# PIX 6.x : Exemple de configuration d'un tunnel VPN PIX-to-PIX simple

## Contenu



## Introduction

Cette configuration permet à deux pare-feu Cisco Secure PIX Firewall d'exécuter un tunnel VPN (réseau privé virtuel) simple de PIX à PIX via Internet ou tout réseau public qui utilise la sécurité IP (IPSec). IPSec est une combinaison de normes ouvertes qui fournit la confidentialité des données, l'intégrité des données et l'authentification de l'origine des données entre des homologues IPSec.

Référez-vous à PIX/ASA 7.x : Exemple de configuration simple de tunnel VPN PIX à PIX pour plus d'informations sur le même scénario où le dispositif de sécurité Cisco exécute le logiciel version 7.x.

## Conditions préalables

### Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

### Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Pare-feu Cisco Secure PIX 515E Firewall VPN avec le logiciel version 6.3(5)
- Pare-feu Cisco Secure PIX 515E Firewall VPN avec le logiciel version 6.3(5)

### Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

## Informations générales

La négociation IPSec peut être décomposée en cinq étapes, ce qui inclut deux phases d'échange de clés Internet (IKE).

1. Un tunnel IPSec est lancé par un trafic intéressant. Le trafic est considéré comme intéressant quand il transite entre les homologues IPSec.
2. Dans la phase 1 d'IKE, les homologues IPSec négocient la stratégie d'association de sécurité IKE. Une fois que les homologues sont authentifiés, un tunnel sécurisé est créé en utilisant Internet Security Association and Key Management Protocol (ISAKMP).
3. Dans la phase 2 d'IKE, les homologues IPSec utilisent le tunnel authentifié et sécurisé pour négocier des transformations d'association de sécurité IPSec. La négociation de la stratégie partagée détermine comment le tunnel IPSec est établi.
4. Le tunnel IPSec est créé et les données sont transférées entre les homologues IPSec en fonction des paramètres IPSec configurés dans les jeux de transformations IPSec.
5. Le tunnel IPSec se termine quand les associations de sécurité IPSec sont supprimées ou quand leur durée de vie expire.

**Remarque:** La négociation IPSec entre les deux PIX échoue si les associations de sécurité sur les deux phases d'IKE ne correspondent pas sur les homologues.

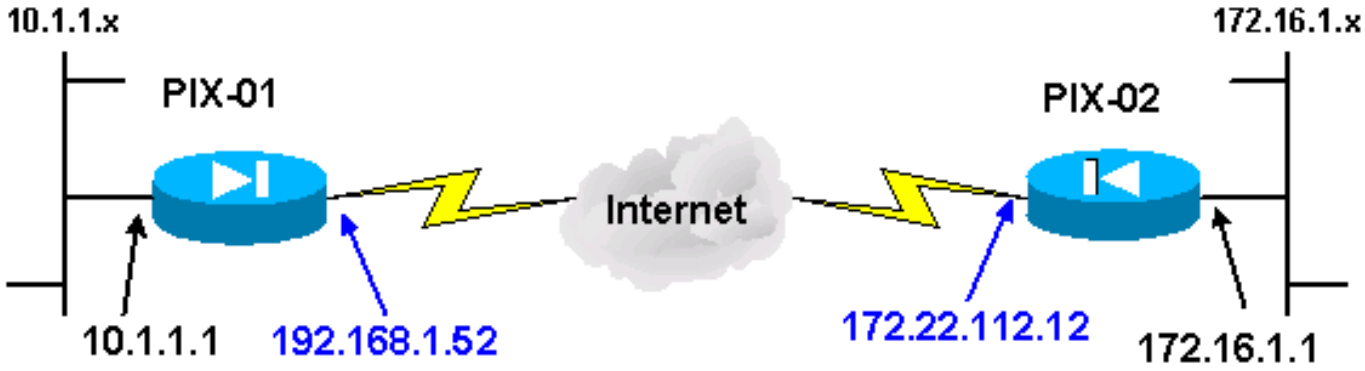
## Configurez

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

**Remarque:** Utilisez l'Outil de recherche de commande (clients inscrits uniquement) pour obtenir plus d'informations sur les commandes utilisées dans ce document.

