

Configuring the Cisco VPN Client to Tunnel to Two Remote Sites Through One Hub PIX

Índice

[Introdução](#)

[Antes de Começar](#)

[Convenções](#)

[Pré-requisitos](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurações](#)

[Verificar](#)

[saída do comando show](#)

[Troubleshooting](#)

[Saída do comando debug](#)

[Informações Relacionadas](#)

[Introdução](#)

Este documento demonstra como configurar um Cisco VPN Client para conectar ao interior de um PIX quando conectado através do túnel a outro PIX. Para isso, deve-se terminar o túnel em uma interface diferente no PIX a que o cliente VPN já está conectado.

Clientes de VPN remota se conectarão ao snow (PIX 525) e receberão um endereço IP incluído no intervalo de 12.0.0.1 a 12.0.0.34. O Cliente VPN poderá estabelecer uma conectividade total com a parte interna da neve (10.0.0.0/24), bem como com a parte interna de outro PIX (chamada de chuva nesta configuração).

[Antes de Começar](#)

[Convenções](#)

Para obter mais informações sobre convenções de documento, consulte as [Convenções de dicas técnicas Cisco](#).

[Pré-requisitos](#)

Antes de tentar utilizar esta configuração, verifique se os seguintes pré-requisitos são atendidos:

- **rain**A configuração para a *chuva* é baseada na configuração de exemplo que [configura um](#)

[túnel PIX a PIX VPN simples usando o IPsec](#). A única diferença é que o pool de IPs, reservado para o cliente, deve ser incluído na lista de acessos do mapa de criptografia. Ou seja nós queremos proteger o tráfego que vai de nosso LAN (11.0.0.0/24) ao LAN privado remota (10.0.0.0/24) e ao cliente remoto (12.0.0.0/24).

- **neve** Para garantir que essa configuração funcione apropriadamente, é necessário ter duas interfaces diferentes conectadas à rede "externa", normalmente o Provedor de serviços de Internet (ISP). Também é necessário ter dois mapas de criptografia. Um crypto map deve ser aplicado ao intf2 (tipicamente o DMZ) que espelhará a configuração da *chuva*; isto protegerá a rede interna (10.0.0.0/24) que vai ao LAN remota (11.0.0.0/24) ao igualmente proteger o pool do cliente VPN (12.0.0.0/24) que vai ao LAN remota. O segundo cripto mapa deve ser aplicado à interface externa (geralmente eth0) como um cripto mapa dinâmico típico, como descrito em [Cisco PIX 5.1-to-VPN Client Wild-card, Pre-shared, Mode Configuration with Extended Authentication](#).

Quando o PIX (*chuva* neste exemplo) tentar conectar ao intf2 de (193.0.0.5), a negociação do Internet Key Exchange (IKE) falhará porque o outro PIX (*neve*) responderá com seu endereço exterior de 193.0.0.1. (Isto é porque o PIX tem tipicamente uma rota padrão à parte externa.) Para resolver a edição, adicionar uma rota específica ao LAN remota à relação do intf2. Igualmente adicionar uma rota do host ao endereço exterior do PIX remoto que atravessa o intf2.

Independentemente da conversão configurada no PIX, você não precisa configurar conversão para o tráfego VPN (conversão nat 0). Para isso, configure duas listas de acesso (no-nat-inside e no-nat-intf2) e aplique-as com os seguintes comandos:

```
nat (inside) 0 access-list no-nat-inside nat (intf2) 0 access-list no-nat-intf2
```

[Componentes Utilizados](#)

As informações neste documento são baseadas nas versões de software e hardware abaixo.

- PIX 525 com a Versão 6.2(2) do Software Cisco PIX Firewall
- PIX 515 com versão de software do firewall PIX segura Cisco 6.2(2)
- Software de Cisco IOS® 7200 (C7200-JO3S56I-M), versão 12.2(6)
- Cisco VPN Client 3.6.1 no Microsoft Windows 2000

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se você estiver trabalhando em uma rede ativa, certifique-se de que entende o impacto potencial de qualquer comando antes de utilizá-lo.

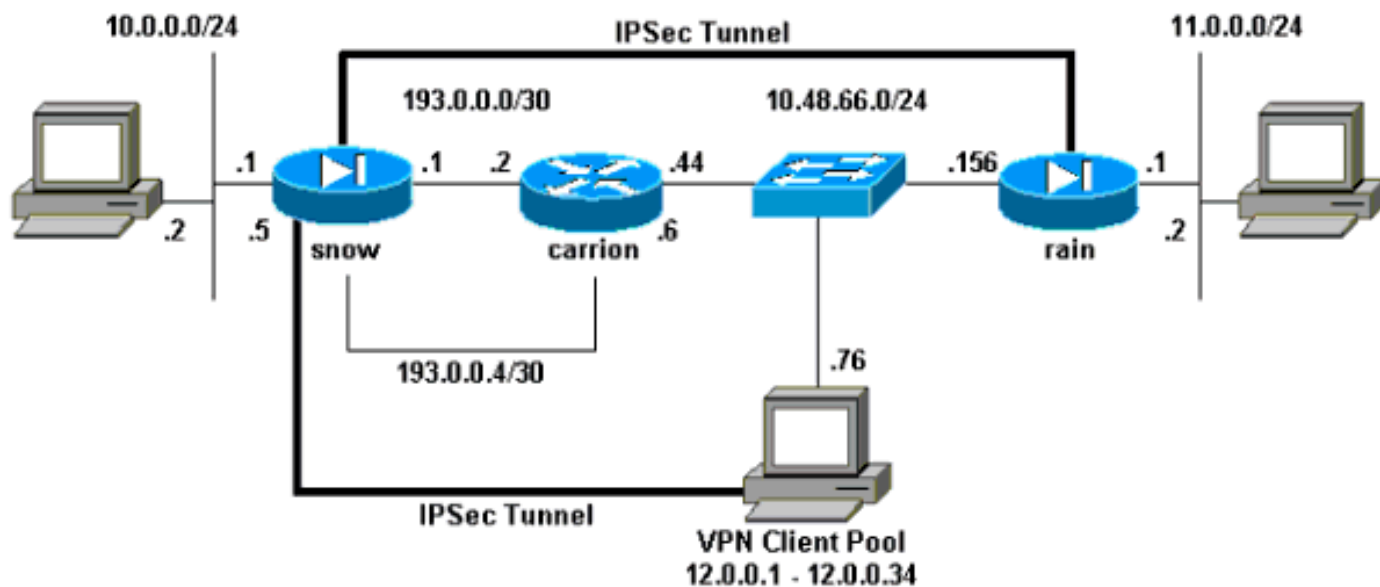
[Configurar](#)

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

Nota: Para localizar informações adicionais sobre os comandos usados neste documento, utilize a Ferramenta Command Lookup (somente clientes [registrados](#)).

[Diagrama de Rede](#)

Este documento utiliza a instalação de rede mostrada no diagrama abaixo.



Configurações

Este documento utiliza as configurações mostradas abaixo.

