

Configurando o IPsec entre o hub e os PIX Remotos com cliente VPN e autenticação estendida

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Informações de Apoio](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurações](#)

[Verificar](#)

[Troubleshooting](#)

[Comandos para Troubleshooting](#)

[Depurações do PIX de hub](#)

[Informações Relacionadas](#)

[Introdução](#)

Este documento ilustra uma configuração IPsec que inclua o gateway para gateway e a funcionalidade do usuário remoto. Com a autenticação estendida (Xauth), o dispositivo é autenticado através da chave pré-compartilhada e o usuário é autenticado através de um desafio do tipo "nome de usuário/senha".

[Pré-requisitos](#)

[Requisitos](#)

Não existem requisitos específicos para este documento.

[Componentes Utilizados](#)

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

- Versão 6.3(3) do PIX Firewall
- Versão Cliente VPN Cisco 3.5

- Versão 2.6 do Cisco Secure ACS for Windows

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 a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

Consulte as [Convenções de Dicas Técnicas da Cisco](#) para obter mais informações sobre convenções de documentos.

Informações de Apoio

Neste exemplo, há um túnel de IPsec do gateway para gateway do PIX remoto ao PIX de hub. Este túnel cifra o tráfego da rede 10.48.67.x atrás do PIX remoto à rede 10.48.66.x atrás do PIX de hub. O PC no Internet pode formar um túnel de IPsec com o PIX de hub à rede 10.48.66.x.

A fim usar os recursos xauth, você deve primeiramente estabelecer sua autenticação básica, autorização, e server da contabilidade (AAA). Use o **comando crypto map client authentication** para dizer ao PIX Firewall para usar o desafio do Xauth (nome de usuário e senha RADIUS/TACACS+) durante a fase 1 de Internet Key Exchange (IKE) a fim autenticar o IKE. Se o Xauth falha, a associação de segurança IKE não está estabelecida. Especifique o mesmo nome de servidor AAA dentro da indicação de **comando crypto map client authentication** que é especificada na indicação de **comando aaa-server**. O usuário remoto deve executar a Versão Cliente VPN Cisco 3.x ou mais tarde.

Nota: Cisco recomenda o Cisco VPN Client 3.5.x ou mais tarde. O cliente VPN 1.1 não trabalha com esta configuração e é fora do âmbito deste documento.

Nota: O 3.6 e mais recente do Cisco VPN Client não apoia o grupo de transformação de DES/sha.

Se precisar restaurar a configuração sem o Xauth, use o comando no crypto map client authentication. O recurso Xauth não é habilitado por padrão.

Nota: A tecnologia de criptografia está sujeita a controles de exportação. É sua responsabilidade conhecer a lei relativa à exportação de tecnologia de criptografia. Refira o [Home Page do departamento de administração de exportação](#) para mais informação. [Envie um email a export@cisco.com](mailto:export@cisco.com) se você tem quaisquer perguntas relativas ao controle de exportação.

Nota: Na versão 5.3 e mais recente do PIX Firewall, as portas radius configuráveis foram introduzidas. Alguns servidores RADIUS utilizam portas RADIUS diferentes de 1645/1646 (geralmente 1812/1813). Em PIX 5.3 e mais recente, a autenticação RADIUS e as portas de relatório podem ser mudadas para outras diferentes do padrão 1645/1646 usando estes comandos:

```
aaa-server radius-authport # aaa-server radius-acctport #
```

