PIX 6.x: مرور نفق IPsec عبر جدار حماية PIX باستخدام قائمة الوصول والتكوين الخاص بـ NAT

المحتويات

المقدمة

يزود هذا وثيقة عينة تشكيل ل IPSec نفق من خلال جدار حماية أن ينجز شبكة عنوان ترجمة (NAT). **لا يعمل هذا التكوين مع ترجمة عنوان المنفذ (PAT) إذا كنت تستخدم إصدارات برنامج Cisco IOS® قبل ولا تتضمن 12.2(13)T.** يمكن إستخدام هذا النوع من التكوين لتنفق حركة مرور IP. لا يمكن إستخدام هذا لتشفير حركة المرور التي لا تمر عبر جدار حماية، مثل تحديثات التوجيه أو IPX. يعد الاتصال النفقي للتوجيه العام (GRE) مناسبا لهذا النوع من التكوين. في المثال في هذا المستند، تمثل موجهات Cisco 2621 و 3660 نقاط النهاية لنفق IPSec التي تنضم إلى شبكتين خاصتين، مع قنوات أو قوائم التحكم في الوصول (ACLs) على PIX التي تقع بينهما للسماح بحركة مرور IPSec.

ملاحظة: NAT هي ترجمة العنوان من فرد إلى آخر، ولا ينبغي الخلط بينها وبين PAT، وهي ترجمة عديدة (داخل جدار الحماية) إلى واحد. راجع التحقق من عملية NAT واستكشاف أخطاء NAT الأساسية وإصلاحها أو كيفية عمل NAT للحصول على مزيد من المعلومات حول عملية NAT وتكوينها.

ملاحظة: قد لا يعمل IPSec مع PAT بشكل صحيح لأن جهاز نقطة نهاية النفق الخارجي لا يمكنه معالجة أنفاق متعددة من عنوان IP واحد. تحتاج إلى الاتصال بموردك لتحديد ما إذا كانت أجهزة نقطة نهاية النفق تعمل مع PAT أم لا. بالإضافة إلى ذلك، في الإصدارات 12.2(13)T والإصدارات الأحدث، يمكن إستخدام ميزة شفافية NAT أيضا من أجل PAT. راجع شفافية IPSec NAT للحصول على مزيد من المعلومات. راجع دعم IPSec ESP من خلال NAT للحصول على مزيد من المعلومات حول هذه الميزات في الإصدار 12.2(13)T والإصدارات الأحدث. أيضا، قبل أن تفتح حالة مع TAC، ارجع إلى NAT غالبا أسئلة، والتي لها العديد من الإجابات على الأسئلة المشتركة.

ارجع إلى مرور نفق IPsec عبر جهاز أمان باستخدام قائمة الوصول و MPF مع مثال تكوين NAT للحصول على مزيد من المعلومات حول كيفية تكوين نفق IPSec من خلال جدار حماية باستخدام NAT على PIX/ASA الإصدار 7.x.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

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

- برنامج IOS الإصدار T.12.0.7 من Cisco [يصل إلى 12.2(13)T دون تضمينه]راجع شفافية IPSec NAT للحصول على إصدارات أحدث.
- الموجه 2621 من Cisco الذي يشغل برنامج Cisco IOS، الإصدار 12.4
- الموجه Cisco 3660 الذي يشغل برنامج Cisco IOS، الإصدار 12.4
- جدار حماية Cisco PIX الذي يشغل الإصدار x.6

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.

