

PIX 6.x: Ejemplo de configuración del Túnel VPN PIX a PIX sencillo

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Antecedentes](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuración de IKE e IPSec](#)

[Configuraciones](#)

[Verificación](#)

[Comandos show del PIX-01](#)

[Comandos show del PIX-02](#)

[Troubleshooting](#)

[Comandos para resolución de problemas](#)

[Información Relacionada](#)

[Introducción](#)

Esta configuración permite que dos firewalls Cisco Secure PIX ejecuten un túnel de red privada virtual simple (VPN) de PIX a PIX sobre Internet o cualquier red pública que utilice la seguridad IP (IPSec). IPSec es una combinación de estándares abiertos que proporciona confidencialidad, integridad y autenticación de datos entre peers IPSec.

Consulte [PIX/ASA 7.x: Ejemplo de configuración del Túnel VPN PIX a PIX sencillo](#) para más información sobre el mismo escenario donde el dispositivo del Cisco Security funciona con la versión de software 7.x.

[prerrequisitos](#)

[Requisitos](#)

No hay requisitos específicos para este documento.

[Componentes Utilizados](#)

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Firewall del Secure PIX de Cisco 515E con la versión de software 6.3(5)
- Firewall del Secure PIX de Cisco 515E con la versión de software 6.3(5)

Convenciones

Consulte [Convenciones de Consejos TécnicosCisco](#) para obtener más información sobre las convenciones del documento.

Antecedentes

El IPSec Negotiation se puede analizar en cinco pasos, que incluye dos fases del Internet Key Exchange (IKE).

1. Un túnel IPSec es iniciado por un tráfico interesado. Se considera que el tráfico es interesante cuando se transmite entre los pares IPSec.
2. En la Fase 1 IKE, las entidades pares IPSec negocian la política establecida de la Asociación de seguridad (SA) IKE. Una vez que se autentican los pares, se crea un túnel seguro por medio de la Asociación de Seguridad en Internet y del Protocolo de administración de clave (ISAKMP).
3. En la fase 2 de IKE, los pares IPSec usan el túnel autenticado y seguro para negociar las transformaciones de IPSec SA. La negociación de la política compartida determina el modo en que se establece el túnel IPSec.
4. Se crea el túnel IPSec y los datos se transfieren entre los pares IPSec según los parámetros IPSec configurados en los conjuntos de transformaciones de IPSec.
5. El túnel IPSec termina cuando los IPSec SAs son borrados o cuando caduca su vigencia.

Nota: El IPSec Negotiation entre los dos PIX falla si los SA en ambas fases IKE no hacen juego en los pares.

Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Nota: Utilice la [herramienta de búsqueda de comandos \(clientes registrados solamente\)](#) para más información sobre los comandos usados en este documento.

Diagrama de la red

Este documento utiliza este diagrama de la red:

Nota: Los esquemas de direccionamiento IP usados en esta configuración no son legalmente enrutables en Internet. Éstos son los direccionamientos del [RFC 1918](#) que se han utilizado en un ambiente de laboratorio.

Configuración de IKE e IPSec

La configuración IPsec en cada PIX varía solamente cuando usted inserta la información de peer y a la convención para nombres elegidas para las correspondencias de criptografía y transforma los conjuntos. La configuración se puede verificar con la **terminal** o los **comandos show de la escritura**. Los comandos importantes son show isakmp, show isakmp policy, show access-list, show crypto ipsec transform-set y show crypto map. Refiera a las [Referencias de Comandos de Secure PIX firewall](#) para más información sobre estos comandos.

Complete estos pasos para configurar el IPsec:

1. [Configure el IKE para las claves del preshared](#)
2. [Configure el IPsec](#)
3. [Configure el Network Address Translation \(NAT\)](#)
4. [Configure las opciones del sistema PIX](#)

[Configure el IKE para las claves del preshared](#)

Publique el **comando isakmp enable** para habilitar el IKE en las interfaces de terminación de IPsec. En este escenario, la interfaz externa es la interfaz de terminación IPsec en ambos PIX. El IKE se configura en ambos PIX. Estos comandos muestran solamente el PIX-01.

```
isakmp enable outside
```

Usted también necesita definir las políticas IKE que se utilizan durante las negociaciones IKE. Publique el **comando isakmp policy** para hacer esto. Cuando usted publica este comando, usted debe asignar un nivel de prioridad para identificar las directivas únicamente. En este caso, la prioridad más alta de 1 se asigna a la directiva. La directiva también se fija para utilizar una clave del preshared, un algoritmo de troceo MD5 para la autenticación de datos, un DES para el Encapsulating Security Payload (ESP), y un group1 de Diffie Hellman. La directiva también se fija para utilizar el curso de la vida 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
```

La configuración de IKE puede verificarse con el comando 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
```

Finalmente, publique el **comando isakmp key** para configurar la clave del preshared y asignar a una dirección de peer. Cuando se utilizan claves compartidas previamente, la misma clave compartida previamente debe coincidir en los pares IPsec. El direccionamiento diferencia, que depende de la dirección IP del peer remoto.

```
isakmp key ***** address 172.22.112.12 netmask 255.255.255.255
```

```
PIX-01#
```