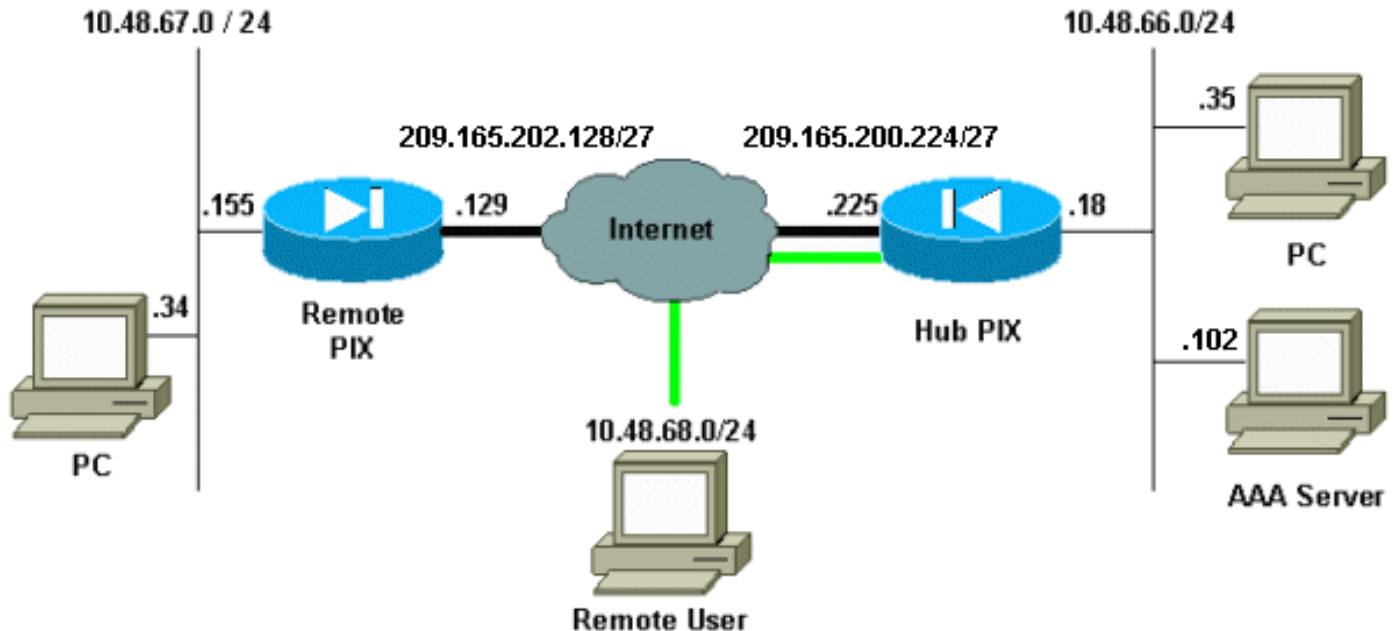
Configurar

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

Nota: Use a ferramenta [Command Lookup Tool](#) ([apenas para clientes registrados](#)) para obter mais informações sobre os comandos usados neste documento.

Diagrama de Rede

Este diagrama usa-se linhas em negrito verdes e pretas a fim indicar os túneis VPN.



Configurações

Este documento utiliza estas configurações.

- [PIX de hub](#)
- [PIX remoto](#)

Nota: Para o exemplo neste documento, o endereço IP de Um ou Mais Servidores Cisco ICM NT do servidor de VPN é 209.165.200.225, o nome do grupo é "vpn3000," e o group password é Cisco.

