PIX 6.x: مثال تكوين نفق VPN البسيط من PIX إلى PIX

المحتويات

المقدمة

يسمح هذا التكوين لجدران حماية PIX الآمنة من Cisco بتشغيل نفق شبكة خاصة افتراضية (VPN) بسيط من PIX إلى PIX عبر الإنترنت أو أي شبكة عامة تستخدم أمان IP (IPSec). IPSec هو مجموعة من المعايير المفتوحة التي توفر سرية البيانات وسلامة البيانات ومصادقة أصل البيانات بين أقران IPSec.

ارجع إلى PIX/ASA 7.x: مثال تكوين نفق VPN البسيط من PIX إلى PIX للحصول على مزيد من المعلومات حول نفس السيناريو حيث يشغل جهاز أمان Cisco الإصدار x.7 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:

- جدار حماية Cisco Secure PIX 515e مع إصدار البرنامج 6.3(5)
- جدار حماية Cisco Secure PIX 515e مع إصدار البرنامج 6.3(5)

الاصطلاحات

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

معلومات أساسية

يمكن تقسيم مفاوضات IPSec إلى خمس خطوات، تتضمن مرحلتين من عملية تبادل مفتاح الإنترنت (IKE).

1. يتم إنشاء نفق IPSec بواسطة حركة مرور مثيرة للاهتمام. تعتبر حركة المرور مثيرة للاهتمام عندما تتنقل بين أقران IPSec.
2. في المرحلة الأولى من IKE، يتفاوض نظراء IPSec على سياسة اقتران أمان IKE (SA) الراسخة. بمجرد مصادقة النظراء، يتم إنشاء نفق آمن باستخدام بروتوكول إدارة المفاتيح وارتباط أمان الإنترنت (ISAKMP).
3. في المرحلة 2 من IKE، يستخدم نظراء IPSec النفق الآمن والمصدع للتفاوض على تحويلات IPSec SA. يحدد التفاوض على السياسة المشتركة كيفية إنشاء نفق IPSec.
4. يتم إنشاء نفق IPSec ونقل البيانات بين نظائر IPSec استنادا إلى معلمات IPSec التي تم تكوينها في مجموعات تحويل IPSec.
5. ينتهي نفق IPSec عند حذف أسماء IPSec أو عند انتهاء صلاحية عمرها الافتراضي.

ملاحظة: يفشل تفاوض IPSec بين PIXs إذا لم تتطابق معايير SAs على كل من مرحلتي IKE مع الأقران.

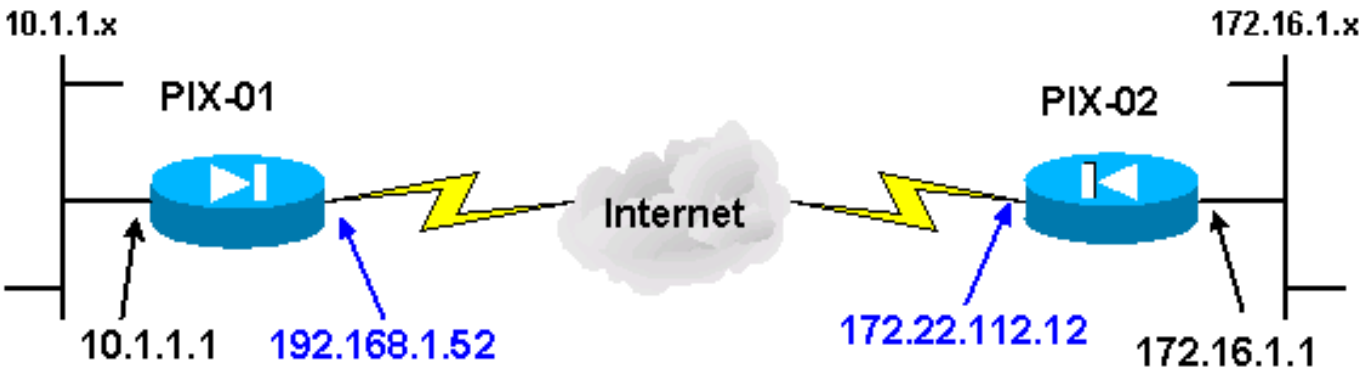
التكوين

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

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

الرسم التخطيطي للشبكة

يستعمل هذا وثيقة هذا شبكة رسم بياني:



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.

