

# Configurando o firewall PIX segura Cisco 6.0 e os Cisco VPN Client que usam o IPsec

## Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configure o PIX](#)

[Configurar o Cisco VPN Client](#)

[Verificar](#)

[Troubleshooting](#)

[Comandos para Troubleshooting](#)

[Exemplo de debug](#)

[Informações Relacionadas](#)

## [Introdução](#)

O software Cisco Secure PIX Firewall versão 6.0 e posteriores são compatíveis com conexões do cliente Cisco VPN 3.x e 4.x. Esta configuração de exemplo mostra duas versões dos clientes VPN que conectam e criptografam o tráfego com o PIX como o ponto final do túnel. Nesta configuração, um pool de endereços é configurado para ser atribuído à segurança IP (IPsec).

## [Pré-requisitos](#)

### [Requisitos](#)

Esta configuração de exemplo supõe que o PIX já se opera com estatísticas apropriadas, conduítes, ou Listas de acesso. Este documento não é pretendido ilustrar estes conceitos básicos, mas mostrar a Conectividade ao PIX de um Cisco VPN Client.

### [Componentes Utilizados](#)

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

- PIX Software Release 6.2(1)**Nota:** Esta instalação foi testada no PIX Software Release 6.2(1), mas deve trabalhar em versões anterior de volta a 6.0(1) assim como em umas liberações

mais atrasadas.

- Versão Cliente VPN Cisco 3.6 Rel**Nota:** Esta instalação foi testada no cliente VPN v4.0 Rel, mas deve trabalhar em versões anterior de volta ao 3.0 e até a versão atual.

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](#)

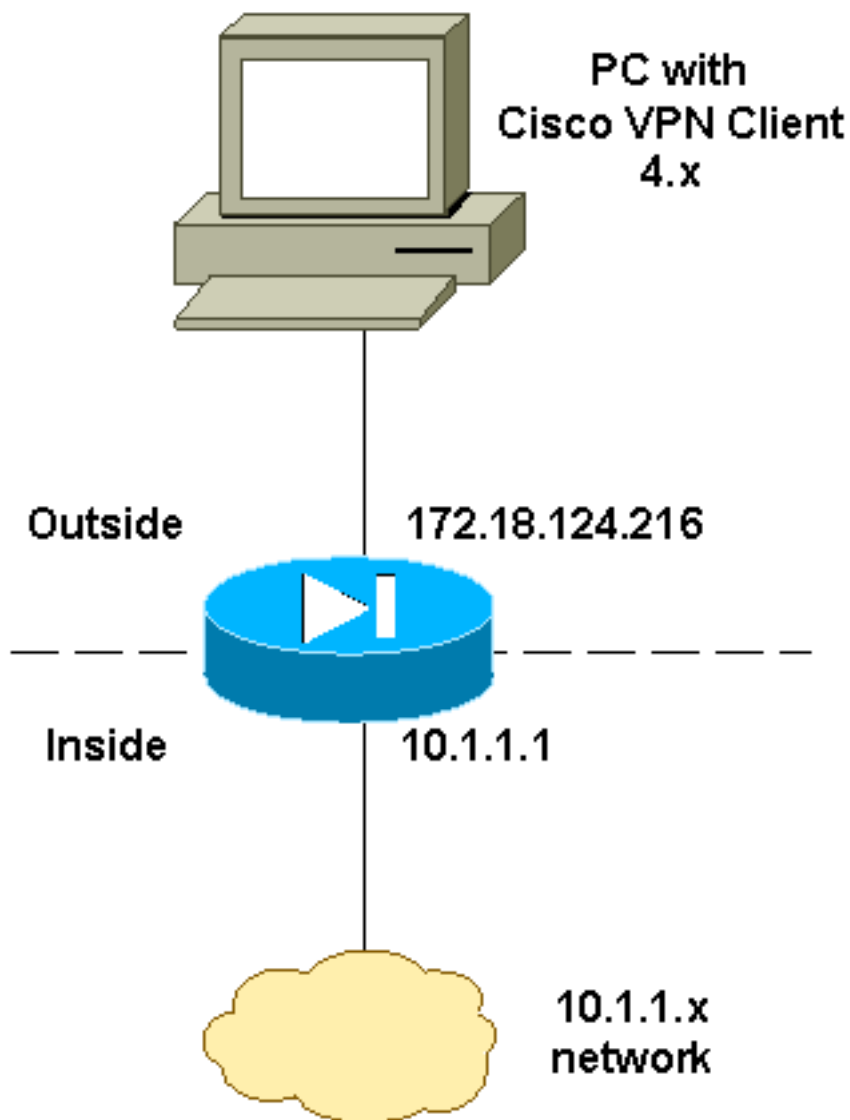
Consulte as [Convenções de Dicas Técnicas da Cisco](#) para obter mais informações sobre convenções de documentos.