Configuração de PIX de hub

```
PIX Version 6.3(3)
interface ethernet0 auto
interface ethernet1 auto
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password OnTrBUG1Tp0edmkr encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname hubfixup 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
!--- Include traffic in the encryption process. access-
list 101 permit ip 10.48.66.0 255.255.255.0 10.48.67.0
255.255.255.0 !--- Accept traffic from the Network
Address Translation (NAT) process access-list nonat
permit ip 10.48.66.0 255.255.255.0 10.48.67.0
255.255.255.0 access-list nonat permit ip 10.48.66.0
255.255.255.0 10.48.68.0 255.255.255.0 pager lines 24
mtu outside 1500 mtu inside 1500 ip address outside
209.165.200.225 255.255.255.224 ip address inside
10.48.66.18 255.255.255.0 ip audit info action alarm ip
audit attack action alarm ip local pool mypool
10.48.68.1-10.48.68.254 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 global (outside) 1 209.16.200.230-
209.16.200.240 netmask 255.255.255.224 global (outside)
1 209.16.200.241 !--- Except traffic from the NAT
process. nat (inside) 0 access-list nonat nat (inside) 1
10.48.66.0 255.255.255.0 0 0 route outside 0.0.0.0
0.0.0.0 209.165.200.226 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 uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+ aaa-server RADIUS
protocol radius aaa-server LOCAL protocol local aaa-
server mytacacs protocol tacacs+ aaa-server mytacacs
(inside) host 10.48.66.102 cisco timeout 5 no snmp-
server location no snmp-server contact snmp-server
community public no snmp-server enable traps floodguard
enable sysopt connection permit-ipsec crypto ipsec
transform-set myset esp-des esp-md5-hmac crypto dynamic-
map dynmap 10 set transform-set myset !--- Use the
crypto-map sequence 10 command for PIX to PIX. crypto
map mymap 10 ipsec-isakmp crypto map mymap 10 match
address 101 crypto map mymap 10 set peer 209.165.202.129
crypto map mymap 10 set transform-set myset !--- Use the
crypto-map sequence 20 command for PIX to VPN Client.
crypto map mymap 20 ipsec-isakmp dynamic dynmap crypto
map mymap client authentication mytacacs crypto map
mymap interface outside isakmp enable outside isakmp key
***** address 209.165.202.129 netmask 255.255.255.255
isakmp identity address isakmp policy 10 authentication
pre-share isakmp policy 10 encryption des isakmp policy
10 hash md5 !--- ISAKMP policy for VPN Client that runs
3.x code needs to be DH group 2. isakmp policy 10 group
2 isakmp policy 10 lifetime 86400 !--- IPsec group
configuration for VPN Client. vpngroup vpn3000 address-
pool mypool vpngroup vpn3000 dns-server 10.48.66.129
vpngroup vpn3000 wins-server 10.48.66.129 vpngroup
vpn3000 default-domain cisco.com vpngroup vpn3000 idle-
time 1800 vpngroup vpn3000 password ***** telnet
timeout 5 ssh timeout 5 console timeout 0 terminal width
80 Cryptochecksum:7293dd9fc7c58ff5d65f042dd6ddbe13 : end

```

Configuração do PIX remoto

```

PIX Version 6.3(3)
interface ethernet0 auto
interface ethernet1 100basetx
interface ethernet2 auto shutdown
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 intf2 security4

```

```

enable password OnTrBUGlTp0edmkr encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname remote
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
access-list 101 permit ip 10.48.67.0 255.255.255.0
10.48.66.0 255.255.255.0 !--- Accept traffic from the
NAT process. access-list nonat permit ip 10.48.67.0
255.255.255.0 10.48.66.0 255.255.255.0 pager lines 24
mtu outside 1500 mtu inside 1500 mtu intf2 1500 ip
address outside 209.165.202.129 255.255.255.224 ip
address inside 10.48.67.155 255.255.255.0 no ip address
intf2 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 no failover ip address intf2 pdm history enable
arp timeout 14400 global (outside) 1 209.16.202.135-
209.16.202.145 netmask 255.255.255.224 global (outside)
1 209.16.202.146 !--- Except traffic from the NAT
process. nat (inside) 0 access-list nonat nat (inside) 1
10.48.0.0 255.255.255.0 0 0 nat (inside) 1 10.48.67.0
255.255.255.0 0 0 route outside 0.0.0.0 0.0.0.0
209.165.202.130 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 uauth 0:05:00 absolute aaa-
server TACACS+ protocol tacacs+ aaa-server RADIUS
protocol radius aaa-server LOCAL protocol local no snmp-
server location no snmp-server contact snmp-server
community public no snmp-server enable traps floodguard
enable sysopt connection permit-ipsec crypto ipsec
transform-set myset esp-des esp-md5-hmac crypto map
mymap 10 ipsec-isakmp !--- Include traffic in the
encryption process. crypto map mymap 10 match address
101 crypto map mymap 10 set peer 209.165.200.225 crypto
map mymap 10 set transform-set myset crypto map mymap
interface outside isakmp enable outside isakmp key
***** address 209.165.200.225 netmask 255.255.255.255
isakmp identity address isakmp policy 10 authentication
pre-share isakmp policy 10 encryption des isakmp policy
10 hash md5 isakmp policy 10 group 2 isakmp policy 10
lifetime 86400 telnet timeout 5 ssh timeout 5 console
timeout 0 terminal width 80
Cryptochecksum:13ef4d29384c65c2cd968b5d9396f6e8 : end

