Configurando um túnel de IPsec entre um roteador Cisco e um NG ponto de verificação

Índice

Introdução

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 do ponto de verificação™ (NG).

Pré-requisitos

Requisitos

Os procedimentos esboçados neste documento são baseados nestas suposições.

- A política básica do ponto de verificação™ NG estabelece-se.
- Todo o acesso, Network Address Translation (NAT), e instalações do roteamento são configurados.
- Trafique do interior do roteador e o interior o ponto de verificação™ NG ao Internet flui.

Componentes Utilizados

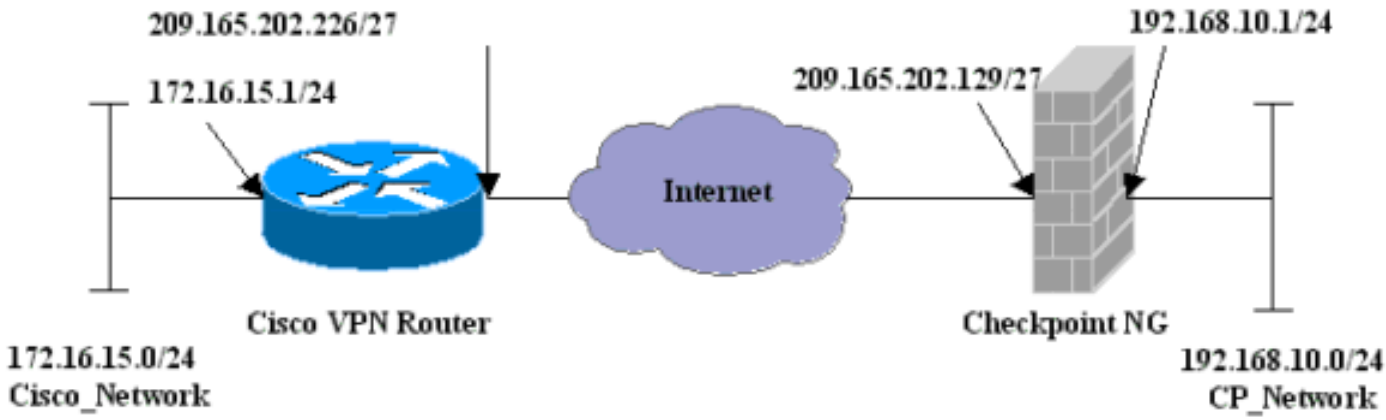
As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco 1751 Router
- Software de Cisco IOS® (C1700-K9O3SY7-M), versão 12.2(8)T4, SOFTWARE DE VERSÃO (fc1)
- Construção 50027 do ponto de verificação™ NG

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.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



Convenções

Para obter mais informações sobre convenções de documento, consulte as Convenções de dicas técnicas Cisco.

Configurar o VPN Router do Cisco 1751

1751 Router de Cisco VPN

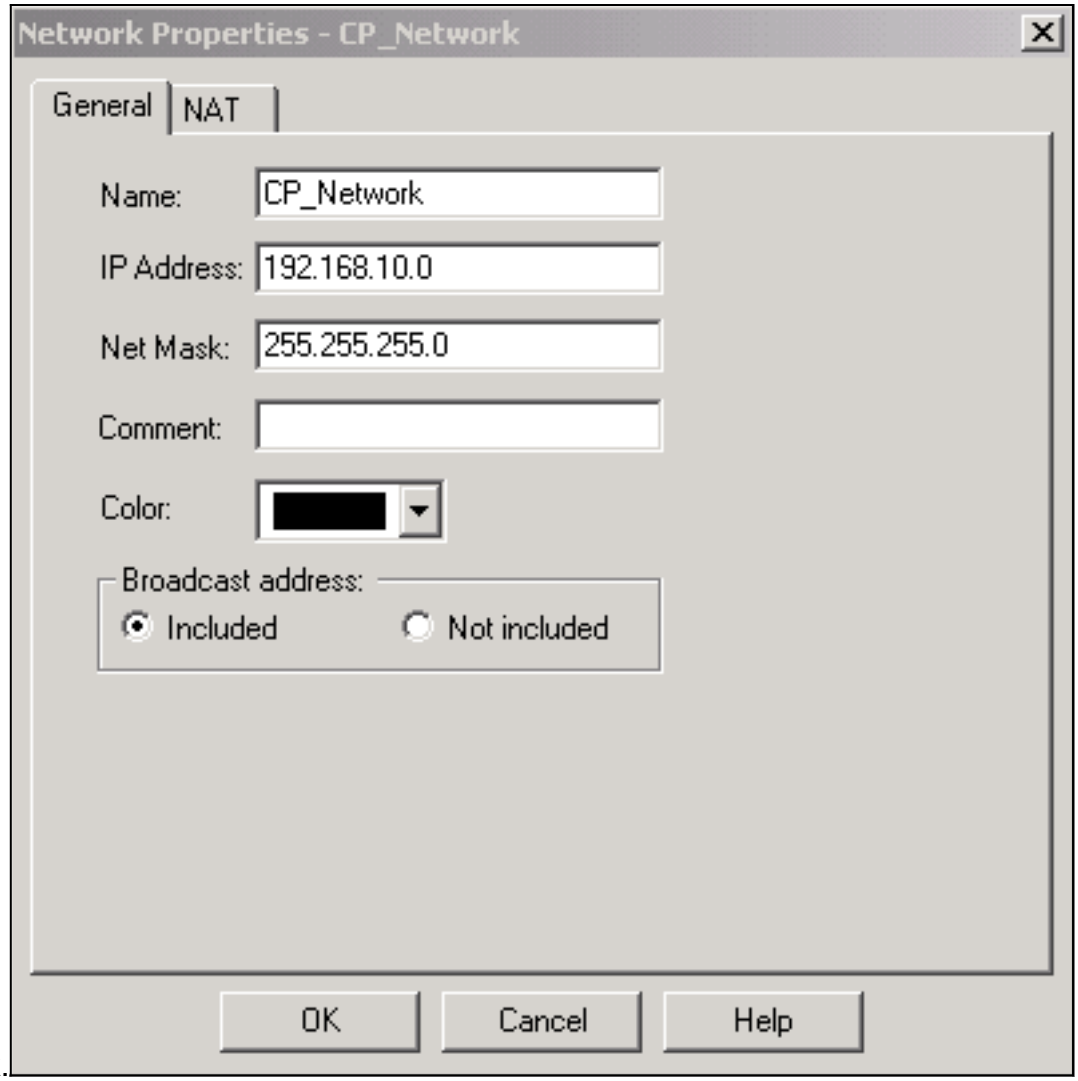
```
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
hostname sv1-6
memory-size iomem 15
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip subnet-zero
no ip domain-lookup
ip audit notify log
ip audit po max-events 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
```

