

Configuração de um túnel de IPSec entre um Cisco Secure PIX Firewall e um Checkpoint NG Firewall

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Diagrama de Rede](#)

[Conventions](#)

[Configure o PIX](#)

[Configurar o ponto de verificação NG](#)

[Verificar](#)

[Verificar a configuração do PIX](#)

[Exibir status do túnel no ponto de controle NG](#)

[Troubleshoot](#)

[Solucionar problemas da configuração do PIX](#)

[Sumarização de rede](#)

[Exibir logs NG do ponto de verificação](#)

[Informações Relacionadas](#)

[Introduction](#)

Este documento demonstra como configurar um túnel IPsec com chaves pré-compartilhadas para comunicação entre duas redes privadas. Neste exemplo, as redes em comunicação são a rede privada 192.168.10.x dentro do Cisco Secure PIX Firewall e a rede privada 10.32.x.x dentro do firewall de próxima geração (NG) ^{Checkpoint™}.

[Prerequisites](#)

[Requirements](#)

Certifique-se de atender a estes requisitos antes de tentar esta configuração:

- O tráfego de dentro do PIX e de dentro do ^{Checkpoint™} NG para a Internet (representado aqui pelas redes 172.18.124.x) deve fluir antes que você inicie essa configuração.
- Os usuários devem estar familiarizados com a negociação de IPSec. Esse processo pode ser dividido em cinco etapas, incluindo duas fases de Internet Key Exchange (IKE). Um túnel de

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

Componentes Utilizados

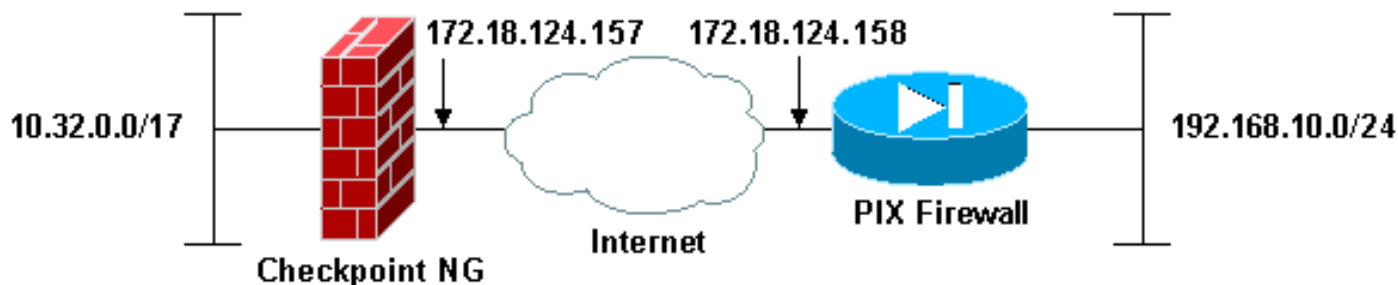
As informações neste documento são baseadas nestas versões de software e hardware:

- Software PIX versão 6.2.1
- Checkpoint™ NG Firewall

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



Conventions

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

Configure o PIX

Esta seção apresenta as informações para configurar os recursos descritos neste documento.

Configuração de PIX

```
PIX Version 6.2(1)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
```

```
hostname PIXRTPVPN
domain-name cisco.com
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol ils 389
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
!--- Interesting traffic to be encrypted to the
Checkpoint™ NG. access-list 101 permit ip 192.168.10.0
255.255.255.0 10.32.0.0 255.255.128.0
!--- Do not perform Network Address Translation (NAT) on
traffic to the Checkpoint™ NG. access-list nonat permit
ip 192.168.10.0 255.255.255.0 10.32.0.0 255.255.128.0
pager lines 24
interface ethernet0 10baset
interface ethernet1 10full
mtu outside 1500
mtu inside 1500
ip address outside 172.18.124.158 255.255.255.0
ip address inside 192.168.10.1 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
pdm history enable
arp timeout 14400
global (outside) 1 interface
!--- Do not perform NAT on traffic to the Checkpoint™
NG. nat (inside) 0 access-list nonat
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
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
aaa-server LOCAL protocol local
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
!--- Permit all inbound IPsec authenticated cipher
sessions. sysopt connection permit-ipsec
no sysopt route dnat
!--- Defines IPsec encryption and authentication
algorithms. crypto ipsec transform-set rtptac esp-3des
esp-md5-hmac
!--- Defines crypto map. crypto map rtprules 10 ipsec-
isakmp
crypto map rtprules 10 match address 101
crypto map rtprules 10 set peer 172.18.124.157
crypto map rtprules 10 set transform-set rtptac
!--- Apply crypto map on the outside interface. crypto
map rtprules interface outside
isakmp enable outside
!--- Defines pre-shared secret used for IKE
```

```

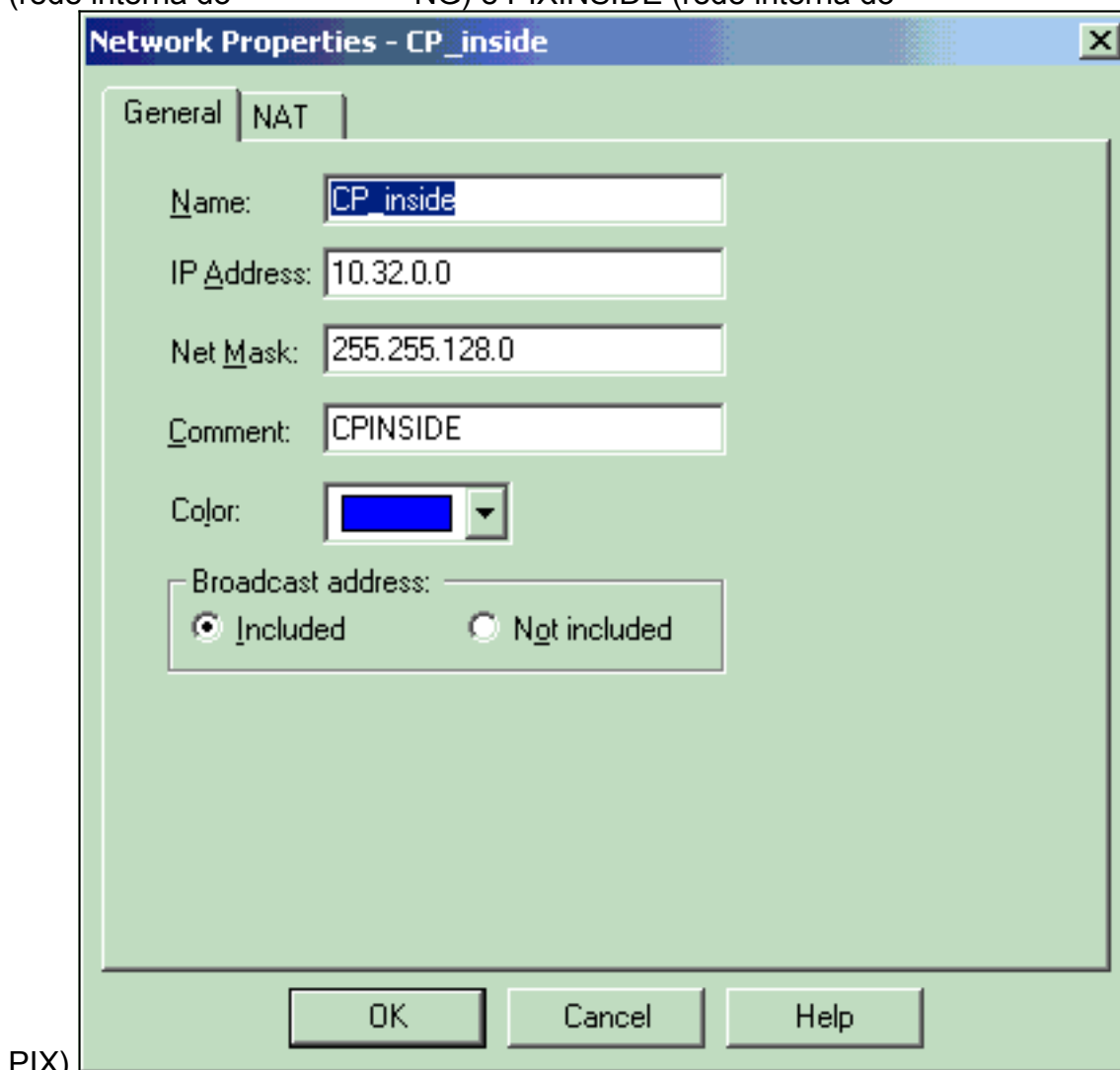
authentication. isakmp key ***** address
172.18.124.157 netmask 255.255.255.255
!--- Defines ISAKMP policy. isakmp policy 1
authentication pre-share
isakmp policy 1 encryption 3des
isakmp policy 1 hash md5
isakmp policy 1 group 2
isakmp policy 1 lifetime 86400
telnet timeout 5
ssh timeout 5
terminal width 80
Cryptochecksum:089b038c8e0dbc38d8ce5ca72cf920a5
: end

```

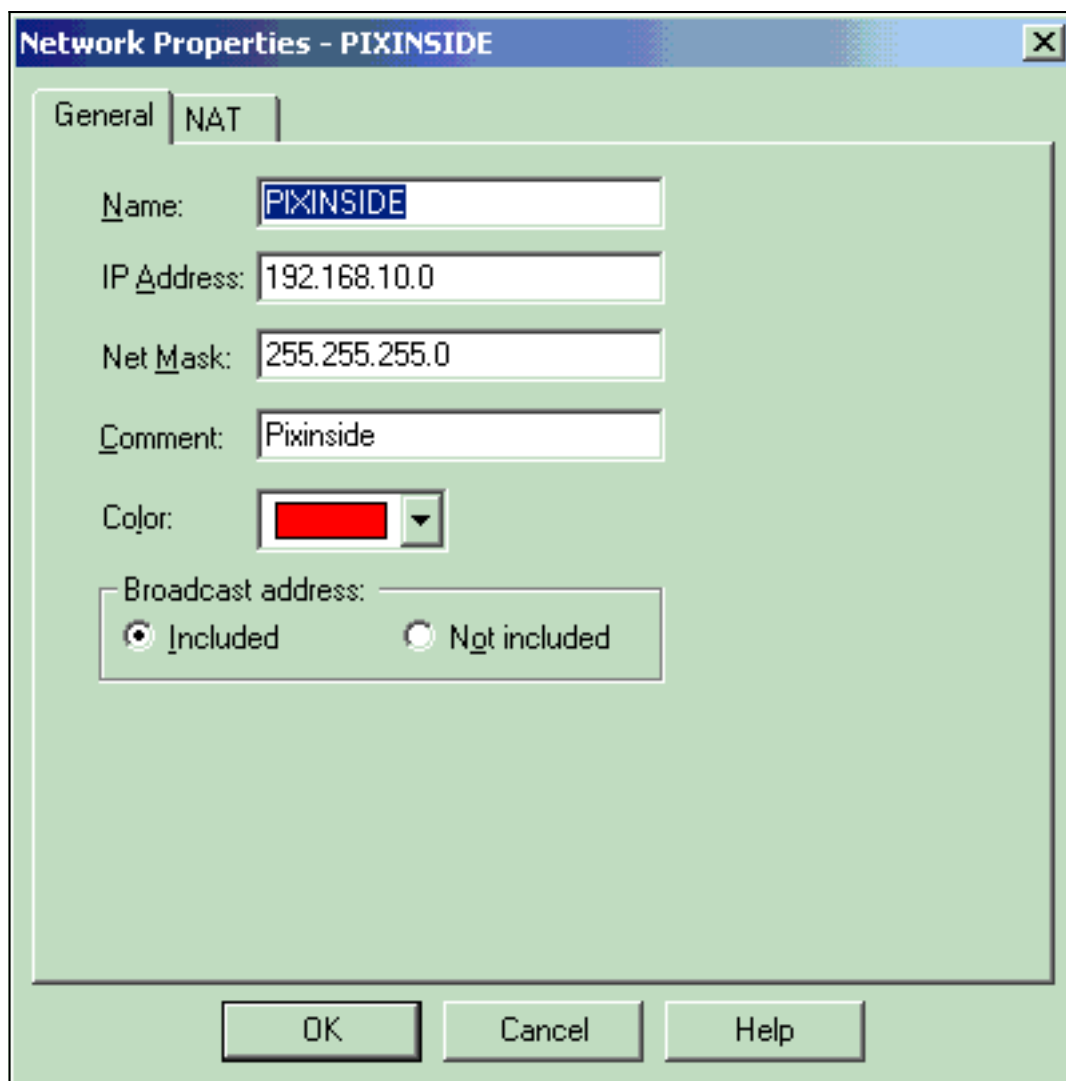
Configurar o ponto de verificação NG

Os objetos e regras de rede são definidos no Checkpoint™ NG para compor a política relacionada à configuração de VPN a ser configurada. Essa política é então instalada usando o Checkpoint™ NG Policy Editor para concluir o lado NG do Checkpoint™ da configuração.

