PIX 6.x: بروتوكول IPsec الديناميكي بين جدار حماية PIX وموجه IOS بشكل ثابت وجدار حماية PIX وموجه IOS الذي يتم معالجته ديناميكيا مع مثال تكوين NAT

المحتويات

المقدمة

يقدم هذا المستند نموذجا لتكوين يوضح لك كيفية تمكين موجه IOS® لقبول إتصالات IPsec الديناميكية من جدار حماية PIX. يجري الموجه عن بعد ترجمة عنوان الشبكة (NAT) إذا وصلت الشبكة الخاصة x.10.0.0 إلى الإنترنت. استثنيت حركة المرور من x.10.0.0 إلى الشبكة الخاصة x.10.1.0 خلف PIX من عملية NAT. يمكن لجدار حماية PIX بدء الاتصالات بالموجه، ولكن الموجه لا يمكنه بدء الاتصالات ب PIX.

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

ارجع إلى PIX 6.x: IPsec الديناميكي بين جدار حماية PIX بعنوان ثابت وموجه IOS الذي يتم توجيهه ديناميكيا باستخدام مثال تكوين NAT للحصول على مزيد من المعلومات حول السيناريو الذي يقبل فيه PIX إتصالات IPsec الديناميكية من الموجه.

ارجع إلى PIX/ASA 7.x والإصدارات الأحدث: بروتوكول IPsec الديناميكي بين بروتوكول PIX معنونة بشكل ثابت وموجه IOS موجه موجه IOS موجه ديناميكي مع مثال تكوين NAT لتمكين جهاز أمان PIX/ASA من قبول إتصالات IPsec الديناميكية من موجه IOS.

ارجع إلى PIX/ASA 7.x والإصدارات الأحدث: بروتوكول IPsec الديناميكي بين موجه IOS تمت معالجته بشكل ثابت ومنفذ PIX تمت معالجته ديناميكيا مع مثال تكوين NAT لمعرفة المزيد حول نفس السيناريو الذي يشغل فيه جهاز

أمان PIX/ASA الإصدار x.7 والإصدارات الأحدث من البرنامج.

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 6.3.4
- جدار حماية PIX الآمن من Cisco طراز 515E
- موجّه Cisco 2811

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.

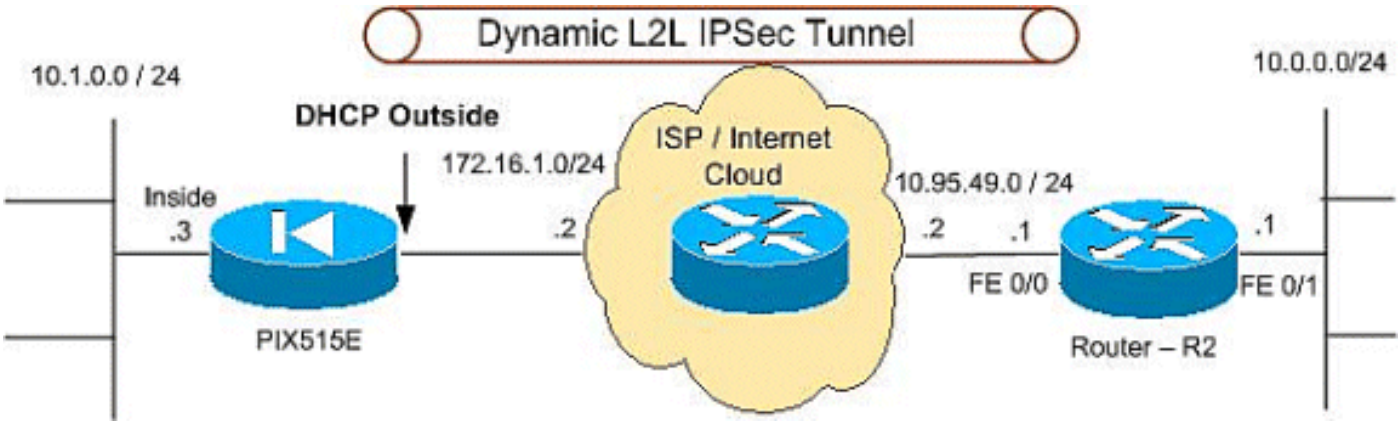
التكوين

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:



التكوينات

يستخدم هذا المستند التكوينات التالية:

- PIX 515e
- R2 (الموجه 2811 من Cisco)