تكوين IKE و IPSec

يختلف تكوين IPSec على كل PIX فقط عندما تقوم بإدخال معلومات النظير واتفاق التسمية الذي تم إختياره لخرائط التشفير ومجموعات التحويل. يمكن التحقق من التكوين باستخدام أوامر **write terminal** أو **show**. الأوامر ذات الصلة هي show isakmp، و**show isakmp policy**، و**show access-list**، و**show crypto IPSec transform-set**، وshow crypto map. راجع مراجع أوامر جدار حماية PIX الآمن من Cisco للحصول على مزيد من المعلومات حول هذه الأوامر.

أكمل الخطوات التالية لتكوين IPSec:

1. تكوين IKE للمفاتيح المسبقة
2. تكوين IPSec
3. تكوين ترجمة عنوان الشبكة (NAT)
4. تكوين خيارات نظام PIX

تكوين IKE للمفاتيح المسبقة

قم بإصدار الأمر **isakmp enable** لتمكين IKE على واجهات إنهاء IPSec. في هذا السيناريو، تكون الواجهة الخارجية هي الواجهة الطرفية IPSec على كل من PIX. تم تكوين IKE على كل من PIX. تظهر هذه الأوامر فقط PIX-01.

```
isakmp enable outside
```

كما تحتاج أيضا إلى تحديد سياسات IKE التي يتم إستخدامها أثناء مفاوضات IKE. قم بإصدار الأمر **isakmp policy** من أجل القيام بذلك. عند إصدار هذا الأمر، يجب عليك تعيين مستوى أولوية حتى يتم تعريف السياسات بشكل فريد. في هذه الحالة، يتم تعيين الأولوية الأعلى من 1 إلى السياسة. كما تم تعيين النهج على إستخدام مفتاح مشترك مسبقا وخوارزمية تجزئة MD5 لمصادقة البيانات و DES لتضمين حمولة الأمان (ESP) ومجموعة Diffie-Hellman1. تم تعيين النهج أيضا لاستخدام العمر الافتراضي ل SA.

```
isakmp policy 1 authentication pre-share
isakmp policy 1 encryption des
isakmp policy 1 hash md5
isakmp policy 1 group 1
isakmp policy 1 lifetime 1000
```

يمكن التحقق من تكوين IKE باستخدام أمر **show isakmp policy**:

```
PIX-01#show isakmp policy
Protection suite of priority 1
.(encryption algorithm: DES - Data Encryption Standard (56 bit keys
hash algorithm: Message Digest 5
authentication method: Pre-Shared Key
(Diffie-Hellman group: #1 (768 bit
lifetime: 1000 seconds, no volume limit
Default protection suite
.(encryption algorithm: DES - Data Encryption Standard (56 bit keys
hash algorithm: Secure Hash Standard
authentication method: Rivest-Shamir-Adleman Signature
(Diffie-Hellman group: #1 (768 bit
lifetime: 86400 seconds, no volume limit
```

أخيرا، قم بإصدار الأمر **isakmp key** من أجل تكوين المفتاح المشترك مسبقا وتخصيص عنوان نظير. يجب أن يتطابق المفتاح المشترك مسبقا نفسه مع نظائر IPSec عند إستخدام المفاتيح المحددة مسبقا. يختلف العنوان، والذي يعتمد على عنوان IP للنظير البعيد.

```
isakmp key ********** address 172.22.112.12 netmask 255.255.255.255
PIX-01#
```

يمكن التحقق من النهج باستخدام الأمر **write terminal** أو **show isakmp**:

```
PIX-01#show isakmp
isakmp enable outside
isakmp key ********** address 172.22.112.12 netmask 255.255.255.255
isakmp identity address
isakmp policy 1 authentication pre-share
isakmp policy 1 encryption des
isakmp policy 1 hash md5
isakmp policy 1 group 1
isakmp policy 1 lifetime 1000
```

تكوين IPSec

يتم بدء IPSec عندما يستقبل أحد PIX حركة مرور البيانات الموجهة ل PIX الآخر داخل الشبكة. تعتبر حركة المرور هذه حركة مرور مثيرة للاهتمام يلزم حمايتها بواسطة IPSec. يتم إستخدام قائمة الوصول لتحديد حركة المرور التي تبدأ مفاوضات IKE و IPSec. تسمح قائمة الوصول هذه بإرسال حركة مرور البيانات من شبكة x.10.1.1، عبر نفق IPSec، إلى شبكة x.172.16.1. تعكس قائمة الوصول الموجودة على تكوين PIX العكسي قائمة الوصول هذه. وهذا مناسب ل PIX-01.

```
access-list 101 permit ip 10.1.1.0 255.255.255.0 172.16.1.0 255.255.255.0
```