### Diagramme du réseau

Ce document utilise ce diagramme de réseau :




**Remarque:** Les schémas d'adressage d'IP utilisés dans cette configuration ne sont pas légalement routables sur Internet. Ce sont des adresses RFC 1918qui ont été utilisées dans un environnement de laboratoire.

## Configuration IKE et IPSec

La configuration IPSec sur chaque PIX varie seulement quand vous insérez les informations sur les homologues et la convention de noms choisies pour les cartes de chiffrement et les jeux de transformations. La configuration peut être vérifiée avec les commandes **write terminal** ou **show**. Les commandes pertinentes sont **show isakmp**, **show isakmp policy**, **show access-list**, **show crypto IPSec transform-set** et **show crypto map**. Référez-vous à la liste de référence des commandes du pare-feu Cisco Secure PIX Firewall pour plus d'informations sur ces commandes.

Complétez les étapes suivantes afin de configurer IPSec :

1. Configurer IKE pour les clés pré-partagées
2. Configurer IPSec
3. Configurer la traduction d'adresses réseau (NAT)
4. Configurer les options système PIX

### Configurer IKE pour les clés pré-partagées

Émettez la commande **isakmp enable** afin d'activer IKE sur les interfaces de terminaison IPSec. Dans ce scénario, l'interface externe est l'interface de terminaison IPSec sur les deux PIX. IKE est configuré sur les deux PIX. Ces commandes montrent seulement PIX-01.

```
isakmp enable outside
```

Vous devez également définir les stratégies IKE qui sont utilisées pendant les négociations IKE. Émettez la commande **isakmp policy** pour ce faire. Quand vous émettez cette commande, vous devez assigner un niveau de priorité de sorte que les stratégies soient identifiées de façon unique. Dans ce cas, la priorité la plus haute 1 est assignée à la stratégie. La stratégie est également définie pour utiliser une clé pré-partagée, un algorithme de hachage MD5 pour l'authentification des données, une norme DES pour Encapsulating Security Payload (ESP) et un Diffie-Hellman group1. La stratégie est également définie pour utiliser la durée de vie des associations de sécurité.

```
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
```

La configuration IKE peut être vérifiée avec la commande **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
```

Enfin, émettez la commande **isakmp key** afin de configurer la clé pré-partagée et affecter une adresse homologue. La même clé pré-partagée doit correspondre sur les homologues IPSec quand des clés pré-partagées sont utilisées. L'adresse diffère, ce qui dépend de l'adresse IP du partenaire distant.

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

La stratégie peut être vérifiée avec la commande **write terminal** ou **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
```

## Configurer IPSec

IPSec est lancé quand l'un des PIX reçoit du trafic qui est destiné à l'autre réseau interne PIX. Ce trafic est considéré comme un trafic intéressant qui doit être protégé par IPSec. Une liste d'accès est utilisée pour déterminer quel trafic lance des négociations IKE et IPSec. Cette liste d'accès permet au trafic d'être envoyé à partir du réseau 10.1.1.x, par l'intermédiaire du tunnel IPSec, au réseau 172.16.1.x. La liste d'accès sur la configuration PIX opposée reflète cette liste d'accès. Cela est approprié pour PIX-01.

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

Le jeu de transformations IPSec définit la stratégie de sécurité que les homologues utilisent pour protéger le flux de données. La transformation IPSec est définie à l'aide de la commande **crypto IPSec transform-set**. Un nom unique doit être choisi pour le jeu de transformations et jusqu'à trois transformations peuvent être sélectionnées pour définir les protocoles de sécurité IPSec. Cette configuration utilise seulement deux transformations : **esp-hmac-md5** et **esp-des**.

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

Les cartes de chiffrement configurent les associations de sécurité IPSec pour le trafic chiffré. Vous devez assigner un nom de carte et un numéro de séquence pour créer une carte de chiffrement.