## [Configurar](#)

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

## [Diagrama de Rede](#)

Este documento utiliza a seguinte configuração de rede:



## Configure o PIX

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

### PIX

```
PIX Version 6.2(1)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password OnTrBUG1Tp0edmkr encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname goss-d3-pix515b
domain-name rtp.cisco.com
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
fixup protocol skinny 2000
names
!
!--- Access list to avoid Network Address Translation
(NAT) !--- on the IPSec packets. access-list 101 permit
```

```
ip 10.1.1.0 255.255.255.0 10.1.2.0 255.255.255.0
pager lines 24
interface ethernet0 auto
interface ethernet1 auto
mtu outside 1500
mtu inside 1500
!
!--- IP addresses on the interfaces ip address outside
172.18.124.216 255.255.255.0 ip address inside 10.1.1.1
255.255.255.0 ip audit info action alarm ip audit attack
action alarm ip local pool ippool 10.1.2.1-10.1.2.254
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
pdm history enable
arp timeout 14400
!
!--- Binding ACL 101 to the NAT statement to avoid NAT
!--- on the IPSec packets. nat (inside) 0 access-list
101
!
!--- Default route to the Internet. route outside
0.0.0.0 0.0.0.0 172.18.124.1 1 timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc
0:10:00 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 http
server enable http 1.2.3.5 255.255.255.255 inside no
snmp-server location no snmp-server contact snmp-server
community public no snmp-server enable traps floodguard
enable ! !--- The sysopt command avoids conduit !--- on
the IPSec encrypted traffic.

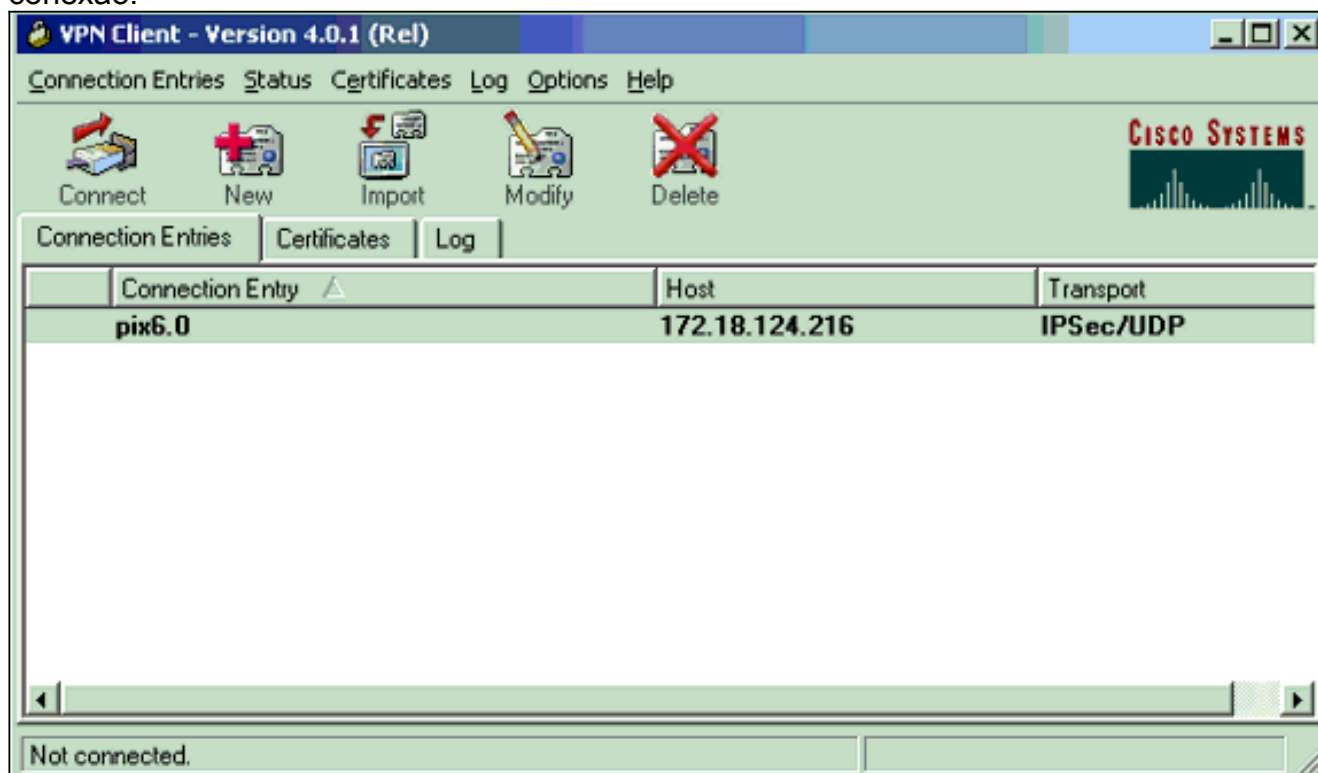
sysopt connection permit-ipsec
no sysopt route dnat
!
!--- Phase 2 encryption type crypto ipsec transform-set
myset esp-des esp-md5-hmac
crypto dynamic-map dynmap 10 set transform-set myset
crypto map mymap 10 ipsec-isakmp dynamic dynmap
!
!--- Binding the IPSec engine on the outside interface.
crypto map mymap interface outside
!
!--- Enabling Internet Security Association and !--- Key
Management Protocol (ISAKMP) key exchange. isakmp enable
outside
isakmp identity address
!
!--- ISAKMP policy for VPN Client running 3.x or 4.x
code. 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
!
!--- IPSec group configuration for either VPN Client.
vpngroup vpn3000 address-pool ippool
vpngroup vpn3000 dns-server 10.1.1.2
vpngroup vpn3000 wins-server 10.1.1.2
vpngroup vpn3000 default-domain cisco.com
vpngroup vpn3000 idle-time 1800
```

```
vpngroup vpn3000 password *****
!--- To allow simultaneous access to the !--- internal
network and to the Internet. vpngroup vpn3000 split-
tunnel 101
telnet timeout 5
ssh timeout 5
terminal width 80
Cryptochecksum:94da63fc0bb8ce167407b3ea21c6642c
: end
[OK]
```