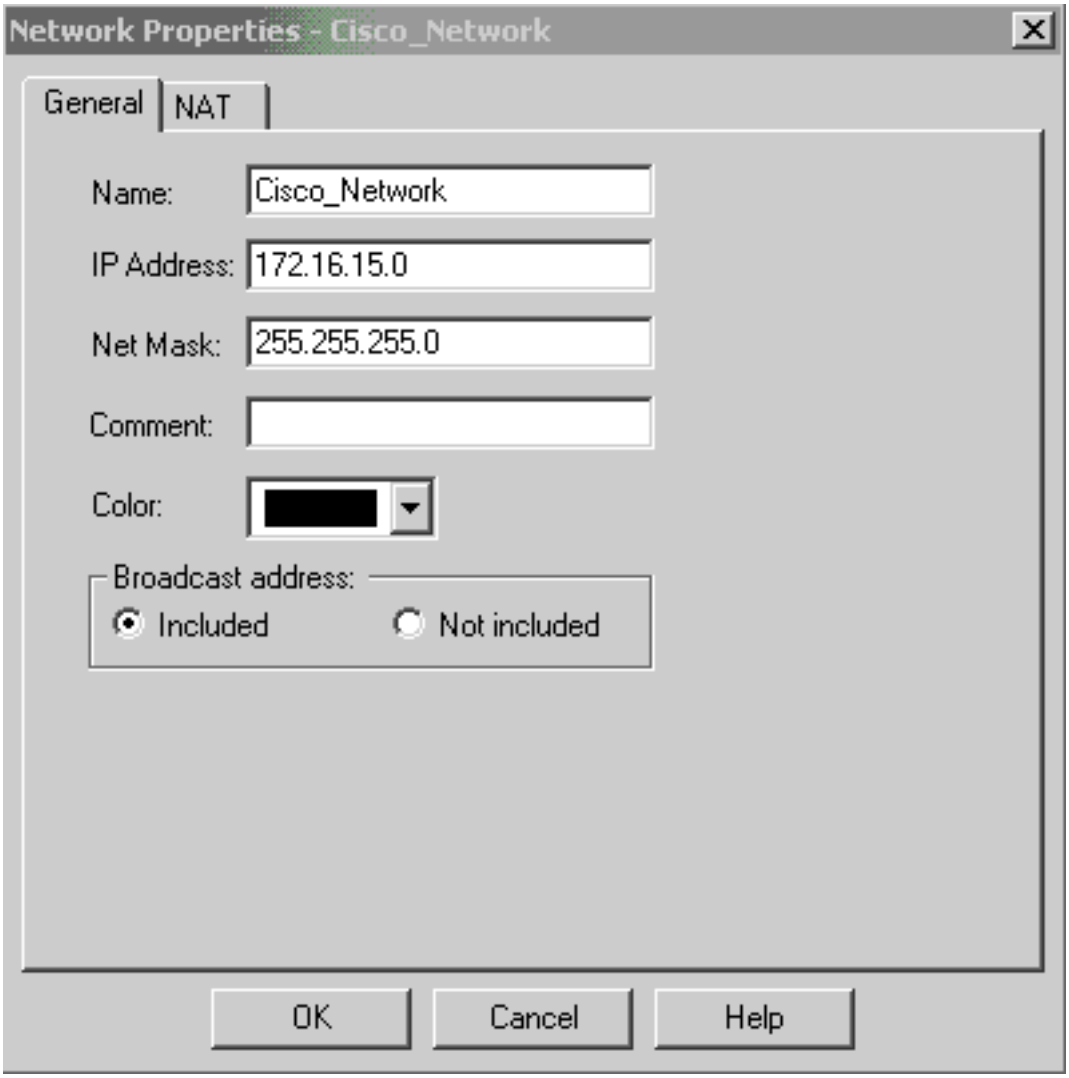
Configurar o NG ponto de verificação

O ponto de verificação™ NG é uma configuração orientada ao objeto. Os objetos de rede e as regras são definidos para compor a política que se refere a configuração de VPN a se estabelecer. Esta política é instalada então usando o editor de política do ponto de verificação™ NG para terminar o lado do ponto de verificação™ NG da configuração de VPN.

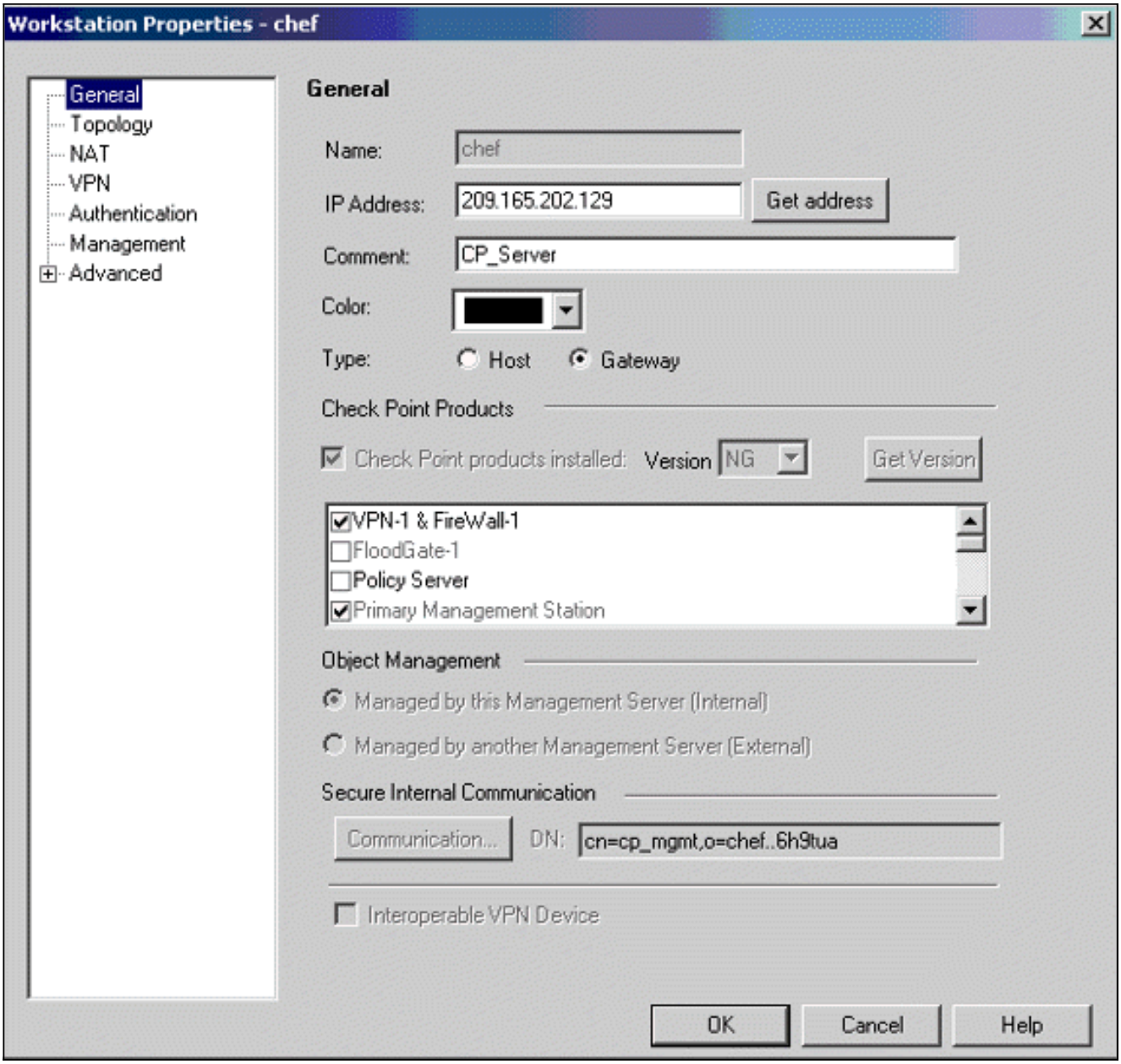
1. Crie a sub-rede da rede Cisco e a sub-rede da rede NG do ponto de verificação™ como objetos de rede. Este é o que é cifrado. Para criar os objetos, selecione **Manage > Network Objects**, a seguir selecione **New > Network**. Incorpore a informação de rede apropriada, a seguir clique a **APROVAÇÃO**.Estes exemplos mostram estabelecido dos objetos chamados CP_Network e