تحدد مجموعة تحويل IPSec سياسة الأمان التي يستخدمها الأقران لحماية تدفق البيانات. يتم تحديد تحويل IPSec باستخدام الأمر **crypto IPSec transform-set**. يجب إختيار اسم فريد لإعداد التحويل ويمكن تحديد ما يصل إلى ثلاث عمليات تحويل لتحديد بروتوكولات أمان IPSec. يستخدم هذا التكوين نقلتين فقط: **esp-hmac-md5** و**esp-des**.

```
crypto IPSec transform-set chevelle esp-des esp-md5-hmac
```

قامت خرائط التشفير بإعداد IPSec SAs لحركة المرور المشفرة. يجب تعيين اسم خريطة ورقم تسلسلي لإنشاء خريطة تشفير. ثم قم بتحديد معلمات خريطة التشفير. تستخدم شبكة خريطة التشفير المعروضة IKE لإنشاء شبكات IPSec SAs، وتشفير أي شيء يطابق قائمة الوصول 101، ولديه نظير مجموعة، وتستخدم مجموعة تحويل **المشفرة** لسن سياسة الأمان لحركة المرور الخاصة بها.

```
crypto map transam 1 IPSec-isakmp
crypto map transam 1 match address 101
crypto map transam 1 set peer 172.22.112.12
crypto map transam 1 set transform-set chevelle
```

بعد تحديد خريطة التشفير، قم بتطبيق خريطة التشفير على واجهة. يجب أن تكون الواجهة التي تختارها هي الواجهة الطرفية IPSec.

```
crypto map transam interface outside
```

قم بإصدار الأمر **show crypto map** للتحقق من سمات خريطة التشفير.

```
PIX-01#show crypto map

{ Crypto Map: "transam" interfaces: { outside

                Crypto Map "transam" 1 IPSec-isakmp
                        Peer = 172.22.112.12
access-list 101 permit ip 10.1.1.0 255.255.255.0 172.16.1.0 255.255.255
                Current peer: 172.22.112.12
        Security association lifetime: 4608000 kilobytes/28800 seconds
                                PFS (Y/N): N
                { ,Transform sets={ chevelle
```

تكوين NAT

يقول هذا الأمر ل PIX ألا يقوم بتحديد أي حركة مرور تعتبر مثيرة للاهتمام ل IPSec. لذلك، يتم إعفاء جميع حركة المرور التي تطابق عبارات أوامر **access-list** من خدمات NAT.

```
access-list NoNAT permit ip 10.1.1.0 255.255.255.0
                255.255.255.0 172.16.1.0
nat (inside) 0 access-list NoNAT
```

تكوين خيارات نظام PIX

لأن جميع الجلسات الواردة يجب أن يتم السماح بها بشكل صريح بواسطة قائمة الوصول أو قناة، يتم إستخدام الأمر **sysopt connection allowed-ipsEC** للسماح بجميع جلسات تشفير IPSec الواردة التي تمت مصادقتها. باستخدام حركة مرور IPSec المحمية، يمكن أن يكون تحقق القناة الثانوية زائدا ويتسبب في فشل إنشاء النفق. يعمل الأمر **sysopt** على ضبط العديد من ميزات التكوين وأمان جدار حماية PIX.

```
sysopt connection permit-IPSec
```

التكوينات

إن يتلقى أنت الإنتاج من **كتابة terminal** أمر من ك cisco أداة، أنت يستطيع استعملت إنتاج مترجم (يسجل زبون فقط) أن يعرض ممكن إصدار ونقطة معينة. يجب أن تسجل دخولك وأن يكون لديك JavaScript ممكن لاستخدام مترجم الإخراج (للعملاء المسجلين فقط).

