

Configurar um túnel IPSec entre um ponto de verificação NG e um roteador

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Diagrama de Rede](#)

[Conventions](#)

[Configurar o Cisco 1751 VPN Router](#)

[Configurar o ponto de verificação NG](#)

[Verificar](#)

[Verificar o roteador Cisco](#)

[Verificar o ponto de verificação NG](#)

[Troubleshoot](#)

[Cisco Router](#)

[Informações Relacionadas](#)

[Introduction](#)

Esse documento demonstra como formar um túnel de IPSec com chaves pré-compartilhadas para unir duas redes privadas:

- A rede privada 172.16.15.x dentro do roteador.
- A rede privada 192.168.10.x dentro da próxima geração (NG) do ^{CheckpointTM}.

[Prerequisites](#)

[Requirements](#)

Os procedimentos descritos neste documento são baseados nestes pressupostos.

- A política básica ^{CheckpointTM} NG é configurada.
- Todas as configurações de acesso, Network Address Translation (NAT) e roteamento são configuradas.
- Tráfego de dentro do roteador e de dentro do ^{CheckpointTM} NG para os fluxos de Internet.

[Componentes Utilizados](#)

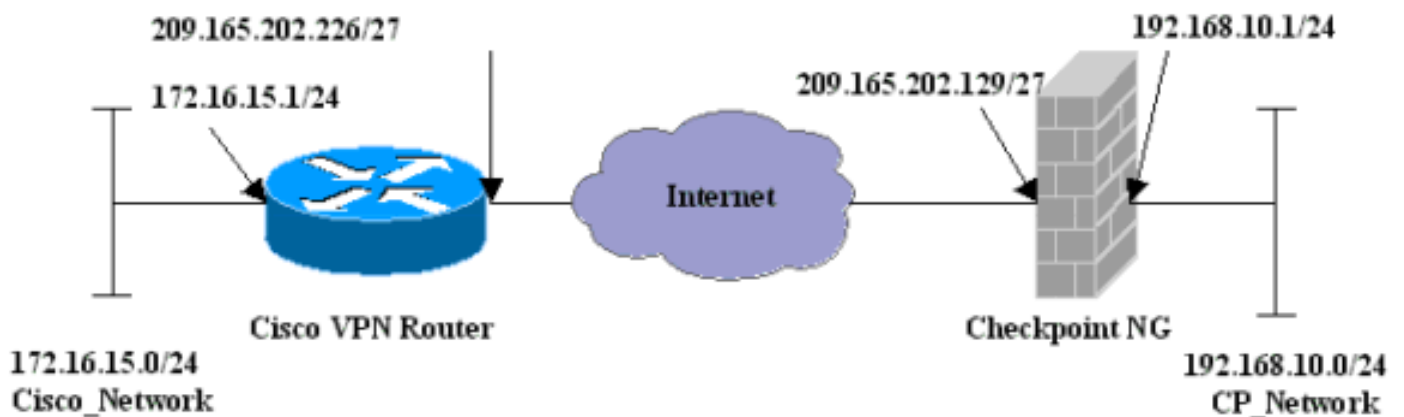
As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco 1751 Router
- Software Cisco IOS® (C1700-K9O3SY7-M), versão 12.2(8)T4, SOFTWARE RELEASE (fc1)
- Checkpoint™ NG Build 50027

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

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

Configurar o Cisco 1751 VPN Router

Roteador Cisco VPN 1751

```
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
hostname svl-6
memory-size iomem 15
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip subnet-zero
no ip domain-lookup
ip audit notify log
ip audit po max-events 100
!--- Internet Key Exchange (IKE) configuration. crypto
isakmp policy 1
    encr 3des
    hash md5
    authentication pre-share
```

```

group 2
lifetime 1800
!--- IPsec configuration. crypto isakmp key aptrules
address 209.165.202.129
!
crypto ipsec transform-set aptset esp-3des esp-md5-hmac
!
crypto map aptmap 1 ipsec-isakmp
set peer 209.165.202.129
set transform-set aptset
match address 110
!
interface Ethernet0/0
ip address 209.165.202.226 255.255.255.224
ip nat outside
half-duplex
crypto map aptmap
!
interface FastEthernet0/0
ip address 172.16.15.1 255.255.255.0
ip nat inside
speed auto
!--- NAT configuration. ip nat inside source route-map
nonat interface Ethernet0/0 overload
ip classless
ip route 0.0.0.0 0.0.0.0 209.165.202.225
no ip http server
ip pim bidir-enable
!--- Encryption match address access list. access-list
110 permit ip 172.16.15.0 0.0.0.255 192.168.10.0
0.0.0.255
!--- NAT access list. access-list 120 deny ip
172.16.15.0 0.0.0.255 192.168.10.0 0.0.0.255
access-list 120 permit ip 172.16.15.0 0.0.0.255 any
route-map nonat permit 10
match ip address 120
line con 0
exec-timeout 0 0
line aux 0
line vty 0 4
password cisco
login
end

```

Configurar o ponto de verificação NG

O Checkpoint™ NG é uma configuração orientada a objeto. Os objetos e regras de rede são definidos 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 da VPN.

1. Crie a sub-rede de rede da Cisco e a sub-rede Checkpoint™ NG como objetos de rede. Isto é o que está criptografado. Para criar os objetos, 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 chamada CP_Network e

Network Properties - CP_Network

General NAT

Name: CP_Network

IP Address: 192.168.10.0

Net Mask: 255.255.255.0

Comment:

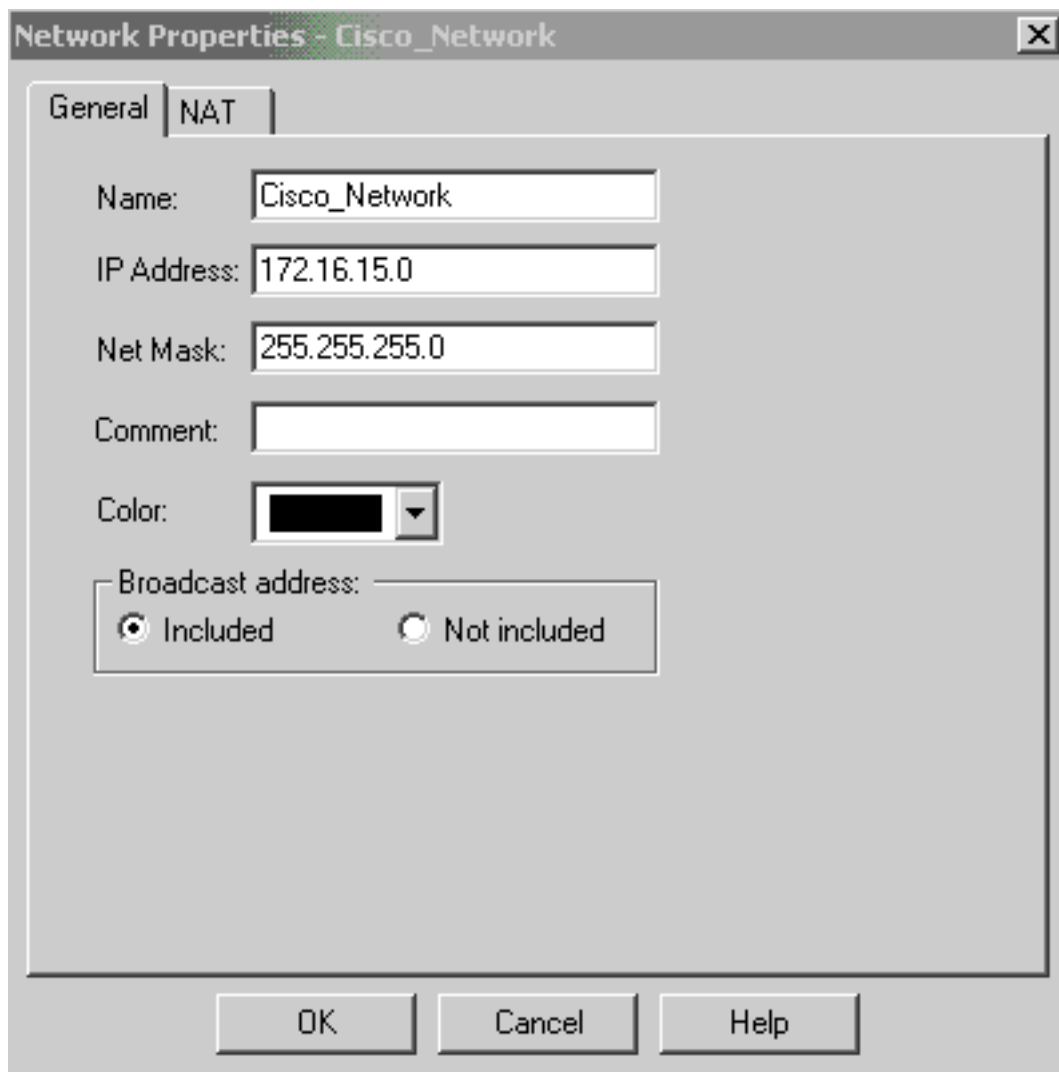
Color:

Broadcast address:

Included Not included

OK Cancel Help

Cisco_Network.