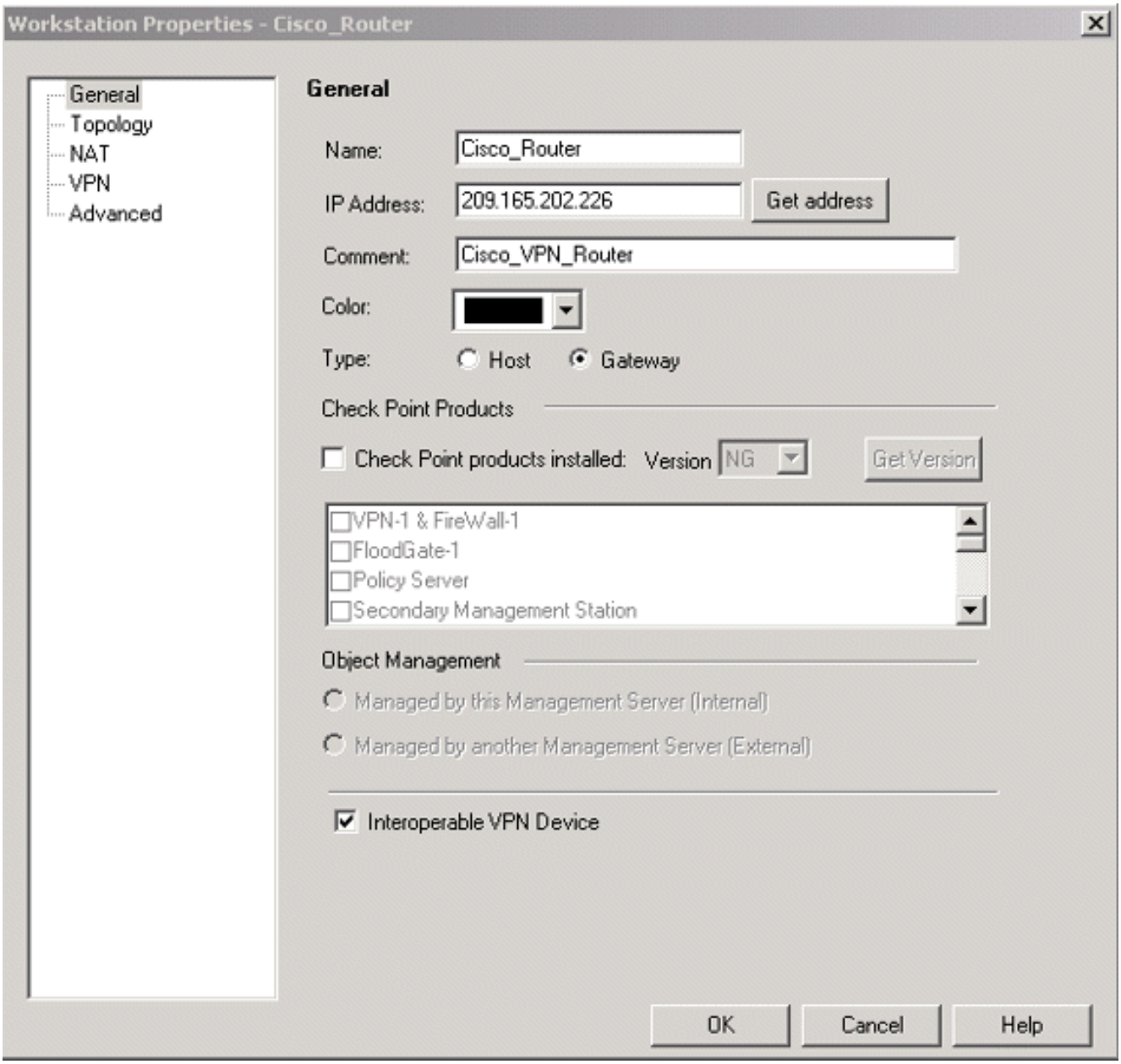


Cisco_Network.