PIX-01 على 192,68,1,52

```
(PIX Version 6.3(5
interface ethernet0 auto
interface ethernet1 auto
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname PIX-01
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
Defines interesting traffic that is protected by ---!
the IPSec tunnel. access-list 101 permit ip 10.1.1.0
255.255.255.0 172.16.1.0 255.255.255.0
Do not perform NAT for traffic to other PIX ---!
Firewall. access-list NoNAT permit ip 10.1.1.0
255.255.255.0 172.16.1.0 255.255.255.0
pager lines 24
mtu outside 1500
mtu inside 1500
mtu intf2 1500
mtu intf3 1500
mtu intf4 1500
mtu intf5 1500
Sets the outside address on the PIX Firewall. ip ---!
address outside 192.168.1.52 255.255.255.0
Sets the inside address on the PIX Firewall. ip ---!
address inside 10.1.1.1 255.255.255.0
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
pdm history enable
arp timeout 14400
This command tells the PIX not to NAT any traffic ---!
!--- deemed interesting for IPSec. nat (inside) 0
access-list NoNAT
Sets the default route to the default gateway. ---!
route outside 0.0.0.0 0.0.0.0 192.168.1.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc
0:10:00 h225 1:00:00
timeout h323 0:05:00 mgcp 0:05:00 sip 0:30:00 sip_media
0:02:00
timeout sip-disconnect 0:02:00 sip-invite 0:03:00
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
Allows IPSec traffic to pass through the PIX ---!
Firewall !--- and does not require an additional conduit
```

```
!--- or access-list statements to permit IPSec traffic.
sysopt connection permit-IPSec
IKE Phase 2: !--- The IPSec transform-set ---!
"chevelle" uses esp-md5-hmac to provide !--- data
.authentication

crypto IPSec transform-set chevelle esp-des esp-md5-hmac
Crypto maps set up the SAs for IPSec traffic. !--- ---!
Indicates that IKE is used to establish IPSec SAs.
crypto map transam 1 IPSec-isakmp
Assigns interesting traffic to peer 172.22.112.12. ---!
crypto map transam 1 match address 101
Sets the IPSec peer. crypto map transam 1 set peer ---!
172.22.112.12
Sets the IPSec transform set "chevelle" !--- to be ---!
used with the crypto map entry "transam". crypto map
transam 1 set transform-set chevelle
Assigns the crypto map transam to the interface. ---!
crypto map transam interface outside
IKE Phase 1: !--- Enables IKE on the interface used ---!
to terminate the IPSec tunnel

isakmp enable outside
Sets the ISAKMP identity of the peer and !--- sets ---!
the pre-shared key between the IPSec peers. !--- The
same preshared key must be configured on the !--- IPSec
peers for IKE authentication. isakmp key ********
address 172.22.112.12 netmask 255.255.255.255
The PIX uses the IP address method by default !--- ---!
for the IKE identity in the IKE negotiations. isakmp
identity address
The ISAKMP policy defines the set of parameters !-- ---!
- that are used for IKE negotiations. !--- If these
parameters are not set, the default parameters are used.
!--- The show isakmp policy command shows the
.differences in !--- the default and configured policy

isakmp policy 1 authentication pre-share
isakmp policy 1 encryption des
isakmp policy 1 hash md5
isakmp policy 1 group 1
isakmp policy 1 lifetime 1000
telnet timeout 5
ssh timeout 5
console timeout 0
terminal width 80
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e
end :
```