- [neve](#)
- [rain](#)
- [restos](#)

neve

```

PIX Version 6.2(2)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 intf2 security10
nameif ethernet3 intf3 security15
nameif ethernet4 intf4 security20
nameif ethernet5 intf5 security25
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname snow
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
fixup protocol skinny 2000
names
access-list acl-out permit icmp any any
access-list acl-intf2 permit icmp any any
access-list vpn-intf2 permit ip 10.0.0.0 255.255.255.0
    11.0.0.0 255.255.255.0
access-list vpn-intf2 permit ip 12.0.0.0 255.255.255.0
    11.0.0.0 255.255.255.0
access-list no-nat-inside permit ip 10.0.0.0
255.255.255.0
    11.0.0.0 255.255.255.0
access-list no-nat-inside permit ip 10.0.0.0
255.255.255.0
    12.0.0.0 255.255.255.0

```

```
access-list no-nat-intf2 permit ip 11.0.0.0
255.255.255.0
    12.0.0.0 255.255.255.0
no pager
logging on
logging console debugging
interface ethernet0 auto
interface ethernet1 auto
interface ethernet2 auto
interface ethernet3 auto shutdown
interface ethernet4 auto shutdown
interface ethernet5 auto shutdown
mtu outside 1500
mtu inside 1500
mtu intf2 1500
mtu intf3 1500
mtu intf4 1500
mtu intf5 1500
ip address outside 193.0.0.1 255.255.255.252
ip address inside 10.0.0.1 255.255.255.0
ip address intf2 193.0.0.5 255.255.255.252
ip address intf3 127.0.0.1 255.255.255.255
ip address intf4 127.0.0.1 255.255.255.255
ip address intf5 127.0.0.1 255.255.255.255
ip audit info action alarm
ip audit attack action alarm
ip local pool remote-VPN 12.0.0.1-12.0.0.34
no failover
failover timeout 0:00:00
failover poll 15
failover ip address outside 0.0.0.0
failover ip address inside 0.0.0.0
failover ip address intf2 0.0.0.0
failover ip address intf3 0.0.0.0
failover ip address intf4 0.0.0.0
failover ip address intf5 0.0.0.0
pdm history enable
arp timeout 14400
global (intf2) 1 interface
nat (inside) 0 access-list no-nat-inside
nat (inside) 1 10.0.0.0 255.255.255.0 0 0
nat (intf2) 0 access-list no-nat-intf2
access-group acl-out in interface outside
access-group acl-intf2 in interface intf2
route outside 0.0.0.0 0.0.0.0 193.0.0.2 1
route intf2 10.48.66.156 255.255.255.255 193.0.0.6 1
route intf2 11.0.0.0 255.255.255.0 193.0.0.6 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
    rpc 0:10:00 h323 0:05:00 sip 0:30:00 sip_media
0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
no floodguard enable
sysopt connection permit-ipsec
no sysopt route dnat
crypto ipsec transform-set TRANS esp-des esp-sha-hmac
crypto ipsec transform-set remote-TRANS esp-des esp-md5-
hmac
```

```
crypto dynamic-map DYN 10 set transform-set remote-TRANS
crypto map vpn-intf2 10 ipsec-isakmp
crypto map vpn-intf2 10 match address vpn-intf2
crypto map vpn-intf2 10 set peer 10.48.66.156
crypto map vpn-intf2 10 set transform-set TRANS
crypto map vpn-intf2 interface intf2
crypto map toOUT 10 ipsec-isakmp dynamic DYN
crypto map toOUT interface outside
isakmp enable outside
isakmp enable intf2
isakmp key ***** address 10.48.66.156 netmask
255.255.255.255
isakmp identity address
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption des
isakmp policy 10 hash sha
isakmp policy 10 group 2
isakmp policy 10 lifetime 86400
vpngroup VPNclient address-pool remote-VPN
vpngroup VPNclient idle-time 1800
vpngroup VPNclient password *****
telnet timeout 5
ssh timeout 5
terminal width 80
Cryptochecksum:c5ad37a1288a0be866edc1dc1c09fcc9
: end
[OK]
```

rain

```
rain# write terminal Building configuration... : Saved :
PIX Version 6.2(2) nameif ethernet0 outside security0
nameif ethernet1 inside security100 nameif ethernet2
intf2 security10 nameif ethernet3 intf3 security15
nameif ethernet4 intf4 security20 nameif ethernet5 intf5
security25 enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted hostname rain fixup
protocol ftp 21 fixup protocol http 80 fixup protocol
h323 1720 fixup protocol rsh 514 fixup protocol rtsp 554
fixup protocol smtp 25 fixup protocol sqlnet 1521 fixup
protocol sip 5060 fixup protocol skinny 2000 names
access-list acl-out permit icmp any any access-list vpn-
to-snow permit ip 11.0.0.0 255.255.255.0 10.0.0.0
255.255.255.0 access-list vpn-to-snow permit ip 11.0.0.0
255.255.255.0 12.0.0.0 255.255.255.0 no pager interface
ethernet0 auto interface ethernet1 auto interface
ethernet2 auto shutdown interface ethernet3 auto
shutdown interface ethernet4 auto shutdown interface
ethernet5 auto shutdown icmp permit any outside mtu
outside 1500 mtu inside 1500 mtu intf2 1500 mtu intf3
1500 mtu intf4 1500 mtu intf5 1500 ip address outside
10.48.66.156 255.255.255.0 ip address inside 11.0.0.1
255.255.255.0 ip address intf2 127.0.0.1 255.255.255.255
ip address intf3 127.0.0.1 255.255.255.255 ip address
intf4 127.0.0.1 255.255.255.255 ip address intf5
127.0.0.1 255.255.255.255 ip audit info action alarm ip
audit attack action alarm no failover failover timeout
0:00:00 failover poll 15 failover ip address outside
0.0.0.0 failover ip address inside 0.0.0.0 failover ip
address intf2 0.0.0.0 failover ip address intf3 0.0.0.0
failover ip address intf4 0.0.0.0 failover ip address
intf5 0.0.0.0 pdm history enable arp timeout 14400 nat
(inside) 0 access-list vpn-to-snow access-group acl-out
in interface outside route outside 10.0.0.0
255.255.255.0 193.0.0.5 1 route outside 12.0.0.0
```

```
255.255.255.0 193.0.0.5 1 route outside 193.0.0.0
255.255.255.0 10.48.66.44 1 timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc
0:10:00 h323 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute aaa-server TACACS+
protocol tacacs+ aaa-server RADIUS protocol radius no
snmp-server location no snmp-server contact snmp-server
community public no snmp-server enable traps no
floodguard enable sysopt connection permit-ipsec no
sysopt route dnat crypto ipsec transform-set TRANS esp-
des esp-sha-hmac crypto map vpn-outside 10 ipsec-isakmp
crypto map vpn-outside 10 match address vpn-to-snow
crypto map vpn-outside 10 set peer 193.0.0.5 crypto map
vpn-outside 10 set transform-set TRANS crypto map vpn-
outside interface outside isakmp enable outside isakmp
key ***** address 193.0.0.5 netmask 255.255.255.255
isakmp policy 10 authentication pre-share isakmp policy
10 encryption des isakmp policy 10 hash sha isakmp
policy 10 group 2 isakmp policy 10 lifetime 86400 telnet
timeout 5 ssh timeout 5 terminal width 80
Cryptochecksum:a2181c3b31cfcf3be90c24f622c17eed : end
[OK]
```

restos

Building configuration...