1. Crie os dois objetos de rede para a rede Checkpoint e a rede PIX Firewall que criptografam o tráfego interessante. Para fazer isso, selecione **Gerenciar > Objetos de Rede** e, em seguida, selecione **Novo > Rede**. Insira as informações de rede apropriadas e clique em **OK**. Esses exemplos mostram uma configuração de objetos de rede chamados CP_Inside (rede interna do Checkpoint™ NG) e PIXINSIDE (rede interna do



PIX).



2. Crie objetos de estação de trabalho para o Checkpoint™ NG e PIX. Para fazer isso, selecione **Gerenciar > Objetos de Rede > Novo > Estação de Trabalho**. Observe que você pode usar o objeto de estação de trabalho Checkpoint™ NG criado durante a configuração Checkpoint™ NG inicial. Selecione as opções para definir a estação de trabalho como Gateway and Interoperable VPN Device e clique em **OK**. Esses exemplos mostram uma configuração de objetos chamados ciscocp (Checkpoint™ NG) e PIX (PIX Firewall).

- General
- Topology
- NAT
- VPN
- Authentication
- Management
- Advanced

General

Name:

IP Address:

Comment:

Color:

Type: Host Gateway

Check Point Products _____

Check Point products installed: Version

- VPN-1 & FireWall-1
- FloodGate-1
- Policy Server
- Primary Management Station

Object Management _____

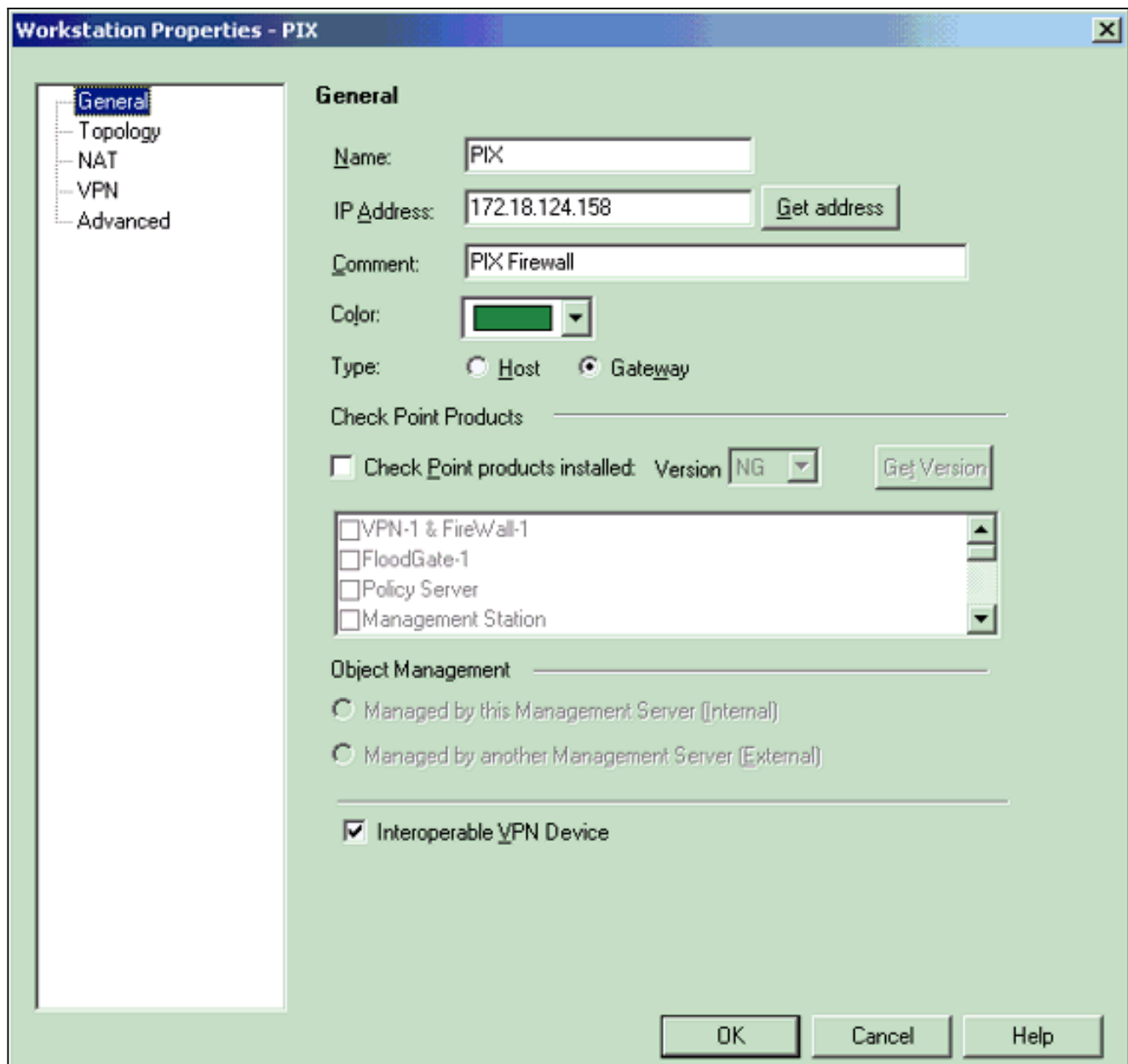
Managed by this Management Server (Internal)

Managed by another Management Server (External)

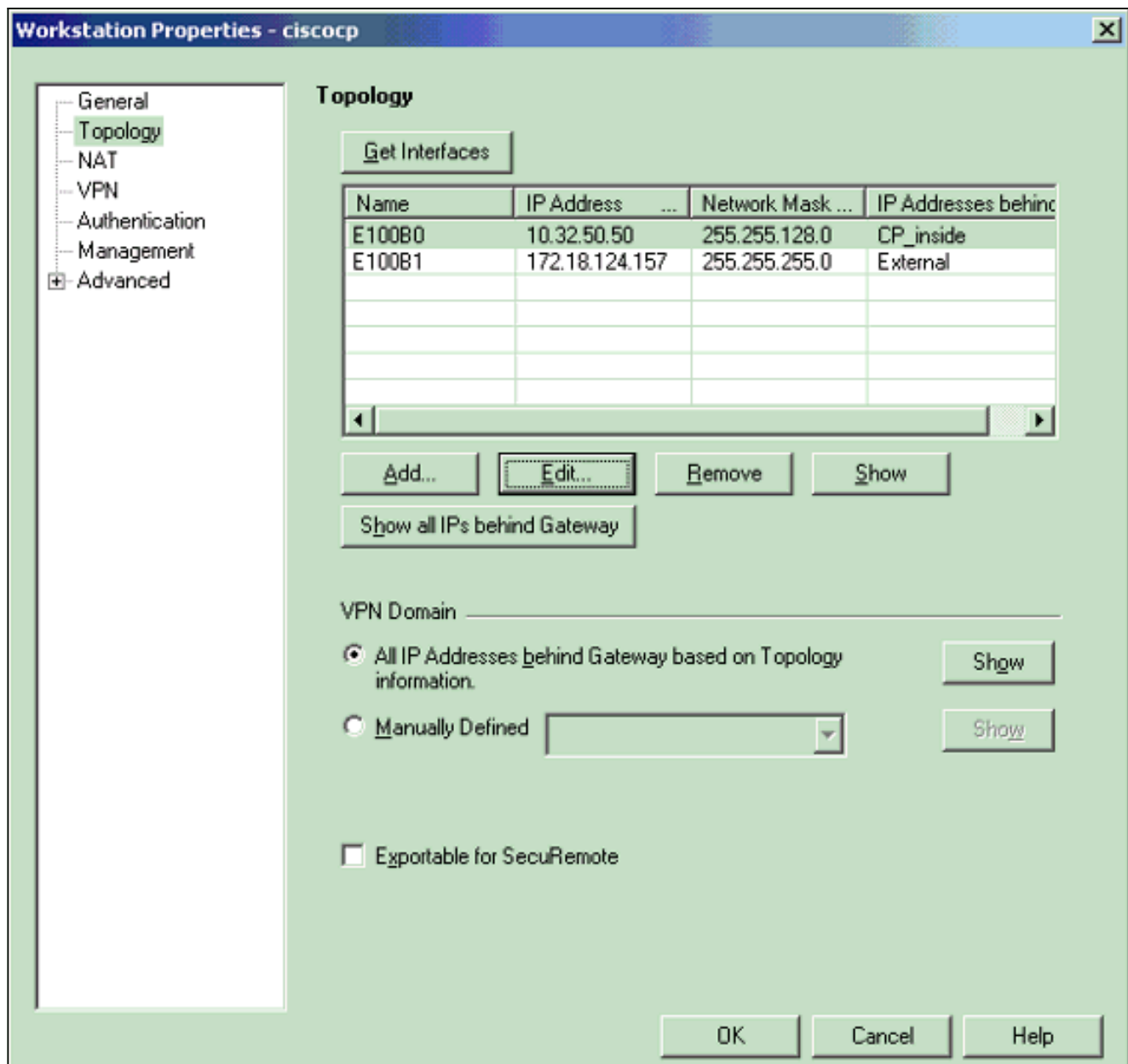
Secure Internal Communication _____

DN:

