ipx routing 00e0.b064.20c1
!
interface Ethernet0
ip address 10.2.2.2 255.255.255.0
 no ip directed-broadcast
 ipx network AA
!
ip route 0.0.0.0 0.0.0.0 10.2.2.1
Output Suppressed ---!
```

2621

```
version 12.4
service timestamps debug uptime
 service timestamps log uptime
 no service password-encryption
!
hostname 2621
!
ip subnet-zero
!
ip audit notify log
ip audit po max-events 100
ipx routing 0030.1977.8f80
 isdn voice-call-failure 0
  cns event-service server
!
crypto isakmp policy 10
 hash md5
 authentication pre-share
crypto isakmp key cisco123 address 10.99.99.2
!
crypto ipsec transform-set myset esp-des esp-md5-hmac
!
crypto map mymap local-address FastEthernet0/1
crypto map mymap 10 ipsec-isakmp
 set peer 10.99.99.2
 set transform-set myset
  match address 101
!
 controller T1 1/0
!
interface Tunnel0
ip address 192.168.100.1 255.255.255.0
 no ip directed-broadcast
 ipx network BB
tunnel source FastEthernet0/0
 tunnel destination 10.3.3.1
```

```
crypto map mymap
!
interface FastEthernet0/0
ip address 10.2.2.1 255.255.255.0
no ip directed-broadcast
duplex auto
speed auto
ipx network AA
!
interface FastEthernet0/1
ip address 10.1.1.2 255.255.255.0
no ip directed-broadcast
duplex auto
speed auto
crypto map mymap
!
ip classless
ip route 10.3.3.0 255.255.255.0 Tunnel0
ip route 10.3.3.1 255.255.255.255 10.1.1.1
ip route 10.99.99.0 255.255.255.0 10.1.1.1
no ip http server
!
access-list 101 permit gre host 10.2.2.1 host 10.3.3.1
!
line con 0
transport input none
line aux 0
line vty 0 4
!
no scheduler allocate
end

Output Suppressed ---!
```

PIX

```
pixfirewall# sh run
Saved :
:
PIX Version 7.0
!
hostname pixfirewall
enable password 2KFQnbNIdI.2KYOU encrypted
names
!
interface Ethernet0
nameif outside
security-level 0
ip address 10.99.99.1 255.255.255.0
!
interface Ethernet1
nameif inside
security-level 100
ip address 10.1.1.1 255.255.255.0
!
global (outside) 1 10.99.99.50-10.99.99.60
nat (inside) 1 0.0.0.0 0.0.0.0 0 0

static (inside,outside) 10.99.99.12 10.1.1.2 netmask
255.255.255.255 0 0
access-list 102 permit esp host 10.99.99.12 host
10.99.99.2
access-list 102 permit udp host 10.99.99.12 host
```

```
10.99.99.2 eq isakmp


route outside 0.0.0.0 0.0.0.0 10.99.99.2 1
route inside 10.2.2.0 255.255.255.0 10.1.1.2 1

Output Suppressed ---!
```

3660

```
version 12.4
service timestamps debug datetime
service timestamps log uptime
no service password-encryption
!
hostname 3660
!
memory-size iomem 30
ip subnet-zero
no ip domain-lookup
!
ipx routing 0030.80f2.2950
cns event-service server
!
crypto isakmp policy 10
 hash md5
 authentication pre-share
crypto isakmp key cisco123 address 10.99.99.12
!
crypto ipsec transform-set myset esp-des esp-md5-hmac
!
crypto map mymap local-address FastEthernet0/0
crypto map mymap 10 ipsec-isakmp
 set peer 10.99.99.12
 set transform-set myset
 match address 101
!
interface Tunnel0
 ip address 192.168.100.2 255.255.255.0
 no ip directed-broadcast
 ipx network BB
 tunnel source FastEthernet0/1
 tunnel destination 10.2.2.1
 crypto map mymap
!
interface FastEthernet0/0
 ip address 10.99.99.2 255.255.255.0
 no ip directed-broadcast
 ip nat outside
 duplex auto
 speed auto
 crypto map mymap
!
interface FastEthernet0/1
 ip address 10.3.3.1 255.255.255.0
 no ip directed-broadcast
 ip nat inside
 duplex auto
 speed auto
 ipx network CC
!
ip nat pool 3660-nat 10.99.99.70 10.99.99.80 netmask
255.255.255.0
```