Current configuration : 3153 bytes

```
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service udp-small-servers
service tcp-small-servers
no service single-slot-reload-enable
!
hostname carrion
!
!
ip subnet-zero
ip tcp intercept list 111
ip tcp intercept connection-timeout 60
ip tcp intercept watch-timeout 10
ip tcp intercept max-incomplete low 2
ip tcp intercept max-incomplete high 3
ip domain-name cisco.com
ip name-server 144.254.6.77
!
ip cef
ip audit notify log
ip audit po max-events 100
ip ssh time-out 120
ip ssh authentication-retries 3
!
call rsvp-sync
!
!
!
!
!
!
!
!
interface Serial0/0
```

```
no ip address
no ip route-cache
no ip mroute-cache
shutdown
no fair-queue
!
interface Serial0/1
no ip address
no ip route-cache
no ip mroute-cache
shutdown
!
interface Serial0/2
no ip address
no ip route-cache
no ip mroute-cache
shutdown
!
interface Serial0/3
no ip address
no ip route-cache
no ip mroute-cache
shutdown
!
interface Serial0/4
no ip address
no ip route-cache
no ip mroute-cache
shutdown
!
interface Serial0/5
no ip address
no ip route-cache
no ip mroute-cache
shutdown
!
interface Serial0/6
no ip address
no ip route-cache
no ip mroute-cache
shutdown
!
interface Serial0/7
no ip address
no ip route-cache
no ip mroute-cache
shutdown
!
interface Serial1/0
no ip address
no ip route-cache
no ip mroute-cache
shutdown
!
interface Serial1/1
no ip address
no ip route-cache
no ip mroute-cache
shutdown
!
interface Serial1/2
no ip address
no ip route-cache
no ip mroute-cache
```

```
shutdown
!
interface Serial1/3
  no ip address
  no ip route-cache
  no ip mroute-cache
  shutdown
!
interface Serial1/4
  no ip address
  no ip route-cache
  no ip mroute-cache
  shutdown
!
interface Serial1/5
  no ip address
  no ip route-cache
  no ip mroute-cache
  shutdown
!
interface Serial1/6
  no ip address
  no ip route-cache
  no ip mroute-cache
  shutdown
!
interface Serial1/7
  no ip address
  no ip route-cache
  no ip mroute-cache
  shutdown
!
interface Serial2/0
  no ip address
  no ip route-cache
  no ip mroute-cache
!
interface Serial2/1
  no ip address
  no ip route-cache
  no ip mroute-cache
!
interface Serial2/2
  no ip address
  no ip route-cache
  no ip mroute-cache
!
interface Serial2/3
  no ip address
  no ip route-cache
  no ip mroute-cache
!
interface Serial2/4
  no ip address
  no ip route-cache
  no ip mroute-cache
!
interface Serial2/5
  no ip address
  no ip route-cache
  no ip mroute-cache
!
interface Serial2/6
  no ip address
```



```
no ip route-cache
no ip mroute-cache
!
interface Serial2/7
no ip address
no ip route-cache
no ip mroute-cache
!
interface Ethernet5/0
ip address 10.48.66.44 255.255.255.0
no ip route-cache
no ip mroute-cache
!
interface Ethernet5/1
ip address 193.0.0.2 255.255.255.252
no ip route-cache
no ip mroute-cache
!
interface Ethernet5/2
ip address 193.0.0.6 255.255.255.252
no ip route-cache
no ip mroute-cache
!
interface Ethernet5/3
no ip address
no ip route-cache
no ip mroute-cache
!
interface Hssi9/1/0
no ip address
shutdown
!
ip classless
no ip http server
ip pim bidir-enable
!
!
!
!
line con 0
line aux 0
line vty 0 4
password ww
login
!
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.

[saída do comando show](#)

show command output (resultado do comando show) para a neve

```
snow# show version Cisco PIX Firewall Version 6.2(2) Compiled on Tue 11-Sep-01 07:45 by morlee
snow up 11 mins 19 secs Hardware: PIX-525, 256 MB RAM, CPU Pentium III 600 MHz Flash E28F128J3 @
0x300, 16MB BIOS Flash AM29F400B @ 0xffffd8000, 32KB 0: ethernet0: address is 0002.b945.9ff1, irq
10 1: ethernet1: address is 0002.b945.9ff2, irq 11 2: ethernet2: address is 00e0.b602.236f, irq
11 3: ethernet3: address is 00e0.b602.236e, irq 10 4: ethernet4: address is 00e0.b602.236d, irq
9 5: ethernet5: address is 00e0.b602.236c, irq 5 Licensed Features: Failover: Enabled VPN-DES:
Enabled VPN-3DES: Disabled Maximum Interfaces: 8 Cut-through Proxy: Enabled Guards: Enabled
Websense: Enabled Inside Hosts: Unlimited Throughput: Unlimited ISAKMP peers: Unlimited Serial
Number: 480380577 (0x1ca206a1) Activation Key: 0x9c2c232e 0xaad98633 0x3667fa1b 0x76404050 snow#
snow(config)# show route outside 0.0.0.0 0.0.0.0 193.0.0.2 1 OTHER static inside 10.0.0.0
255.255.255.0 10.0.0.1 1 CONNECT static intf2 10.48.66.156 255.255.255.255 193.0.0.6 1 OTHER
static intf2 11.0.0.0 255.255.255.0 193.0.0.6 1 OTHER static intf3 127.0.0.1 255.255.255.255
127.0.0.1 1 CONNECT static outside 193.0.0.0 255.255.255.252 193.0.0.1 1 CONNECT static intf2
193.0.0.4 255.255.255.252 193.0.0.5 1 CONNECT static snow(config)# show access-list access-list
acl-out permit icmp any any (hitcnt=0) access-list acl-intf2 permit icmp any any (hitcnt=0)
access-list vpn-intf2 permit ip 10.0.0.0 255.255.255.0 11.0.0.0 255.255.255.0 (hitcnt=12)
access-list vpn-intf2 permit ip 12.0.0.0 255.255.255.0 11.0.0.0 255.255.255.0 (hitcnt=34)
access-list no-nat-inside permit ip 10.0.0.0 255.255.255.0 11.0.0.0 255.255.255.0 (hitcnt=18)
access-list no-nat-inside permit ip 10.0.0.0 255.255.255.0 12.0.0.0 255.255.255.0 (hitcnt=32)
access-list no-nat-intf2 permit ip 11.0.0.0 255.255.255.0 12.0.0.0 255.255.255.0 (hitcnt=50)
access-list dynacl6 permit ip host 193.0.0.1 host 12.0.0.1 (hitcnt=0) access-list dynacl7 permit
ip any host 12.0.0.1 (hitcnt=6) snow(config)# show crypto isa sa Total : 2 Embryonic : 0 dst src
state pending created 10.48.66.156 193.0.0.5 QM_IDLE 0 1 193.0.0.1 10.48.66.76 QM_IDLE 0 2
snow(config)# show crypto ipsec sa interface: intf2 Crypto map tag: vpn-intf2, local addr.
193.0.0.5 local ident (addr/mask/prot/port): (10.0.0.0/255.255.255.0/0/0) remote ident
(addr/mask/prot/port): (11.0.0.0/255.255.255.0/0/0) current_peer: 10.48.66.156 PERMIT,
flags={origin_is_acl,} #pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0 #pkts decaps: 0, #pkts
decrypt: 0, #pkts verify 0 #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.: 193.0.0.5, remote crypto endpt.: 10.48.66.156 path mtu 1500, ipsec overhead 0, media mtu
1500 current outbound spi: 0 inbound esp sas: inbound ah sas: inbound pcp sas: outbound esp sas:
outbound ah sas: outbound pcp sas: local ident (addr/mask/prot/port):
(12.0.0.0/255.255.255.0/0/0) remote ident (addr/mask/prot/port): (11.0.0.0/255.255.255.0/0/0)
current_peer: 10.48.66.156 PERMIT, flags={origin_is_acl,} #pkts encaps: 6, #pkts encrypt: 6,
#pkts digest 6 #pkts decaps: 6, #pkts decrypt: 6, #pkts verify 6 #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.: 193.0.0.5, remote crypto endpt.:
10.48.66.156 path mtu 1500, ipsec overhead 56, media mtu 1500 current outbound spi: 8312e721
inbound esp sas: spi: 0x661d4fad(1713196973) transform: esp-des esp-sha-hmac , in use settings
={Tunnel, } slot: 0, conn id: 1, crypto map: vpn-intf2 sa timing: remaining key lifetime
(k/sec): (4607999/27978) IV size: 8 bytes replay detection support: Y inbound ah sas: inbound
pcp sas: outbound esp sas: spi: 0x8312e721(2199054113) transform: esp-des esp-sha-hmac , in use
settings ={Tunnel, } slot: 0, conn id: 2, crypto map: vpn-intf2 sa timing: remaining key
lifetime (k/sec): (4607999/27978) IV size: 8 bytes replay detection support: Y outbound ah sas:
outbound pcp sas: interface: outside Crypto map tag: toOUT, local addr. 193.0.0.1 local ident
(addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0) remote ident (addr/mask/prot/port):
(12.0.0.1/255.255.255.255/0/0) current_peer: 10.48.66.76 dynamic allocated peer ip: 12.0.0.1
PERMIT, flags={} #pkts encaps: 6, #pkts encrypt: 6, #pkts digest 6 #pkts decaps: 28, #pkts
decrypt: 28, #pkts verify 28 #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.: 193.0.0.1, remote crypto endpt.: 10.48.66.76 path mtu 1500, ipsec overhead 56, media mtu
1500 current outbound spi: 62c47dd7 inbound esp sas: spi: 0x331a3e87(857357959) transform: esp-
des esp-md5-hmac , in use settings ={Tunnel, } slot: 0, conn id: 7, crypto map: toOUT sa timing:
remaining key lifetime (k/sec): (4607996/27359) IV size: 8 bytes replay detection support: Y
inbound ah sas: inbound pcp sas: outbound esp sas: spi: 0x62c47dd7(1657044439) transform: esp-
des esp-md5-hmac , in use settings ={Tunnel, } slot: 0, conn id: 8, crypto map: toOUT sa timing:
remaining key lifetime (k/sec): (4607999/27359) IV size: 8 bytes replay detection support: Y
outbound ah sas: outbound pcp sas: local ident (addr/mask/prot/port):
(193.0.0.1/255.255.255.255/0/0) remote ident (addr/mask/prot/port):
(12.0.0.1/255.255.255.255/0/0) current_peer: 10.48.66.76 dynamic allocated peer ip: 12.0.0.1
PERMIT, flags={} #pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0 #pkts decaps: 0, #pkts
decrypt: 0, #pkts verify 0 #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.: 193.0.0.1, remote crypto endpt.: 10.48.66.76 path mtu 1500, ipsec overhead 56, media mtu
```

1500 current outbound spi: 4e13c751 inbound esp sas: spi: 0x4f3e0026(1329463334) transform: esp-des esp-md5-hmac , in use settings ={Tunnel, } slot: 0, conn id: 3, crypto map: toOUT sa timing: remaining key lifetime (k/sec): (4608000/27972) IV size: 8 bytes replay detection support: Y inbound ah sas: inbound pcp sas: outbound esp sas: spi: 0x4e13c751(1309919057) transform: esp-des esp-md5-hmac , in use settings ={Tunnel, } slot: 0, conn id: 4, crypto map: toOUT sa timing: remaining key lifetime (k/sec): (4608000/27963) IV size: 8 bytes replay detection support: Y outbound ah sas: outbound pcp sas:

show command output (resultado do comando show) para a chuva