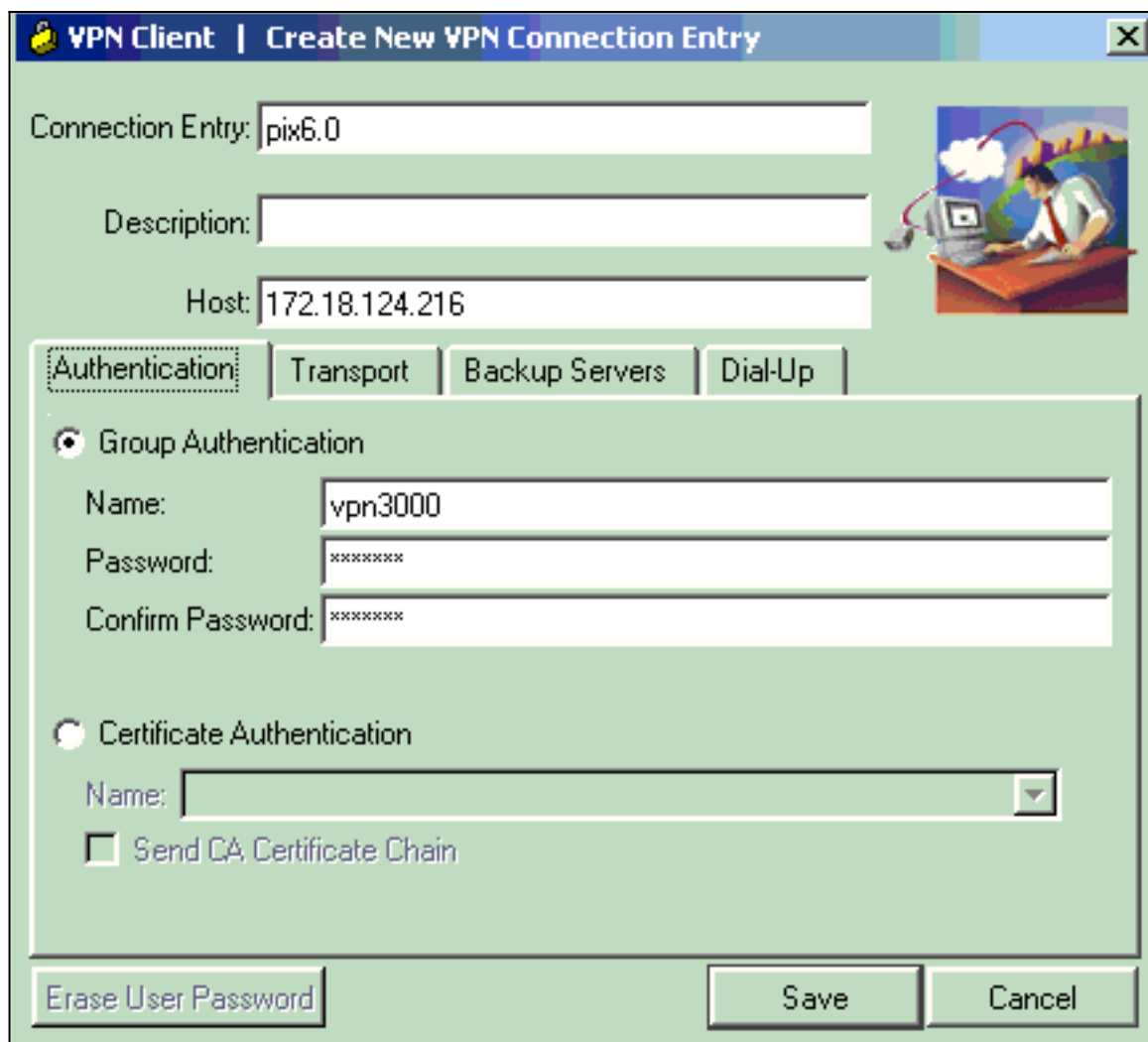
## Configurar o Cisco VPN Client

Termine estas etapas a fim criar uma nova conexão usando o cliente VPN.