```

Refira a seção das “configurações” de [configurar o PIX ao PIX e o cliente VPN 3.x](#) para informações detalhadas sobre de como estabelecer o cliente VPN. Também, refira [como adicionar a autenticação de AAA \(Xauth\) ao PIX IPSec 5.2 e mais atrasado](#) para obter informações adicionais sobre da configuração da autenticação de AAA ao PIX IPSec.

Verificar

Esta seção fornece informações que você pode usar para confirmar se a sua configuração funciona corretamente.

A [Output Interpreter Tool \(apenas para clientes registrados\)](#) (OIT) suporta determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

- `show crypto isakmp sa` — Mostra as associações de segurança da Fase 1.
- `show crypto ipsec sa` — Mostra associações de segurança da Fase 2.

Troubleshooting

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

Comandos para Troubleshooting

A [Output Interpreter Tool \(apenas para clientes registrados\)](#) (OIT) suporta determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

Nota: Consulte [Informações Importantes sobre Comandos de Depuração](#) antes de usar comandos **debug**.

Estes debugs devem ser executado em ambos os roteadores de IPsec (pares). As associações de segurança devem ser limpas em ambos os peers.

- `debug crypto isakmp` — Exibe erros durante a Fase 1.
- `debug crypto ipsec` — Exibe erros durante a Fase 2.
- `debug crypto engine` — Exibe informações a partir do cripto mecanismo.
- `clear crypto isakmp sa` — Cancela as associações de segurança da fase 1.
- `clear crypto ipsec sa` — Cancela as associações de segurança da fase 2.
- `debugar o raio [sessão | tudo | username do usuário]` — disponível em PIX 6.2, este comando registra a informação de sessão do RADIUS e os atributos de pacotes de informação de RADIUS enviados e recebidos.
- `debugar tacacs [sessão|<user_name> do usuário]` — disponível em PIX 6.3, este comando registra a informação TACACS.
- `debugar aaa [autenticação|autorização|explicar|interno]` — disponível em PIX 6.3, informação de subsistema das mostras AAA.

Depurações do PIX de hub

Nota: Esteja ciente que às vezes quando a negociação de IPsec é bem sucedida, não todo o debug obtém mostrado no PIX devido à identificação de bug Cisco [CSCdu84168 \(clientes registrados somente\)](#) qual é uma duplicata da identificação de bug Cisco interna [CSCdt31745 \(clientes registrados somente\)](#). Isto não é ainda resolvido até à data da escrita deste documento.

Nota: Às vezes o IPsec VPN dos clientes VPN não pode terminar no PIX. A fim resolver esta edição, assegure-se de que o PC cliente não tenha nenhuns Firewall. Se os Firewall estão

presente, verifique se a porta 500 e 4500 UDP é desabilitada. Se este é o caso, permita o IPsec sobre o TCP ou desbloqueie as portas UDP.