```
rain# show version Cisco PIX Firewall Version 6.2(2) Compiled on Tue 11-Sep-01 07:45 by morlee
rain up 2 hours 23 mins Hardware: PIX-525, 256 MB RAM, CPU Pentium III 600 MHz Flash E28F128J3 @
0x300, 16MB BIOS Flash AM29F400B @ 0xffffd8000, 32KB 0: ethernet0: address is 0002.b945.a001, irq
10 1: ethernet1: address is 0002.b945.a002, irq 11 2: ethernet2: address is 00e0.b602.4797, irq
11 3: ethernet3: address is 00e0.b602.4796, irq 10 4: ethernet4: address is 00e0.b602.4795, irq
9 5: ethernet5: address is 00e0.b602.4794, irq 5 Licensed Features: Failover: Enabled VPN-DES:
Enabled VPN-3DES: Enabled Maximum Interfaces: 8 Cut-through Proxy: Enabled Guards: Enabled
Websense: Enabled Inside Hosts: Unlimited Throughput: Unlimited ISAKMP peers: Unlimited Serial
Number: 480380580 (0x1ca206a4) Activation Key: 0x3a08e996 0x3d4a15af 0x604a1272 0xd8fbe3b8 rain#
show route outside 10.0.0.0 255.255.255.0 193.0.0.5 1 OTHER static outside 10.48.66.0
255.255.255.0 10.48.66.156 1 CONNECT static inside 11.0.0.0 255.255.255.0 11.0.0.1 1 CONNECT
static outside 12.0.0.0 255.255.255.0 193.0.0.5 1 OTHER static outside 193.0.0.0 255.255.255.0
10.48.66.44 1 OTHER static rain# show crypto isa sa Total : 2 Embryonic : 0 dst src state
pending created 10.48.66.156 193.0.0.5 QM_IDLE 0 1 193.0.0.5 10.48.66.156 QM_IDLE 0 2 rain# show
crypto ipsec sa interface: outside Crypto map tag: vpn-outside, local addr. 10.48.66.156 local
ident (addr/mask/prot/port): (11.0.0.0/255.255.255.0/0/0) remote ident (addr/mask/prot/port):
(10.0.0.0/255.255.255.0/0/0) current_peer: 193.0.0.5 PERMIT, flags={origin_is_acl,} #pkts
encaps: 8, #pkts encrypt: 8, #pkts digest 8 #pkts decaps: 8, #pkts decrypt: 8, #pkts verify 8
#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.: 10.48.66.156,
remote crypto endpt.: 193.0.0.5 path mtu 1500, ipsec overhead 56, media mtu 1500 current
outbound spi: 0 inbound esp sas: inbound ah sas: inbound pcp sas: outbound esp sas: outbound ah
sas: outbound pcp sas: local ident (addr/mask/prot/port): (11.0.0.0/255.255.255.0/0/0) remote
ident (addr/mask/prot/port): (12.0.0.0/255.255.255.0/0/0) current_peer: 193.0.0.5 PERMIT,
flags={origin_is_acl,} #pkts encaps: 22, #pkts encrypt: 22, #pkts digest 22 #pkts decaps: 22,
#pkts decrypt: 22, #pkts verify 22 #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.: 10.48.66.156, remote crypto endpt.: 193.0.0.5 path mtu 1500, ipsec overhead
56, media mtu 1500 current outbound spi: 661d4fad inbound esp sas: spi: 0x8312e721(2199054113)
transform: esp-des esp-sha-hmac , in use settings ={Tunnel, } slot: 0, conn id: 1, crypto map:
vpn-outside sa timing: remaining key lifetime (k/sec): (4607999/27529) IV size: 8 bytes replay
detection support: Y inbound ah sas: inbound pcp sas: outbound esp sas: spi:
0x661d4fad(1713196973) transform: esp-des esp-sha-hmac , in use settings ={Tunnel, } slot: 0,
conn id: 2, crypto map: vpn-outside sa timing: remaining key lifetime (k/sec): (4607999/27529)
IV size: 8 bytes replay detection support: Y outbound ah sas: outbound pcp sas:
```

show command output (resultado do comando show) para o cadáver