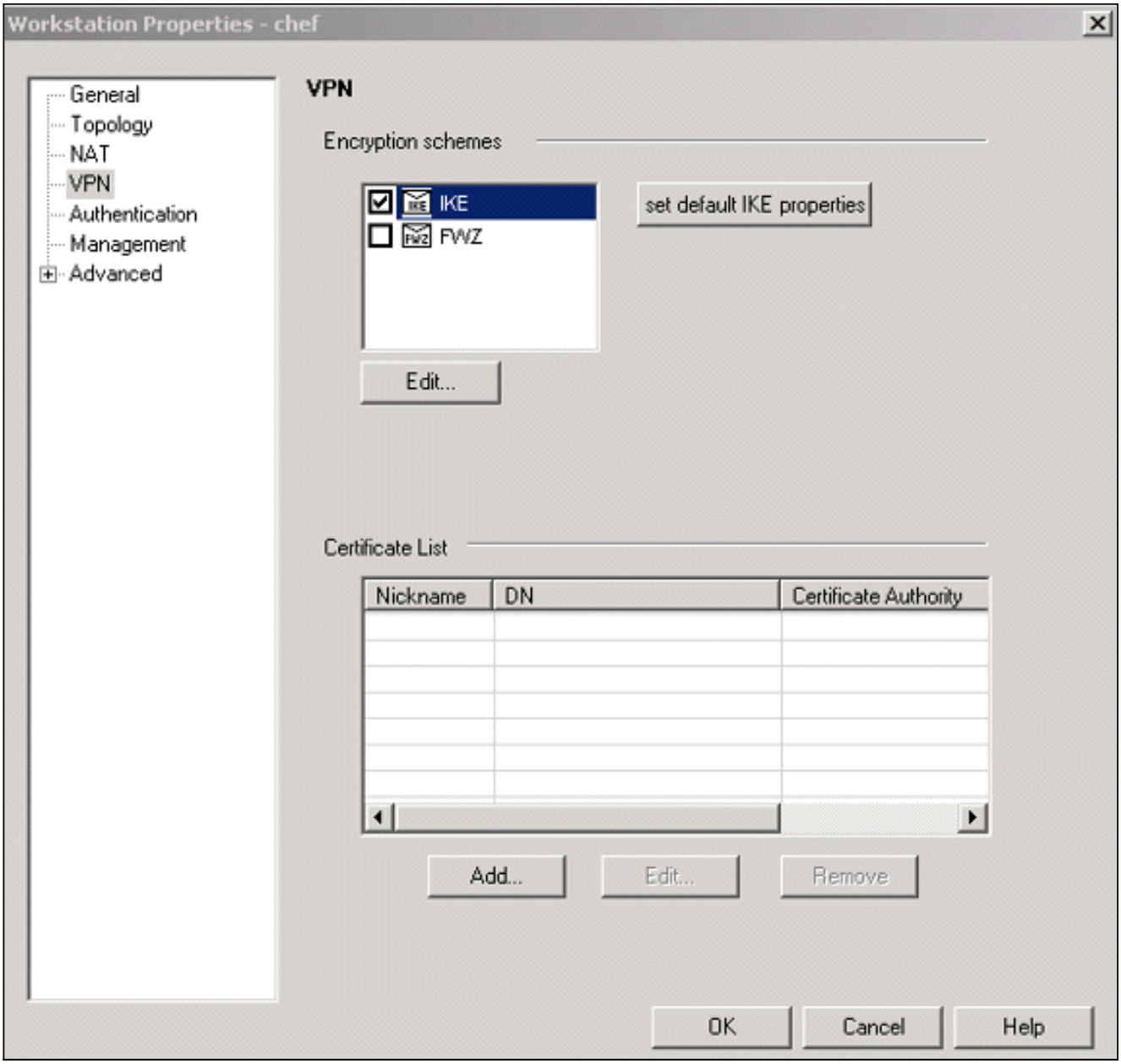


2. Crie os objetos de Cisco_Router e de Checkpoint_NG como objetos da estação de trabalho. Estes são os dispositivos VPN. Para criar os objetos, selecione **Manage > Network Objects**, a seguir selecione **New > Workstation**.Note que você pode usar o objeto da estação de trabalho do ponto de verificação™ NG criado durante a instalação do ponto de verificação inicial™ NG. Selecione as opções para ajustar a estação de trabalho como o **gateway** e o **dispositivo interoperáveis VPN**.Estes exemplos mostram estabelecido dos objetos chamados cozinheiro chefe e
Cisco_Router.

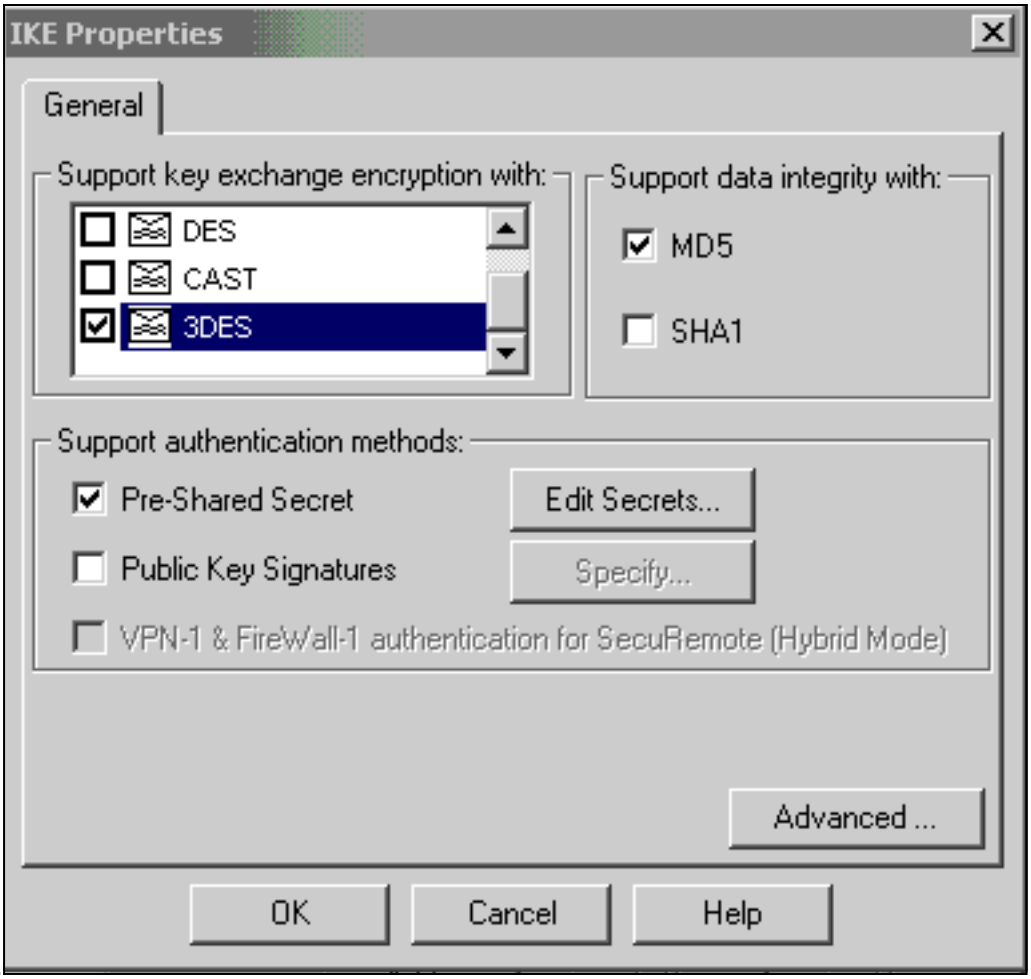

Workstation Properties - chef
General
Topology
NAT
VPN
Authentication
Management
Advanced
General
Name:
chef
IP Address:
209.165.202.129
Get address
Comment:
CP_Server
Color:
Type:
Host
Gateway
Check Point Products
Check Point products installed:
Version
NG
Get Version
VPN-1 & FireWall-1
FloodGate-1
Policy Server
Primary Management Station
Object Management
Managed by this Management Server (Internal)
Managed by another Management Server (External)
Secure Internal Communication
Communication...
DN:
cn=cp_mgmt,o=chef..6h9tua
Interoperable VPN Device
OK
Cancel
Help