2. Crie os objetos Cisco_Router e Checkpoint_NG como objetos da estação de trabalho. Esses são os dispositivos VPN. Para criar os objetos, selecione **Gerenciar > Objetos de Rede** e, em seguida, selecione **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 e Interoperable VPN Device**. Esses exemplos mostram uma configuração de objetos chamada chef e Cisco_Router.

General

Topology

NAT

VPN

Authentication

Management

+ Advanced

General

Name: chef

IP Address: 209.165.202.129

Get address

Comment: CP_Server

Color: Type: Host Gateway

Check Point Products

 Check Point products installed: Version NG

- 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)

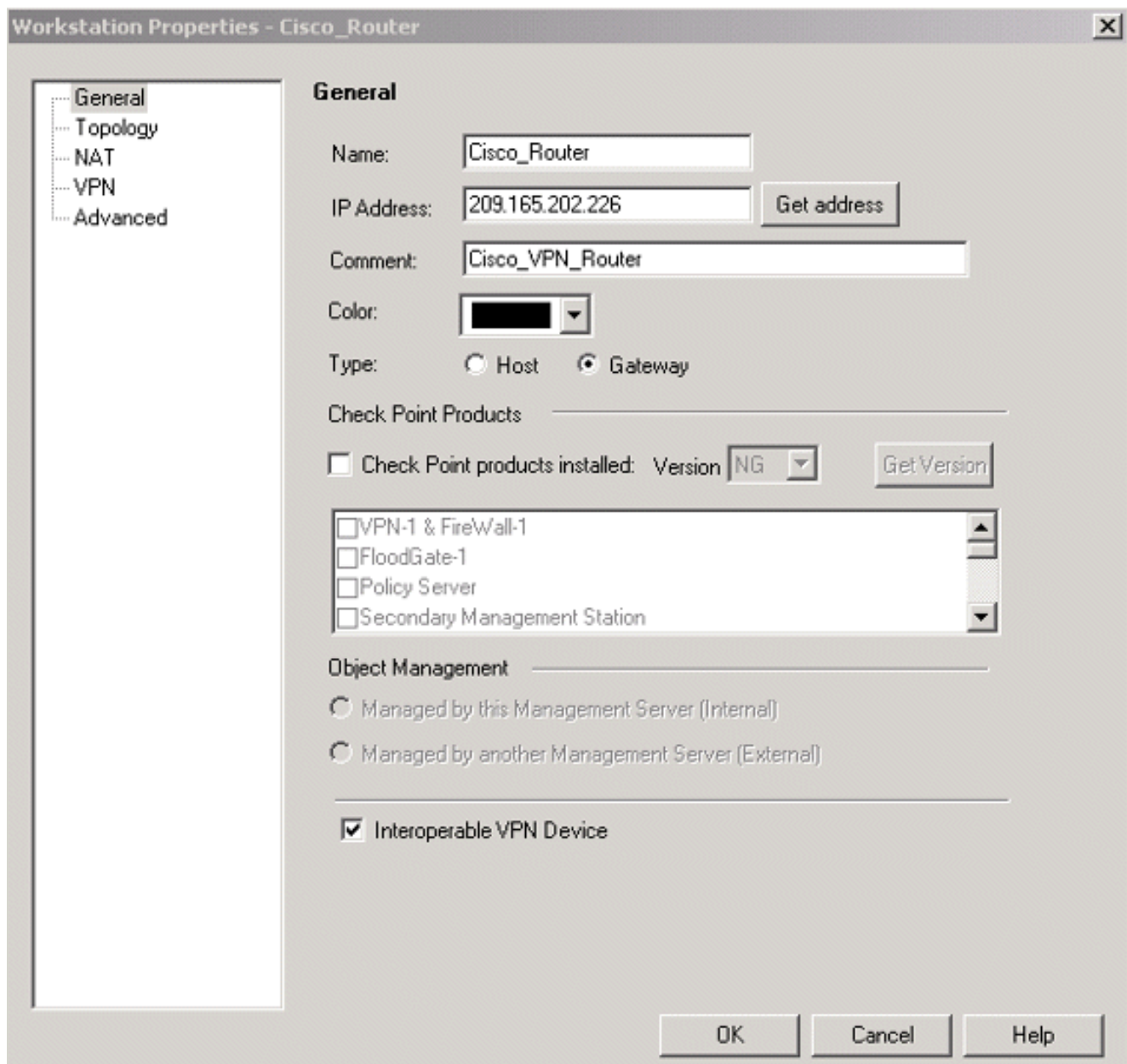
Secure Internal Communication

 DN: cn=cp_mgmt,o=chef.6h9tua Interoperable VPN Device

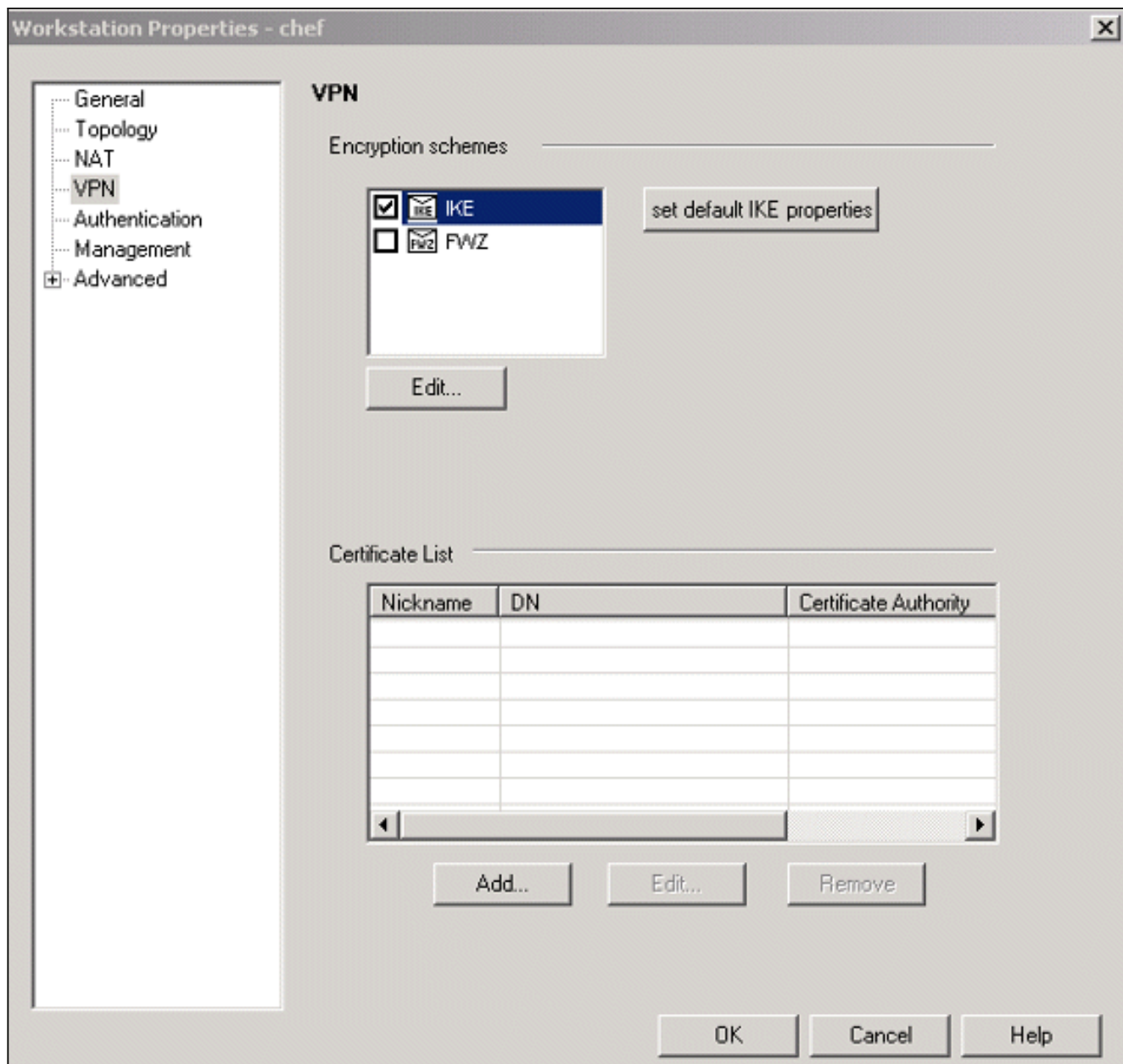
OK

Cancel

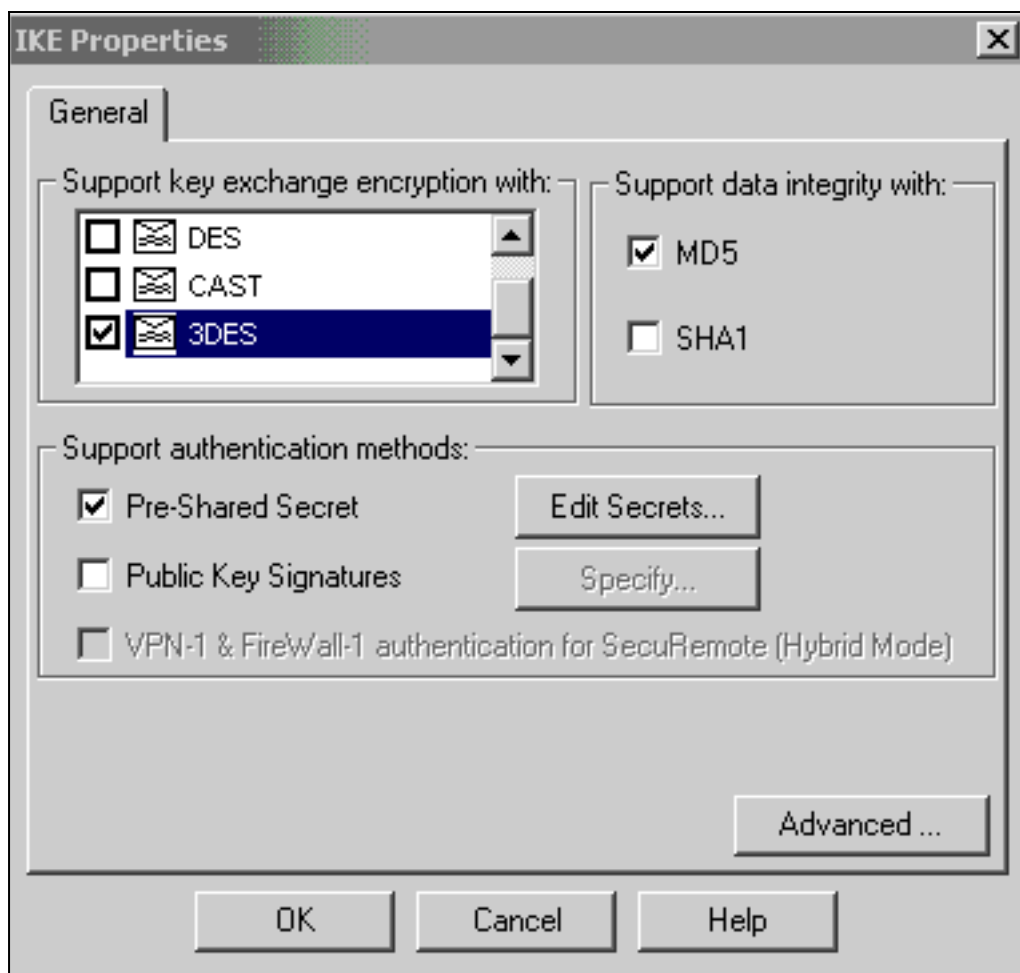
Help



3. Configure o IKE na guia VPN e clique em **Editar**.

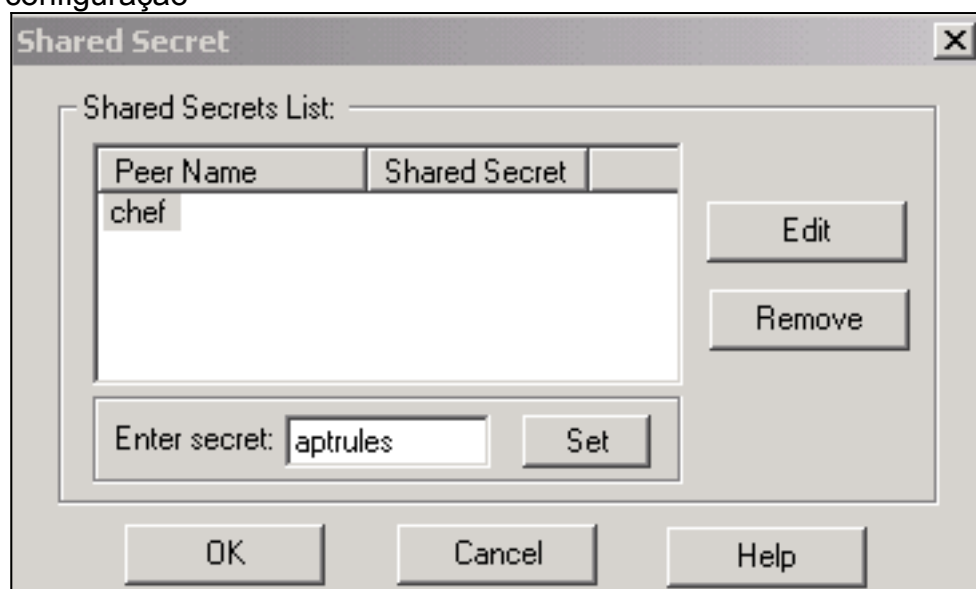


4. Configure a política de troca de chaves e clique em **Editar**



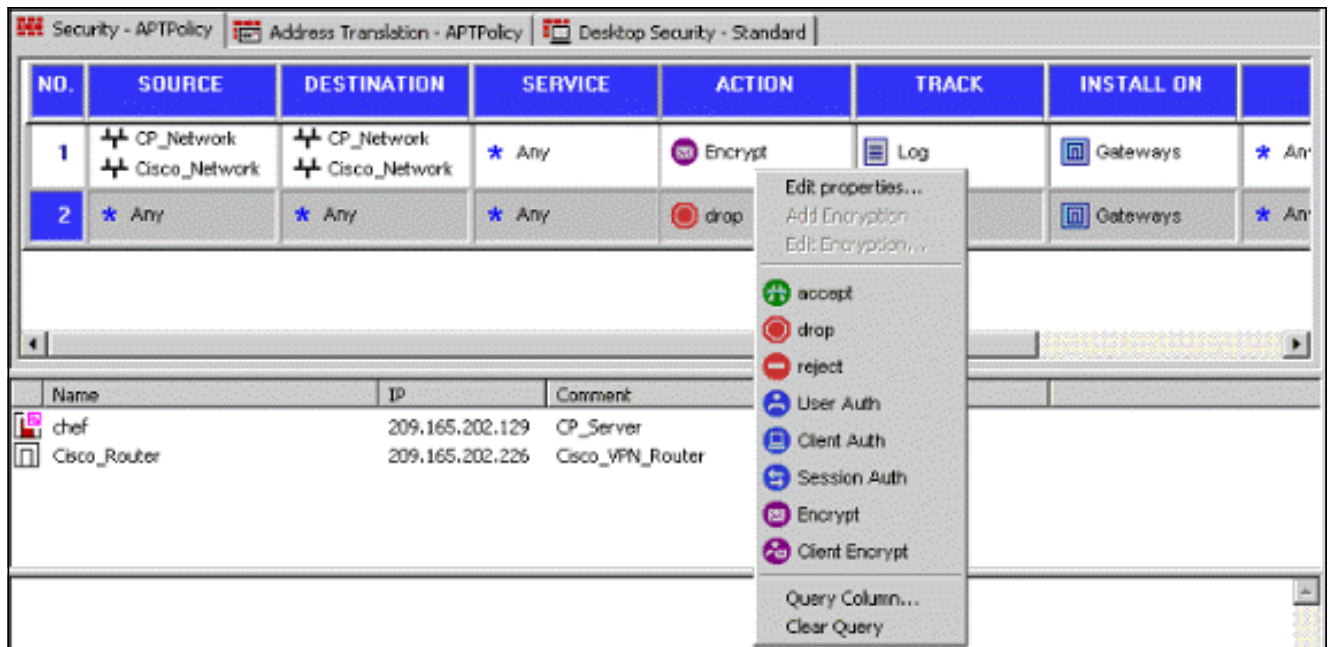
segredos.