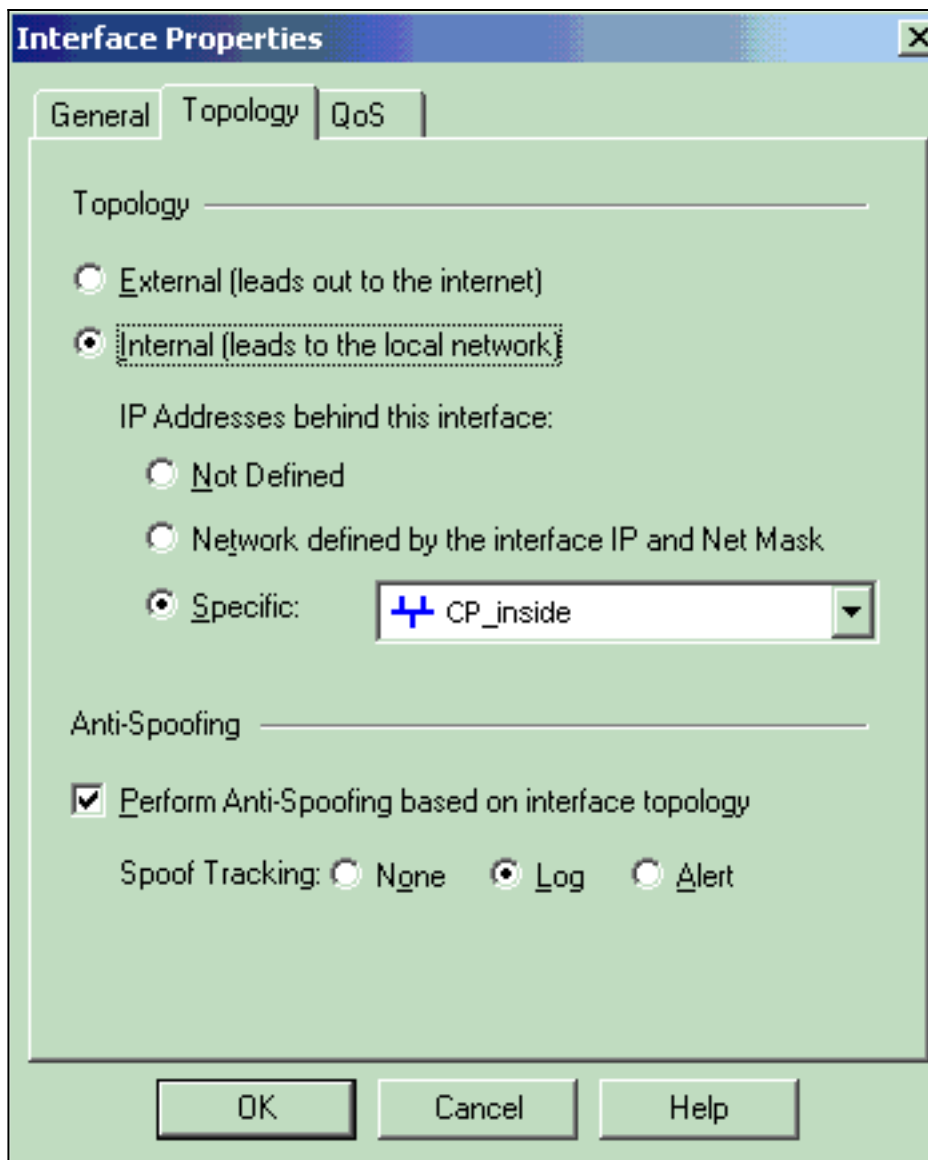
Interoperable VPN Device



3. Selecione **Gerenciar > Objetos de rede > Editar** para abrir a janela Propriedades da estação de trabalho para a estação de trabalho Checkpoint™ NG (ciscop neste exemplo). Selecione **Topologia** nas opções no lado esquerdo da janela e selecione a rede a ser criptografada. Clique em **Edit** para definir as propriedades da interface.

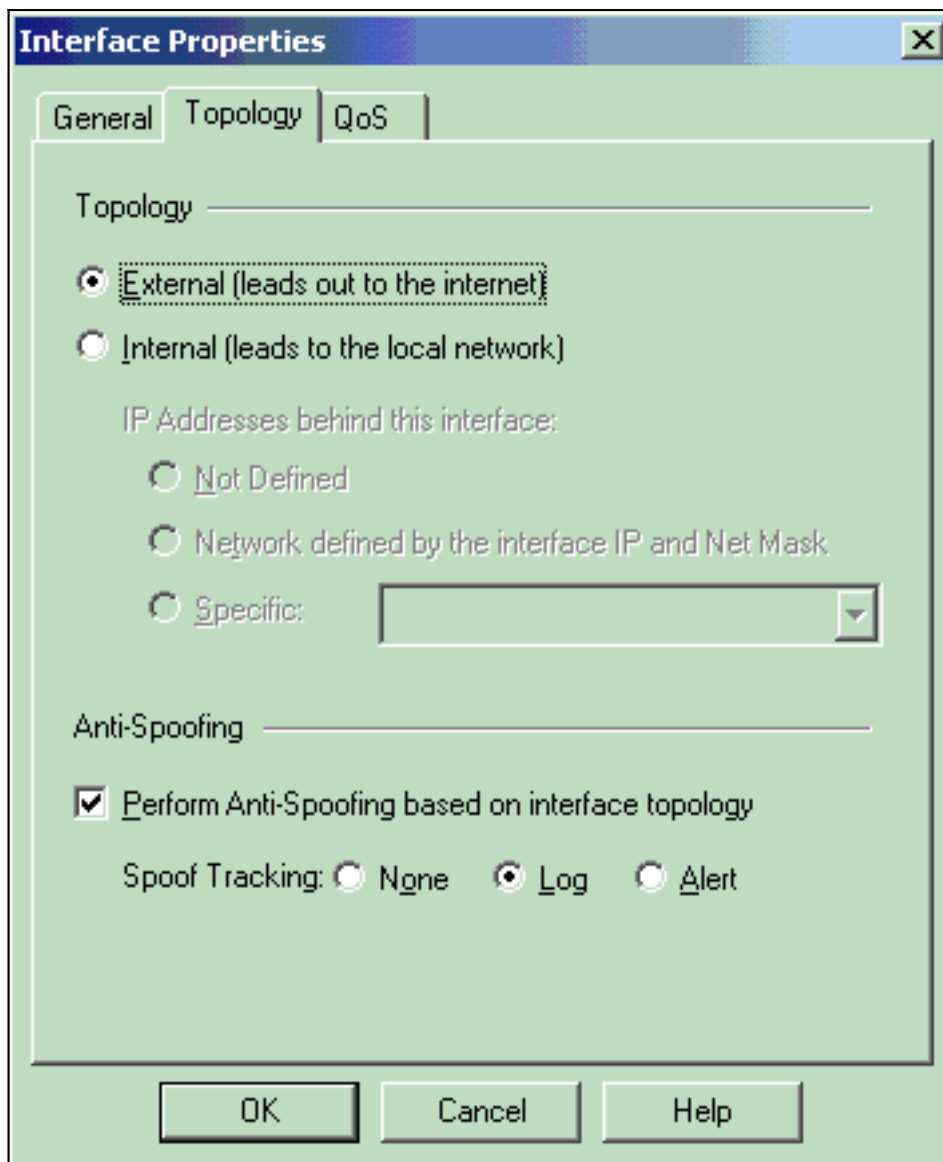


4. Selecione a opção para designar a estação de trabalho como interna e especifique o endereço IP apropriado. Click **OK**. Nesta configuração, CP_inside é a rede interna do Checkpoint™ NG. As seleções de topologia mostradas aqui designam a estação de trabalho como interna e especificam o endereço como



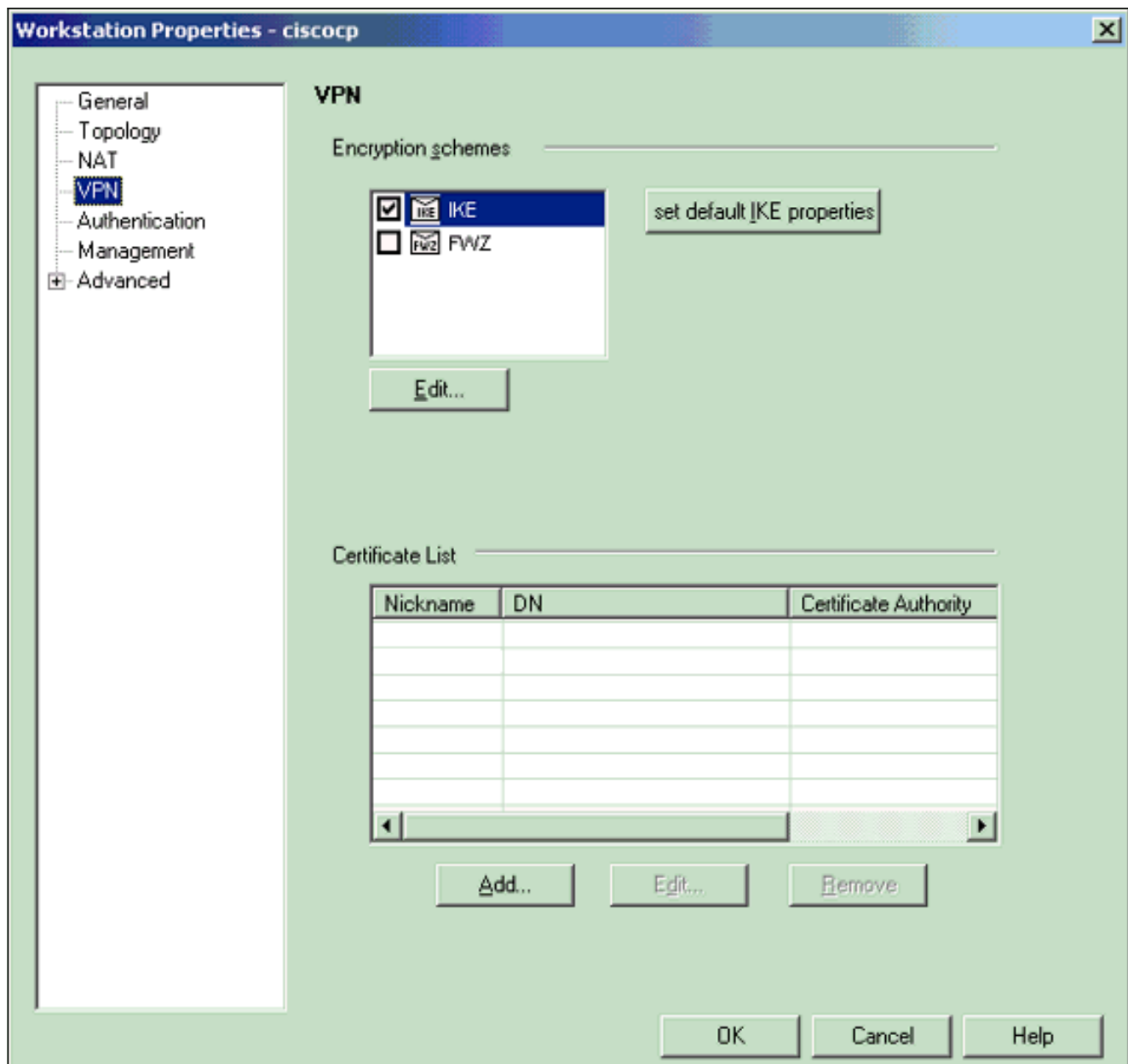
CP_inside.