3. Configurar o IKE na aba VPN, a seguir clique-o **editam**.

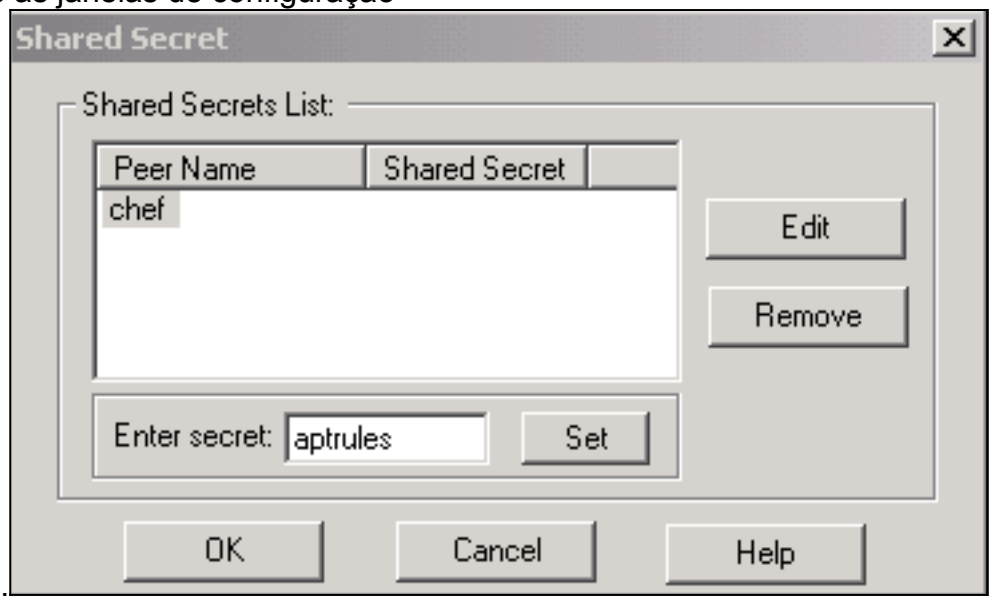


4. Configurar a política de trocas de chave, e o clique **edita**



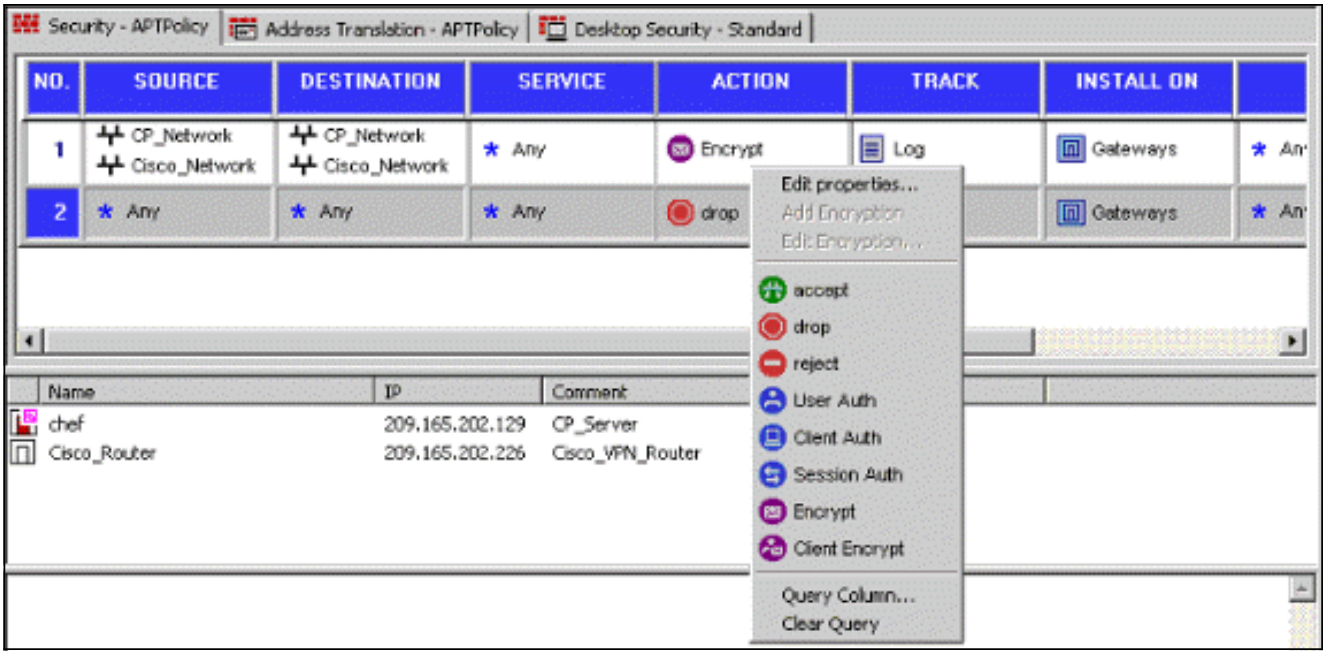
segredos.

5. Ajuste as chaves pré-compartilhada a ser usadas, a seguir clique a **APROVAÇÃO** diversas vezes até que as janelas de configuração

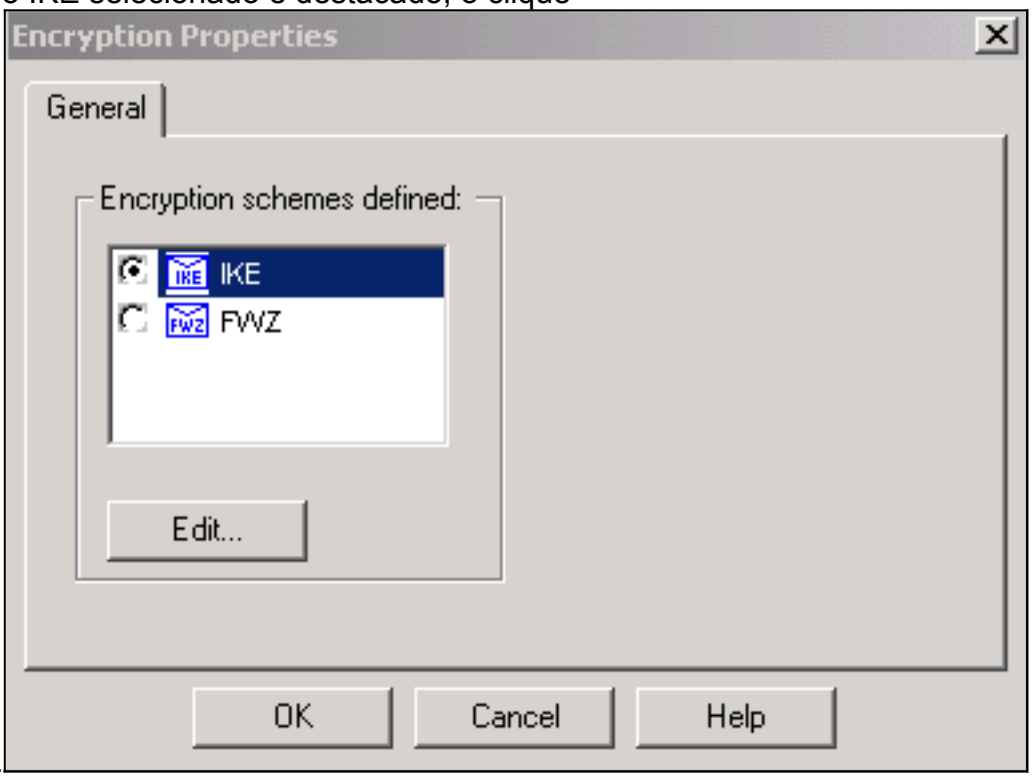


desapareçam.