```
carrion# show version Cisco Internetwork Operating System Software IOS (tm) RSP Software (RSP-
JK903SV-M), Version 12.2(6), RELEASE SOFTWARE (fc2) Copyright (c) 1986-2001 by cisco Systems,
Inc. Compiled Wed 07-Nov-01 21:44 by pwade Image text-base: 0x600109C8, data-base: 0x61B42000
ROM: System Bootstrap, Version 11.1(2) [nitin 2], RELEASE SOFTWARE (fc1) BOOTLDR: RSP Software
(RSP-BOOT-M), Version 12.2(6), RELEASE SOFTWARE (fc2) carrion uptime is 2 weeks, 3 days, 22
hours, 32 minutes System returned to ROM by reload at 12:27:14 UTC Wed Oct 10 2001 System image
file is "slot0:rsp-jk9o3sv-mz.122-6.bin" cisco RSP2 (R4700) processor with 131072K/2072K bytes
of memory. R4700 CPU at 100Mhz, Implementation 33, Rev 1.0 Last reset from power-on G.703/E1
software, Version 1.0. G.703/JT2 software, Version 1.0. X.25 software, Version 3.0.0. SuperLAT
software (copyright 1990 by Meridian Technology Corp). Bridging software. TN3270 Emulation
software. Chassis Interface. 1 EIP controller (4 Ethernet). 3 FSIP controllers (24 Serial). 1
VIP2 controller (1 HSSI). 4 Ethernet/IEEE 802.3 interface(s) 24 Serial network interface(s) 1
HSSI network interface(s) 123K bytes of non-volatile configuration memory. 20480K bytes of Flash
PCMCIA card at slot 0 (Sector size 128K). 8192K bytes of Flash internal SIMM (Sector size 256K).
No slave installed in slot 7. Configuration register is 0x2002
```

Troubleshooting

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

Saída do comando debug

Nota: Antes de emitir **comandos debug**, consulte [Informações importantes sobre comandos debug](#).

Saída do comando debug para neve