Debuga de um túnel de IPsec dinâmico entre o hub e os PIX Remotos

```
crypto_isakmp_process_block:src:209.165.202.129,
dest:209.165.200.225 spt:500 dpt:500
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 MD5
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_ERROR
crypto_isakmp_process_block:src:209.165.202.129, dest:209.165.200.225 spt:500 dpt:500 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): received xauth v6 vendor id
ISAKMP (0): processing vendor id payload ISAKMP (0): remote peer supports dead peer detection
ISAKMP (0): processing vendor id payload ISAKMP (0): processing vendor id payload ISAKMP (0):
speaking to another IOS box! return status is IKMP_NO_ERROR
crypto_isakmp_process_block:src:209.165.202.129, dest:209.165.200.225 spt:500 dpt:500 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: Created a peer struct for
209.165.202.129, peer port 62465 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 ISAKMP
(0): sending INITIAL_CONTACT notify ISAKMP (0): sending NOTIFY message 24578 protocol 1 VPN
Peer: ISAKMP: Added new peer: ip:209.165.202.129/500 Total VPN Peers:1 VPN Peer: ISAKMP: Peer
ip:209.165.202.129/500 Ref cnt incremented to:1 Total VPN Peers:1
crypto_isakmp_process_block:src:209.165.202.129, dest:209.165.200.225 spt:500 dpt:500 ISAKMP
(0): processing NOTIFY payload 24578 protocol 1 spi 0, message ID = 863921625 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 209.165.202.129 return status is IKMP_NO_ERR_NO_TRANS
crypto_isakmp_process_block:src:209.165.202.129, dest:209.165.200.225 spt:500 dpt:500 OAK_QM
exchange oakley_process_quick_mode: OAK_QM_IDLE ISAKMP (0): processing SA payload. message ID =
2542705093 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-MD5 ISAKMP (0): atts are
acceptable.IPSEC(validate_proposal_request): proposal part #1, (key eng. msg.) dest=
209.165.200.225, src= 209.165.202.129, dest_proxy= 10.48.66.0/255.255.255.0/0/0 (type=4),
src_proxy= 10.48.67.0/255.255.255.0/0/0 (type=4), 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 = 2542705093 ISAKMP (0): processing ID payload. message ID =
2542705093 ISAKMP (0): ID_IPV4_ADDR_SUBNET src 10.48.67.0/255.255.255.0 prot 0 port 0 ISAKMP
(0): processing ID payload. message ID = 2542705093 ISAKMP (0): ID_IPV4_ADDR_SUBNET dst
10.48.66.0/255.255.255.0 prot 0 port 0 IPSEC(key_engine): got a queue event...
IPSEC(spi_response): getting spi 0x858c841a(2240578586) for SA from 209.165.202.129 to
209.165.200.225 for prot 3 return status is IKMP_NO_ERROR
crypto_isakmp_process_block:src:209.165.202.129, dest:209.165.200.225 spt:500 dpt:500 OAK_QM
exchange oakley_process_quick_mode: OAK_QM_AUTH_AWAIT ISAKMP (0): Creating IPsec SAs inbound SA
from 209.165.202.129 to 209.165.200.225 (proxy 10.48.67.0 to 10.48.66.0) has spi 2240578586 and
conn_id 3 and flags 4 lifetime of 28800 seconds lifetime of 4608000 kilobytes outbound SA from
209.165.200.225 to 209.165.202.129 (proxy 10.48.66.0 to 10.48.67.0) has spi 681010504 and
conn_id 4 and flags 4 lifetime of 28800 seconds lifetime of 4608000 kilobytesIPSEC(key_engine):
got a queue event... IPSEC(initialize_sas): , (key eng. msg.) dest= 209.165.200.225, src=
209.165.202.129, dest_proxy= 10.48.66.0/255.255.255.0/0/0 (type=4), src_proxy=
```