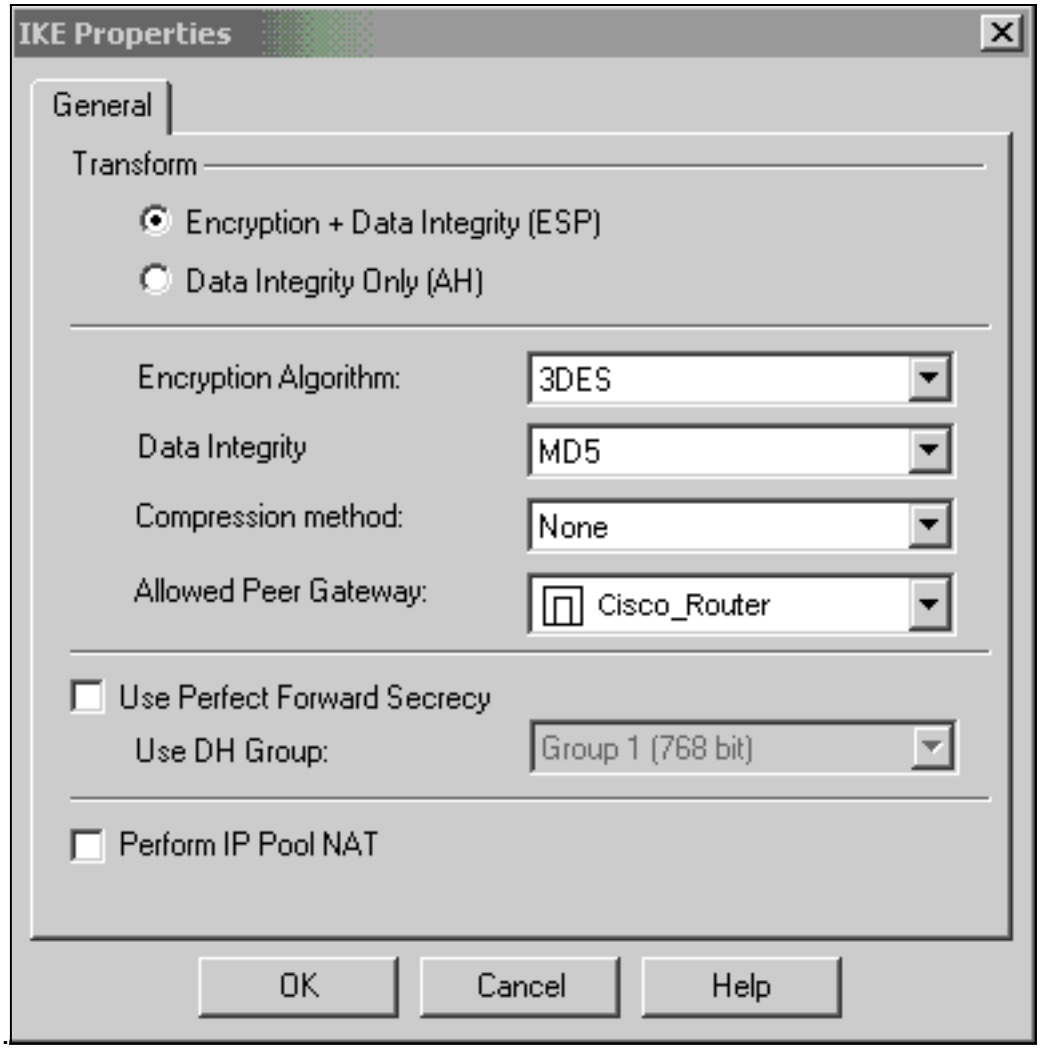
6. Selecione o **Regras > Adicionar Regras > Parte Superior** para configurar as regras de criptografia para a política.A regra na parte superior está a primeira regra executada antes que toda a outra regra que puder contornear a criptografia. Configurar a fonte e o destino para incluir o CP_Network e o Cisco_Network, como mostrado aqui. Uma vez que você adicionou a seção da ação da criptografia da regra, clicar com o botão direito a **ação** e selecione-a **Edit Properties**.