```
snow# show debug debug crypto ipsec 1 debug crypto isakmp 1 debug crypto engine debug icmp trace
debug fover status tx Off rx Off open Off cable Off txdmp Off rxdmp Off ifc Off rxip Off txip
Off get Off put Off verify Off switch Off fail Off fmsg Off snow# no debug icmp trace ICMP trace
off snow# snow# snow# snow# snow# configure terminal ! the client is connecting !!!!!!!!!!!!!!!
Type help or '?' for a list of available commands. snow# crypto_isakmp_process_block: src
10.48.66.76, dest 193.0.0.1 VPN Peer: ISAKMP: Added new peer: ip:10.48.66.76 Total VPN Peers:1
VPN Peer: ISAKMP: Peer ip:10.48.66.76 Ref cnt incremented to:1 Total VPN Peers:1 OAK_AG exchange
ISAKMP (0): processing SA payload. message ID = 0 ISAKMP (0): Checking ISAKMP transform 1
against priority 10 policy ISAKMP: encryption 3DES-CBC ISAKMP: hash SHA ISAKMP: default group 2
ISAKMP: extended auth pre-share ISAKMP: life type in seconds ISAKMP: life duration (VPI) of 0x0
0x20 0xc4 0x9b ISAKMP (0): atts are not acceptable. Next payload is 3 ISAKMP (0): Checking
ISAKMP transform 2 against priority 10 policy ISAKMP: encryption 3DES-CBC ISAKMP: hash MD5
ISAKMP: default group 2 ISAKMP: extended auth pre-share ISAKMP: life type in seconds ISAKMP:
life duration (VPI) of 0x0 0x20 0xc4 0x9b ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 3 against priority 10 policy ISAKMP: encryption 3DES-CBC
ISAKMP: hash SHA ISAKMP: default group 2 ISAKMP: auth pre-share ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x0 0x20 0xc4 0x9b ISAKMP (0): atts are not acceptable. Next
payload is 3 ISAKMP (0): Checking ISAKMP transform 4 against priority 10 policy ISAKMP:
encryption 3DES-CBC ISAKMP: hash MD5 ISAKMP: default group 2 ISAKMP: auth pre-share ISAKMP: life
type in seconds ISAKMP: life duration (VPI) of 0x0 0x20 0xc4 0x9b ISAKMP (0): atts are not
acceptable. Next payload is 3 ISAKMP (0): Checking ISAKMP transform 5 against priority 10 policy
ISAKMP: encryption DES-CBC ISAKMP: hash SHA ISAKMP: default group 2 ISAKMP: extended auth pre-
share ISAKMP: life type in seconds ISAKMP: life duration (VPI) of 0x0 0x20 0xc4 0x9b ISAKMP (0):
atts are not acceptable. Next payload is 3 ISAKMP (0): Checking ISAKMP transform 6 against
priority 10 policy ISAKMP: encryption DES-CBC ISAKMP: hash MD5 ISAKMP: default group 2 ISAKMP:
extended auth pre-share ISAKMP: life type in seconds ISAKMP: life duration (VPI) of 0x0 0x20
0xc4 0x9b ISAKMP (0): atts are not acceptable. Next payload is 3 ISAKMP (0): Checking ISAKMP
transform 7 against priority 10 policy ISAKMP: encryption DES-CBC ISAKMP: hash SHA ISAKMP:
default group 2 ISAKMP: auth pre-share ISAKMP: life type in seconds ISAKMP: life duration (VPI)
of 0x0 0x20 0xc4 0x9b ISAKMP (0): atts are acceptable. Next payload is 3 ISAKMP (0): processing
KE payload. message ID = 0 ISAKMP (0): processing NONCE payload. message ID = 0 ISAKMP (0):
processing ID payload. message ID = 0 ISAKMP (0): processing vendor id payload ISAKMP (0):
processing vendor id payload ISAKMP (0): remote peer supports dead peer detection ISAKMP (0):
processing vendor id payload ISAKMP (0): speaking to a Unity client ISAKMP: Created a peer node
for 10.48.66.76 ISAKMP (0): ID payload next-payload : 10 type : 1 protocol : 17 port : 500
length : 8 ISAKMP (0): Total payload length: 12 return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 10.48.66.76, dest 193.0.0.1 OAK_AG exchange ISAKMP (0):
processing HASH payload. message ID = 0 ISAKMP (0): processing NOTIFY payload 24578 protocol 1
spi 0, message ID = 0 ISAKMP (0): processing notify INITIAL_CONTACTIPSEC(key_engine): got a
queue event... IPSEC(key_engine_delete_sas): rec'd delete notify from ISAKMP
IPSEC(key_engine_delete_sas): delete all SAs shared with 10.48.66.76 ISAKMP (0): SA has been
authenticated return status is IKMP_NO_ERROR crypto_isakmp_process_block: src 10.48.66.76, dest
193.0.0.1 ISAKMP_TRANSACTION exchange ISAKMP (0:0): processing transaction payload from
10.48.66.76. message ID = 0 ISAKMP: Config payload CFG_REQUEST ISAKMP (0:0): checking request:
ISAKMP: attribute IP4_ADDRESS (1) ISAKMP: attribute IP4_NETMASK (2) ISAKMP: attribute IP4_DNS
(3) ISAKMP: attribute IP4_NBNS (4) ISAKMP: attribute ADDRESS_EXPIRY (5) Unsupported Attr: 5
ISAKMP: attribute APPLICATION_VERSION (7) Unsupported Attr: 7 ISAKMP: attribute UNKNOWN (28672)
```

Unsupported Attr: 28672 ISAKMP: attribute UNKNOWN (28673) Unsupported Attr: 28673 ISAKMP: attribute UNKNOWN (28674) ISAKMP: attribute UNKNOWN (28676) ISAKMP: attribute UNKNOWN (28679) Unsupported Attr: 28679 ISAKMP: attribute UNKNOWN (28680) Unsupported Attr: 28680 ISAKMP: attribute UNKNOWN (28677) Unsupported Attr: 28677 ISAKMP (0:0): responding to peer config from 10.48.66.76. ID = 1245965288 return status is IKMP_NO_ERROR crypto_isakmp_process_block: src 10.48.66.76, dest 193.0.0.1 OAK_QM exchange oakley_process_quick_mode: OAK_QM_IDLE ISAKMP (0): processing SA payload. message ID = 2141307752 ISAKMP : Checking IPsec proposal 1 ISAKMP: transform 1, ESP_3DES ISAKMP: attributes in transform: ISAKMP: authenticator is HMAC-MD5 ISAKMP: encaps is 1 ISAKMP: SA life type in seconds ISAKMP: SA life duration (VPI) of 0x0 0x20 0xc4 0x9b IPSEC(validate_proposal): transform proposal (prot 3, trans 3, hmac_alg 1) not supported ISAKMP (0): atts not acceptable. Next payload is 0 ISAKMP (0): skipping next ANDED proposal (1) ISAKMP : Checking IPsec proposal 2 ISAKMP: transform 1, ESP_3DES ISAKMP: attributes in transform: ISAKMP: authenticator is HMAC-SHA ISAKMP: encaps is 1 ISAKMP: SA life type in seconds ISAKMP: SA life duration (VPI) of 0x0 0x20 0xc4 0x9b IPSEC(validate_proposal): transform proposal (prot 3, trans 3, hmac_alg 2) not supported ISAKMP (0): atts not acceptable. Next payload is 0 ISAKMP (0): skipping next ANDED proposal (2) ISAKMP : Checking IPsec proposal 3 ISAKMP: transform 1, ESP_3DES ISAKMP: attributes in transform: ISAKMP: authenticator is HMAC-MD5 ISAKMP: encaps is 1 ISAKMP: SA life type in seconds ISAKMP: SA life duration (VPI) of 0x0 0x20 0xc4 0x9b IPSEC(validate_proposal): transform proposal (prot 3, trans 3, hmac_alg 1) not supported ISAKMP (0): atts not acceptable. Next payload is 0 ISAKMP : Checking IPsec proposal 4 ISAKMP: transform 1, ESP_3DES ISAKMP: attributes in transform: ISAKMP: authenticator is HMAC-SHA ISAKMP: encaps is 1 ISAKMP: SA life type in seconds ISAKMP: SA life duration (VPI) of 0x0 0x20 0xc4 0x9b IPSEC(validate_proposal): transform proposal (prot 3, trans 3, hmac_alg 2) not supported ISAKMP (0): atts not acceptable. Next payload is 0 ISAKMP : Checking IPsec proposal 5 ISAKMP: transform 1, ESP_DES ISAKMP: attributes in transform: ISAKMP: authenticator is HMAC-MD5 ISAKMP: encaps is 1 ISAKMP: SA life type in seconds ISAKMP: SA life duration (VPI) of 0x0 0x20 0xc4 0x9b ISAKMP (0): atts are acceptable. ISAKMP (0): bad SPI size of 2 octets! ISAKMP : Checking IPsec proposal 6 ISAKMP: transform 1, ESP_DES ISAKMP: attributes in transform: ISAKMP: authenticator is HMAC-SHA ISAKMP: encaps is 1 ISAKMP: SA life type in seconds ISAKMP: SA life duration (VPI) of 0x0 0x20 0xc4 0x9b IPSEC(validate_proposal): transform proposal (prot 3, trans 2, hmac_alg 2) not supported ISAKMP (0): atts not acceptable. Next payload is 0 ISAKMP (0): skipping next ANDED proposal (6) ISAKMP : Checking IPsec proposal 7 ISAKMP: transform 1, ESP_DES ISAKMP: attributes in transform: ISAKMP: authenticator is HMAC-MD5 ISAKMP: encaps is 1 ISAKMP: SA life type in seconds ISAKMP: SA life duration (VPI) of 0x0 0x20 0xc4 0x9b ISAKMP (0): atts are acceptable. IPSEC(validate_proposal_request): proposal part #1, (key eng. msg.) dest= 193.0.0.1, src= 10.48.66.76, dest_proxy= 193.0.0.1/255.255.255.255/0/0 (type=1), src_proxy= 12.0.0.1/255.255.255.255/0/0 (type=1), protocol= ESP, transform= esp-des esp-md5-hmac , lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4 ISAKMP (0): processing NONCE payload. message ID = 2141307752 ISAKMP (0): processing ID payload. message ID = 2141307752 ISAKMP (0): ID_IPV4_ADDR src 12.0.0.1 prot 0 port 0 ISAKMP (0): processing ID payload. message ID = 2141307752 ISAKMP (0): ID_IPV4_ADDR dst 193.0.0.1 