10.48.67.0/255.255.255.0/0/0 (type=4), protocol= ESP, transform= esp-des esp-md5-hmac , lifedur= 28800s and 4608000kb, spi= 0x858c841a(2240578586), conn_id= 3, keysize= 0, flags= 0x4
IPSEC(initialize_sas): , (key eng. msg.) src= 209.165.200.225, dest= 209.165.202.129, src_proxy= 10.48.66.0/255.255.255.0/0/0 (type=4), dest_proxy= 10.48.67.0/255.255.255.0/0/0 (type=4),
protocol= ESP, transform= esp-des esp-md5-hmac , lifedur= 28800s and 4608000kb, spi= 0x28976548(681010504), conn_id= 4, keysize= 0, flags= 0x4 VPN Peer: IPSEC: Peer
ip:209.165.202.129/500 Ref cnt incremented to:2 Total VPN Peers:1 VPN Peer: IPSEC: Peer
ip:209.165.202.129/500 Ref cnt incremented to:3 Total VPN Peers:1 return status is IKMP_NO_ERROR

[Debuga quando você conectar o cliente VPN ao PIX de hub](#)

```
crypto_isakmp_process_block:src:10.48.68.2,  
dest:209.165.200.225 spt:500 dpt:500OAK_AG exchange  
ISAKMP (0): processing SA payload. message ID = 0  
ISAKMP (0): Checking ISAKMP transform 1 against priority 10 policy  
ISAKMP: encryption AES-CBC  
ISAKMP: hash SHA  
ISAKMP: default group 2  
ISAKMP: extended auth pre-share (init)  
ISAKMP: life type in seconds  
ISAKMP: life duration (VPI) of 0x0 0x20 0xc4 0x9b  
ISAKMP: keylength of 256  
ISAKMP (0): atts are not acceptable. Next payload is 3  
ISAKMP (0): Checking ISAKMP transform 2 against priority 10 policy  
ISAKMP: encryption AES-CBC  
ISAKMP: hash MD5  
ISAKMP: default group 2  
ISAKMP: extended auth pre-share (init)  
ISAKMP: life type in seconds  
ISAKMP: life duration (VPI) of 0x0 0x20 0xc4 0x9b  
ISAKMP: keylength of 256  
ISAKMP (0): atts are not acceptable. Next payload is 3  
ISAKMP (0): Checking ISAKMP transform 3 against priority 10 policy  
ISAKMP: encryption AES-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: keylength of 256  
ISAKMP (0): atts are not acceptable. Next payload is 3  
ISAKMP (0): Checking ISAKMP transform 4 against priority 10 policy  
ISAKMP: encryption AES-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: keylength of 256  
ISAKMP (0): atts are not acceptable. Next payload is 3  
ISAKMP (0): Checking ISAKMP transform 5 against priority 10 policy  
ISAKMP: encryption AES-CBC  
ISAKMP: hash SHA  
ISAKMP: default group 2  
ISAKMP: extended auth pre-share (init)  
ISAKMP: life type in seconds  
ISAKMP: life duration (VPI) of 0x0 0x20 0xc4 0x9b  
ISAKMP: keylength of 128  
ISAKMP (0): atts are not acceptable. Next payload is 3  
ISAKMP (0): Checking ISAKMP transform 6 against priority 10 policy  
ISAKMP: encryption AES-CBC  
ISAKMP: hash MD5  
ISAKMP: default group 2
```



```
ISAKMP:      extended auth pre-share (init)
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x20 0xc4 0x9b
ISAKMP:      keylength of 128
ISAKMP (0):  atts are not acceptable. Next payload is 3
ISAKMP (0):  Checking ISAKMP transform 7 against priority 10 policy
ISAKMP:      encryption AES-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:      keylength of 128
ISAKMP (0):  atts are not acceptable. Next payload is 3
ISAKMP (0):  Checking ISAKMP transform 8 against priority 10 policy
ISAKMP:      encryption AES-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:      keylength of 128
ISAKMP (0):  atts are not acceptable. Next payload is 3
ISAKMP (0):  Checking ISAKMP transform 9 against priority 10 policy
ISAKMP:      encryption 3DES-CBC
ISAKMP:      hash SHA