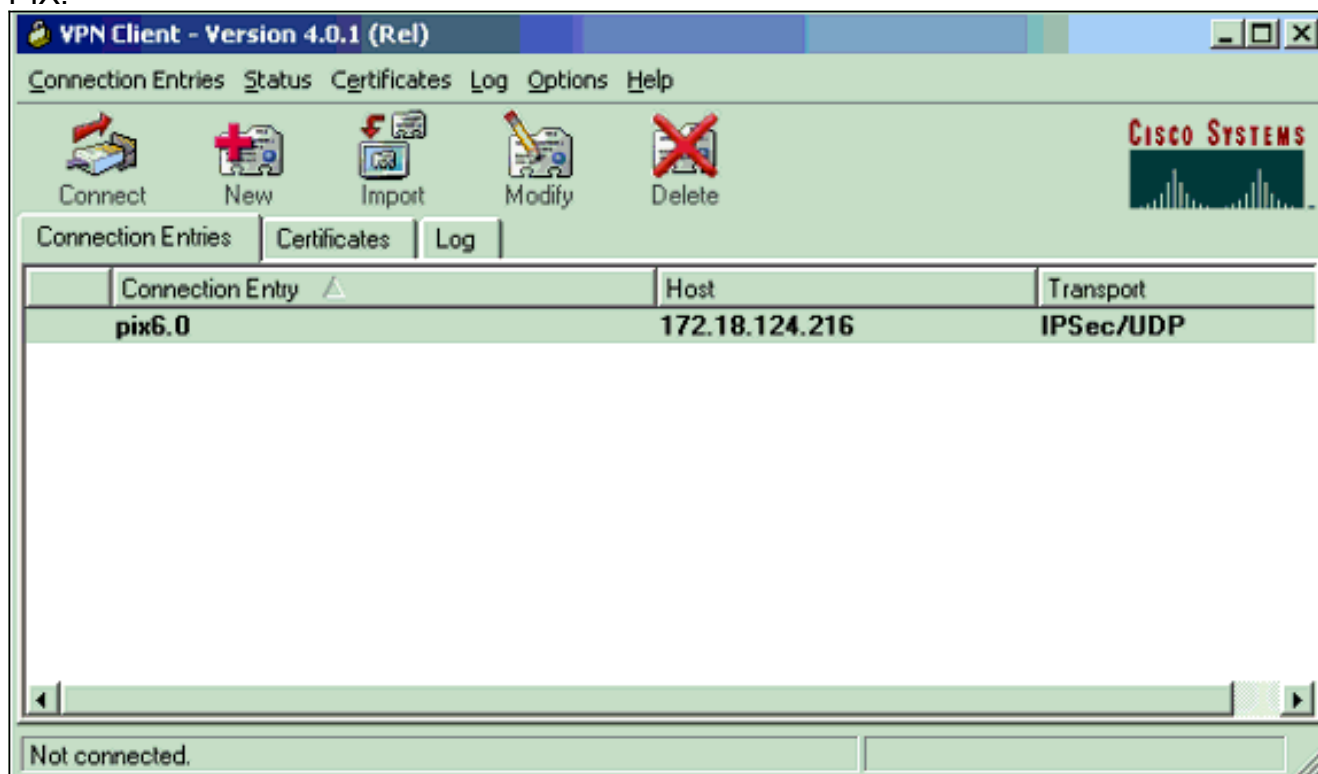
1. Inicie o VPN Client e, em seguida, clique em New para criar uma nova conexão.