- Defina as chaves pré-compartilhadas a serem usadas e clique em **OK** várias vezes até que as janelas de configuração

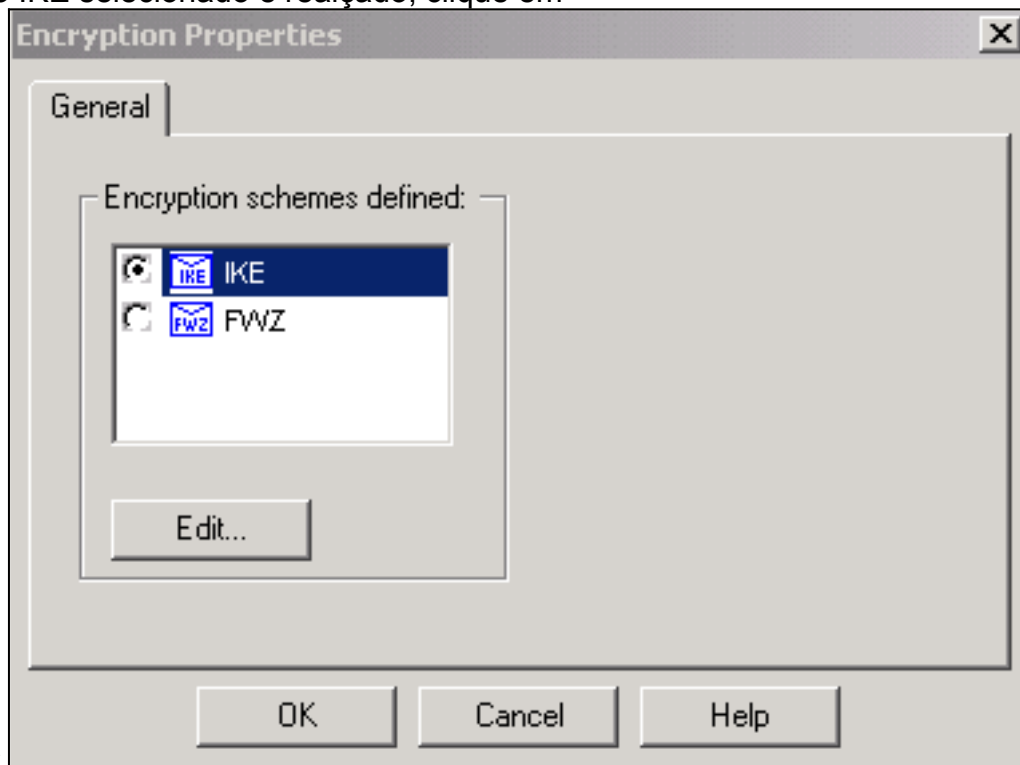


desapareçam.

- Selecione **Regras > Adicionar Regras > Superior** para configurar as regras de criptografia para a política. A regra na parte superior é a primeira regra executada antes de qualquer outra regra que possa ignorar a criptografia. Configure a origem e o destino para incluir o CP_Network e o Cisco_Network, como mostrado aqui. Depois de adicionar a seção Criptografar ação da regra, clique com o botão direito do mouse em **Ação** e selecione **Editar propriedades**.