ISAKMP:      default group 2
ISAKMP:      extended auth pre-share (init)
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x20 0xc4 0x9b
ISAKMP (0):  atts are not acceptable.
crypto_isakmp_process_block:src:10.48.68.2, dest:209.165.200.225 spt:500 dpt:500
crypto_isakmp_process_block:src:10.48.68.2, dest:209.165.200.225 spt:500 dpt:500
ISAKMP_TRANSACTION exchange
ISAKMP (0:0): processing transaction payload from 10.48.68.2.message ID = 17138612
ISAKMP: Config payload CFG_REPLY return status is IKMP_ERR_NO_RETRANS
ISAKMP (0:0): initiating peer config to 10.48.68.2. ID = 134858975 (0x809c8df)
crypto_isakmp_process_block:src:10.48.68.2, dest:209.165.200.225 spt:500 dpt:500
ISAKMP_TRANSACTION exchange
ISAKMP (0:0): processing transaction payload from 10.48.68.2. message ID = 17138612
ISAKMP: Config payload CFG_ACK
return status is IKMP_NO_ERROR
crypto_isakmp_process_block:src:10.48.68.2, dest:209.165.200.225 spt:500 dpt:500
ISAKMP_TRANSACTION exchange
ISAKMP (0:0): processing transaction payload from 10.48.68.2. message ID = 17138612
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      UNKNOWN (28672)
        Unsupported Attr: 28672
ISAKMP: attribute      UNKNOWN (28673)
        Unsupported Attr: 28673
ISAKMP: attribute      ALT_DEF_DOMAIN (28674)
ISAKMP: attribute      ALT_SPLIT_INCLUDE (28676)
ISAKMP: attribute      ALT_SPLITDNS_NAME (28675)
ISAKMP: attribute      ALT_PFS (28679)
ISAKMP: attribute      ALT_BACKUP_SERVERS (28681)
ISAKMP: attribute      APPLICATION_VERSION (7)
ISAKMP: attribute      UNKNOWN (28680)
```

```
Unsupported Attr: 28680
ISAKMP: attribute UNKNOWN (28682)
Unsupported Attr: 28682
ISAKMP: attribute UNKNOWN (28677)
Unsupported Attr: 28677
ISAKMP (0:0): responding to peer config from 10.48.68.2. ID = 1128513895
return status is IKMP_NO_ERROR
crypto_isakmp_process_block:src:10.48.68.2, dest:209.165.200.225 spt:500 dpt:500
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_IDLE
ISAKMP (0): processing SA payload. message ID = 3681346539
ISAKMP : Checking IPsec proposal 1
ISAKMP: transform 1, ESP_AES
ISAKMP: attributes in transform:
ISAKMP: authenticator is HMAC-MD5
ISAKMP: key length is 256
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 12, 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_AES
ISAKMP: attributes in transform:
ISAKMP: authenticator is HMAC-SHA
ISAKMP: key length is 256
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 12, hmac_alg 2) not supported
ISAKMP (0):atts not acceptable. Next payload is 0
ISAKMP (0): skipping next ANDED proposal (2)
crypto_isakmp_process_block:src:10.48.68.2, dest:209.165.200.225 spt:500 dpt:500
hub(config)#
hub(config)#
hub(config)#
hub(config)#
crypto_isakmp_process_block:src:10.48.68.2, dest:209.165.200.225 spt:500 dpt:500
ISAKMP (0): processing NOTIFY payload 36136 protocol 1
spi 0, message ID = 3784834735
ISAKMP (0): received DPD_R_U_THERE from peer 10.48.68.2
ISAKMP (0): sending NOTIFY message 36137 protocol 1
return status is IKMP_NO_ERR_NO_TRANS
```

[Informações Relacionadas](#)

- [Página de Suporte de Negociação IPsec/Protocolos IKE](#)
- [Cisco Secure ACS para página de suporte do Windows](#)
- [Referências de comando PIX](#)
- [Página de suporte do PIX](#)
- [TACACS+ na Documentação do IOS](#)
- [Página de suporte de TACACS+](#)
- [Solicitações de Comentários \(RFCs\)](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)