Puede verificarse la política con el comando write terminal o 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
```

[IPSec de la configuración](#)

Se inicia el IPSec cuando uno de los PIX recibe el tráfico que es destinado para la otra red interna PIX. Este tráfico se considera tráfico interesante que necesita la protección de IPSec. Una lista de acceso se utiliza para determinar qué tráfico inicia el IKE y los IPSec Negotiations. Esta lista de acceso permite que el tráfico sea enviado de la red 10.1.1.x, vía el túnel IPsec, a la red 172.16.1.x. La lista de acceso en la configuración PIX del contrario duplica esta lista de acceso. Esto es apropiado para el PIX-01.

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

El IPSec transforma el conjunto define la política de seguridad que los pares utilizan para proteger el flujo de datos. El IPSec transforma se define usando el **comando crypto ipsec transform-set**. Se debe seleccionar un nombre exclusivo para el conjunto de transformaciones y se pueden seleccionar hasta tres transformaciones para definir los protocolos de seguridad IPSec. Esta configuración utiliza solamente dos transforma: **esp-hmac-md5** y **ESP-DES**.

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

Los mapas de criptografía configuran SA IPSec para el tráfico encriptación. Usted debe asignar un nombre de asignación y un número de secuencia para crear una correspondencia de criptografía. Entonces usted define los parámetros de la correspondencia de criptografía. El transam de la correspondencia de criptografía visualizado utiliza el IKE para establecer el SA de IPSec, cifra cualquier cosa que hace juego el access-list 101, tiene un par del conjunto, y utiliza el **chevelle transform-set** para decretar su política de seguridad para el tráfico.

```
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
```

Después de que usted defina la correspondencia de criptografía, aplique la correspondencia de criptografía a una interfaz. La interfaz que usted elige debe ser la interfaz de terminación de IPSec.

```
crypto map transam interface outside
```

Publique el **comando show crypto map** de verificar los atributos de la correspondencia de criptografía.

```
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, }
```

Configure el NAT

Este comando dice a PIX no al NAT cualquier tráfico juzgado como interesante para el IPSec. Así, todo el tráfico que hace juego las declaraciones de **comando access-list** está exento de los servicios 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
```

Opciones del sistema de la configuración PIX

Porque todas las sesiones entrantes deben ser permitidas explícitamente por una lista de acceso o un conducto, utilizan al **comando sysopt connection permit-ipsec** de permitir a todas las IPSec entrante sesiones de cifrado autenticadas. Con el tráfico protegido por IPSec, la revisión del conducto secundario puede ser redundante y hacer la creación de túnel fallar. Las diversas características de la Seguridad y de configuración del firewall PIX del **sysopt command tunes**.

```
sysopt connection permit-IPSec
```

Configuraciones

Si usted tiene la salida de un **comando write terminal** de su dispositivo de Cisco, usted puede utilizar el [Output Interpreter \(clientes registrados solamente\)](#) para visualizar los problemas potenciales y los arreglos. Usted debe ser abierto una sesión y hacer el Javascript habilitar para utilizar el [Output Interpreter \(clientes registrados solamente\)](#).

PIX-01 en 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 en 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

```

Verificación

En esta sección encontrará información que puede utilizar para confirmar que su configuración esté funcionando correctamente.

La herramienta [Output Interpreter](#) (sólo para clientes [registrados](#)) permite utilizar algunos comandos "show" y ver un análisis del resultado de estos comandos.

- **muestre IPsec crypto sa** — Este comando visualiza el estado actual del SA de IPsec y es útil en determinar si se está cifrando el tráfico.
- **muestre isakmp crypto sa** — Este comando muestra al estado actual del IKE SA.

Comandos show del PIX-01

Comandos show del 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
172.22.112.12    192.168.1.52    QM_IDLE        0
1Maui-PIX-01#

```

Comandos show del PIX-02

Comandos show del 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
172.22.112.12    192.168.1.52    QM_IDLE        0
PIX-02#

```

La interfaz interior del PIX no se puede hacer ping para la formación de túnel a menos que el comando del [Acceso de administración](#) se configure en el modo de configuración global.

PIX-02(config)#**management-access** inside

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

Troubleshooting

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

Comandos para resolución de problemas

Nota: Los comandos **clear** deben ser realizados en el modo de configuración.

- **clear crypto ipsec sa** — Este comando reajusta el SA de IPsec después de los intentos fallidos de negociar un túnel VPN.
- **clear crypto isakmp sa** — Este comando reajusta el ISAKMP SA después de los intentos fallidos de negociar un túnel VPN.

Nota: Consulte [información importante en los comandos debug](#) antes de ejecutar los comandos debug.

- **IPsec del debug crypto** — Este comando muestra si un cliente es negociación porción IPsec de la conexión VPN.
- **isakmp del debug crypto** — Este comando muestra si los pares están negociando la porción ISAKMP de la conexión VPN.

Después de que la conexión sea completa, puede ser verificada usando los **comandos show**.

Información Relacionada

- [Página de Soporte de PIX](#)
- [Referencia de Comandos PIX](#)
- [Request For Comments \(RFC\)](#)
- [Página de Soporte del Protocolo IKE/la Negociación de IPsec](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)