5. Na janela Propriedades da estação de trabalho, selecione a interface externa no CheckpointTM NG que sai para a Internet e clique em **Editar** para definir as propriedades da interface. Selecione a opção para designar a topologia como externa e clique em

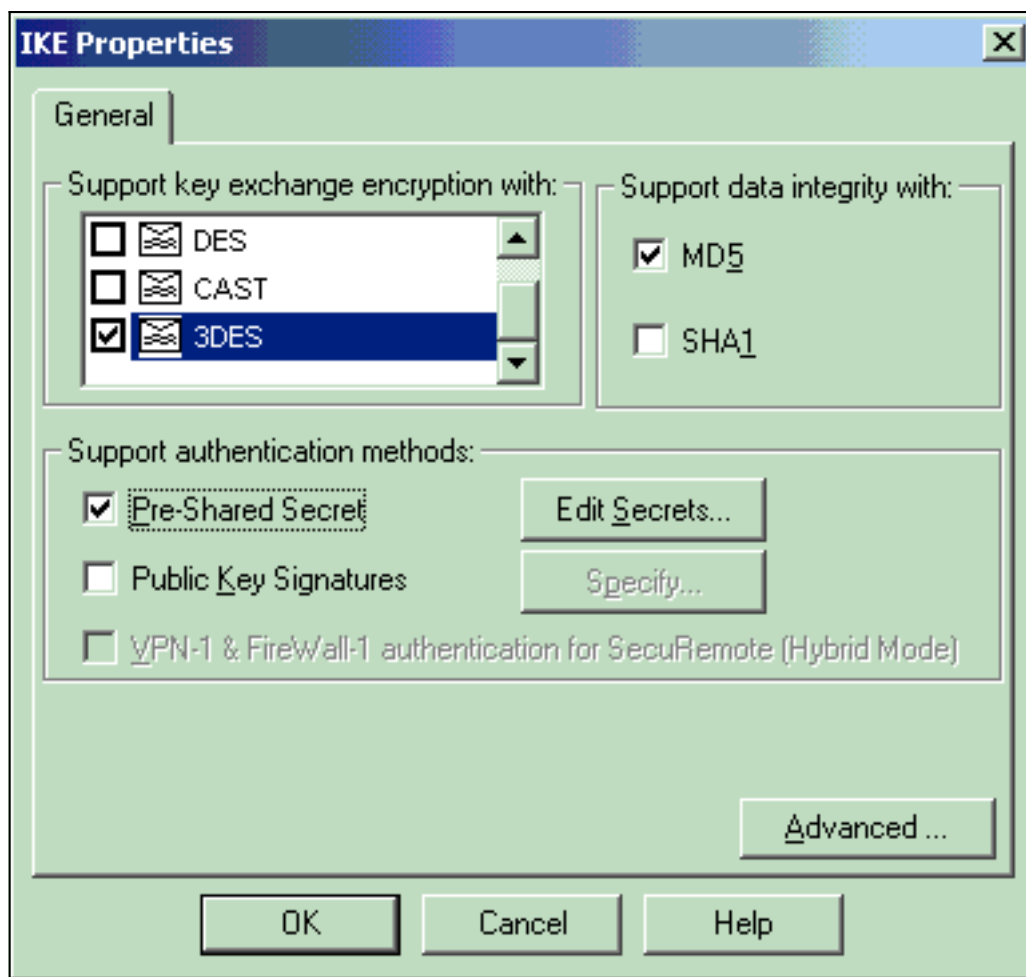


OK.

6. Na janela Propriedades da estação de trabalho no Checkpoint™ NG, selecione VPN nas opções no lado esquerdo da janela e selecione parâmetros IKE para algoritmos de criptografia e autenticação. Clique em **Editar** para configurar as propriedades de IKE.

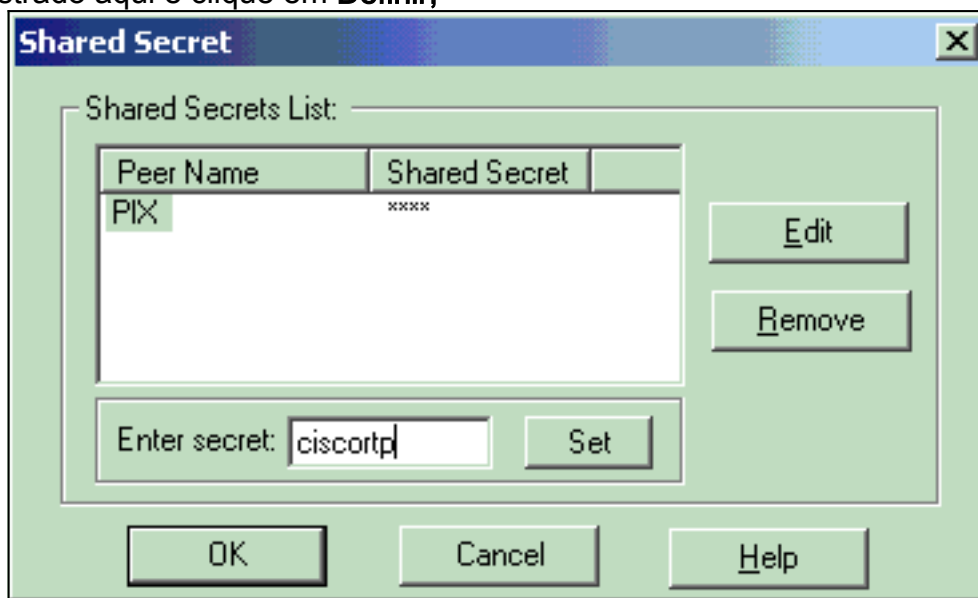


7. Configure as propriedades de IKE:Selecione a opção para a criptografia **3DES** para que as propriedades IKE sejam compatíveis com o comando **isakmp policy # encryption 3des**.Selecione a opção para **MD5** para que as propriedades de IKE sejam compatíveis com o comando **crypto isakmp policy # hash**



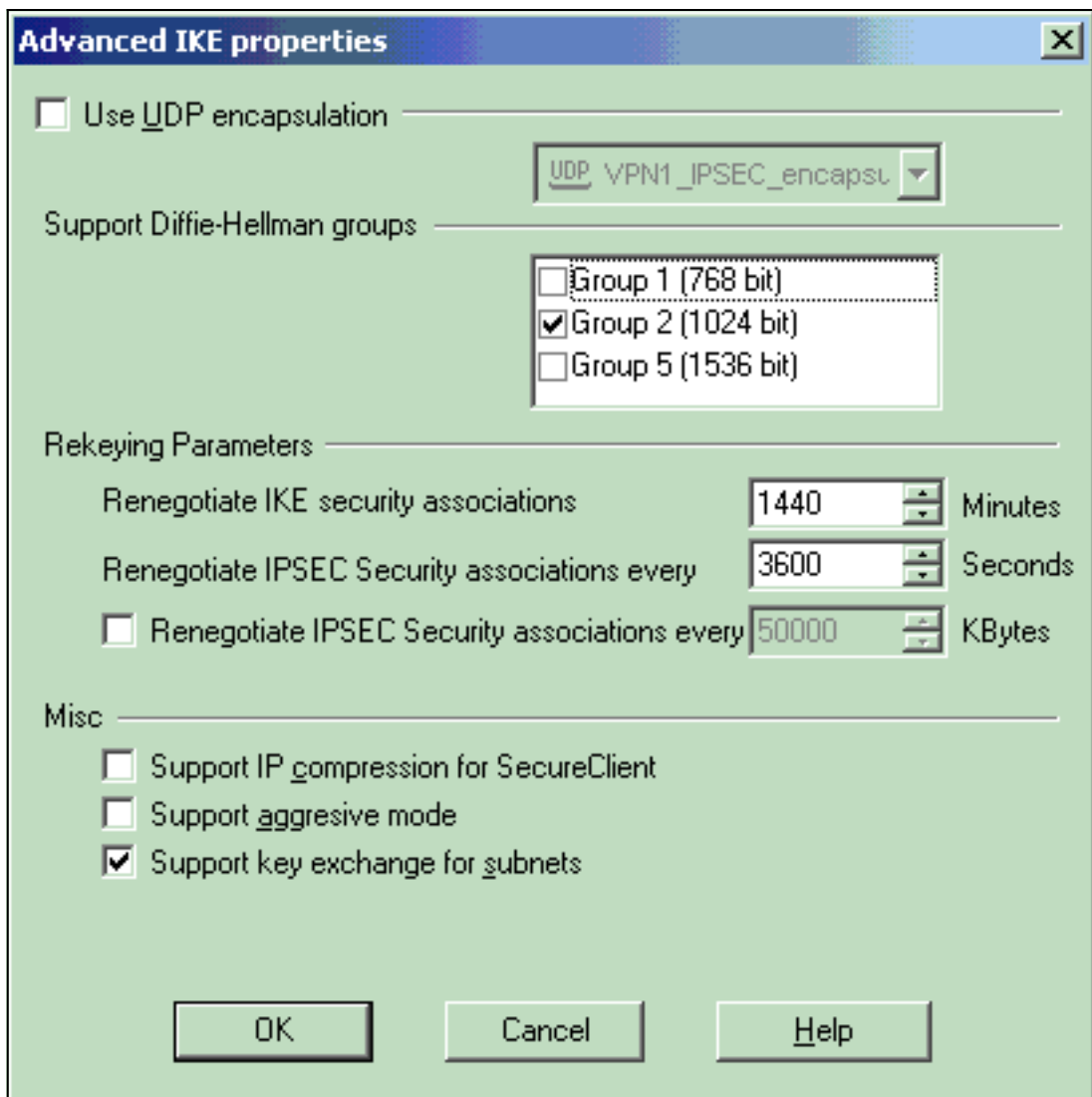
md5.

8. Selecione a opção de autenticação para Segredos pré-compartilhados e clique em Editar segredos para definir a chave pré-compartilhada como compatível com o comando PIX `isakmp key key address address netmask` . Clique em **Editar** para inserir sua chave como mostrado aqui e clique em **Definir**,



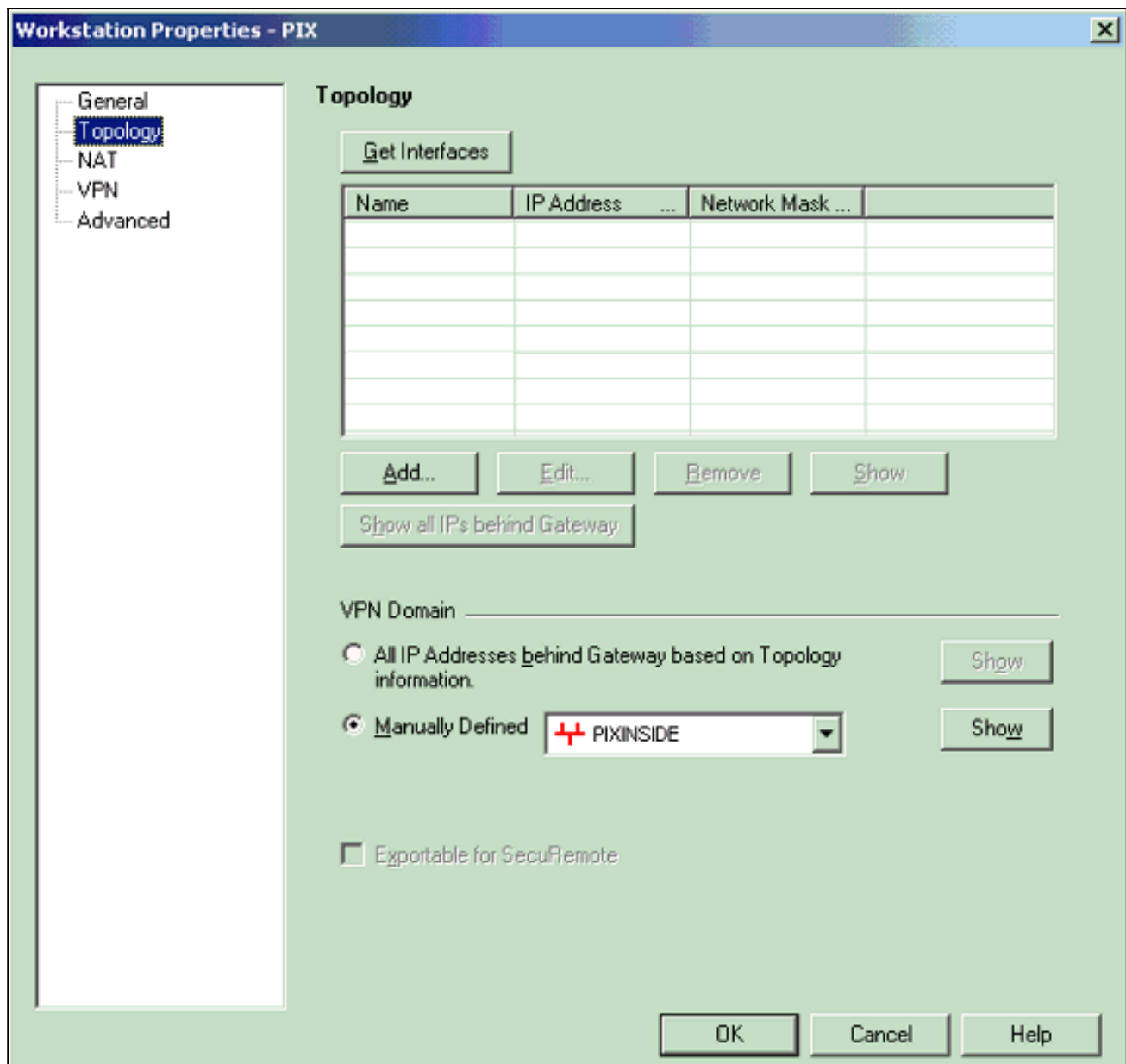
OK.