7. Com o IKE selecionado e destacado, o clique **edita**.

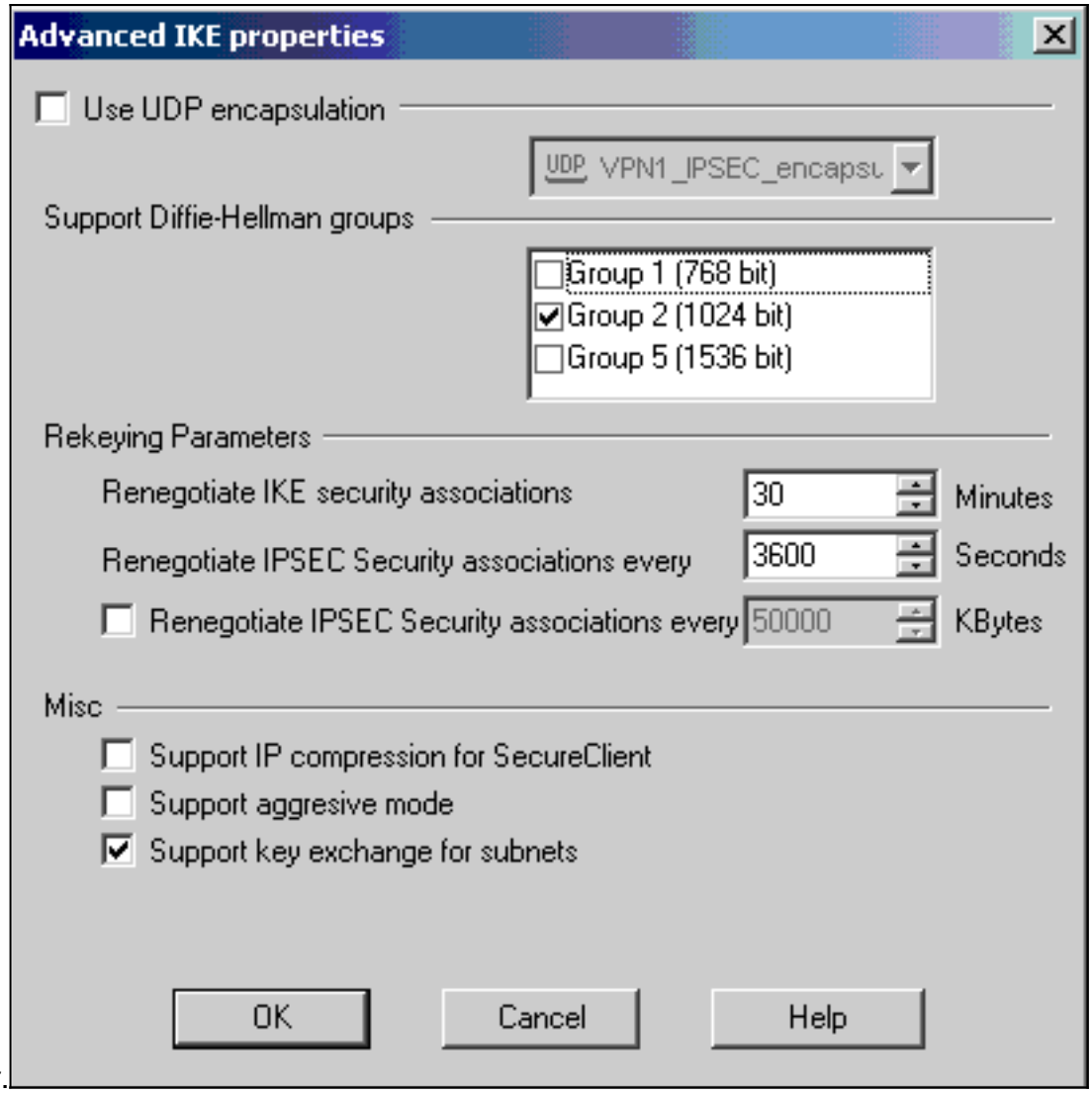


8. Confirme a configuração de



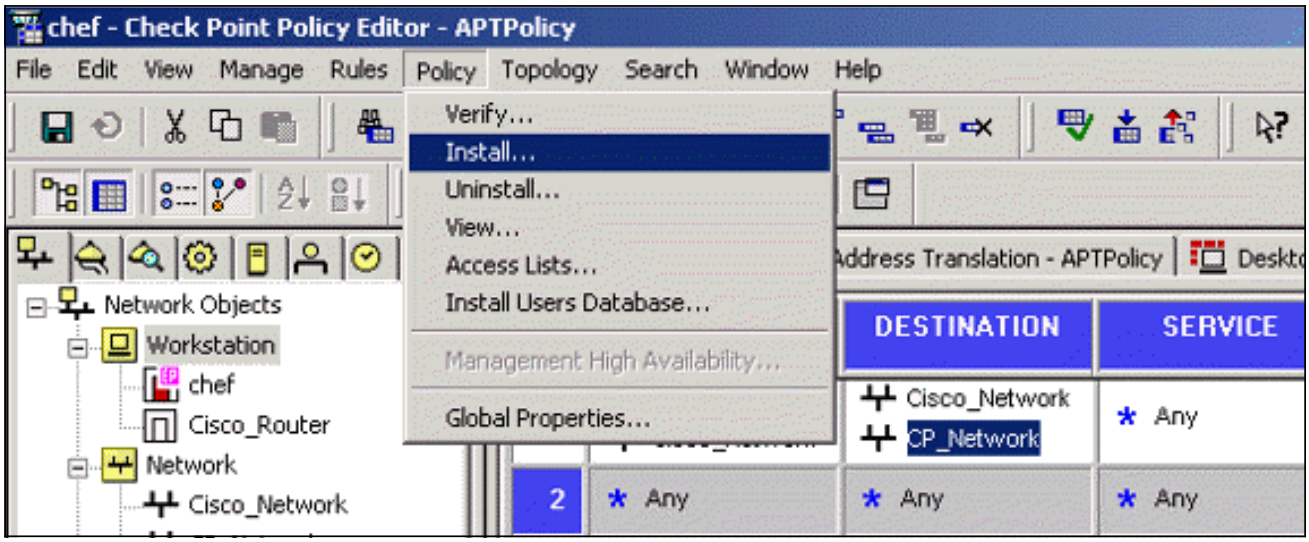
IKE.

9. Uma das questões principal com executar o VPN entre dispositivos Cisco e outros dispositivos IPSec é a negociação nova das trocas de chave. Assegure-se de que o ajuste para a troca IKE no roteador Cisco seja exatamente o mesmo que aquele configurado no ponto de verificação™ NG.**Nota:** O valor real deste parâmetro é dependente de sua política de segurança corporativa particular.Neste exemplo, a configuração de IKE no roteador foi ajustada a 30 minutos com o **comando lifetime 1800**. O mesmo valor tem que ser ajustado no ponto de verificação™ NG.Para ajustar este valor no ponto de verificação™ NG, seleto **controle o objeto de rede**, a seguir selecione o objeto do ponto de verificação™ NG e o clique **edita**. Selecione então o **VPN**, e edite o IKE. Selecione o **avanço** e configurar os Parâmetros de novo encaixe. Depois que você configura as trocas de chave para o objeto de rede NG do ponto de verificação™, execute a mesma configuração da negociação nova das trocas de chave para o objeto de rede de Cisco_Router.**Nota:** Assegure-se de que você tenha o grupo Diffie-Hellman correto selecionado combinar isso configurado no

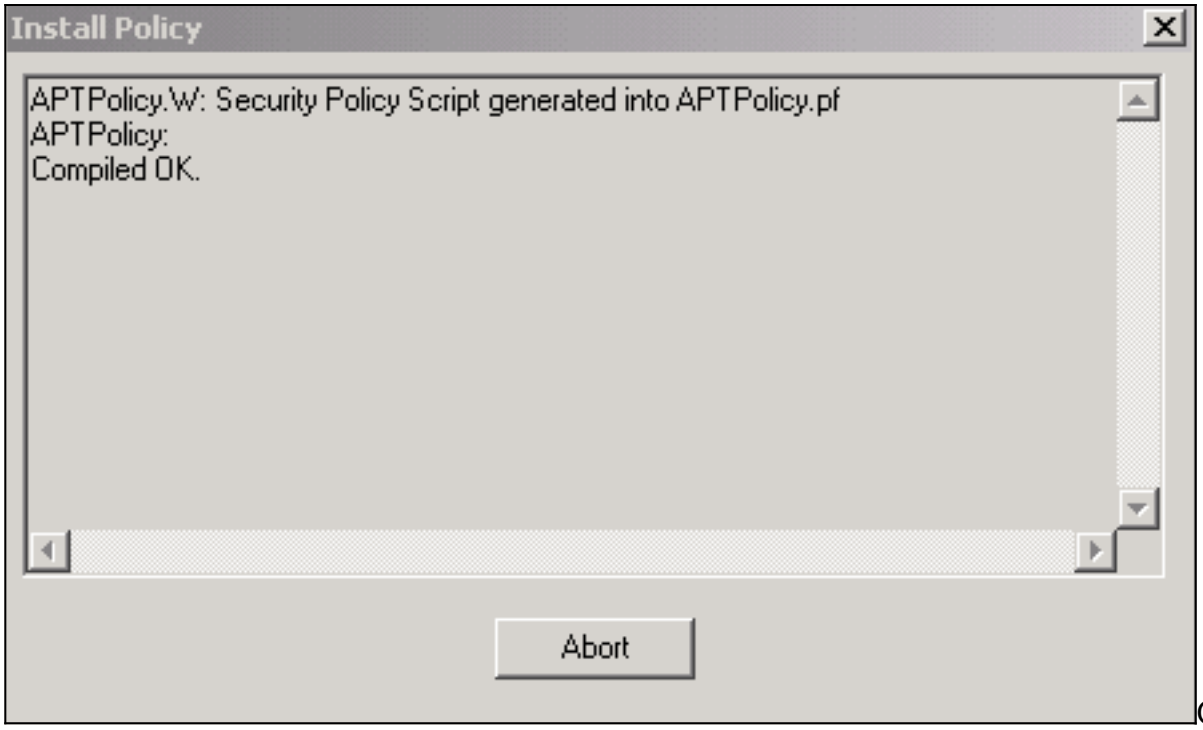


roteador.

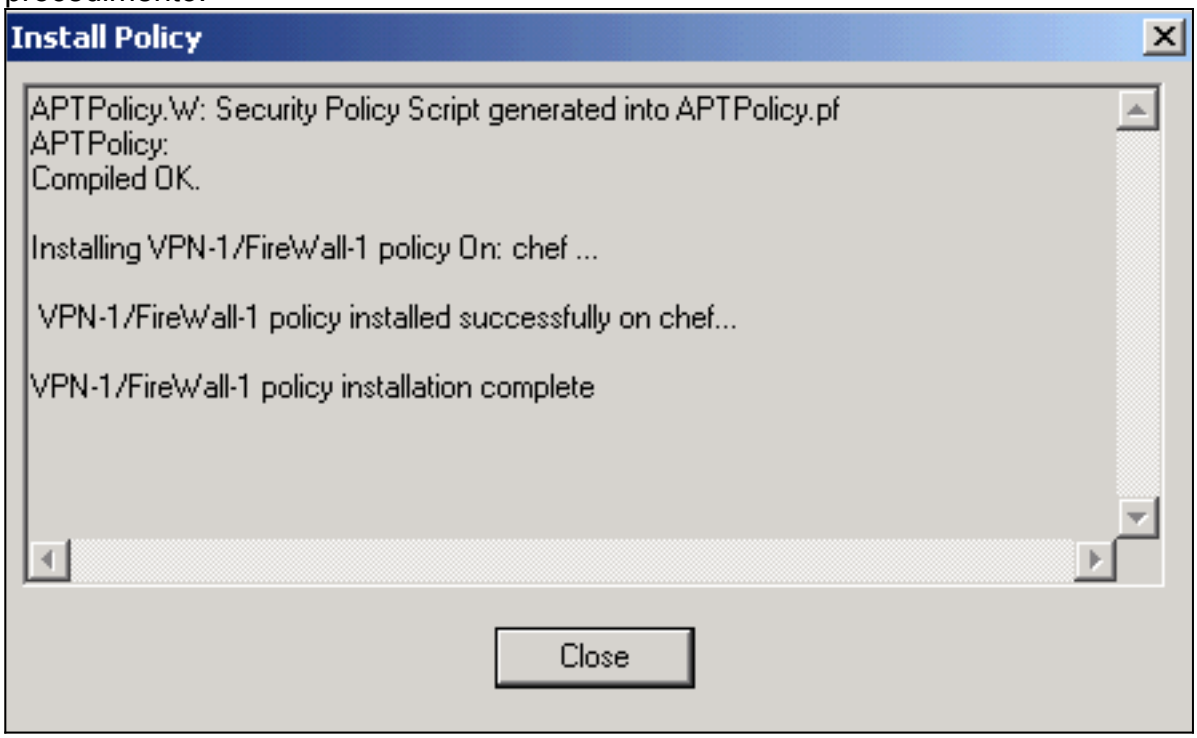
10. A configuração das normas está completa. Salvar a política e a **política** seleta **> instala** para permiti-
la.



