PIX 6.x: بروتوكول IPsec الديناميكي بين جدار حماية PIX ذي عنوان ثابت وموجه IOS الذي يتم توجيهه ديناميكيا مع مثال تكوين NAT

المحتويات

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

المقدمة

يقدم هذا المستند نموذجا لتكوين كيفية تمكين PIX من قبول إتصالات IPsec الديناميكية. يجري الموجه عن بعد ترجمة عنوان الشبكة (NAT) إذا وصلت الشبكة الخاصة x.10.1.1 إلى الإنترنت. يتم إستبعاد حركة المرور من x.10.1.1 إلى الشبكة الخاصة x.192.168.1 خلف PIX من عملية NAT. يمكن للموجه بدء الاتصالات ب PIX، ولكن PIX لا يمكنه بدء الاتصالات بالموجه.

يستخدم هذا التكوين جدار حماية PIX لإنشاء أنفاق ديناميكية لشبكة LAN إلى شبكة LAN (L2L) عبر بروتوكول IPsec باستخدام موجه Cisco IOS® الذي يستقبل عناوين IP الديناميكية على الواجهة العامة الخاصة به (خارج الواجهة). يوفر بروتوكول تكوين الاستضافة الديناميكية (DHCP) آلية من أجل تخصيص عناوين IP بشكل ديناميكي من مزود الخدمة (ISP). وهذا يسمح بإعادة إستخدام عناوين IP عندما لا تعود البيئات المضيفة بحاجة إليها.

ارجع إلى IPsec من الموجه إلى PIX الديناميكي إلى الثابت مع مثال تكوين NAT للحصول على مزيد من المعلومات حول سيناريو حيث يقبل الموجه إتصالات IPsec الديناميكية من جهاز أمان PIX الذي يشغل x.6.

ارجع إلى IPsec بين موجه IOS ثابت وموجه PIX/ASA 7.x ديناميكي مع مثال تكوين NAT لتمكين جهاز أمان PIX/ASA لقبول إتصالات IPsec الديناميكية من موجه Cisco IOS.

ارجع إلى IPsec بين PIX/ASA 7.x ثابت وموجه IOS الديناميكي مع مثال تكوين NAT لمعرفة المزيد حول نفس السيناريو حيث يقوم جهاز أمان PIX/ASA بتشغيل الإصدار x.7 من البرنامج والإصدارات الأحدث.

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 12.4 من Cisco
- برنامج جدار حماية Cisco PIX الإصدار 6.3.1
- جدار حماية PIX الآمن من Cisco طراز 515E
- موجّه Cisco 7206

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة 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.

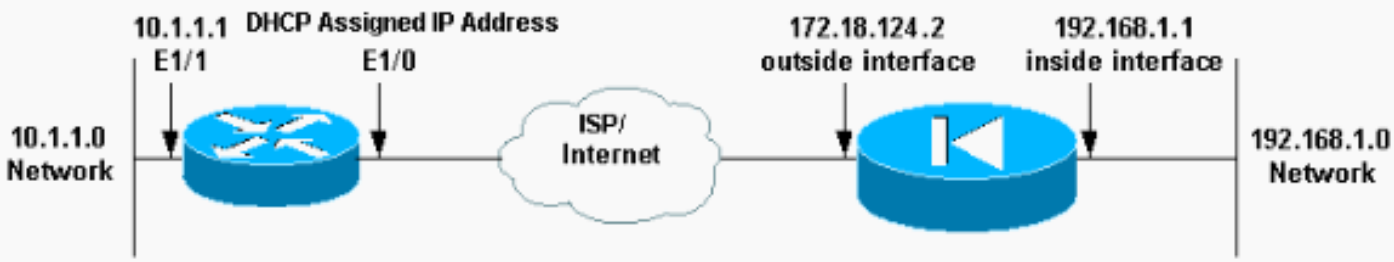
التكوين

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.



التكوينات

يستخدم هذا المستند هذه التكوينات.

- (ELF (PIX
- MOP (الموجه 7204 من Cisco)