9. Na janela de propriedades de IKE, clique em **Avançado...** e alterar estas configurações: Desmarque a opção para o **modo agressivo de suporte**. Selecione a opção **Support key exchange for subnets**. Clique em **OK** quando

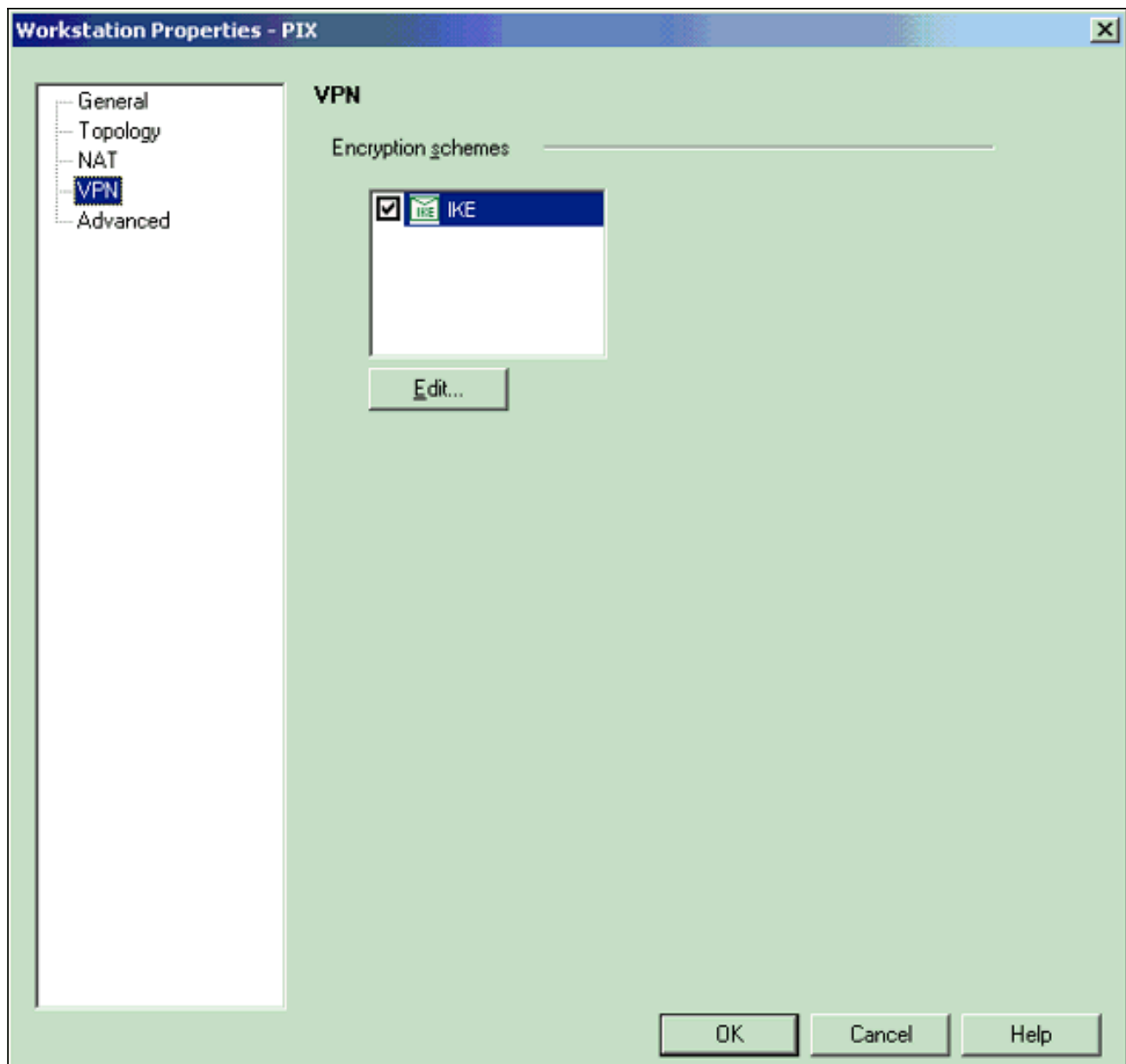


terminar.

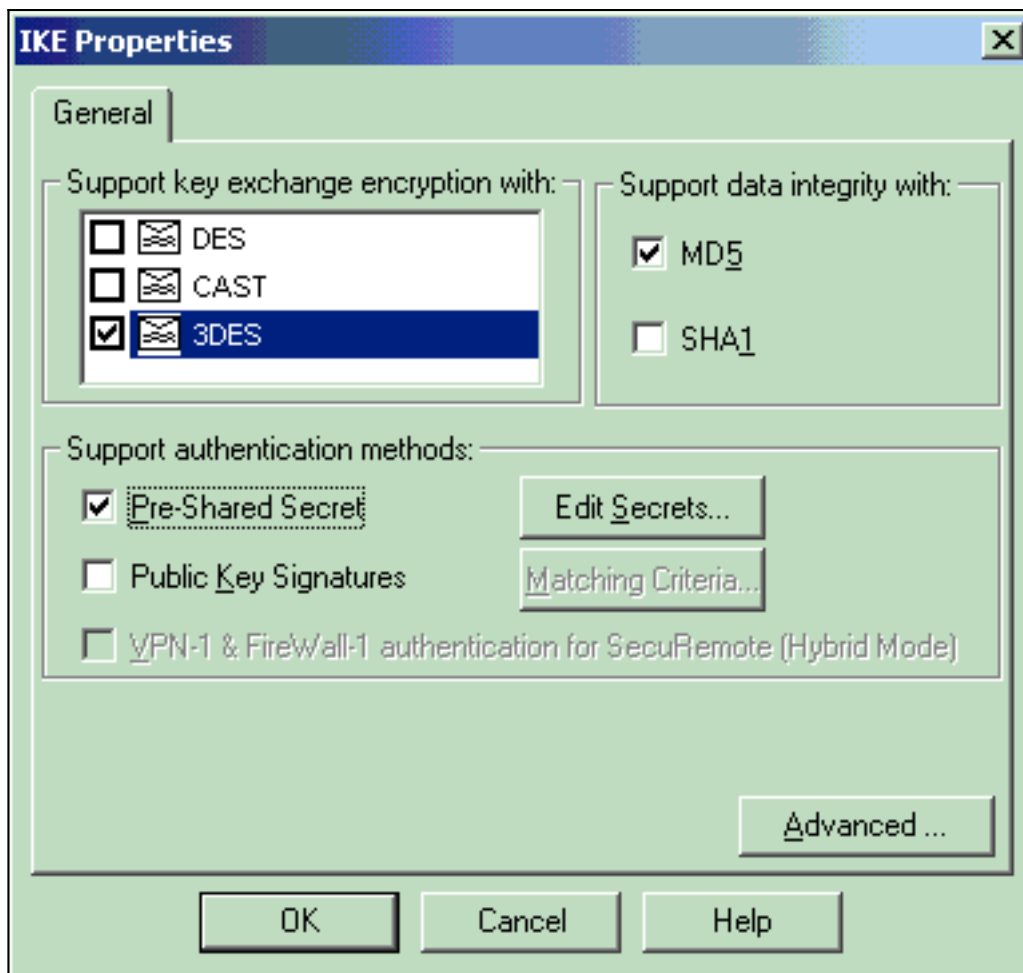
10. Selecione **Gerenciar > Objetos de rede > Editar** para abrir a janela Propriedades da estação de trabalho do PIX. Selecione **Topologia** nas opções no lado esquerdo da janela para definir manualmente o domínio VPN. Nesta configuração, PIXINSIDE (rede interna do PIX) é definido como o domínio VPN.



11. Selecione **VPN** nas opções no lado esquerdo da janela e selecione IKE como esquema de criptografia. Clique em **Editar** para configurar as propriedades de IKE.

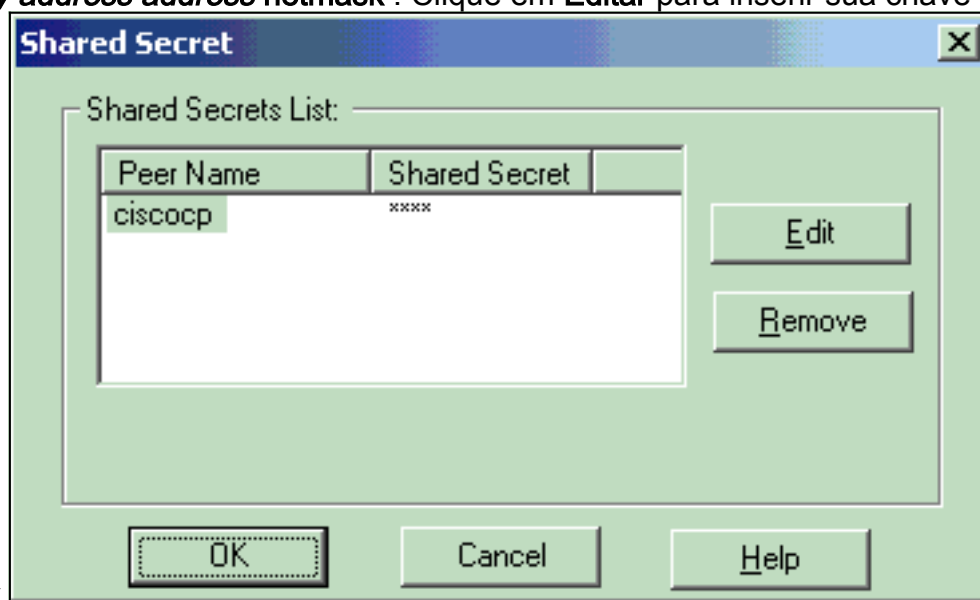


12. Configure as propriedades de IKE como mostrado aqui: Selecione a opção para a criptografia **3DES** para que as propriedades IKE sejam compatíveis com o comando **isakmp policy # encryption 3des**. Selecione a opção para **MD5** para que as propriedades de IKE sejam compatíveis com o comando **crypto isakmp policy # hash**