PIX 515e

```
(PIX Version 6.3(4
interface ethernet0 100full
interface ethernet1 100full
interface ethernet2 shut
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 intf2 security4
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname PIX515E
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
names

The access control list (ACL) to avoid NAT on the ---!
IPsec packets. access-list NO-NAT permit ip 10.1.0.0
255.255.255.0 10.0.0.0 255.255.255.0
The ACL to apply on crypto map. !--- Include the ---!
private-network-to-private-network traffic !--- in the
encryption process. access-list 101 permit ip 10.1.0.0
255.255.255.0 10.0.0.0 255.255.255.0
pager lines 24
logging on
mtu outside 1500
mtu inside 1500
mtu intf2 1500
.ISP will providthe the Outside IP address ---!
ip address outside dhcp

ip address inside 10.1.0.3 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
no failover
failover timeout 0:00:00
failover poll 15
no failover ip address outside
no failover ip address inside
no failover ip address intf2
pdm history enable
arp timeout 14400
global (outside) 1 interface
nat (inside) 0 access-list NO-NAT
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
```

```
route outside 10.0.0.0 255.255.255.0 172.16.1.5 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc
0:10:00 h225 1:00:00
timeout h323 0:05:00 mgcp 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 TACACS+ max-failed-attempts 3
aaa-server TACACS+ deadtime 10
aaa-server RADIUS protocol radius
aaa-server RADIUS max-failed-attempts 3
aaa-server RADIUS deadtime 10
aaa-server LOCAL protocol local
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
sysopt connection permit-ipsec

IPsec configuration, Phase 2. crypto ipsec ---!
transform-set DYN-TS esp-des esp-md5-hmac
crypto map IPSEC 10 ipsec-isakmp
crypto map IPSEC 10 match address 101
crypto map IPSEC 10 set peer 10.95.49.1
crypto map IPSEC 10 set transform-set DYN-TS
crypto map IPSEC interface outside
Internet Security Association and Key Management ---!
Protocol (ISAKMP) !--- policy, Phase 1. !--- Note: In
real show run output, the pre-shared key appears as
.*******

isakmp enable outside
isakmp key cisco123 address 10.95.49.1 netmask
255.255.255.255
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
console timeout 0
terminal width 80
Cryptochecksum:f0294298e214a947fc2e03f173e4a405
end :
```

R2 (الموجه 2811 من Cisco)

```
R2#show running-configuration
...Building configuration

Current configuration : 1916 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname r1800
!
```

```
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
resource policy
!
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip subnet-zero
ip cef
!
!
no ip dhcp use vrf connected
!
!
no ip ips deny-action ips-interface
!
no ftp-server write-enable
!
!
ISAKMP policy, Phase 1. crypto isakmp policy 10 ---!
hash md5
authentication pre-share
crypto isakmp key 6 cisco123 address 0.0.0.0 0.0.0.0
!
!
IPsec policy, Phase 2. crypto ipsec transform-set ---!
DYN-TS esp-des esp-md5-hmac
!
crypto dynamic-map DYN 10
set transform-set DYN-TS
match address 101
!
!
crypto map IPSEC 10 ipsec-isakmp dynamic DYN
!
!
!
interface FastEthernet0/0
ip address 10.95.49.1 255.255.255.0
ip nat outside
ip virtual-reassembly
load-interval 30
duplex auto
speed auto
crypto map IPSEC
!
interface FastEthernet0/1
ip address 10.0.0.1 255.255.255.0
ip nat inside
ip virtual-reassembly
duplex auto
speed auto
!
ip classless
ip route 10.1.0.0 255.255.255.0 10.95.49.2
!
ip http server
no ip http secure-server
Except the private network from the NAT process. ip ---!
```

```
nat inside source list 102 interface FastEthernet0/0
overload
!
Include the private-network-to-private-network !--- ---!
traffic in the encryption process. access-list 101
permit ip 10.0.0.0 0.0.0.255 10.1.0.0 0.0.0.255

Except the private network from the NAT process. ---!
access-list 102 deny ip 10.0.0.0 0.0.0.255 10.1.0.0
0.0.0.255
access-list 102 permit ip 10.0.0.0 0.0.0.255 any
!
!
control-plane
!
!
line con 0
exec-timeout 0 0
line aux 0
line vty 0 4
exec-timeout 0 0
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 .

- 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.

قم بتنفيذ أوامر PIX هذه في وضع التكوين.

- مسح التشفير sa isakmp—يمحو المرحلة 1 من SAs.
- مسح تشفير IPsec—يمحو المرحلة 2 SAs.

أنجزت هذا مسحاج تخديد أمر في يمكن أسلوب.

- مسح التشفير isakmp—يمحو المرحلة 1 من SAs.
- مسح التشفير sa—يمسح المرحلة 2 SAs.

استكشاف الأخطاء وإصلاحها

أستخدم هذا القسم 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**— عرض 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

- حلول أستكشاف أخطاء الشبكة الخاصة الظاهرية (VPN) عبر بروتوكول IPSec للوصول عن بعد و L2L الأكثر شيوعا
- برنامج جدار حماية Cisco PIX
- مراجع أوامر جدار حماية PIX الآمن من Cisco
- طلبات التعليقات (RFCs)
- مفاوضة IPSec/بروتوكولات IKE

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).