# PIX 6.x: Exemplo de Configuração de Túnel VPN PIX para PIX Simples

## Contents



# Introduction

Esta configuração permite que dois Cisco Secure PIX Firewalls executem um túnel de rede privada virtual (VPN) simples do PIX ao PIX pela Internet ou por qualquer rede pública que use Segurança IP (IPsec). A IPsec é uma combinação de padrões abertos que fornecem confidencialidade de dados, integridade de dados e autenticação da origem de dados entre peers IPSec.

Refira ao PIX/ASA 7.x: Exemplo de Configuração de Túnel VPN PIX para PIX Simples para obter mais informações sobre o mesmo cenário em que o Cisco Security Appliance executa a versão de software 7.x.

# Prerequisites

## Requirements

Não existem requisitos específicos para este documento.

## Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco Secure PIX Firewall 515E com software versão 6.3(5)
- Cisco Secure PIX Firewall 515E com software versão 6.3(5)

### Conventions

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

## Informações de Apoio

A negociação de IPSec pode ser dividida em cinco etapas, o que inclui duas fases de Internet Key Exchange (IKE).

1. Um túnel de IPSec é iniciado por um tráfego interessante. O tráfego é considerado interessante quando ele é transmitido entre os peers IPSec.
2. Na Fase 1 IKE, os correspondentes IPSec negociam a política de Associação de segurança (SA) IKE estabelecida. Quando os peers são autenticados, um túnel seguro é criado com o uso do Internet Security Association and Key Management Protocol (ISAKMP).
3. Em IKE Phase 2, os correspondentes de IPSec utilizam o túnel autenticado e seguro para negociar transformações de IPSec AS. A negociação da política compartilhada determina como o túnel de IPSec é estabelecido.
4. O túnel de IPSec é criado e os dados são transferidos entre peers de IPSec com base nos parâmetros de IPSec configurados em grupos de transformação do IPSec.
5. O túnel de IPSec finaliza quando os IPSec SAs são excluídos ou quando sua vida útil expira.

**Observação:** a negociação de IPSec entre os dois PIXs falhará se os SAs em ambas as fases do IKE não coincidirem com os correspondentes.

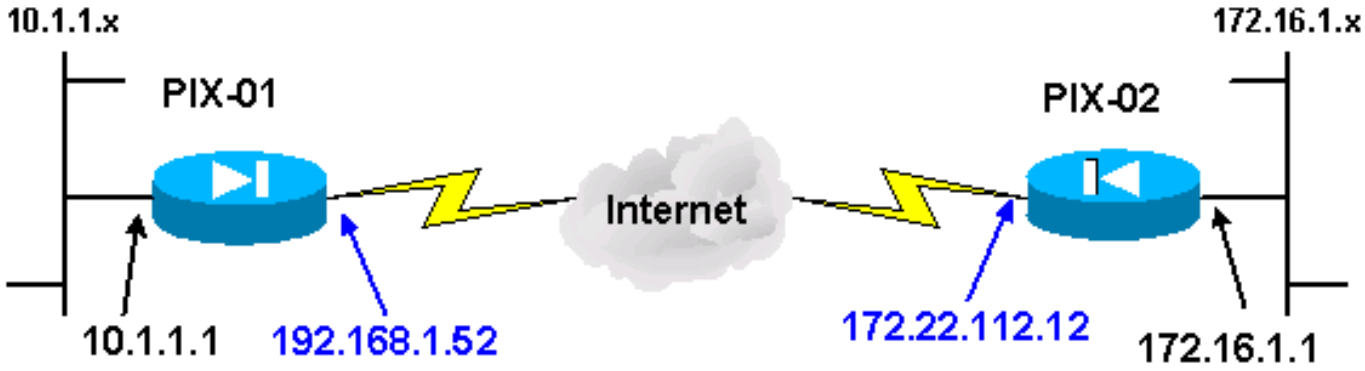
## Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

**Observação:** use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados neste documento.

### Diagrama de Rede

Este documento usa este diagrama de rede:




**Observação:** os esquemas de endereçamento IP usados nesta configuração não são legalmente roteáveis na Internet. Esses são endereços RFC 1918 que foram usados em um ambiente de laboratório.

## Configuração de IKE e IPSec

A configuração de IPSec em cada PIX só varia quando você insere as informações do peer e a convenção de nomenclatura escolhida para os mapas de criptografia e os conjuntos de transformação. A configuração pode ser verificada com os comandos **write terminal** ou **show**. Os comandos relevantes são show isakmp, show isakmp policy, show access-list, show crypto ipsec transform-set e show crypto map. Consulte Referências de Comando do Cisco Secure PIX Firewall para obter mais informações sobre esses comandos.