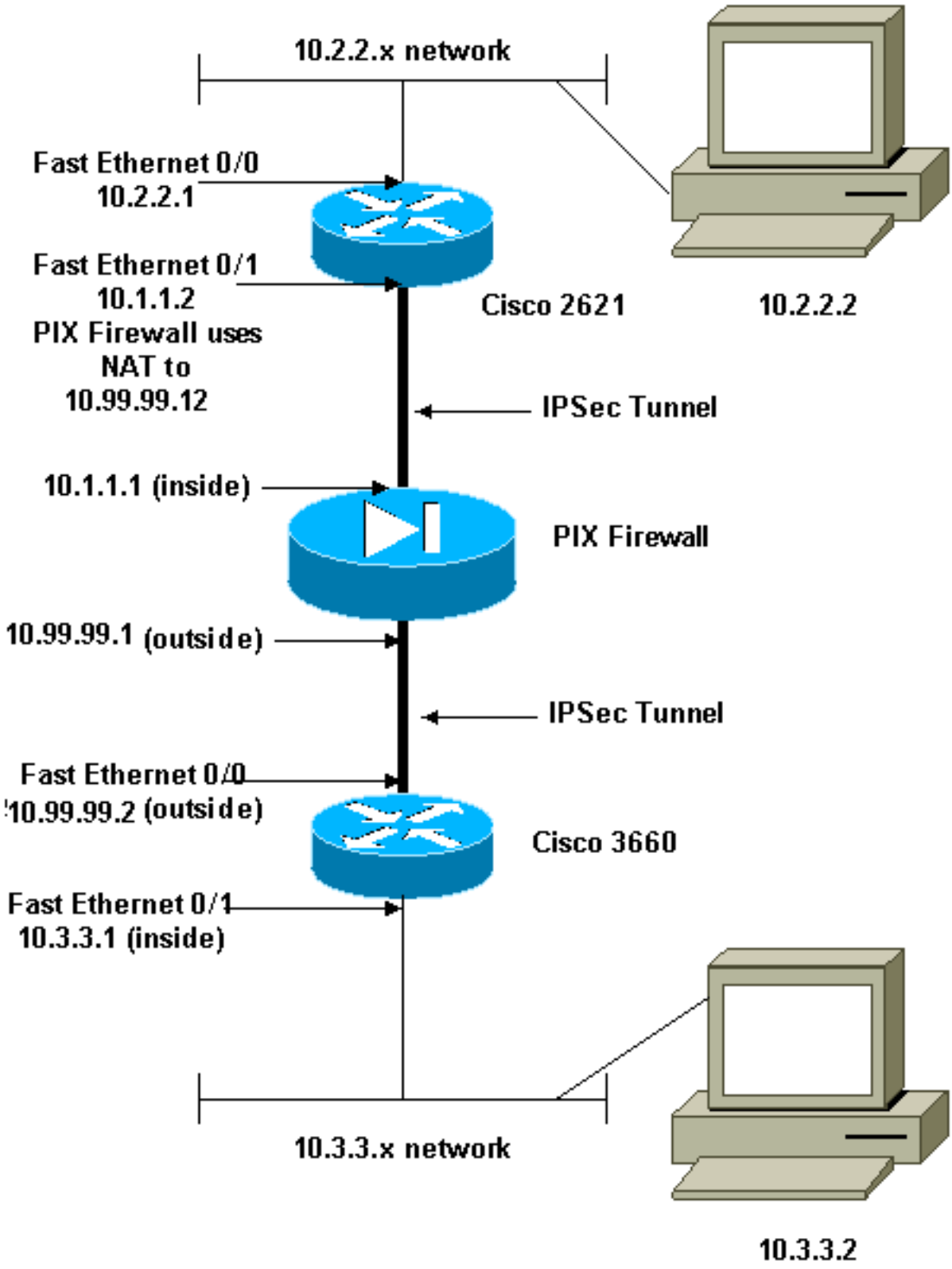
التكوين

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:



ملاحظة: ال ip ليس يخاطب خطة يستعمل في هذا تشكيل قانونيا routable على الإنترنت. هذا rfc 1918 عنوان أي يتلقى يكون استعملت في مختبر بيئة.

التكوينات

يستخدم هذا المستند التكوينات التالية:

- تكوين Cisco 2621
- التكوين الجزئي لجدار حماية PIX من Cisco
- تكوين Cisco 3660

تكوين Cisco 2621

```
Current configuration:
!
version 12.4
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname goss-2621
!
ip subnet-zero
!
ip audit notify log
ip audit po max-events 100
isdn voice-call-failure 0
cns event-service server
!
crypto isakmp policy 10 !--- IKE Policy
 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 !--- IPSec Policy
 set peer 10.99.99.2
 set transform-set myset
 match address 101 !--- Include the private-network-to-private-network
!--- traffic in the encryption process.
!
controller T1 1/0
!
interface FastEthernet0/0
 ip address 10.2.2.1 255.255.255.0
 no ip directed-broadcast
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 10.1.1.2 255.255.255.0
 no ip directed-broadcast
 duplex auto
 speed auto
 crypto map mymap !--- Apply to interface.
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.1.1.1
no ip http server
access-list 101 permit ip 10.2.2.0 0.0.0.255 10.3.3.0 0.0.0.255 !--- Include the private-network-to-private-network
!--- traffic in the encryption process.
line con 0
 transport input none
line aux 0
line vty 0 4
!
no scheduler allocate
end
```