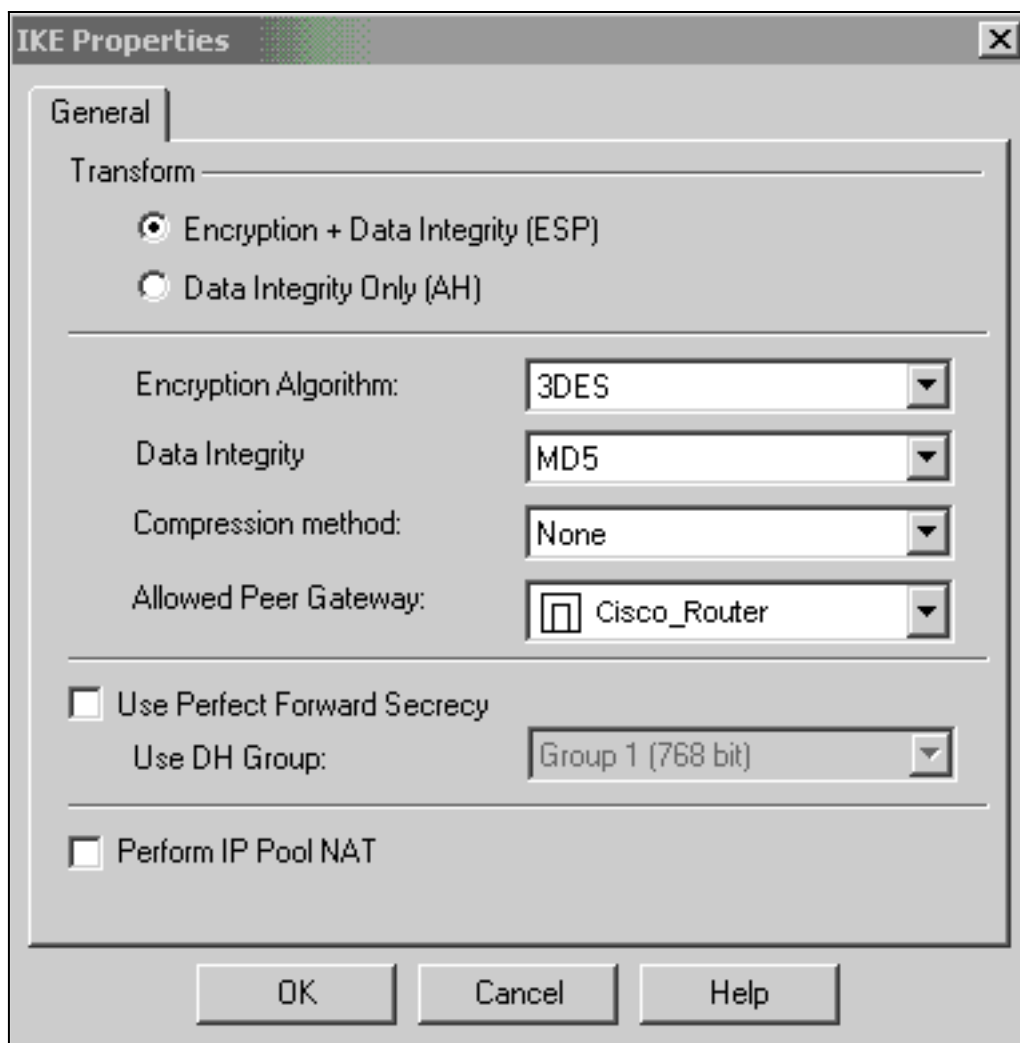


7. Com o IKE selecionado e realçado, clique em



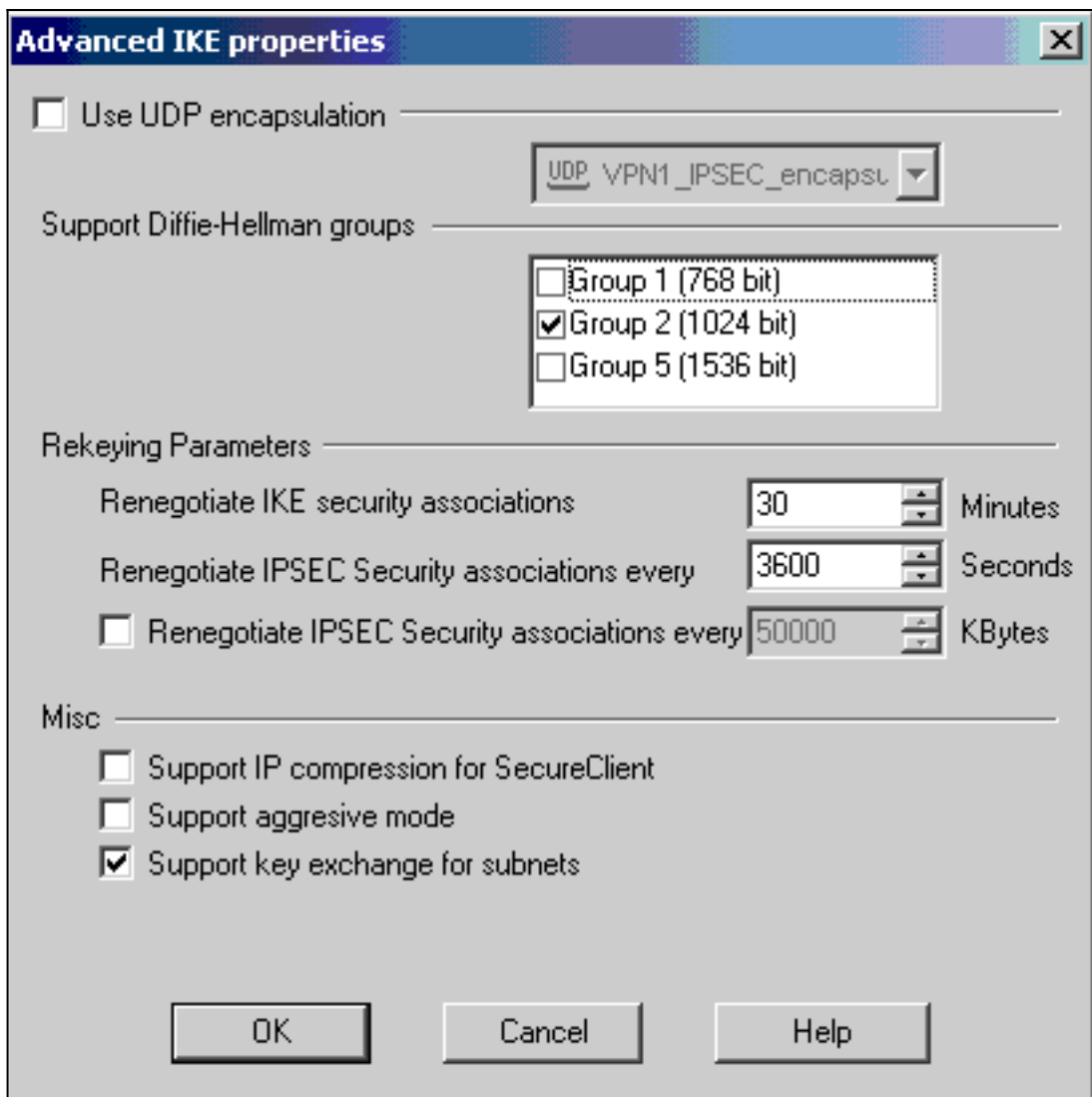
Editar.

8. Confirme a configuração



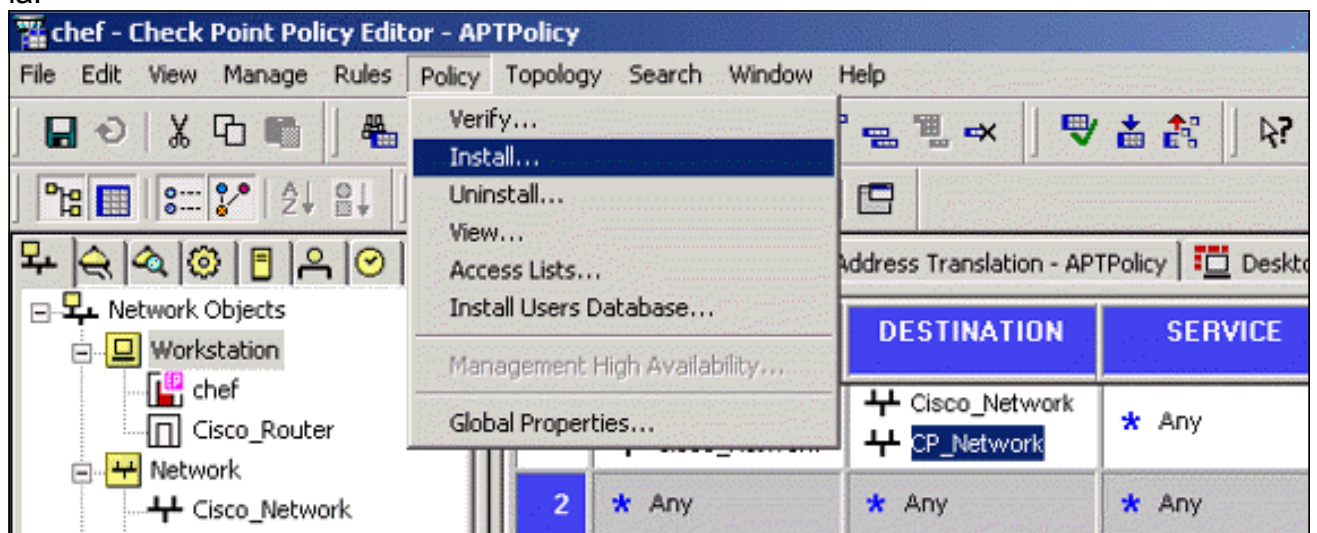
IKE.

9. Um dos principais problemas com a execução de VPN entre dispositivos Cisco e outros dispositivos IPsec é a renegociação de troca de chaves. Certifique-se de que a configuração para a troca IKE no roteador Cisco seja exatamente a mesma que a configurada no CheckpointTM NG. **Observação:** o valor real desse parâmetro depende de sua política de segurança corporativa específica. Neste exemplo, a [configuração de IKE no roteador](#) foi definida para 30 minutos com o comando **lifetime 1800**. O mesmo valor tem de ser definido no CheckpointTM NG. Para definir esse valor no CheckpointTM NG, selecione **Gerenciar objeto de rede**, selecione o objeto NG CheckpointTM e clique em **Editar**. Em seguida, selecione **VPN** e edite o IKE. Selecione **Avançar** e configure os parâmetros de chaveamento. Depois de configurar a troca de chaves para o objeto de rede NG CheckpointTM, execute a mesma configuração da Renegociação de troca de chaves para o objeto de rede Cisco_Router. **Observação:** certifique-se de que o grupo Diffie-Hellman correto esteja selecionado para corresponder ao configurado no