Alors vous définissez les paramètres de la carte de chiffrement. La carte de chiffrement transam affichée utilise IKE pour établir des associations de sécurité IPSec, chiffre tout ce qui correspond à la liste d'accès 101, a un homologue défini et emploie la commande **chevelle transform-set** pour activer sa stratégie de sécurité pour le trafic.

```
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
```

Après avoir défini la carte de chiffrement, appliquez-la à l'interface. L'interface que vous choisissez doit être l'interface de terminaison IPSec.

```
crypto map transam interface outside
```

Émettez la commande **show crypto map** pour vérifier les attributs de la carte de chiffrement.

```
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, }
```

## Configurer NAT

Cette commande indique au PIX de ne pas appliquer NAT au trafic considéré comme intéressant pour IPSec. Ainsi, tout trafic qui correspond aux instructions de la commande **access-list** est exempté des services NAT.

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

## Configurer les options système PIX

Puisque toutes les sessions entrantes doivent être explicitement autorisées par une liste d'accès ou un conduit, la commande **sysopt connection permit-ipsec** est utilisée pour permettre toutes les sessions de chiffrement authentifiées IPSec entrantes. Avec le trafic protégé IPSec, le contrôle du conduit secondaire peut être redondant et faire échouer la création du tunnel. La commande **sysopt** règle diverses fonctionnalités de sécurité de pare-feu et de configuration PIX.

```
sysopt connection permit-IPSec
```

# Configurations

Si vous disposez de la sortie d'une commande **write terminal** de votre périphérique Cisco, vous pouvez utiliser l'Outil Interpréteur de sortie (clients inscrits uniquement) pour afficher les problèmes potentiels ainsi que les correctifs. Vous devez être connecté et avoir JavaScript activé pour utiliser l'Outil Interpréteur de sortie (clients inscrits uniquement) .

## PIX-01 à 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 à 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
```

## Vérifiez

Cette section présente des informations que vous pouvez utiliser pour vous assurer que votre configuration fonctionne correctement.

Certaines commandes **show** sont prises en charge par l'Output Interpreter Tool (clients enregistrés uniquement), qui vous permet de voir une analyse de la sortie de la commande show.

- **show crypto IPSec sa -** Cette commande affiche l'état actuel des associations de sécurité IPSec et est utile pour déterminer si le trafic est chiffré.
- **show crypto isakmp sa -** Cette commande montre l'état actuel des associations de sécurité IKE.

## Commandes PIX-01 show

**Commandes PIX-01 show**

```
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
172.22.112.12    192.168.1.52    QM_IDLE          0
1Maui-PIX-01#
```

## Commandes PIX-02 show

### Commandes PIX-02 show

```
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
172.22.112.12    192.168.1.52    QM_IDLE          0
PIX-02#
```

L'interface interne du PIX ne peut pas faire l'objet d'un ping pour la formation d'un tunnel à moins que la commande **management-access** soit configurée dans le mode de configuration globale.

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

# Dépannez

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

## Dépannage des commandes

**Remarque:** Les commandes **clear** doivent être exécutées en mode de configuration.

- **clear crypto IPSec sa -** Cette commande réinitialise les associations de sécurité IPSec après des échecs de tentative de négocier un tunnel VPN.
- **clear crypto isakmp sa -** Cette commande réinitialise les associations de sécurité ISAKMP après des échecs de tentative de négocier un tunnel VPN.

**Remarque:** Reportez-vous à Informations importantes sur les commandes de débogage avant d'émettre des commandes **debug**.

- **debug crypto IPSec -** Cette commande montre si un client négocie la partie IPSec de la connexion VPN.
- **debug crypto isakmp -** Cette commande montre si les homologues négocient la partie ISAKMP de la connexion VPN.

Une fois la connexion terminée, elle peut être vérifiée utilisant les commandes **show**.

# Informations connexes

- Page de support PIX
- Référence des commandes PIX
- Request For Comments (RFC)
- Page de support pour Protocole IKE/Négociation Ipsec
- Support et documentation techniques - Cisco Systems