2. Insira as informações de configuração para a nova conexão. No campo de entrada de conexão, atribua um nome a sua entrada. No campo do host, incorpore o endereço IP de Um ou Mais Servidores Cisco ICM NT da interface pública do PIX. Escolha a aba da **autenticação**, e incorpore então o grupo e a senha (duas vezes - para a confirmação). Quando você terminou, clique a **salv guarda**.



3. Clique em Connect para conectar ao PIX.



[Verificar](#)

Use esta seção 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.

- **mostre isakmp cripto sa** — Veja todas as associações de segurança atuais do Internet Key Exchange (IKE) (SA) em um par.
- **mostre IPsec cripto sa** — Veja os ajustes usados por SA atuais.

## [Troubleshooting](#)

Use esta seção para resolver problemas de configuração.

### [Comandos para Troubleshooting](#)

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

- **IPsec do debug crypto** — Use para ver as negociações de IPSEC de fase 2.
- **isakmp do debug crypto** — Use para ver as negociações de ISAKMP de fase 1.
- **motor do debug crypto** — Mostra o tráfego que é cifrado.

### [Exemplo de debug](#)

Esta é uma amostra de um debug correto gerado com o cliente de Cisco VPN 3.0.x:

```
goss-d3-pix515b#debug crypto isakmp
goss-d3-pix515b#debug crypto ipsec
goss-d3-pix515b#debug crypto engine
goss-d3-pix515b#show debug
debug crypto ipsec 1
debug crypto isakmp 1
debug crypto engine
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
goss-d3-pix515b# goss-d3-pix515b#
crypto_isakmp_process_block: src 172.18.124.96, dest 172.18.124.216
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 not acceptable. Next payload is 3  
ISAKMP (0): Checking ISAKMP transform 8 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 0x20 0xc4 0x9b  
**ISAKMP (0): atts are acceptable. Next payload is 0**  
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 172.18.124.96
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 172.18.124.96, dest 172.18.124.216
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_CONTACT
IPSEC(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 172.18.124.96
ISAKMP (0): SA has been authenticated
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 172.18.124.96, dest 172.18.124.216
ISAKMP_TRANSACTION exchange
ISAKMP (0:0): processing transaction payload
    from 172.18.124.96. 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 (0:0): responding to peer config from 172.18.124.96.
    ID = 525416177
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 172.18.124.96, dest 172.18.124.216
OAK_QM exchange
oakley_process_quick_mode:
```

OAK\_QM\_IDLE

ISAKMP (0): processing SA payload. message ID = 805890102

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= 172.18.124.216, src= 172.18.124.96,  
 dest\_proxy= 172.18.124.216/255.255.255.255/0/0 (type=1),  
 src\_proxy= 10.1.2.1/255.255.255.255/0/0 (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 = 805890102