Conclua estes passos para configurar o IPSec:

1. Configurar IKE para chaves pré-compartilhadas
2. Configurar IPSec
3. Configurar a Conversão de Endereço de Rede (NAT)
4. Configurar opções do sistema PIX

### Configurar IKE para chaves pré-compartilhadas

Emita o comando **isakmp enable** para habilitar IKE nas interfaces de terminação IPSec. Nesse cenário, a interface externa é a interface de término IPSec nos dois PIXs. O IKE é configurado em ambos os PIXs. Esses comandos mostram apenas PIX-01.

```
isakmp enable outside
```

Você também precisa definir as políticas de IKE usadas durante as negociações de IKE. Execute o comando **isakmp policy** para fazer isso. Ao emitir esse comando, você deve atribuir um nível de prioridade para que as políticas sejam identificadas de forma exclusiva. Nesse caso, a prioridade mais alta de 1 é atribuída à política. A política também é definida para usar uma chave pré-compartilhada, um algoritmo de hash MD5 para autenticação de dados, um DES para Encapsulating Security Payload (ESP) e um Diffie-Hellman group1. A política também é definida para usar a vida útil do 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
```

A configuração IKE pode ser verificada com o 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, execute o comando **isakmp key** para configurar a chave pré-compartilhada e atribuir um endereço de peer. A mesma chave previamente compartilhada deve corresponder nos peers IPSec durante o uso de chaves previamente compartilhadas. O endereço é diferente, o que depende do endereço IP do peer remoto.

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

A política pode ser verificada com o comando 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
```

## Configurar IPSec

O IPSec é iniciado quando um dos PIXs recebe o tráfego destinado ao outro PIX dentro da rede. Este tráfego é considerado um tráfego interessante que precisa ser protegido por IPSec. Uma lista de acesso é usada para determinar qual tráfego inicia as negociações de IKE e IPSec. Essa lista de acesso permite que o tráfego seja enviado da rede 10.1.1.x, através do túnel IPSec, para a rede 172.16.1.x. A lista de acesso na configuração de PIX oposta espelha essa lista de acesso. Isso é apropriado para o PIX-01.

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

O conjunto de transformação de IPSec define a política de segurança que os colegas usam para

proteger o fluxo de dados. A transformação de IPSec é definida usando o comando **crypto IPSec transform-set**. Deve ser escolhido um nome exclusivo para o grupo de transformação e até três transformações podem ser selecionadas para definir os protocolos de segurança IPSec. Essa configuração usa apenas duas transformações: **esp-hmac-md5** e **esp-des**.

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

Os mapas de criptografia configuram SAs do IPSec para tráfego criptografado. Você deve atribuir um nome de mapa e um número de sequência para criar um mapa de criptografia. Em seguida, você define os parâmetros do mapa de criptografia. O transam de mapa de criptografia exibido usa IKE para estabelecer SAs de IPSec, criptografa qualquer coisa que corresponda à lista de acesso 101, tem um par definido e usa o **chevelle** transform-set para promulgar sua política de segurança para o tráfego.

```
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
```

Depois de definir o mapa de criptografia, aplique o mapa de criptografia a uma interface. A interface escolhida deve ser a interface de terminação IPSec.

```
crypto map transam interface outside
```

Emita o comando **show crypto map** para verificar os atributos do mapa de criptografia.

```
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 o NAT

Esse comando diz ao PIX para não enviar NAT nenhum tráfego considerado como interessante para IPSec. Assim, todo o tráfego que corresponde às instruções do comando **access-list** está isento dos serviços 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
```

## Configurar opções do sistema PIX

Como todas as sessões de entrada devem ser explicitamente permitidas por uma lista de acesso ou um canal, o comando **sysopt connection permit-IPSec** é usado para permitir todas as sessões de cifras autenticadas IPSec de entrada. Com o tráfego protegido IPSec, a verificação de conduíte secundário pode ser redundante e causar falha na criação do túnel. O comando **sysopt** ajusta vários recursos de segurança e configuração de firewall PIX.

```
sysopt connection permit-IPSec
```

## Configurações

Se tiver a saída de um comando write terminal do dispositivo Cisco, você poderá usar o Output Interpreter (somente para clientes registrados) para exibir os possíveis problemas e soluções. Você deve estar conectado e ter o JavaScript habilitado para usar o Output Interpreter (somente clientes registrados) .

**PIX-01 em 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 em 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
```

# Verificar

Esta seção fornece informações que você pode usar para confirmar se sua configuração está funcionando adequadamente.

A Output Interpreter Tool (somente clientes registrados) oferece suporte a determinados comandos show, o que permite exibir uma análise da saída do comando show.

- **show crypto IPSec sa** — Este comando exibe o status atual das SAs de IPSec e é útil para determinar se o tráfego está sendo criptografado.
- **show crypto isakmp sa** — Este comando mostra o estado atual dos SAs IKE.

## Comandos show do PIX-01

**Comandos show do 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 do PIX-02

### Comandos show do 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#
```

A interface interna do PIX não pode receber ping para a formação do túnel, a menos que o comando management-access esteja configurado no modo de configuração global.

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

# Troubleshoot

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

## Comandos para Troubleshooting

**Observação:** os comandos **clear** devem ser executados no modo de configuração.

- **clear crypto IPSec sa** — Este comando redefine as SAs de IPSec após tentativas com falha para negociar um túnel VPN.
- **clear crypto isakmp sa** — Este comando redefine as SAs ISAKMP após tentativas com falha de negociar um túnel VPN.

**Nota:Consulte Informações Importantes sobre Comandos de Depuração antes de usar os comandos debug.**

- **debug crypto IPSec** —Este comando mostra se um cliente está negociando a parte IPSec da conexão VPN.
- **debug crypto isakmp** — Este comando mostra se os peers estão negociando a parte ISAKMP da conexão VPN.

Após a conclusão da conexão, ela pode ser verificada usando os comandos **show**.

## Informações Relacionadas

- Página de suporte do PIX
- Referências de comando PIX
- Solicitação de comentários (RFCs)
- Página do suporte de protocolo do IPsec Negotiation/IKE
- Suporte Técnico e Documentação - Cisco Systems