PIX-02 على 172,22,112,12

```
(PIX Version 6.3(5
interface ethernet0 auto
interface ethernet1 auto
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname PIX-02
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
Defines interesting traffic that is protected by ---!
the IPSec tunnel. access-list 101 permit ip 172.16.1.0
255.255.255.0 10.1.1.0 255.255.255.0
Do not perform NAT for traffic to other PIX ---!
Firewall. access-list NoNAT permit ip 172.16.1.0
255.255.255.0 10.1.1.0 255.255.255.0
pager lines 24
mtu outside 1500
mtu inside 1500
mtu intf2 1500
mtu intf3 1500
mtu intf4 1500
mtu intf5 1500
Sets the outside address on the PIX Firewall. ip ---!
address outside 172.22.112.12 255.255.255.0
Sets the inside address on the PIX Firewall. ip ---!
address inside 172.16.1.1 255.255.255.0
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
pdm history enable
arp timeout 14400
This command tells the PIX not to NAT any traffic ---!
!--- deemed interesting for IPSec. nat (inside) 0
access-list NoNAT
Sets the default route to the default gateway. ---!
route outside 0.0.0.0 0.0.0.0 172.22.112.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc
0:10:00 h225 1:00:00
timeout h323 0:05:00 mgcp 0:05:00 sip 0:30:00 sip_media
0:02:00
timeout sip-disconnect 0:02:00 sip-invite 0:03:00
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
Allows IPSec traffic to pass through the PIX ---!
Firewall !--- and does not require an additional conduit
!--- or access-list statements to permit IPSec traffic.
sysopt connection permit-IPSec
```

```
IKE Phase 2:  !--- The IPSec transform set defines ---!
 the negotiated security policy !--- that the peers use
 to protect the data flow. !--- The IPSec transform-set
  "toyota" uses hmac-md5 authentication header !--- and
                      .encapsulates the payload with des

 crypto IPSec transform-set toyota esp-des esp-md5-hmac
 Crypto maps set up the SAs for IPSec traffic. !--- ---!
      Indicates that IKE is used to establish IPSec SAs.
                                crypto map bmw 1 IPSec-isakmp
  Assigns interesting traffic to peer 192.168.1.52. ---!
                              crypto map bmw 1 match address 101
         Sets IPSec peer. crypto map bmw 1 set peer ---!
                                                  192.168.1.52
    Sets the IPSec transform set "toyota" !--- to be ---!
  used with the crypto map entry "bmw". crypto map bmw 1
                                    set transform-set toyota
Assigns the crypto map bmw to the interface. crypto ---!
                                    map bmw interface outside
IKE Phase 1: !--- Enables IKE on the interface used ---!
                                  .to terminate IPSec tunnel


                                            isakmp enable outside
 Sets the ISAKMP identity of the peer and !--- sets ---!
the preshared key between the IPSec peers. !--- The same
preshared key must be configured on the !--- IPSec peers
      for IKE authentication. isakmp key ******** address
                          192.168.1.52 netmask 255.255.255.255
 The PIX uses the IP address method by default !--- ---!
    for the IKE identity in the IKE negotiations. isakmp
                                            identity address
The ISAKMP policy defines the set of parameters !-- ---!
      - that are used for IKE negotiations. !--- If these
parameters are not set, the default parameters are used.
                    isakmp policy 1 authentication pre-share
                             isakmp policy 1 encryption des
                                   isakmp policy 1 hash md5
                                  isakmp policy 1 group 1
                               isakmp policy 1 lifetime 1000
                                          telnet timeout 5
                                             ssh timeout 5
                                        console timeout 0
                                        terminal width 80
                  Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e
                                                      end :
```

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 IPSec sa**— يعرض هذا الأمر الحالة الحالية لملقمات أمان IPSec ويكون مفيدا في تحديد ما إذا كان يتم تشفير حركة مرور البيانات.
- **show crypto isakmp sa**— يعرض هذا الأمر الحالة الحالية لشبكات IKE.

أوامر عرض PIX-01

أوامر عرض PIX-01

```
PIX-01#show crypto IPSec sa
                                    interface: outside
      Crypto map tag: transam, local addr. 192.168.1.52

                     local ident (addr/mask/prot/port):
                           ((10.1.1.0/255.255.255.0/0/0
                    remote ident (addr/mask/prot/port):
                         ((172.16.1.0/255.255.255.0/0/0
                            current_peer: 172.22.112.12
                           {,PERMIT, flags={origin_is_acl
This verifies that encrypted packets are being sent ---!
  !--- and received without any errors. #pkts encaps: 3,
                          #pkts encrypt: 3, #pkts digest 3
       pkts decaps: 3, #pkts decrypt: 3, #pkts verify 3#
                 pkts compressed: 0, #pkts decompressed: 0#
  pkts not compressed: 0, #pkts compr. failed: 0, #pkts#
                                       decompress failed: 0
                          send errors 2, #recv errors 0#

local crypto endpt.: 192.168.1.52, remote crypto endpt.:
                                                172.22.112.12
         path mtu 1500, IPSec overhead 56, media mtu 1500
                          current outbound spi: 6f09cbf1
Shows inbound SAs that are established. inbound esp ---!
                                                    :sas
                                  (spi: 0x70be0c04(1891503108
                              transform: esp-des esp-md5-hmac
                                  { ,in use settings ={Tunnel
                 slot: 0, conn id: 1, crypto map: transam
               sa timing: remaining key lifetime (k/sec):
                                           ((4607999/28430
                                        IV size: 8 bytes
                              replay detection support: Y

                                                :inbound ah sas

                                               :inbound pcp sas
  Shows outbound SAs that are established. outbound ---!
                                                   :ESP sas
                                  (spi: 0x6f09cbf1(1862913009
                              transform: esp-des esp-md5-hmac
                                  { ,in use settings ={Tunnel
                 slot: 0, conn id: 2, crypto map: transam
               sa timing: remaining key lifetime (k/sec):
                                           ((4607999/28430
                                        IV size: 8 bytes
                              replay detection support: Y

                                                :outbound ah sas

                                              :outbound PCP sas

  The ISAKMP SA is in the quiescent state (QM_IDLE) ---!
  when it exists. !--- The ISAKMP SA is idle. The ISAKMP
  SA remains authenticated with its !--- peer and can be
   used for subsequent Quick Mode exchanges. PIX-01#show
                                          crypto isakmp sa
    dst             src          state       pending
                                                created
       QM_IDLE        0    192.168.1.52    172.22.112.12
                                          1Maui-PIX-01#
```