ISAKMP (0): processing ID payload. message ID = 805890102  
ISAKMP (0): ID\_IPV4\_ADDR src 10.1.2.1 prot 0 port 0  
ISAKMP (0): processing ID payload. message ID = 805890102  
ISAKMP (0): ID\_IPV4\_ADDR dst 172.18.124.216 prot 0 port 0  
IPSEC(key\_engine): got a queue event...  
IPSEC(spi\_response): getting spi 0x13b00d31(330304817) for SA  
 from 172.18.124.96 to 172.18.124.216 for prot 3

return status is IKMP\_NO\_ERROR  
crypto\_isakmp\_process\_block: src 172.18.124.96, dest 172.18.124.216  
OAK\_QM exchange  
oakley\_process\_quick\_mode:  
OAK\_QM\_IDLE  
ISAKMP (0): processing SA payload. message ID = 935083707

ISAKMP : Checking IPsec proposal 1

ISAKMP: transform 1, ESP\_3DES  
ISAKMP: attributes in transform:  
ISAKMP: authenticator is HMAC-MD5  
crypto\_isakmp\_process\_block: src 172.18.124.96, dest 172.18.124.216  
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 172.18.124.96 to 172.18.124.216  
(proxy 10.1.2.1 to 172.18.124.216)  
 has spi 330304817 and conn\_id 1 and flags 4  
 lifetime of 2147483 seconds  
 outbound SA from 172.18.124.216 to 172.18.124.96  
(proxy 172.18.124.216 to 10.1.2.1)  
 has spi 2130279708 and conn\_id 2 and flags 4

```
lifetime of 2147483 secondsIPSEC(key_engine): got a queue event...
IPSEC(initialize_sas): ,
(key eng. msg.) dest= 172.18.124.216, src= 172.18.124.96,
dest_proxy= 172.18.124.216/0.0.0.0/0/0 (type=1),
src_proxy= 10.1.2.1/0.0.0.0/0/0 (type=1),
protocol= ESP, transform= esp-des esp-md5-hmac ,
lifedur= 2147483s and 0kb,
spi= 0x13b00d31(330304817), conn_id= 1, keysize= 0, flags= 0x4
IPSEC(initialize_sas): ,
(key eng. msg.) src= 172.18.124.216, dest= 172.18.124.96,
src_proxy= 172.18.124.216/0.0.0.0/0/0 (type=1),
dest_proxy= 10.1.2.1/0.0.0.0/0/0 (type=1),
protocol= ESP, transform= esp-des esp-md5-hmac ,
lifedur= 2147483s and 0kb,
spi= 0x7ef97d1c(2130279708), conn_id= 2, keysize= 0, flags= 0x4

return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 172.18.124.96, dest 172.18.124.216
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 172.18.124.96 to 172.18.124.216
(proxy 10.1.2.1 to 0.0.0.0)
has spi 4139858833 and conn_id 3 and flags 4
lifetime of 2147483 seconds
outbound SA from 172.18.124.216 to 172.18.124.96 (
proxy 0.0.0.0 to 10.1.2.1)
has spi 1487433401 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= 172.18.124.216, src= 172.18.124.96,
dest_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),
src_proxy= 10.1.2.1/0.0.0.0/0/0 (type=1),
protocol= ESP, transform= esp-des esp-md5-hmac ,
lifedur= 2147483s and 0kb,
spi= 0xf6IPSEC(initialize_sas): ,
(key eng. msg.) src= 172.18.124.216, dest= 172.18.124.96,
src_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),
dest_proxy= 10.1.2.1/0.0.0.0/0/0 (type=1),
protocol= ESP, transform= esp-des esp-md5-hmac ,
lifedur= 2147483s and 0kb,
spi= 0x58a86eb9(1487433401), conn_id= 4, keysize= 0, flags= 0x4
```

```
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 172.18.124.96, dest 172.18.124.216
ISAKMP (0): processing NOTIFY payload 36136 protocol 1
spi 0, message ID = 1617869510
ISAKMP (0): received DPD_R_U_THERE from peer 172.18.124.96
ISAKMP (0): sending NOTIFY message 36137 protocol 1
return status is IKMP_NO_ERR_NO_TRANS
goss-d3-pix515b#
goss-d3-pix515b#
goss-d3-pix515b#no debug crypto isakmp
goss-d3-pix515b#no debug crypto ipsec
goss-d3-pix515b#no debug crypto engine
goss-d3-pix515b#
```

## [Informações Relacionadas](#)

- [Páginas de Suporte do IPSec](#)
- [Referências do comando Cisco Secure PIX Firewall](#)
- [Página de Suporte dos Cisco PIX 500 Series Security Appliances](#)
- [Request For Comments \(RFC\)](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)