(ELF (PIX
`...Building configuration`

```
Saved :
:
(PIX Version 6.3(1
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 intf2 security10
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname elf
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
fixup protocol skinny 2000
names
Access control list (ACL) to avoid NAT on the IPsec ---!
packets. access-list nonat permit ip 192.168.1.0
255.255.255.0 10.1.1.0 255.255.255.0
pager lines 24
logging on
logging buffered debugging
interface ethernet0 auto
interface ethernet1 auto
interface ethernet2 auto shutdown
mtu outside 1500
mtu inside 1500
mtu intf2 1500
ip address outside 172.18.124.2 255.255.255.0
ip address inside 192.168.1.1 255.255.255.0
ip address intf2 127.0.0.1 255.255.255.255
ip audit info action alarm
ip audit attack action alarm
no failover
failover timeout 0:00:00
failover poll 15
failover ip address outside 0.0.0.0
failover ip address inside 0.0.0.0
failover ip address intf2 0.0.0.0
pdm history enable
arp timeout 14400
global (outside) 1 interface
Binds ACL nonat to the NAT statement to avoid NAT on --!
the IPsec packets nat (inside) 0 access-list nonat
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
Permits Internet Control Message Protocol (ICMP) ---!
traffic for testing. !--- Do not enable it in a live
network. conduit permit icmp any any
route outside 0.0.0.0 0.0.0.0 172.18.124.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc
0:10:00
h323 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
+aaa-server TACACS+ protocol tacacs
aaa-server RADIUS protocol radius
+aaa-server LOCAL protocol tacacs
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
```

```
floodguard enable
sysopt connection permit-ipsec
no sysopt route dnat
IPsec configuration crypto ipsec transform-set ---!
router-set esp-des esp-md5-hmac
crypto dynamic-map cisco 1 set transform-set router-set
crypto map dyn-map 10 ipsec-isakmp dynamic cisco
crypto map dyn-map interface outside
isakmp enable outside
Internet Security Association and Key Management ---!
Protocol (ISAKMP) !--- policy for accepting dynamic
connections from remote PIX. !--- Note: In real show run
output, the pre-shared key appears as *******. isakmp
key cisco123 address 0.0.0.0 netmask 0.0.0.0
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption des
isakmp policy 10 hash md5
isakmp policy 10 group 1
isakmp policy 10 lifetime 86400
telnet timeout 5
ssh timeout 5
terminal width 80
Cryptochecksum:eeb67d5df47045f7e6ac4aa090aab683
end :
[OK]
#elf
```

MOP (الموجه 7204 من Cisco)

```
mop#show running-configuration
...Building configuration

Current configuration : 1916 bytes
!
version 12.4
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname mop
!
!
ip subnet-zero
!
!
no ip domain-lookup
!
ip cef
ip audit notify log
ip audit po max-events 100
!
Internet Key Exchange (IKE) policies crypto isakmp ---!
policy 1
hash md5
authentication pre-share
crypto isakmp key cisco123 address 172.18.124.2
!
!
IPsec policies crypto ipsec transform-set pix-set ---!
esp-des esp-md5-hmac
!
crypto map pix 10 ipsec-isakmp
set peer 172.18.124.2
```

```
set transform-set pix-set
match address 101
!
interface FastEthernet0/0
no ip address
shutdown
duplex half
!
interface Ethernet1/0
ip address dhcp
ip nat outside
duplex half
crypto map pix
!
interface Ethernet1/1
ip address 10.1.1.1 255.255.255.0
ip nat inside
duplex half
!
Except the private network from the NAT process. ip ---!
nat inside source route-map nonat interface Ethernet1/0
overload
ip classless
ip route 0.0.0.0 0.0.0.0 Ethernet1/0
no ip http server
ip pim bidir-enable
!
Include the private-network-to-private-network !--- ---!
traffic in the encryption process. access-list 101
permit ip 10.1.1.0 0.0.0.255 192.168.1.0 0.0.0.255
Except the private network from the NAT process. ---!
access-list 110 deny ip 10.1.1.0 0.0.0.255 192.168.1.0
0.0.0.255
access-list 110 permit ip 10.1.1.0 0.0.0.255 any
!
route-map nonat permit 10
match ip address 110
!
line con 0
exec-timeout 0 0
line aux 0
line vty 0 4
login
!
!
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** .

أنت يستطيع ركضت هذا **عرض** أمر على ال PIX وعلى المسحاج تخديد.

- **show crypto isakmp sa**— يعرض جميع اقترانات أمان IKE الحالية (SAs) في نظير.
- **show crypto ipSec**—يعرض الإعدادات المستخدمة من قبل IPsec) SAs) الحالية.
- **show crypto engine connections active**—يعرض الاتصالات والمعلومات الحالية المتعلقة بالحزم المشفرة

وغير المشفرة (الموجه فقط).
يجب مسح SAs على كلا الأقران.

- يتم تنفيذ أوامر PIX في وضع التكوين.**مسح التشفير sa** isakmp—يمحو المرحلة 1 من SAs.**مسح تشفير IPsec**—يمحو المرحلة 2 SAs.
- يتم تنفيذ أوامر الموجه في وضع التمكين.**مسح التشفير isakmp**—يمحو المرحلة 1 من SAs.**مسح التشفير sa**—يمسح المرحلة 2 SAs.

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

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**.

- **show crypto isakmp sa**— يعرض جميع شبكات IKE الحالية في نظير.
- **show crypto ipSec**—يعرض الإعدادات المستخدمة من قبل IPsec) SAs) الحالية.
- **show crypto engine connections active**—يعرض الاتصالات والمعلومات الحالية المتعلقة بالحزم المشفرة وغير المشفرة (الموجه فقط).

معلومات ذات صلة

- صفحة دعم مفاوضة IPsec/بروتوكولات IKE
- أجهزة الأمان PIX 500 Series Security Appliances
- مراجع أوامر جدار حماية PIX الآمن من Cisco
- طلبات 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).