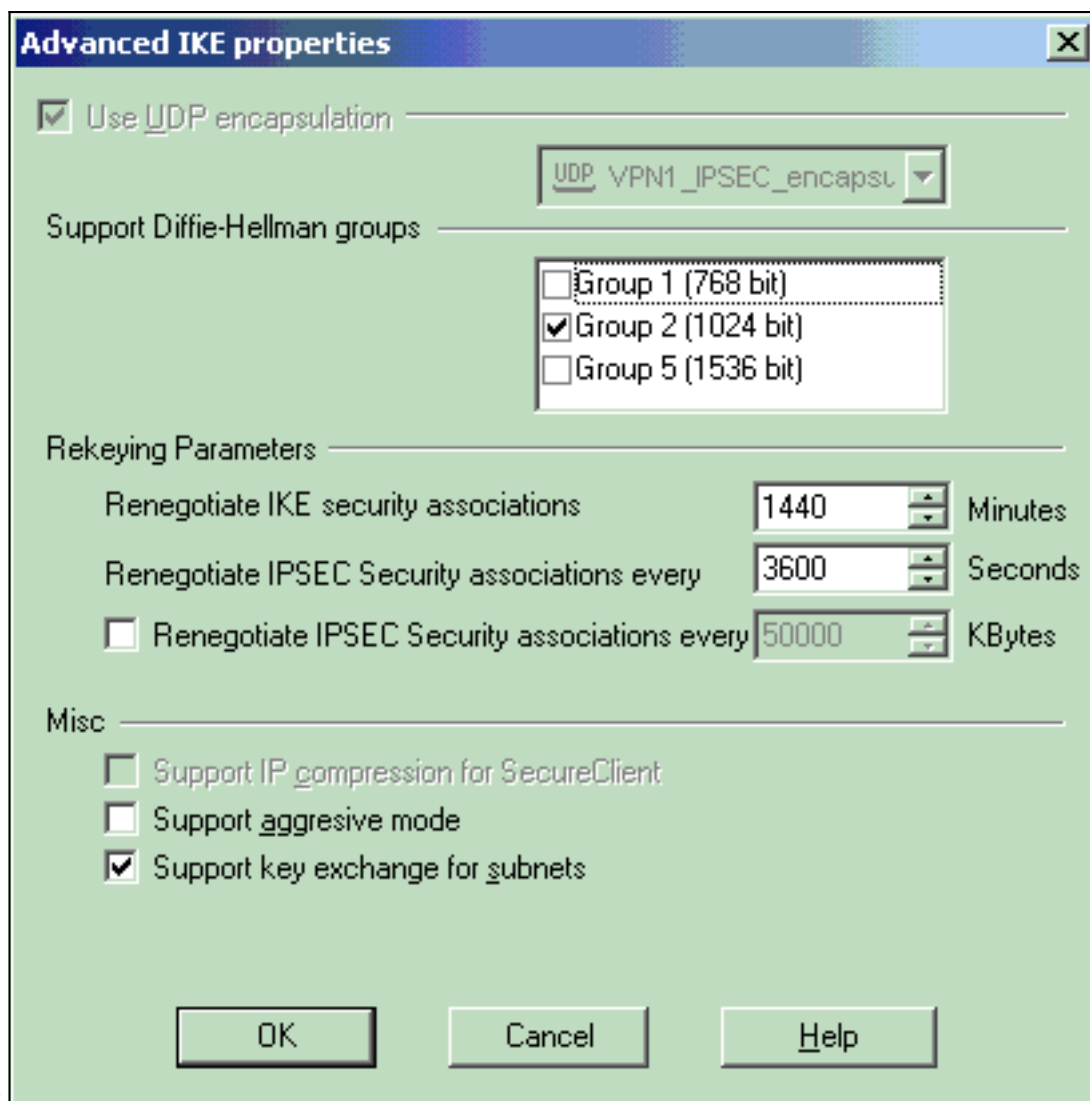
md5.

13. Selecione a opção de autenticação para Segredos pré-compartilhados e clique em Editar segredos para definir a chave pré-compartilhada como compatível com o comando PIX `isakmp key key address address netmask`. Clique em **Editar** para inserir sua chave e clique



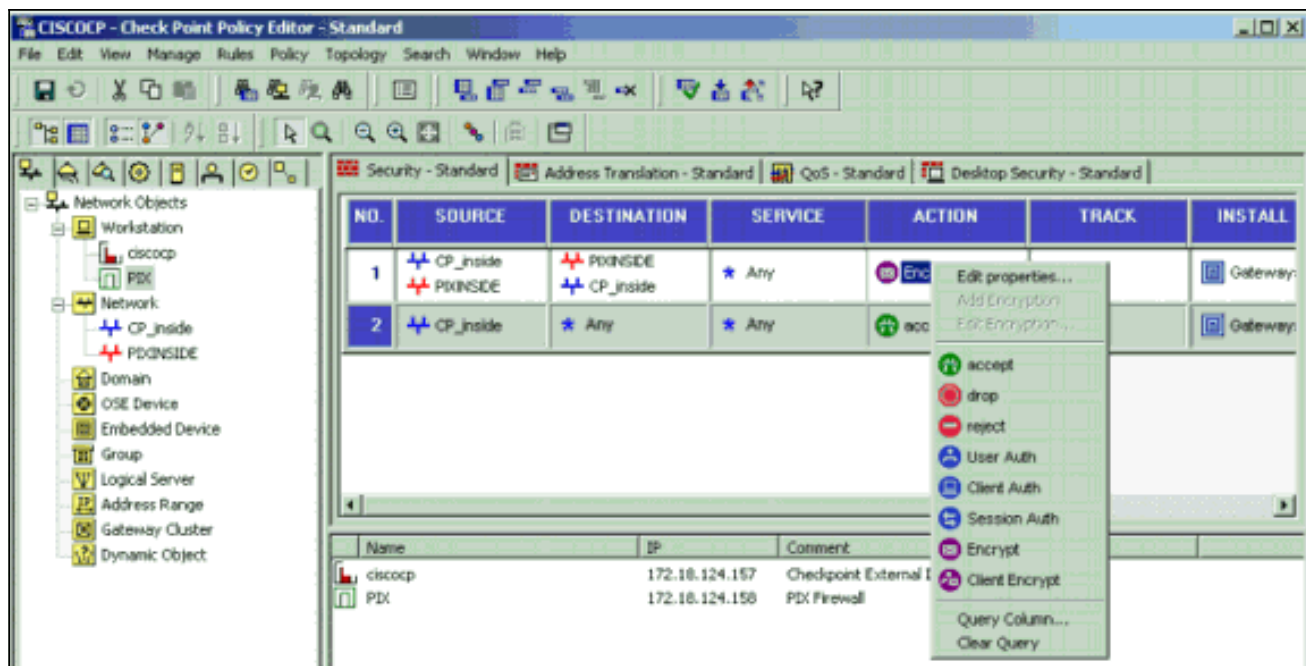
em Definir, OK.

14. Na janela de propriedades de IKE, clique em **Avançado...** e alterar essas configurações. Selecione o grupo Diffie-Hellman apropriado para propriedades IKE. Desmarque a opção para o **modo agressivo de suporte**. Selecione a opção **Support key exchange for subnets**. Clique em OK, OK quando

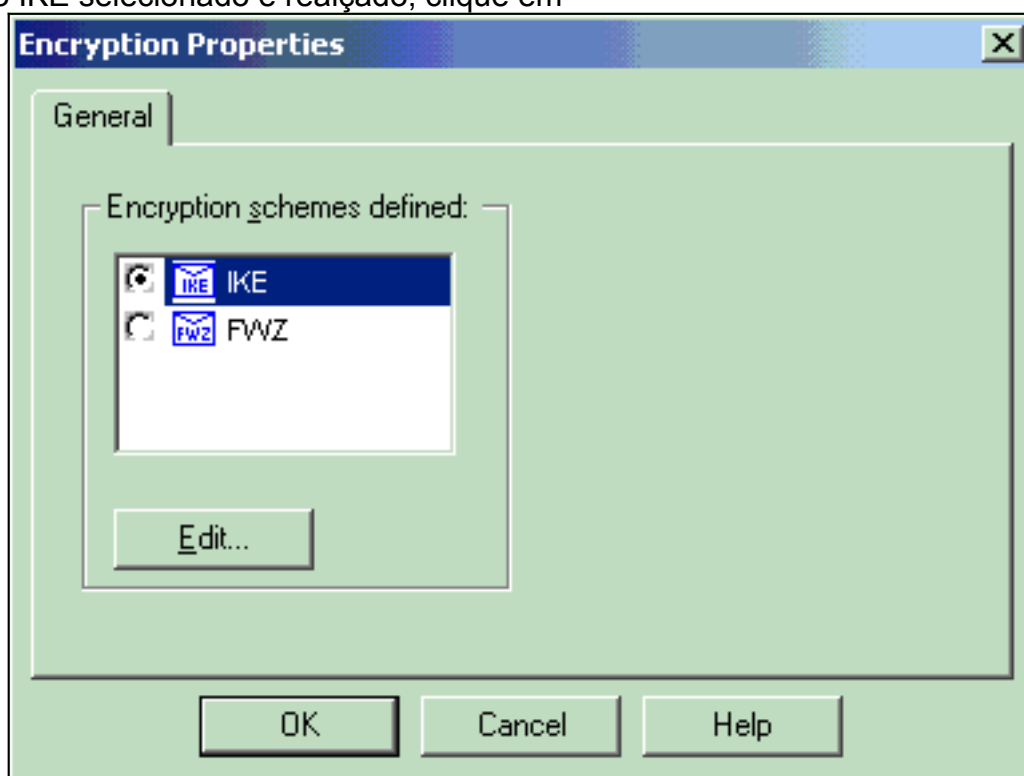


terminar.

15. Selecione **Regras > Adicionar Regras > Superior** para configurar as regras de criptografia para a política. Na janela Editor de políticas, insira uma regra com uma origem CP_inside (rede interna do CheckpointTM NG) e PIXINSIDE (rede interna do PIX) nas colunas origem e destino. Defina valores para **Serviço = Qualquer**, **Ação = Criptografar** e **Rastreamento = Log**. Quando tiver adicionado a seção Criptografar ação da regra, clique com o botão direito do mouse em **Ação** e selecione **Editar propriedades**.