prot 0 port 0 IPSEC(key_engine): got a queue event... IPSEC(spi_response): getting spi 0x4f3e0026(1329463334) for SA from 10.48.66.76 to 193.0.0.1 for prot 3 return status is IKMP_NO_ERROR crypto_isakmp_process_block: src 10.48.66.76, dest 193.0.0.1 OAK_QM exchange oakley_process_quick_mode: OAK_QM_IDLE ISAKMP (0): processing SA payload. message ID = 2151626816 ISAKMP : Checking IPsec proposal 1 ISAKMP: transform 1, ESP_3DES ISAKMP: attributes in transform: ISAKMP: authenticator is HMAC-MD5 crypto_isakmp_process_block: src 10.48.66.76, dest 193.0.0.1 OAK_QM exchange oakley_process_quick_mode: OAK_QM_AUTH_AWAITmap_alloc_entry: allocating entry 3 map_alloc_entry: allocating entry 4 ISAKMP (0): Creating IPsec SAs inbound SA from 10.48.66.76 to 193.0.0.1 (proxy 12.0.0.1 to 193.0.0.1) has spi 1329463334 and conn_id 3 and flags 4 lifetime of 2147483 seconds outbound SA from 193.0.0.1 to 10.48.66.76 (proxy 193.0.0.1 to 12.0.0.1) has spi 1309919057 and conn_id 4 and flags 4 lifetime of 2147483 seconds IPSEC(key_engine): got a queue event... IPSEC(initialize_sas): , (key eng. msg.) dest= 193.0.0.1, src= 10.48.66.76, dest_proxy= 193.0.0.1/0.0.0.0/0/0 (type=1), src_proxy= 12.0.0.1/0.0.0.0/0/0 (type=1), protocol= ESP, transform= esp-des esp-md5-hmac , lifedur= 2147483s and 0kb, spi= 0x4f3e0026(1329463334), conn_id= 3, keysize= 0, flags= 0x4 IPSEC(initialize_sas): , (key eng. msg.) src= 193.0.0.1, dest= 10.48.66.76, src_proxy= 193.0.0.1/0.0.0.0/0/0 (type=1), dest_proxy= 12.0.0.1/0.0.0.0/0/0 (type=1), protocol= ESP, transform= esp-des esp-md5-hmac , lifedur= 2147483s and 0kb, spi= 0x4e13c751(1309919057), conn_id= 4, keysize= 0, flags= 0x4 VPN Peer: IPSEC: Peer ip:10.48.66.76 Ref cnt incremented to:2 Total VPN Peers:1 VPN Peer: IPSEC: Peer ip:10.48.66.76 Ref cnt incremented to:3 Total VPN Peers:1 return status is IKMP_NO_ERROR crypto_isakmp_process_block: src 10.48.66.76, dest 193.0.0.1 OAK_QM exchange oakley_process_quick_mode: OAK_QM_AUTH_AWAITmap_alloc_entry: allocating entry 7 map_alloc_entry: allocating entry 8 ISAKMP (0): Creating IPsec SAs inbound SA from 10.48.66.76 to 193.0.0.1 (proxy 12.0.0.1 to 0.0.0.0) has

spi 857357959 and conn_id 7 and flags 4 lifetime of 2147483 seconds outbound SA from 193.0.0.1 to 10.48.66.76 (proxy 0.0.0.0 to 12.0.0.1) has spi 1657044439 and conn_id 8 and flags 4 lifetime of 2147483 seconds IPSEC(key_engine): got a queue event... IPSEC(initialize_sas): , (key eng. msg.) dest= 193.0.0.1, src= 10.48.66.76, dest_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4), src_proxy= 12.0.0.1/0.0.0.0/0/0 (type=1), protocol= ESP, transform= esp-des esp-md5-hmac , lifedur= 2147483s and 0kb, spi= 0x331a3e87(857357959), conn_id= 7, keysize= 0, flags= 0x4 IPSEC(initialize_sas): , (key eng. msg.) src= 193.0.0.1, dest= 10.48.66.76, src_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4), dest_proxy= 12.0.0.1/0.0.0.0/0/0 (type=1), protocol= ESP, transform= esp-des esp-md5-hmac , lifedur= 2147483s and 0kb, spi= 0x62c47dd7(1657044439), conn_id= 8, keysize= 0, flags= 0x4 VPN Peer: IPSEC: Peer ip:10.48.66.76 Ref cnt incremented to:4 Total VPN Peers:1 VPN Peer: IPSEC: Peer ip:10.48.66.76 Ref cnt incremented to:5 Total VPN Peers:1 return status is IKMP_NO_ERROR602301: sa created, (sa) sa_dest= 193.0.0.1, sa_prot= 50, sa_spi= 0x4f3e0026(1329463334), sa_trans= esp-des esp-md5-hmac , sa_conn_id= 3 602301: sa created, (sa) sa_dest= 10.48.66.76, sa_prot= 50, sa_spi= 0x4e13c751(1309919057), sa_trans= esp-des esp-md5-hmac , sa_conn_id= 4 602301: sa created, (sa) sa_dest= 193.0.0.1, sa_prot= 50, sa_spi= 0x331a3e87(857357959), sa_trans= esp-des esp-md5-hmac , sa_conn_id= 7 602301: sa created, (sa) sa_dest= 10.48.66.76, sa_prot= 50, sa_spi= 0x62c47dd7(1657044439), sa_trans= esp-des esp-md5-hmac , sa_conn_id= 8 ISADB: reaper checking SA 0x81153ac0, conn_id = 0 snow# snow# snow# snow# 302010: 0 in use, 0 most used snow# snow# snow# snow# snow# ! client will now ping 11.0.0.2 Type help or '?' for a list of available commands. snow# 6 VPN Peer: ISAKMP: Added new peer: ip:10.48.66.156 Total VPN Peers:2 VPN Peer: ISAKMP: Peer ip:10.48.66.156 Ref cnt incremented to:1 Total VPN Peers:2 ISAKMP (0): beginning Main Mode exchange09001: Built local-host intf2:11.0.0. crypto_isakmp_process_block: src 10.48.66.156, dest 193.0.0.5 OAK_MM exchange ISAKMP (0): processing SA payload. message ID = 0 ISAKMP (0): Checking ISAKMP transform 1 against priority 10 policy ISAKMP: encryption DES-CBC ISAKMP: hash SHA ISAKMP: default group 2 ISAKMP: auth pre-share ISAKMP: life type in seconds ISAKMP: life duration (VPI) of 0x0 0x1 0x51 0x80 ISAKMP (0): atts are acceptable. Next payload is 0 ISAKMP (0): SA is doing pre-shared key authentication using id type ID_IPV4_ADDR return status is IKMP_NO_ERROR2 702303: sa_request, (key eng. msg. crypto_isakmp_process_block: src 10.48.66.156, dest 193.0.0.5 OAK_MM exchange ISAKMP (0): processing KE payload. message ID = 0 ISAKMP (0): processing NONCE payload. message ID = 0 ISAKMP (0): processing vendor id payload ISAKMP (0): processing vendor id payload ISAKMP (0): remote peer supports dead peer detection ISAKMP (0): processing vendor id payload ISAKMP (0): speaking to another IOS box! ISAKMP (0): ID payload next-payload : 8 type : 1 protocol : 17 port : 500 length : 8 ISAKMP (0): Total payload length: 12 return status is IKMP_NO_ERROR crypto_isakmp_process_block: src 10.48.66.156, dest 193.0.0.5 OAK_MM exchange ISAKMP (0): processing ID payload. message ID = 0 ISAKMP (0): processing HASH payload. message ID = 0 ISAKMP (0): SA has been authenticated ISAKMP (0): beginning Quick Mode exchange, M-ID of - 931180733:c87f4f43IPSEC(key_engine): got a queue event... IPSEC(spi_response): getting spi 0x661d4fad(1713196973) for SA from 10.48.66.156 to 193.0.0.5 for prot 3 return status is IKMP_NO_ERROR ISAKMP (0): sending INITIAL_CONTACT notify crypto_isakmp_process_block: src 10.48.66.156, dest 193.0.0.5 OAK_QM exchange oakley_process_quick_mode: OAK_QM_IDLE ISAKMP (0): processing SA payload. message ID = 3363786563 ISAKMP : Checking IPsec proposal 1 ISAKMP: transform 1, ESP_DES ISAKMP: attributes in transform: ISAKMP: encaps is 1 ISAKMP: SA life type in seconds ISAKMP: SA life duration (basic) of 28800 ISAKMP: SA life type in kilobytes ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0 ISAKMP: authenticator is HMAC-SHA ISAKMP (0): atts are acceptable.IPSEC(validate_proposal_request): proposal part #1, (key eng. msg.) dest= 10.48.66.156, src= 193.0.0.5, dest_proxy= 11.0.0.0/255.255.255.0/0/0 (type=4), src_proxy= 12.0.0.0/255.255.255.0/0/0 (type=4), protocol= ESP, transform= esp-des esp-sha-hmac , lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4 ISAKMP (0): processing NONCE payload. message ID = 3363786563 ISAKMP (0): processing ID payload. message ID = 3363786563 ISAKMP (0): processing ID payload. message ID = 3363786563map_alloc_entry: allocating entry 1 map_alloc_entry: allocating entry 2 ISAKMP (0): Creating IPsec SAs inbound SA from 10.48.66.156 to 193.0.0.5 (proxy 11.0.0.0 to 12.0.0.0) has spi 1713196973 and conn_id 1 and flags 4 lifetime of 28800 seconds lifetime of 4608000 kilobytes outbound SA from 193.0.0.5 to 10.48.66.156 (proxy 12.0.0.0 to 11.0.0.0) has spi 2199054113 and conn_id 2 and flags 4 lifetime of 28800 seconds lifetime of 4608000 kilobytesIPSEC(key_engine): got a queue event... IPSEC(initialize_sas): , (key eng. msg.) dest= 193.0.0.5, src= 10.48.66.156, dest_proxy= 12.0.0.0/255.255.255.0/0/0 (type=4), src_proxy= 11.0.0.0/255.255.255.0/0/0 (type=4), protocol= ESP, transform= esp-des esp-sha-hmac , lifedur= 28800s and 4608000kb, spi= 0x661d4fad(1713196973), conn_id= 1, keysize= 0, flags= 0x4 IPSEC(initialize_sas): , (key eng. msg.) src= 193.0.0.5, dest= 10.48.66.156, src_proxy= 12.0.0.0/255.255.255.0/0/0 (type=4), dest_proxy= 11.0.0.0/255.255.255.0/0/0 (type=4), protocol= ESP, transform= esp-des esp-sha-hmac , lifedur= 28800s and 4608000kb, spi= 0x8312e721(2199054113), conn_id= 2, keysize= 0, flags= 0x4 VPN Peer: IPSEC: Peer ip:10.48.66.156 Ref cnt incremented to:2 Total VPN Peers:2 VPN Peer: IPSEC: Peer ip:10.48.66.156 Ref cnt

