PIX 6.x: Exemplo de configuração do túnel PIX a PIX VPN simples

Índice

Introdução

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 do túnel PIX a PIX VPN simples para obter mais informações sobre da mesma encenação onde o dispositivo do Cisco Security executa a versão de software 7.x.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

- Firewall do PIX seguro Cisco 515E com versão de software 6.3(5)
- Firewall do PIX seguro Cisco 515E com versão de software 6.3(5)

Convenções

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, que inclui duas fases de intercâmbio de chave de Internet (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 correspondentes forem autenticados, um túnel seguro é criado, com uso da associação de segurança da Internet e protocolo de gerenciamento chave (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.

Nota: A negociação de IPSec entre os dois PIX falha se os SA em ambas as fases IKE não combinam nos pares.

Configurar

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

Nota: Use a ferramenta de consulta de comandos (clientes registrados somente) para obter mais informações sobre dos comandos usados neste documento.

Diagrama de Rede

Este documento usa este diagrama da rede:

Nota: Os esquemas de endereçamento IP usados nesta configuração não são legalmente roteáveis na Internet. Estes são os endereços do RFC 1918 que foram usados em um ambiente de laboratório.

Configuração de IKE e IPSec

A configuração IPSec em cada PIX varia somente quando você introduz a informação de peer e a convenção de nomeação escolhidas para os crypto map e transforma grupos. A configuração pode ser verificada com o **terminal** ou os **comandos show da escrita**. Os comandos relevantes são show isakmp, show isakmp policy, show access-list, show crypto ipsec transform-set e show crypto map. Refira referências de comando do Cisco secure PIX firewall para obter mais informações sobre destes comandos.

Termine estas etapas a fim configurar o IPsec:

1. Configurar o IKE para chaves Preshared
2. Configurar o IPsec
3. Configurar o Network Address Translation (NAT)
4. Configurar opções de sistema PIX

Configurar o IKE para chaves Preshared

Emita o **comando isakmp enable** a fim permitir o 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 PIX. Estes comandos mostram somente o PIX-01.

```
isakmp enable outside
```

Você igualmente precisa de definir as políticas de IKE que são usadas durante as negociações de IKE. Emita o **comando isakmp policy** a fim fazer isto. Quando você emite este comando, você deve atribuir um nível da prioridade de modo que as políticas sejam identificadas excepcionalmente. Neste caso, a prioridade mais alta de 1 é atribuída à política. A política é ajustada igualmente para usar uma chave preshared, um algoritmo de hashing MD5 para a autenticação de dados, um DES para o Encapsulating Security Payload (ESP), e um grupo1 de Diffie-Hellman. A política é ajustada igualmente para usar a 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
```

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, emita o **comando isakmp key** a fim configurar a chave preshared 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 difere, que depende do endereço IP de Um ou Mais Servidores Cisco ICM NT 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 o IPsec

O IPsec é iniciado quando um dos PIX recebe o tráfego que é destinado para a outra rede interna PIX. Este tráfego é considerado um tráfego interessante que precisa ser protegido por IPSec. Uma lista de acessos é usada para determinar que tráfego inicia o IKE e as negociações de IPSec. Esta lista de acessos permite o tráfego ser enviada da rede 10.1.1.x, através do túnel de IPsec, à rede 172.16.1.x. A lista de acessos na configuração de PIX do oposto espelha esta lista de acessos. Isto 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 IPsec transforma o grupo define a política de segurança que os pares se usam para proteger o fluxo de dados. O IPsec transforma é definido 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. Esta configuração usa somente dois transforma: **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 crypto map. Então você define os parâmetros do crypto map. O transam do crypto map indicado usa o IKE para estabelecer o sas de IPSec, cifra qualquer coisa que combina o access-list 101, tem um par do grupo, e usa o **chevelle transform-set** para decretar 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 que você define o crypto map, aplique o crypto map a uma relação. A relação que você escolhe deve ser a interface de terminação IPSec.

```
crypto map transam interface outside
```

Emita o **comando show crypto map** verificar os atributos do crypto map.

```
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, }
```

Configurar o NAT

Este comando diz ao PIX não ao NAT todo o tráfego julgado como interessante para o IPsec. Assim, todo o tráfego que combina as indicações de **comando access-list** é 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 de sistema PIX

Porque todas as sessões de entrada devem explicitamente ser permitidas por uma lista de acessos ou por uma conduíte, o **comando sysopt connection permit-ipsec** é usado permitir todas as sessões de cifra autenticadas IPSec de entrada. Com tráfego protegido de IPSec, a verificação de canalização secundária pode ser redundante e fazer com que a criação de túnel falhe. Características da Segurança e de configuração do PIX Firewall do **sysopt command tunes as** várias.

```
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 ser entrado e tido o Javascript permitido de usar o Output Interpreter (clientes registrados somente).

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.

- **mostre IPsec cripto sa** — Este comando indica o status atual do sas de IPSec e é útil em determinar se o tráfego está sendo cifrado.
- **mostre isakmp cripto sa** — Este comando mostra o estado atual do IKE SA.

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 ser sibilada para a formação de túnel a menos que o comando do acesso de gerenciamento for configurado no modo de configuração global.

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

Troubleshooting

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

Comandos para Troubleshooting

Nota: Os comandos clear devem ser executados no modo de configuração.

- **clear crypto ipsec sa** — Este comando restaura o sas de IPSec depois que falhas de tentativa negociar um túnel VPN.
- **clear crypto isakmp sa** — Este comando restaura o ISAKMP SA depois que falhas de tentativa negociar um túnel VPN.

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

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

Depois que a conexão está completa, pode-se verificar usando os **comandos show**.

Informações Relacionadas

- Página de suporte do PIX
- Referências de comando PIX
- Request For Comments (RFC)
- Página do suporte de protocolo do IPsec Negotiation/IKE
- Suporte Técnico e Documentação - Cisco Systems