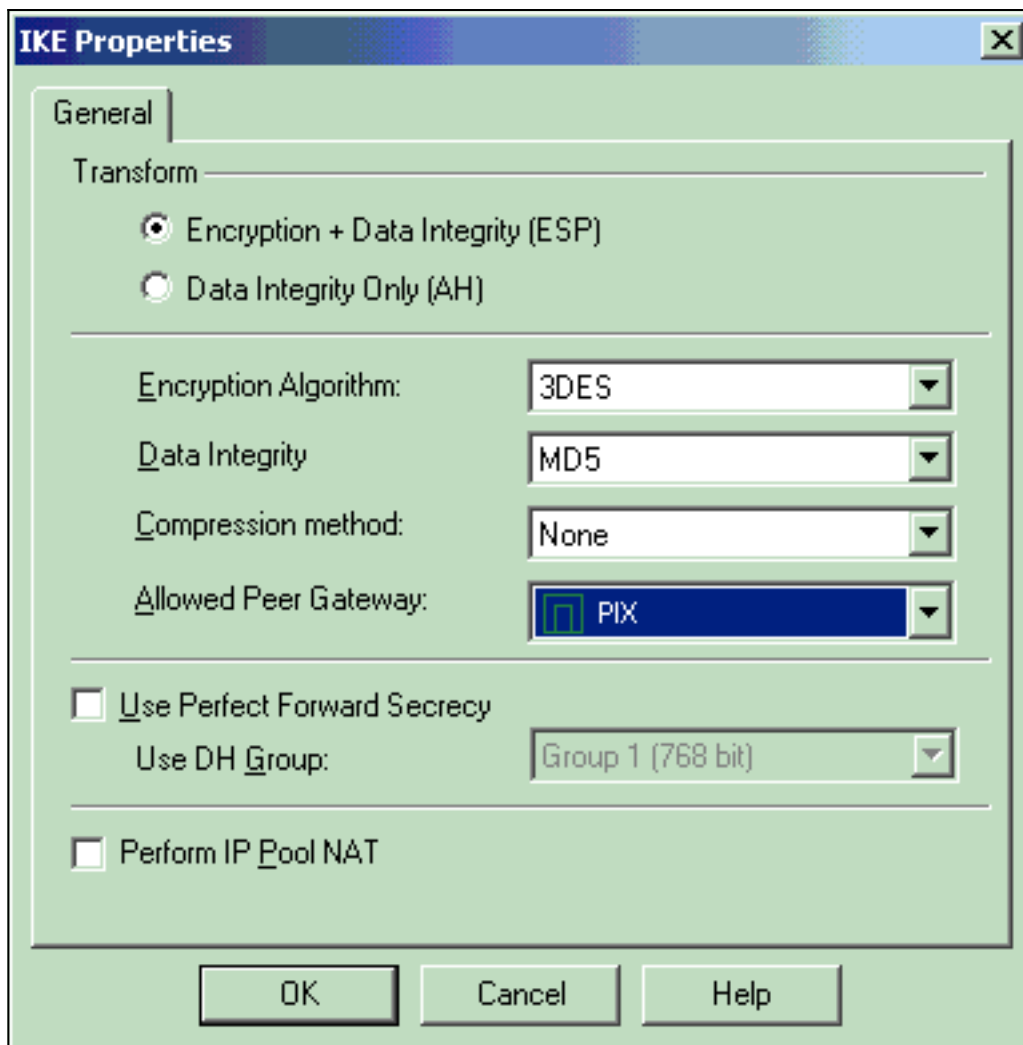


16. Com o IKE selecionado e realçado, clique em



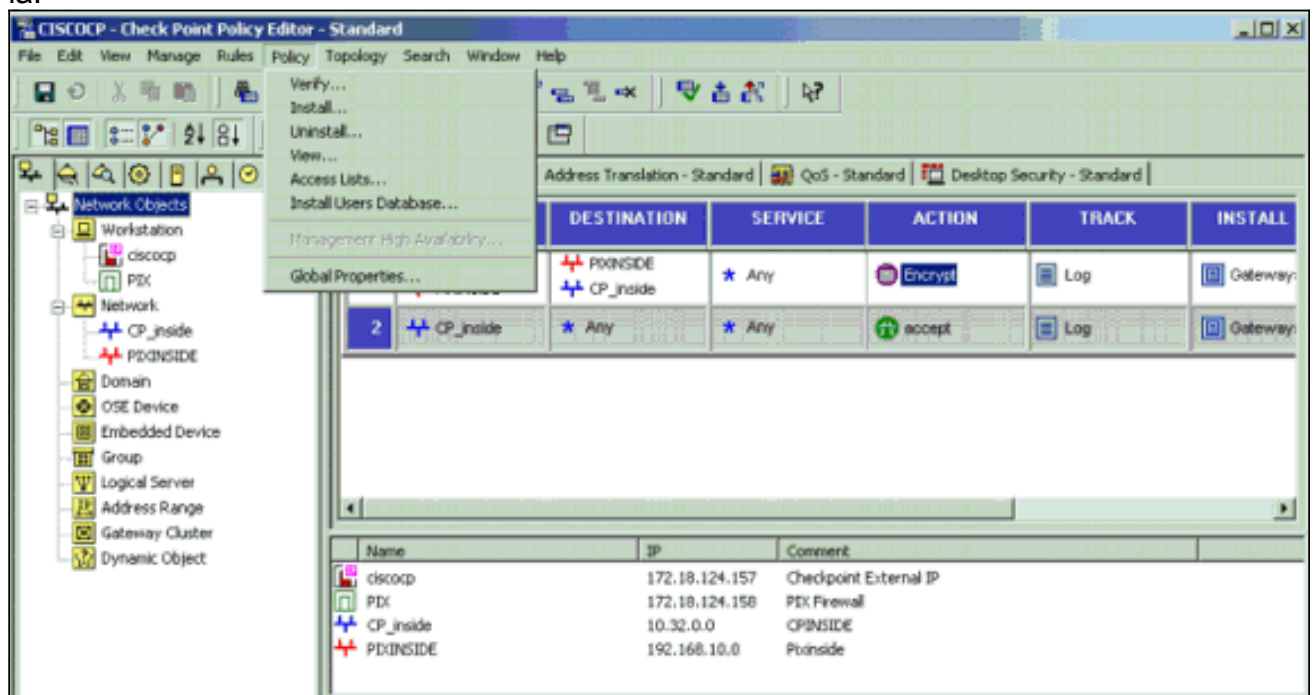
Editar.

17. Na janela Propriedades de IKE, altere as propriedades para concordar com as transformações IPsec de PIX no comando **crypto ipsec transform-set rtpac esp-3des esp-md5-hmac**. Defina a opção Transform como **Encryption + Data Integrity (ESP)**, defina Encryption Algorithm como **3DES**, defina Data Integrity como **MD5** e defina o Allowed Peer Gateway para corresponder ao gateway PIX externo (aqui chamado de PIX). Click

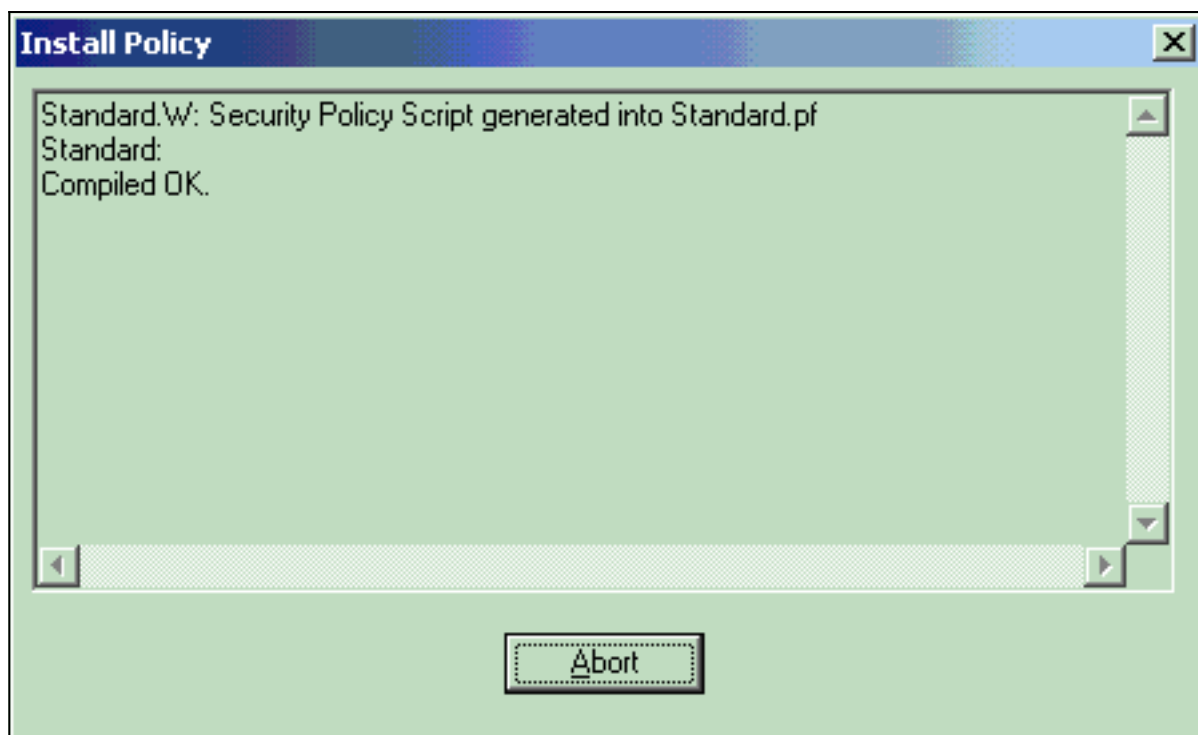


OK.

18. Depois de configurar o Checkpoint™ NG, salve a diretiva e selecione **Policy > Install** para ativá-la.

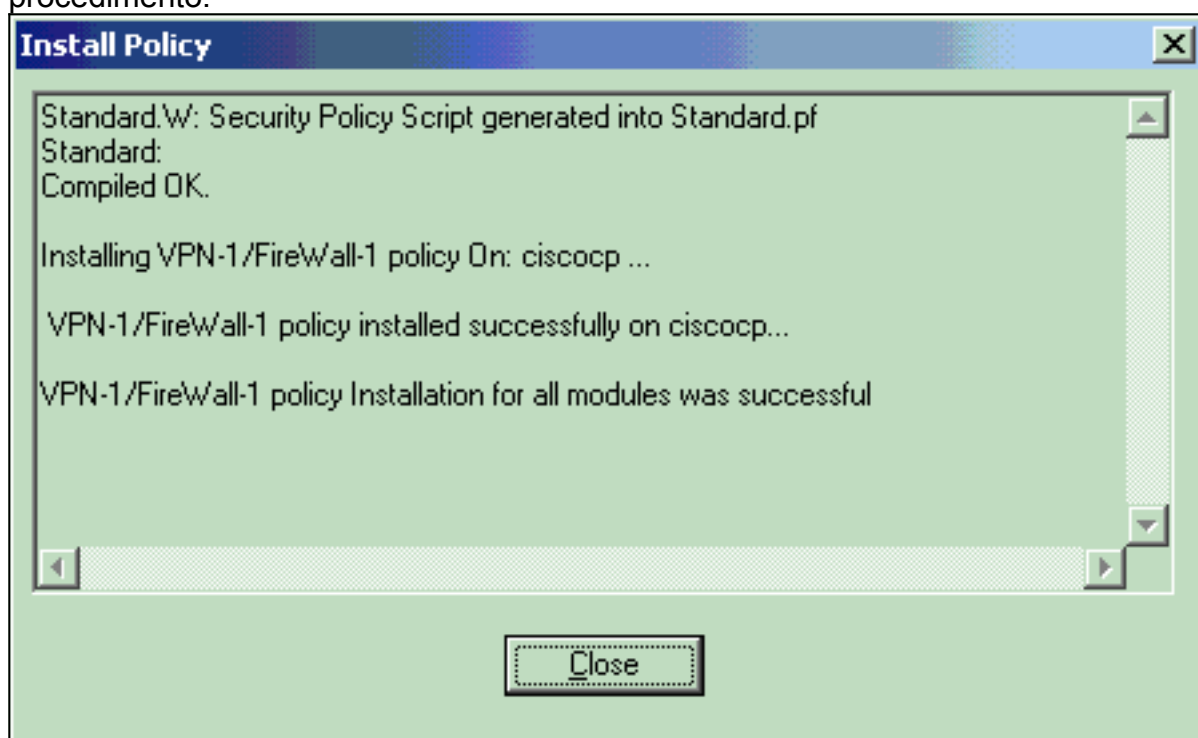


A janela de instalação exibe notas de progresso à medida que a política é compilada.