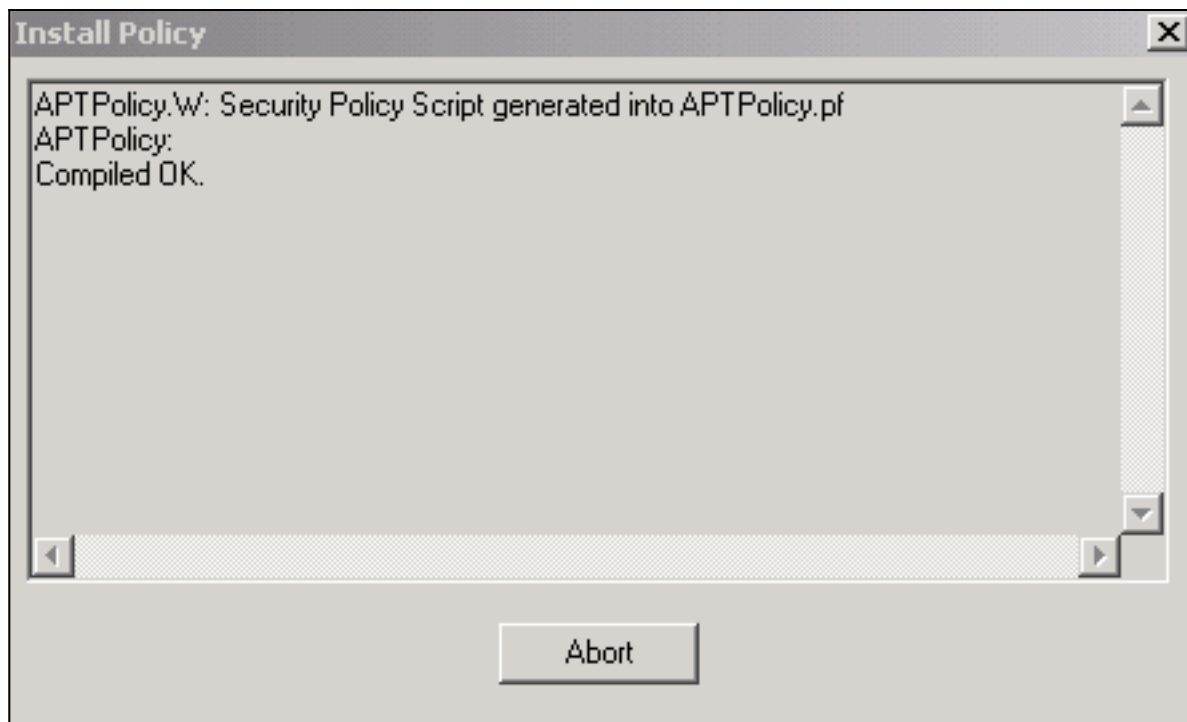


roteador.

10. A configuração da política está concluída. Salve a diretiva e selecione **Policy > Install (Política > Instalar)** para ativá-la.

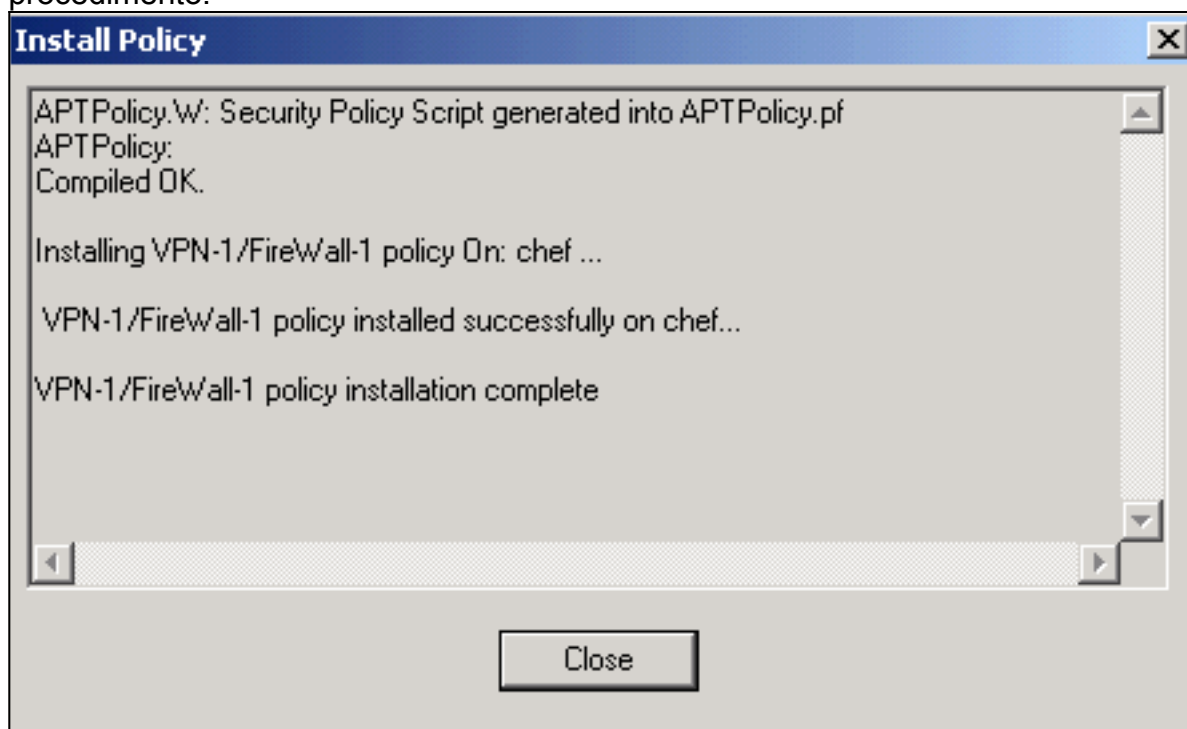


A janela de instalação exibe notas de progresso à medida que a política é compilada.



Quando

o a janela de instalação indicar que a instalação da diretiva está concluída, clique em **Fechar** para concluir o procedimento.



Verificar

Esta seção fornece informações que você pode usar para confirmar se sua configuração está funcionando adequadamente.

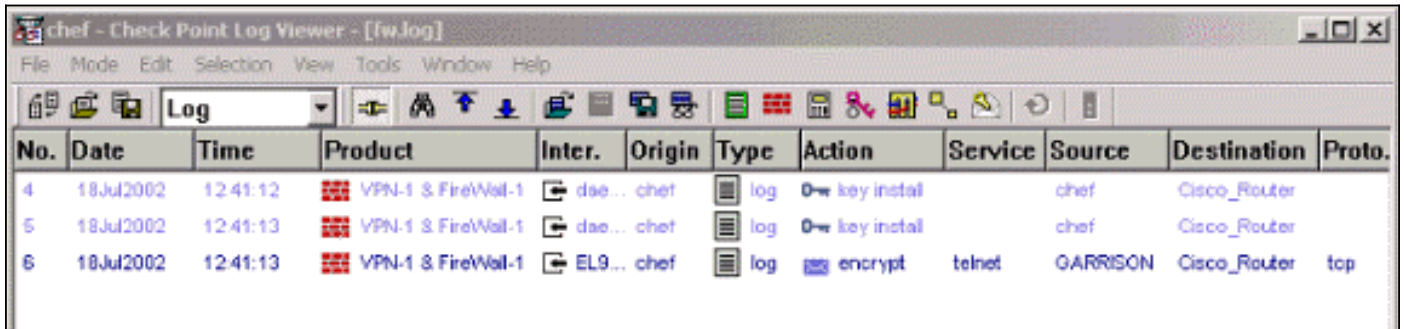
Verificar o roteador Cisco

A [Output Interpreter Tool \(somente clientes registrados\)](#) oferece suporte a determinados comandos show, o que permite exibir uma análise da saída do comando show.

- **show crypto isakmp sa** — Exibe todas as associações de segurança atuais (SAs) de IKE em um peer.
- **show crypto ipsec sa** — Exibe as configurações usadas pelas SAs atuais.