أوامر عرض PIX-02

أوامر عرض PIX-02

```
PIX-02#show crypto IPSec sa

                                    interface: outside
        Crypto map tag: bmw, local addr. 172.22.112.12

                                local ident (addr/mask/prot/port):
                                    ((172.16.1.0/255.255.255.0/0/0
                                remote ident (addr/mask/prot/port):
                                    ((10.1.1.0/255.255.255.0/0/0
                                      current_peer: 192.168.1.52
                                    {,PERMIT, flags={origin_is_acl
This verifies that encrypted packets are !--- being ---!
    sent and recede without any errors. #pkts encaps: 3,
                                #pkts encrypt: 3, #pkts digest 3
      pkts decaps: 3, #pkts decrypt: 3, #pkts verify 3#
                            pkts compressed: 0, #pkts decompressed: 0#
  pkts not compressed: 0, #pkts compr. Failed: 0, #pkts#
                                        decompress failed: 0
                                send errors 0, #recv errors 0#

      local crypto endpt.: 172.22.112.12, remote crypto
                                        endpt.: 192.168.1.52
       path mtu 1500, IPSec overhead 56, media mtu 1500
                                current outbound spi: 70be0c04
Shows inbound SAs that are established. Inbound ESP ---!
                                                    :sas
                                    (spi: 0x6f09cbf1(1862913009
                                transform: esp-des esp-md5-hmac
                                    { ,in use settings ={Tunnel
                              slot: 0, conn id: 1, crypto map: bmw
                            sa timing: remaining key lifetime (k/sec):
                                                ((4607999/28097
                                              IV size: 8 bytes
                                    replay detection support: Y

                                                :inbound ah sas

                                               :inbound PCP sas
  Shows outbound SAs that are established. Outbound ---!
                                                   :ESP sas
                                    (spi: 0x70be0c04(1891503108
                                transform: esp-des esp-md5-hmac
                                    { ,in use settings ={Tunnel
                              slot: 0, conn id: 2, crypto map: bmw
                            sa timing: remaining key lifetime (k/sec):
                                                ((4607999/28097
                                              IV size: 8 bytes
                                    replay detection support: Y

                                               :outbound ah sas

                                              :outbound PCP sas

  The ISAKMP SA is in the quiescent state (QM_IDLE) ---!
  when it exists. !--- The ISAKMP SA is idle. The ISAKMP
  SA remains authenticated with its !--- peer and can be
   used for subsequent Quick Mode exchanges. PIX-02#show
                                            crypto isakmp sa
```

dst	src	state	pending created
QM_IDLE	0	192.168.1.52	172.22.112.12

PIX-02#

لا يمكن إختبار الواجهة الداخلية ل PIX لتكوين نفق ما لم يتم تكوين الأمر management-access في وضع التكوين العام.

```
PIX-02(config)#management-access inside
PIX-02(config)#show management-access
management-access inside
```

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

أوامر استكشاف الأخطاء وإصلاحها

ملاحظة: يجب تنفيذ أوامر **clear** في وضع التكوين.

- **مسح crypto IPSec sa**— يقوم هذا الأمر بإعادة تعيين IPSec SAs بعد محاولات فاشلة للتفاوض على نفق VPN.
- **مسح crypto isakmp sa**— يقوم هذا الأمر بإعادة تعيين ISAKMP SAs بعد محاولات فاشلة للتفاوض على نفق VPN.

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

- **debug crypto IPSec**—يوضح هذا الأمر ما إذا كان العميل يتفاوض مع جزء IPSec من اتصال VPN.
- **debug crypto isakmp**— يوضح هذا الأمر ما إذا كان النظراء يتفاوضون على جزء ISAKMP من اتصال VPN.

بعد اكتمال الاتصال، يمكن التحقق منه باستخدام أوامر **show**.

معلومات ذات صلة

- صفحة دعم PIX
- مرجع أوامر PIX
- طلب التعليقات (RFCs)
- مفاوضة IPSec/صفحة دعم بروتوكول IKE
- 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).