Quando

o a janela de instalação indicar que a instalação da política está concluída. Clique em **Fechar** para concluir o procedimento.



Verificar

Verificar a configuração do PIX

Use esta seção para confirmar se a sua configuração funciona corretamente.

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

Inicie um ping de uma das redes privadas para a outra rede privada para testar a comunicação entre as duas redes privadas. Nesta configuração, um ping foi enviado do lado do PIX (192.168.10.2) para a rede interna ^{Checkpoint™} NG (10.32.50.51).

- **show crypto isakmp sa** — Exibe todas as SAs IKE atuais em um peer.

```
show crypto isakmp sa
Total      : 1
Embryonic  : 0

      dst                src                state    pending    created
172.18.124.157  172.18.124.158  QM_IDLE      0          1
```

- **show crypto ipsec sa** — Exibe as configurações usadas pelas SAs atuais.

```
PIX501A#show cry ipsec sa

interface: outside
  Crypto map tag: rtprules, local addr. 172.18.124.158

local ident (addr/mask/prot/port): (192.168.10.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (10.32.0.0/255.255.128.0/0/0)
current_peer: 172.18.124.157
  PERMIT, flags={origin_is_acl,}
#pkts encaps: 19, #pkts encrypt: 19, #pkts digest 19
#pkts decaps: 19, #pkts decrypt: 19, #pkts verify 19
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
#send errors 1, #recv errors 0

local crypto endpt.: 172.18.124.158, remote crypto endpt.: 172.18.124.157
path mtu 1500, ipsec overhead 56, media mtu 1500
current outbound spi: 6b15a355

inbound esp sas:
  spi: 0xc3ed238c7(3469883591)
    transform: esp-3des esp-md5-hmac ,
    in use settings ={Tunnel, }
    slot: 0, conn id: 3, crypto map: rtprules
    sa timing: remaining key lifetime (k/sec): (4607998/27019)
    IV size: 8 bytes
    replay detection support: Y

inbound ah sas:
inbound pcp sas:

outbound esp sas:
  spi: 0x6b15a355(1796580181)
    transform: esp-3des esp-md5-hmac ,
    in use settings ={Tunnel, }
    slot: 0, conn id: 4, crypto map: rtprules
    sa timing: remaining key lifetime (k/sec): (4607998/27019)
    IV size: 8 bytes
    replay detection support: Y

outbound ah sas:

outbound pcp sas:
```

[Exibir status do túnel no ponto de controle NG](#)

Vá para o Editor de políticas e selecione **Janela > Status do sistema** para exibir o status do túnel.

Troubleshoot

Solucionar problemas da configuração do PIX

A [Output Interpreter Tool \(somente clientes registrados\) \(OIT\) oferece suporte a 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.

Use estes comandos para ativar as depurações no PIX Firewall.

- **debug crypto engine** — Exibe mensagens de depuração sobre mecanismos de criptografia, que executam criptografia e descriptografia.
- **debug crypto isakmp** — Exibe mensagens sobre eventos de IKE.

```
VPN Peer: ISAKMP: Added new peer: ip:172.18.124.157 Total VPN Peers:1
VPN Peer: ISAKMP: Peer ip:172.18.124.157 Ref cnt incremented to:1 Total VPN Peers:1
ISAKMP (0): beginning Main Mode exchange
crypto_isakmp_process_block: src 172.18.124.157, dest 172.18.124.158
OAK_MM exchange
ISAKMP (0): processing SA payload. message ID = 0
ISAKMP (0): Checking ISAKMP transform 1 against priority 1 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 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 172.18.124.157, dest 172.18.124.158
OAK_MM exchange
ISAKMP (0): processing KE payload. message ID = 0
ISAKMP (0): processing NONCE payload. message ID = 0
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 172.18.124.157, dest 172.18.124.158
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 322868148:133e93b4 IPSEC(key_engine): got a
queue event...
IPSEC(spi_response): getting spi 0xcd238c7(3469883591) for SA
from 172.18.124.157 to 172.18.124.158 for prot 3
return status is IKMP_NO_ERROR
ISAKMP (0): sending INITIAL_CONTACT notify
ISAKMP (0): sending NOTIFY message 24578 protocol 1
ISAKMP (0): sending INITIAL_CONTACT notify
crypto_isakmp_process_block: src 172.18.124.157, dest 172.18.124.158
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_IDLE
ISAKMP (0): processing SA payload. message ID = 322868148
ISAKMP : Checking IPsec proposal 1
ISAKMP: transform 1, ESP_3DES
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= 172.18.124.157, src= 172.18.124.158,
dest_proxy= 10.32.0.0/255.255.128.0/0/0 (type=4),
src_proxy= 192.168.10.0/255.255.255.0/0/0 (type=4),
protocol= ESP, transform= esp-3des esp-md5-hmac ,
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
ISAKMP (0): processing NONCE payload. message ID = 322868148
ISAKMP (0): processing ID payload. message ID = 322868148
ISAKMP (0): processing ID payload. message ID = 322868148
ISAKMP (0): processing NOTIFY payload 24576 protocol 3
spi 3469883591, message ID = 322868148
ISAKMP (0): processing responder lifetime
ISAKMP (0): processing NOTIFY payload 24576 protocol 3
spi 3469883591, message ID = 322868148
ISAKMP (0): processing responder lifetime
ISAKMP (0): Creating IPsec SAs
inbound SA from 172.18.124.157 to 172.18.124.158 (proxy 10.32.0.0 to 192.168.10.0)
has spi 3469883591 and conn_id 3 and flags 4
lifetime of 28800 seconds
lifetime of 4608000 kilobytes
outbound SA from 172.18.124.158 to 172.18.124.157 (proxy 192.168.10.0 to 10.32.0.0)
has spi 1796580181 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= 172.18.124.158, src= 172.18.124.157,
dest_proxy= 192.168.10.0/255.255.255.0/0/0 (type=4),
src_proxy= 10.32.0.0/255.255.128.0/0/0 (type=4),
protocol= ESP, transform= esp-3des esp-md5-hmac ,
lifedur= 28800s and 4608000kb,
spi= 0xcd238c7(3469883591), conn_id= 3, keysize= 0, flags= 0x4
IPSEC(initialize_sas): ,
(key eng. msg.) src= 172.18.124.158, dest= 172.18.124.157,
src_proxy= 192.168.10.0/255.255.255.0/0/0 (type=4),
dest_proxy= 10.32.0.0/255.255.128.0/0/0 (type=4),
protocol= ESP, transform= esp-3des esp-md5-hmac ,
lifedur= 28800s and 4608000kb,
spi= 0x6b15a355(1796580181), conn_id= 4, keysize= 0, flags= 0x4
VPN Peer: IPSEC: Peer ip:172.18.124.157 Ref cnt incremented to:2 Total VPN Peers:1
VPN Peer: IPSEC: Peer ip:172.18.124.157 Ref cnt incremented to:3 Total VPN Peers:1
return status is IKMP_NO_ERROR

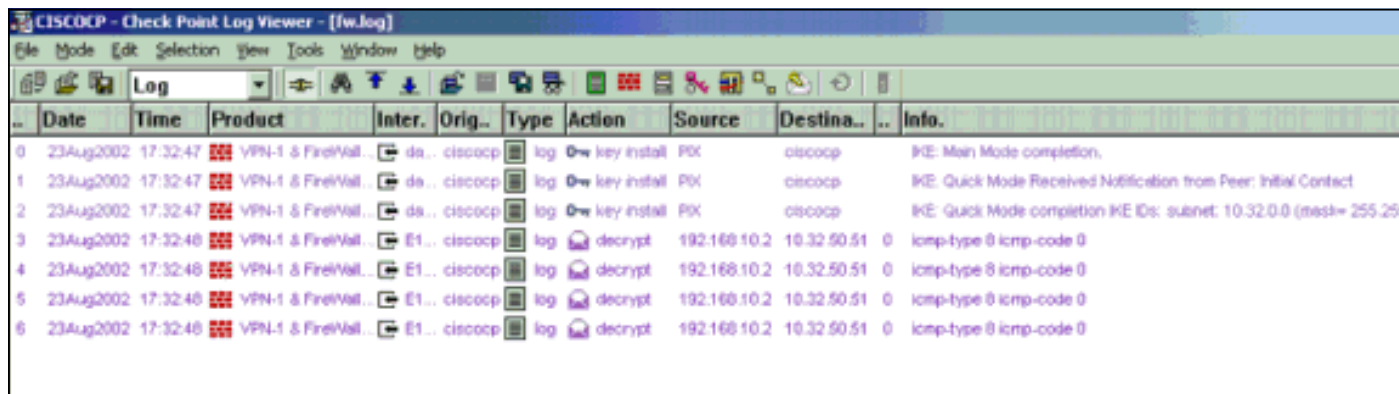
```

[Sumarização de rede](#)

Quando várias redes internas adjacentes são configuradas no domínio de criptografia no ponto de verificação, o dispositivo pode resumi-las automaticamente em relação ao tráfego interessante. Se a lista de controle de acesso de criptografia (ACL) no PIX não estiver configurada para corresponder, o túnel provavelmente falhará. Por exemplo, se as redes internas de 10.0.0.0 /24 e 10.0.1.0 /24 estiverem configuradas para serem incluídas no túnel, elas podem ser resumidas em 10.0.0.0 /23.

[Exibir logs NG do ponto de verificação](#)

Selecione **Window > Log Viewer** para exibir os logs.



..	Date	Time	Product	Inter.	Orig..	Type	Action	Source	Destina..	..	Info.
0	23Aug2002	17:32:47	VPN-1 & FireWall...	da..	ciscocp	log	key install	PIX	ciscocp		IKE: Main Mode completion.
1	23Aug2002	17:32:47	VPN-1 & FireWall...	da..	ciscocp	log	key install	PIX	ciscocp		IKE: Quick Mode Received Notification from Peer: Initial Contact
2	23Aug2002	17:32:47	VPN-1 & FireWall...	da..	ciscocp	log	key install	PIX	ciscocp		IKE: Quick Mode completion IKE IDs: subnet: 10.32.0.0 (mask= 255.25
3	23Aug2002	17:32:48	VPN-1 & FireWall...	E1..	ciscocp	log	decrypt	192.168.10.2	10.32.50.51	0	icmp-type 0 icmp-code 0
4	23Aug2002	17:32:48	VPN-1 & FireWall...	E1..	ciscocp	log	decrypt	192.168.10.2	10.32.50.51	0	icmp-type 0 icmp-code 0
5	23Aug2002	17:32:48	VPN-1 & FireWall...	E1..	ciscocp	log	decrypt	192.168.10.2	10.32.50.51	0	icmp-type 0 icmp-code 0
6	23Aug2002	17:32:48	VPN-1 & FireWall...	E1..	ciscocp	log	decrypt	192.168.10.2	10.32.50.51	0	icmp-type 0 icmp-code 0

[Informações Relacionadas](#)

- [Cisco PIX Firewall Software](#)
- [Referências do comando Cisco Secure PIX Firewall](#)
- [Avisos de campo de produto de segurança \(incluindo PIX\)](#)
- [Solicitações de Comentários \(RFCs\)](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)