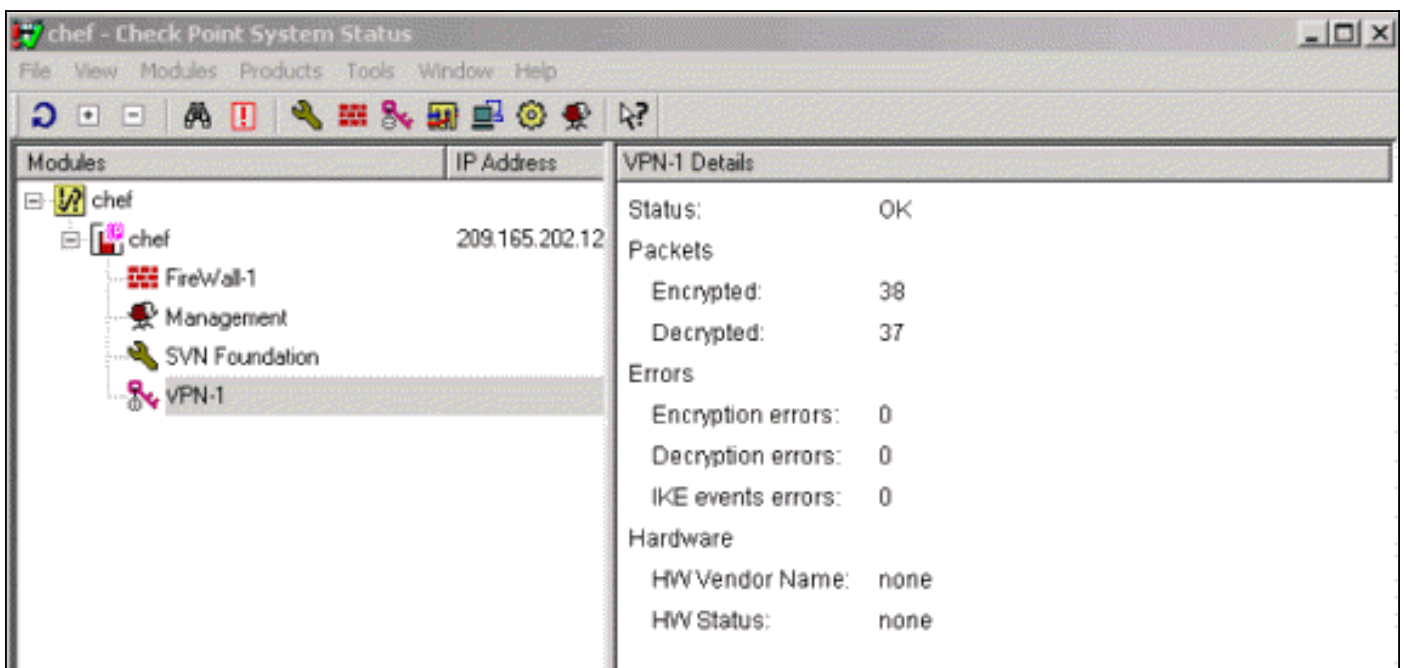
Verificar o ponto de verificação NG

Para visualizar os registros, selecione **Janela > Visualizador de registros**.



| No. | Date | Time | Product | Inter. | Origin | Type | Action | Service | Source | Destination | Proto. |
|-----|-----------|----------|--------------------|--------|--------|------|------------|---------|----------|--------------|--------|
| 4 | 18Jul2002 | 12:41:12 | VPN-1 & FireWall-1 | dae... | chef | log | key instal | | chef | Cisco_Router | |
| 5 | 18Jul2002 | 12:41:13 | VPN-1 & FireWall-1 | dae... | chef | log | key instal | | chef | Cisco_Router | |
| 6 | 18Jul2002 | 12:41:13 | VPN-1 & FireWall-1 | EL9... | chef | log | encrypt | telnet | GARRISON | Cisco_Router | tcp |

Para exibir o status do sistema, selecione **Janela > Status do sistema**.



| Modules | IP Address | VPN-1 Details |
|----------------|----------------|----------------------|
| chef | | Status: OK |
| chef | 209.165.202.12 | Packets |
| FireWall-1 | | Encrypted: 38 |
| Management | | Decrypted: 37 |
| SVN Foundation | | Errors |
| VPN-1 | | Encryption errors: 0 |
| | | Decryption errors: 0 |
| | | IKE events errors: 0 |
| | | Hardware |
| | | HW Vendor Name: none |
| | | HW Status: none |

Troubleshoot

Cisco Router

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

Para obter informações adicionais sobre solução de problemas, consulte [Solução de problemas de segurança de IP - Entendendo e usando comandos debug](#).

Observação: antes de inserir o comando **debug**, consulte [Informações importantes sobre os comandos debug](#).

- **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.
- **debug crypto ipsec** — Exibe eventos de IPSec.
- **clear crypto isakmp** — Limpa todas as conexões IKE ativas.
- **clear crypto sa** — Limpa todas as SAs de IPSec.

Saída bem-sucedida do log de depuração

```

18:05:32: ISAKMP (0:0): received packet from
      209.165.202.129 (N) NEW SA
18:05:32: ISAKMP: local port 500, remote port 500
18:05:32: ISAKMP (0:1): Input = IKE_MSG_FROM_PEER,
      IKE_MM_EXCH
Old State = IKE_READY New State = IKE_R_MM1
18:05:32: ISAKMP (0:1): processing SA payload. message ID = 0
18:05:32: ISAKMP (0:1): processing vendor id payload
18:05:32: ISAKMP (0:1): vendor ID seems Unity/DPD
      but bad major
18:05:32: ISAKMP (0:1): found peer pre-shared key
      matching 209.165.202.129
18:05:32: ISAKMP (0:1): Checking ISAKMP transform 1
      against priority 1 policy
18:05:32: ISAKMP: encryption 3DES-CBC
18:05:32: ISAKMP: hash MD5
18:05:32: ISAKMP: auth pre-share
18:05:32: ISAKMP: default group 2
18:05:32: ISAKMP: life type in seconds
18:05:32: ISAKMP: life duration (VPI) of 0x0 0x0 0x7 0x8
18:05:32: ISAKMP (0:1): atts are acceptable. Next payload is 0
18:05:33: ISAKMP (0:1): processing vendor id payload
18:05:33: ISAKMP (0:1): vendor ID seems Unity/DPD but bad major
18:05:33: ISAKMP (0:1): Input = IKE_MSG_INTERNAL,
      IKE_PROCESS_MAIN_MODE
Old State = IKE_R_MM1 New State = IKE_R_MM1
18:05:33: ISAKMP (0:1): sending packet to 209.165.202.129 (R)
      MM_SA_SETUP
18:05:33: ISAKMP (0:1): Input = IKE_MSG_INTERNAL,
      IKE_PROCESS_COMPLETE
Old State = IKE_R_MM1 New State = IKE_R_MM2
18:05:33: ISAKMP (0:1): received packet from 209.165.202.129 (R)
      MM_SA_SETUP
18:05:33: ISAKMP (0:1): Input = IKE_MSG_FROM_PEER,
      IKE_MM_EXCH
Old State = IKE_R_MM2 New State = IKE_R_MM3
18:05:33: ISAKMP (0:1): processing KE payload.
      message ID = 0
18:05:33: ISAKMP (0:1): processing NONCE payload.
      message ID = 0
18:05:33: ISAKMP (0:1): found peer pre-shared key
      matching 209.165.202.129
18:05:33: ISAKMP (0:1): SKEYID state generated
18:05:33: ISAKMP (0:1): Input = IKE_MSG_INTERNAL,
      IKE_PROCESS_MAIN_MODE
Old State = IKE_R_MM3 New State = IKE_R_MM3
18:05:33: ISAKMP (0:1): sending packet to 209.165.202.129 (R)
      MM_KEY_EXCH
18:05:33: ISAKMP (0:1): Input = IKE_MSG_INTERNAL,
      IKE_PROCESS_COMPLETE
Old State = IKE_R_MM3 New State = IKE_R_MM4
18:05:33: ISAKMP (0:1): received packet from 209.165.202.129 (R)