```
ip nat inside source list 1 pool 3660-nat
                                 ip classless
                  ip route 0.0.0.0 0.0.0.0 Tunnel0
          ip route 10.2.2.1 255.255.255.255 10.99.99.1
       ip route 10.99.99.12 255.255.255.255 10.99.99.1
                                 no ip http server
                                                  !
        access-list 1 permit 10.3.3.0 0.0.0.255
access-list 101 permit gre host 10.3.3.1 host 10.2.2.1
                                                  !
                                       line con 0
                              transport input none
                                       line aux 0
                                    line vty 0 4
                                           login
                                                  !
                                             end
                                 Output Suppressed ---!
```

جهاز 2513b

```
                                 ipx routing 00e0.b063.e811
                                                  !
                                  interface Ethernet0
                          ip address 10.3.3.2 255.255.255.0
                              no ip directed-broadcast
                                    ipx network CC
                                                  !
                          ip route 0.0.0.0 0.0.0.0 10.3.3.1

                                 Output Suppressed ---!
```

التحقق من الصحة

يوفر هذا القسم معلومات يمكنك إستخدامها للتأكد من أن التكوين يعمل بشكل صحيح.

يتم دعم بعض أوامر **العرض بواسطة** أداة مترجم الإخراج (العملاء المسجلون فقط)، والتي تتيح لك عرض تحليل إخراج أمر **العرض**.

- show crypto ips sa - يعرض اقترانات أمان المرحلة 2.
- show crypto isakmp sa - يعرض إتصالات الجلسة المشفرة النشطة الحالية لجميع محركات التشفير.
- إختياري: show interfaces tunnel *number* - *يعرض معلومات واجهة النفق*.
- show ip route - يعرض جميع مسارات IP الثابتة، أو تلك التي تم تثبيتها باستخدام وظيفة تنزيل المسار (AAA) (المصادقة والتفويض والمحاسبة).
- show ipx route - يعرض محتويات جدول توجيه IPX.

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

أوامر استكشاف الأخطاء وإصلاحها

يتم دعم بعض أوامر **العرض بواسطة** أداة مترجم الإخراج (العملاء المسجلون فقط)، والتي تتيح لك عرض تحليل إخراج أمر **العرض**.

ملاحظة: قبل إصدار أوامر **تصحيح الأخطاء**، يرجى الاطلاع على المعلومات المهمة في أوامر تصحيح الأخطاء.

- debug crypto Engine - يعرض حركة مرور البيانات التي يتم تشفيرها.
- debug crypto ipSec - يعرض مفاوضات IPSec للمرحلة 2.
- debug crypto isakmp - يعرض مفاوضات بروتوكول إدارة المفاتيح وارتباط أمان الإنترنت (ISAKMP) للمرحلة الأولى.
- إختياري: debug ip routing - *يعرض معلومات حول تحديثات جدول توجيه بروتوكول معلومات التوجيه (RIP) وتحديثات ذاكرة التخزين المؤقت للمسار.*
- {debug ipx routing {activity | events - تصحيح أخطاء توجيه IPX {activity | events} - يعرض معلومات حول حزم توجيه IPX التي يرسلها الموجه ويستلمها.

إزالة اقترانات الأمان (SAs)

- مسح بروتوكول IPSEC ل Crytpo SA - مسح جميع اقترانات أمان IPSec.
- مسح التشفير isakmp - مسح اقترانات أمان IKE.
- *إختياريا:* مسح مسار IPX * - يحذف جميع المسارات من جدول توجيه IPX.

معلومات ذات صلة

- صفحات دعم منتجات أمان IP (IPSec)
- صفحات دعم GRE
- 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).