التكوين الجزئي لجدار حماية PIX من Cisco

```
fixup protocol dns maximum-length 512
fixup protocol ftp 21
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol http 80
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol sip 5060
fixup protocol sip udp 5060
fixup protocol skinny 2000
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol tftp 69
The fixup protocol esp-ike command is disabled by ---!
.default

fixup protocol esp-ike

ip address outside 10.99.99.1 255.255.255.0
ip address inside 10.1.1.1 255.255.255.0
Range of registered IP addresses for use. global ---!
(outside) 1 10.99.99.50-10.99.99.60 !--- Translate any
internal source address when !--- going out to the
Internet. 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

or access-list acl-out permit esp host 10.99.99.2 ---!
host 10.99.99.12
access-list acl-out permit udp host 10.99.99.2 host
10.99.99.12 eq isakmp
access-list acl-out permit udp host 10.99.99.2 host
10.99.99.12 eq 4500
It is important to permit UDP port 4500 for NAT-T ---!
because the PIX is acting !--- as a NAT device between
the routers. access-group acl-out in interface outside
isakmp enable outside isakmp enable inside Command
configured in order to enable NAT-T isakmp nat-traversal
20 route outside 0.0.0.0 0.0.0.0 99.99.99.2 1 route
inside 10.2.2.0 255.255.255.0 10.1.1.2 1
```

ملاحظة: يتم تعطيل الأمر **fix protocol esp-ike** بشكل افتراضي. إذا تم إصدار أمر **إصلاح بروتوكول esp-ike**، يتم تشغيل الإصلاح، ويحافظ جدار حماية PIX على منفذ المصدر الخاص بتبادل مفتاح الإنترنت (IKE). كما أنها تنشئ ترجمة PAT لحركة مرور ESP. وبالإضافة إلى ذلك، إذا كان إصلاح esp-ike قيد التشغيل، لا يمكن تمكين اقتران أمان الإنترنت وبروتوكول إدارة المفاتيح (ISAKMP) على أي واجهة.

تكوين Cisco 3660

```
version 12.4
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname goss-3660
!
ip subnet-zero
!
cns event-service server
!
IKE Policy 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
IPSec Policy crypto map mymap 10 ipsec-isakmp ---!
set peer 10.99.99.12
set transform-set myset
Include the private-network-to-private-network ---!
traffic !--- in the encryption process. match address
101
!
interface FastEthernet0/0
ip address 10.99.99.2 255.255.255.0
no ip directed-broadcast
ip nat outside
duplex auto
speed auto
Apply to interface. 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
!
interface Ethernet3/0
no ip address
no ip directed-broadcast
shutdown
!
interface Serial3/0
no ip address
no ip directed-broadcast
no ip mroute-cache
shutdown
!
interface Ethernet3/1
no ip address
no ip directed-broadcast
interface Ethernet4/0
no ip address
no ip directed-broadcast
shutdown
!
interface TokenRing4/0
no ip address
no ip directed-broadcast
shutdown
ring-speed 16
!
Pool from which inside hosts translate to !--- the ---!
globally unique 10.99.99.0/24 network. ip nat pool
OUTSIDE 10.99.99.70 10.99.99.80 netmask 255.255.255.0
Except the private network from the NAT process. ---!
ip nat inside source route-map nonat pool OUTSIDE
ip classless
ip route 0.0.0.0 0.0.0.0 10.99.99.1
no ip http server
!
Include the private-network-to-private-network ---!
```

```
traffic !--- in the encryption process. access-list 101
        permit ip 10.3.3.0 0.0.0.255 10.2.2.0 0.0.0.255
     access-list 101 deny   ip 10.3.3.0 0.0.0.255 any
 Except the private network from the NAT process. ---!
 access-list 110 deny   ip 10.3.3.0 0.0.0.255 10.2.2.0
                                              0.0.0.255
     access-list 110 permit ip 10.3.3.0 0.0.0.255 any
                            route-map nonat permit 10
                                match ip address 110
                                                   !
                                         line con 0
                                transport input none
                                         line aux 0
                                       line vty 0 4
                                                   !
                                                 end
```

التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

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

- **show crypto ips sa**—يعرض اقترانات أمان المرحلة 2.
- **show crypto isakmp sa**—يعرض اقترانات أمان المرحلة 1.
- **show crypto engine connections active**—أستخدم لعرض الحزم المشفرة وغير المشفرة.

استكشاف الأخطاء وإصلاحها

أستخدم هذا القسم لاستكشاف أخطاء التكوين وإصلاحها.

أوامر استكشاف الأخطاء وإصلاحها

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

- **debug crypto engine**—يعرض حركة مرور البيانات التي يتم تشفيرها.
- **debug crypto ipSec**—أستخدم للاطلاع على مفاوضات IPSec الخاصة بالمرحلة 2.
- **debug crypto isakmp**—أستخدم للاطلاع على مفاوضات ISAKMP الخاصة بالمرحلة 1.

التخلص من الرابطات الأمنية

- **مسح تشفير isakmp**—مسح جمعيات أمان IKE.
- **مسح** اقترانات أمان IPSec **للتشفير** عبر **IPsec**.

معلومات ذات صلة

- أجهزة الأمان Cisco PIX 500 Series Security Appliances
- مراجع أوامر جدار حماية PIX الآمن من Cisco
- صفحة دعم ترجمة عناوين الشبكة (NAT)

- طلب التعليقات (RFCs)
- 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).