```

```
MM_KEY_EXCH
18:05:33: ISAKMP (0:1): Input = IKE_MESG_FROM_PEER,
IKE_MM_EXCH
Old State = IKE_R_MM4 New State = IKE_R_MM5
18:05:33: ISAKMP (0:1): processing ID payload.
message ID = 0
18:05:33: ISAKMP (0:1): processing HASH payload.
message ID = 0
18:05:33: ISAKMP (0:1): SA has been authenticated
with 209.165.202.129
18:05:33: ISAKMP (0:1): Input = IKE_MESG_INTERNAL,
IKE_PROCESS_MAIN_MODE
Old State = IKE_R_MM5 New State = IKE_R_MM5
18:05:33: ISAKMP (0:1): SA is doing pre-shared key authentication
using id type ID_IPV4_ADDR
18:05:33: ISAKMP (1): ID payload
next-payload : 8
type : 1
protocol : 17
port : 500
length : 8
18:05:33: ISAKMP (1): Total payload length: 12
18:05:33: ISAKMP (0:1): sending packet to 209.165.202.129
(R) QM_IDLE
18:05:33: ISAKMP (0:1): Input = IKE_MESG_INTERNAL,
IKE_PROCESS_COMPLETE
Old State = IKE_R_MM5 New State = IKE_P1_COMPLETE
18:05:33: ISAKMP (0:1): Input = IKE_MESG_INTERNAL,
IKE_PHASE1_COMPLETE
Old State = IKE_P1_COMPLETE
New State = IKE_P1_COMPLETE
18:05:33: ISAKMP (0:1): received packet from 209.165.202.129 (R)
QM_IDLE
18:05:33: ISAKMP (0:1): processing HASH payload.
message ID = -1335371103
18:05:33: ISAKMP (0:1): processing SA payload.
message ID = -1335371103
18:05:33: ISAKMP (0:1): Checking IPSec proposal 1
18:05:33: ISAKMP: transform 1, ESP_3DES
18:05:33: ISAKMP: attributes in transform:
18:05:33: ISAKMP: SA life type in seconds
18:05:33: ISAKMP: SA life duration (VPI) of 0x0 0x0 0xE 0x10
18:05:33: ISAKMP: authenticator is HMAC-MD5
18:05:33: ISAKMP: encaps is 1
18:05:33: ISAKMP (0:1): atts are acceptable.
18:05:33: IPSEC(validate_proposal_request): proposal part #1,
(key eng. msg.) INBOUND local= 209.165.202.226, remote= 209.165.202.129,
local_proxy= 172.16.15.0/255.255.255.0/0/0 (type=4),
remote_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
18:05:33: ISAKMP (0:1): processing NONCE payload.
message ID = -1335371103
18:05:33: ISAKMP (0:1): processing ID payload.
message ID = -1335371103
18:05:33: ISAKMP (0:1): processing ID payload.
message ID = -1335371103
18:05:33: ISAKMP (0:1): asking for 1 spis from ipsec
18:05:33: ISAKMP (0:1): Node -1335371103,
Input = IKE_MESG_FROM_PEER, IKE_QM_EXCH
Old State = IKE_QM_READY New State = IKE_QM_SPI_STARVE
18:05:33: IPSEC(key_engine): got a queue event...
18:05:33: IPSEC(spi_response): getting spi 2147492563 for SA
```


from 209.165.202.226 to 209.165.202.129 for prot 3
18:05:33: ISAKMP: received ke message (2/1)
18:05:33: ISAKMP (0:1): sending packet to
209.165.202.129 (R) QM_IDLE
18:05:33: ISAKMP (0:1): Node -1335371103,
Input = IKE_MESG_FROM_IPSEC, IKE_SPI_REPLY
Old State = IKE_QM_SPI_STARVE New State = IKE_QM_R_QM2
18:05:33: ISAKMP (0:1): received packet
from 209.165.202.129 (R) QM_IDLE
18:05:33: ISAKMP (0:1): Creating IPsec SAs
18:05:33: inbound SA from 209.165.202.129 to 209.165.202.226
(proxy 192.168.10.0 to 172.16.15.0)
18:05:33: has spi 0x800022D3 and conn_id 200 and flags 4
18:05:33: lifetime of 3600 seconds
18:05:33: outbound SA from 209.165.202.226 to 209.165.202.129
(proxy 172.16.15.0 to 192.168.10.0)
18:05:33: has spi -2006413528 and conn_id 201 and flags C
18:05:33: lifetime of 3600 seconds
18:05:33: ISAKMP (0:1): deleting node -1335371103 error
FALSE reason "quick mode done (await())"
18:05:33: ISAKMP (0:1): Node -1335371103, Input = IKE_MESG_FROM_PEER,
IKE_QM_EXCH
Old State = IKE_QM_R_QM2 New State = IKE_QM_PHASE2_COMPLETE
18:05:33: IPSEC(key_engine): got a queue event...
18:05:33: IPSEC(initialize_sas): ,
(key eng. msg.) INBOUND local= 209.165.202.226,
remote=209.165.202.129,
local_proxy= 172.16.15.0/255.255.255.0/0/0 (type=4),
remote_proxy= 192.168.10.0/255.255.255.0/0/0 (type=4),
protocol= ESP, transform= esp-3des esp-md5-hmac ,
lifedur= 3600s and 0kb,
spi= 0x800022D3(2147492563), conn_id= 200, keysize= 0,
flags= 0x4
18:05:33: IPSEC(initialize_sas): ,
(key eng. msg.) OUTBOUND local= 209.165.202.226,
remote=209.165.202.129,
local_proxy= 172.16.15.0/255.255.255.0/0/0 (type=4),
remote_proxy= 192.168.10.0/255.255.255.0/0/0 (type=4),
protocol= ESP, transform= esp-3des esp-md5-hmac ,
lifedur= 3600s and 0kb,

spi= 0x88688F28(2288553768), conn_id= 201, keysize= 0,
flags= 0xC
18:05:33: IPSEC(create_sa): sa created,
(sa) sa_dest= 209.165.202.226, sa_prot= 50,
sa_spi= 0x800022D3(2147492563),
sa_trans= esp-3des esp-md5-hmac , sa_conn_id= 200
18:05:33: IPSEC(create_sa): sa created,
(sa) sa_dest= 209.165.202.129, sa_prot= 50,
sa_spi= 0x88688F28(2288553768),
sa_trans= esp-3des esp-md5-hmac , sa_conn_id= 201
18:05:34: ISAKMP (0:1): received packet
from 209.165.202.129 (R) QM_IDLE
18:05:34: ISAKMP (0:1): phase 2 packet is a duplicate
of a previous packet.
18:05:34: ISAKMP (0:1): retransmitting due to retransmit phase 2
18:05:34: ISAKMP (0:1): ignoring retransmission, because phase2
node marked dead -1335371103
18:05:34: ISAKMP (0:1): received packet
from 209.165.202.129 (R) QM_IDLE
18:05:34: ISAKMP (0:1): phase 2 packet is a duplicate
of a previous packet.

```
18:05:34: ISAKMP (0:1): retransmitting due to retransmit phase 2
18:05:34: ISAKMP (0:1): ignoring retransmission, because phase2
node marked dead -1335371103
```

```
svl-6#show crypto isakmp sa
```

```
dst src state conn-id slot
209.165.202.226 209.165.202.129 QM_IDLE 1 0
```

```
svl-6#show crypto ipsec sa
```

```
interface: Ethernet0/0
Crypto map tag: aptmap, local addr. 209.165.202.226
local ident (addr/mask/prot/port): (172.16.15.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (192.168.10.0/255.255.255.0/0/0)
current_peer: 209.165.202.129
PERMIT, flags={origin_is_acl,}
#pkts encaps: 21, #pkts encrypt: 21, #pkts digest 21
#pkts decaps: 24, #pkts decrypt: 24, #pkts verify 24
#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.: 209.165.202.226, remote crypto endpt.: 209.165.202.129
path mtu 1500, media mtu 1500
current outbound spi: 88688F28
inbound esp sas:
spi: 0x800022D3(2147492563)
transform: esp-3des esp-md5-hmac ,
in use settings = {Tunnel, }
slot: 0, conn id: 200, flow_id: 1, crypto map: aptmap
sa timing: remaining key lifetime (k/sec): (4607997/3559)
IV size: 8 bytes
replay detection support: Y
inbound ah sas:
inbound pcp sas:
outbound esp sas:
spi: 0x88688F28(2288553768)
transform: esp-3des esp-md5-hmac ,
in use settings = {Tunnel, }
slot: 0, conn id: 201, flow_id: 2, crypto map: aptmap
sa timing: remaining key lifetime (k/sec): (4607997/3550)
IV size: 8 bytes
replay detection support: Y
outbound ah sas:
outbound pcp sas:
```

```
svl-6#show crypto engine conn act
```

| ID | Interface | IP- | Address | State | Algorithm | Encrypt | Decrypt |
|-----|-------------|-----------------|---------|--------------------|-----------|-----------|---------|
| 1 | Ethernet0/0 | 209.165.202.226 | set | HMAC_MD5+3DES_56_C | 0 | 0 | |
| 200 | Ethernet0/0 | 209.165.202.226 | set | HMAC_MD5+3DES_56_C | 0 | 24 | |
| 201 | Ethernet0/0 | 209.165.202.226 | set | HMAC_MD5+3DES_56_C | 21 | 0 | |

[Informações Relacionadas](#)

- [Página de suporte do IPSec](#)
- [Suporte Técnico - Cisco Systems](#)