```
incremented to:3 Total VPN Peers:2 return status is IKMP_NO_ERROR) src= 193.0.0.5, dest=
10.48.66.156, src_proxy= 12.0.0.0/255.255.255.0/0/0 (type=4), dest_proxy=
11.0.0.0/255.255.255.0/0/0 (type=4), protocol= ESP, transform= esp-des esp-sha-hmac , lifedur=
28800s and 4608000kb, spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4004 602301: sa created,
(sa) sa_dest= 193.0.0.5, sa_prot= 50, sa_spi= 0x661d4fad(1713196973), sa_trans= esp-des esp-sha-
hmac , sa_conn_id= 1 602301: sa created, (sa) sa_dest= 10.48.66.156, sa_prot= 50, sa_spi=
0x8312e721(2199054113), sa_trans= esp-des esp-sha-hmac , sa_conn_id= 2
```

Saída do comando debug para rain

```
rain# ! client will now ping 11.0.0.2
Type help or '?' for a list of available commands.
rain# sh debug
debug crypto ipsec 1
debug crypto isakmp 1
debug crypto engine
debug fover status
txOff
rxOff
openOff
cableOff
txdmpOff
rxdmpOff
ifcOff
rxipOff
txipOff
getOff
putOff
verifyOff
switchOff
failOff
fmsgOff
rain#

crypto_isakmp_process_block: src 193.0.0.5, dest 10.48.66.156
VPN Peer: ISAKMP: Peer ip:193.0.0.5
  Ref cnt incremented to:2 Total VPN Peers:1
OAK_MM exchange
ISAKMP (0): processing SA payload. message ID = 0

ISAKMP (0): Checking ISAKMP transform 1 against priority 10 policy
ISAKMP:      encryption DES-CBC
ISAKMP:      hash SHA
ISAKMP:      default group 2
ISAKMP:      auth pre-share
ISAKMP (0): atts are acceptable. Next payload is 0
ISAKMP (0): SA is doing pre-shared key authentication using id type ID_FQDN
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 193.0.0.5, dest 10.48.66.156
OAK_MM exchange
ISAKMP (0): processing KE payload. message ID = 0

ISAKMP (0): processing NONCE payload. message ID = 0

ISAKMP (0): processing vendor id payload

ISAKMP (0): processing vendor id payload

ISAKMP (0): remote peer supports dead peer detection

ISAKMP (0): processing vendor id payload

ISAKMP (0): speaking to another IOS box!
```

```
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 193.0.0.5, dest 10.48.66.156
OAK_MM exchange
ISAKMP (0): processing ID payload. message ID = 0
ISAKMP (0): processing HASH payload. message ID = 0
ISAKMP (0): SA has been authenticated

ISAKMP (0): ID payload
next-payload : 8
type          : 2
protocol      : 17
port         : 500
length       : 9
ISAKMP (0): Total payload length: 13
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 193.0.0.5, dest 10.48.66.156
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_IDLE
ISAKMP (0): processing SA payload. message ID = 3363786563

ISAKMP : Checking IPsec proposal 1

ISAKMP: transform 1, ESP_DES
ISAKMP:  attributes in transform:
ISAKMP:  encaps is 1
ISAKMP:  SA life type in seconds
ISAKMP:  SA life duration (basic) of 28800
ISAKMP:  SA life type in kilobytes
ISAKMP:  SA life duration (VPI) of 0x0 0x46 0x50 0x0
ISAKMP:  authenticator is HMAC-SHA
ISAKMP (0): atts are acceptable.IPSEC(validate_proposal_request):
  proposal part #1,
(key eng. msg.) dest= 10.48.66.156, src= 193.0.0.5,
  dest_proxy= 11.0.0.0/255.255.255.0/0/0 (type=4),
  src_proxy= 12.0.0.0/255.255.255.0/0/0 (type=4),
  protocol= ESP, transform= esp-des esp-sha-hmac ,
  lifedur= 0s and 0kb,
  spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4

ISAKMP (0): processing NONCE payload. message ID = 3363786563

ISAKMP (0): processing ID payload. message ID = 3363786563
ISAKMP (0): ID_IPV4_ADDR_SUBNET src 12.0.0.0/255.255.255.0 prot 0 port 0
ISAKMP (0): processing ID payload. message ID = 3363786563
ISAKMP (0): ID_IPV4_ADDR_SUBNET dst 11.0.0.0/255.255.255.0 prot 0 port 0
ISAKMP (0): processing NOTIFY payload 24578 protocol 1
spi 0, message ID = 3363786563
ISAKMP (0): processing notify INITIAL_CONTACTIPSEC(key_engine):
  got a queue event...
IPSEC(key_engine_delete_sas): rec'd delete notify from ISAKMP
IPSEC(key_engine_delete_sas): delete all SAs shared with          193.0.0.5
IPSEC(key_engine): got a queue event...
IPSEC(spi_response): getting spi 0x8312e721(2199054113) for SA
from          193.0.0.5 to          10.48.66.156 for prot 3

return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 193.0.0.5, dest 10.48.66.156
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_AUTH_AWAITmap_alloc_entry: allocating entry 1
map_alloc_entry: allocating entry 2
```



```
ISAKMP (0): Creating IPsec SAs
  inbound SA from      193.0.0.5 to    10.48.66.156 (proxy
12.0.0.0 to          11.0.0.0)
  has spi 2199054113 and conn_id 1 and flags 4
  lifetime of 28800 seconds
  lifetime of 4608000 kilobytes
  outbound SA from    10.48.66.156 to    193.0.0.5 (proxy
11.0.0.0 to          12.0.0.0)
  has spi 1713196973 and conn_id 2 and flags 4
  lifetime of 28800 seconds
  lifetime of 4608000 kilobytesIPSEC(key_engine): got a queue event...
IPSEC(initialize_sas): ,
(key eng. msg.) dest= 10.48.66.156, src= 193.0.0.5,
  dest_proxy= 11.0.0.0/255.255.255.0/0/0 (type=4),
  src_proxy= 12.0.0.0/255.255.255.0/0/0 (type=4),
  protocol= ESP, transform= esp-des esp-sha-hmac ,
  lifedur= 28800s and 4608000kb,
  spi= 0x8312e721(2199054113), conn_id= 1, keysize= 0, flags= 0x4
IPSEC(initialize_sas): ,
(key eng. msg.) src= 10.48.66.156, dest= 193.0.0.5,
  src_proxy= 11.0.0.0/255.255.255.0/0/0 (type=4),
  dest_proxy= 12.0.0.0/255.255.255.0/0/0 (type=4),
  protocol= ESP, transform= esp-des esp-sha-hmac ,
  lifedur= 28800s and 4608000kb,
  spi= 0x661d4fad(1713196973), conn_id= 2, keysize= 0, flags= 0x4

VPN Peer: IPSEC: Peer ip:193.0.0.5 Ref cnt incremented to:3 Total VPN Peers:1
VPN Peer: IPSEC: Peer ip:193.0.0.5 Ref cnt incremented to:4 Total VPN Peers:1
return status is IKMP_NO_ERROR
ISADB: reaper checking SA 0x810a9b98, conn_id = 0
ISADB: reaper checking SA 0x810b9240, conn_id = 0
rain#
```

[Informações Relacionadas](#)

- [Página de Suporte do Cisco VPN Client](#)
- [Página de suporte do IPsec](#)
- [Página de suporte do PIX](#)
- [Solicitações de Comentários \(RFCs\)](#)
- [Suporte Técnico - Cisco Systems](#)