A janela de instalação indica notas de andamento enquanto a política é compilada.



Quando a janela de instalação indica que a instalação de política está completa, clique **perto do** revestimento o procedimento.



Verificar

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

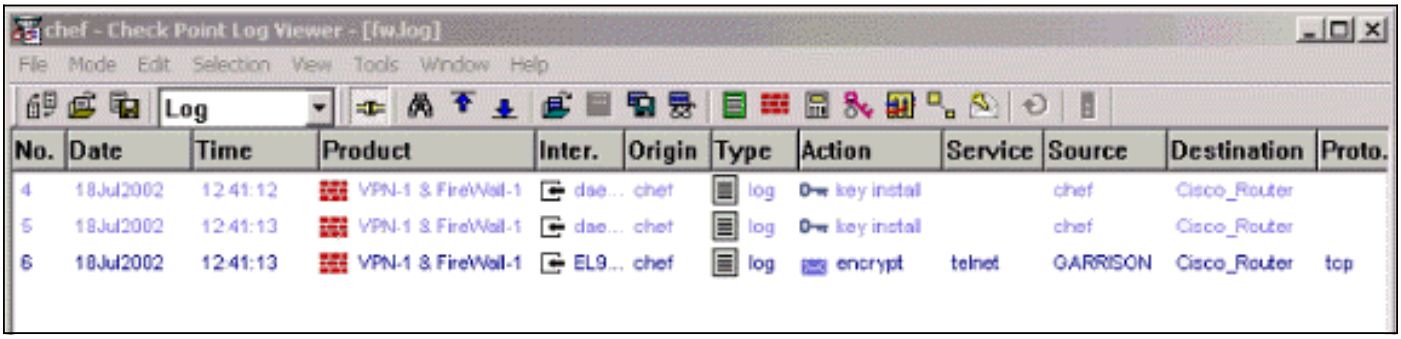
Verifique o roteador Cisco

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

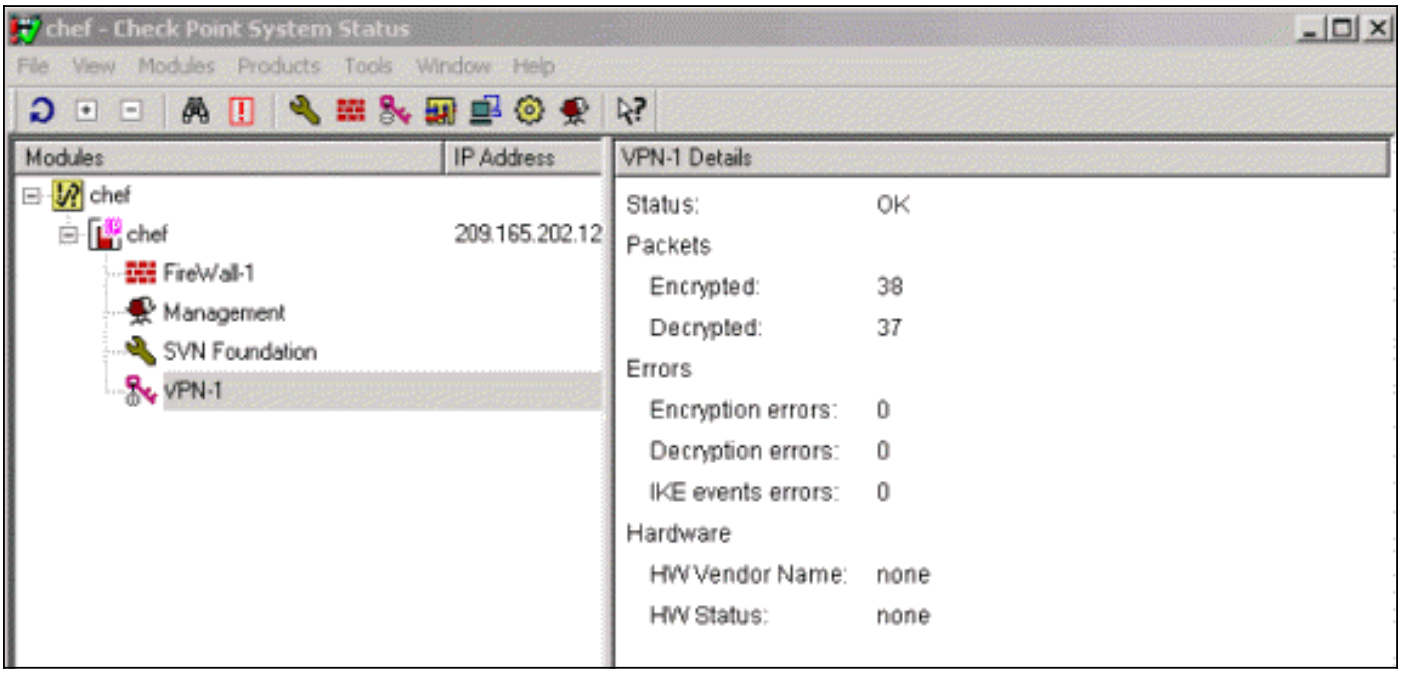
- **show crypto isakmp sa** — Exibe todas as associações de segurança atuais (SAs) de IKE em um peer.
- **mostre IPsec cripto sa** — Indica os ajustes usados por SA atuais.

Verifique o NG ponto de verificação

Para ver os logs, selecione o **Janela > visor de Log**.



Para ver o status de sistema, selecione o **Janela > Status de Sistema**.



Troubleshooting

Cisco Router

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

Para a informação adicional de Troubleshooting, refira por favor o Troubleshooting de Segurança IP - compreendendo e usando comandos debug.

Nota: Antes de emitir comandos de depuração, consulte as informações importantes sobre eles.

- **motor do debug crypto** — Os indicadores debugam mensagens sobre as crypto-engines, que

executam a criptografia e a descriptografia.

- debug crypto isakmp - Exibe mensagens sobre eventos IKE.
- **debug crypto ipsec** — Exibe eventos de IPSec.
- **cancele o isakmp cripto** — Cancela todas as conexões do IKE ativo.
- **cancele o sa cripto** — Cancela todo o sas de IPSec.

Bem sucedido debugar o registro de saída

```
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_MESG_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_MESG_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_MESG_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_MESG_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_MESG_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_MESG_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 sv1-6#**show crypto isakmp sa** dst src state conn-id slot 209.165.202.226 209.165.202.129 QM_IDLE 1 0 sv1-6#**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: sv1-6#**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