Configuração de um Túnel IPSec - Cisco VPN 5000 Concentrator to Checkpoint 4.1 Firewall

Contents

Introduction

Esse documento demonstra como formar um túnel de IPsec com chaves pré-compartilhadas para unir duas redes privadas. Ele une uma rede privada dentro do Cisco VPN 5000 Concentrator (192.168.1.x) a uma rede privada dentro do Checkpoint 4.1 Firewall (10.32.50.x). Pressupõe-se que o tráfego de dentro do VPN Concentrator e de dentro do Checkpoint para a Internet (representado neste documento pelas redes 172.18.124.x) flua antes de você iniciar essa configuração.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

- Cisco VPN 5000 Concentrator
- Software Cisco VPN 5000 Concentrator versão 5.2.19.0001
- Checkpoint 4.1 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.

Conventions

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

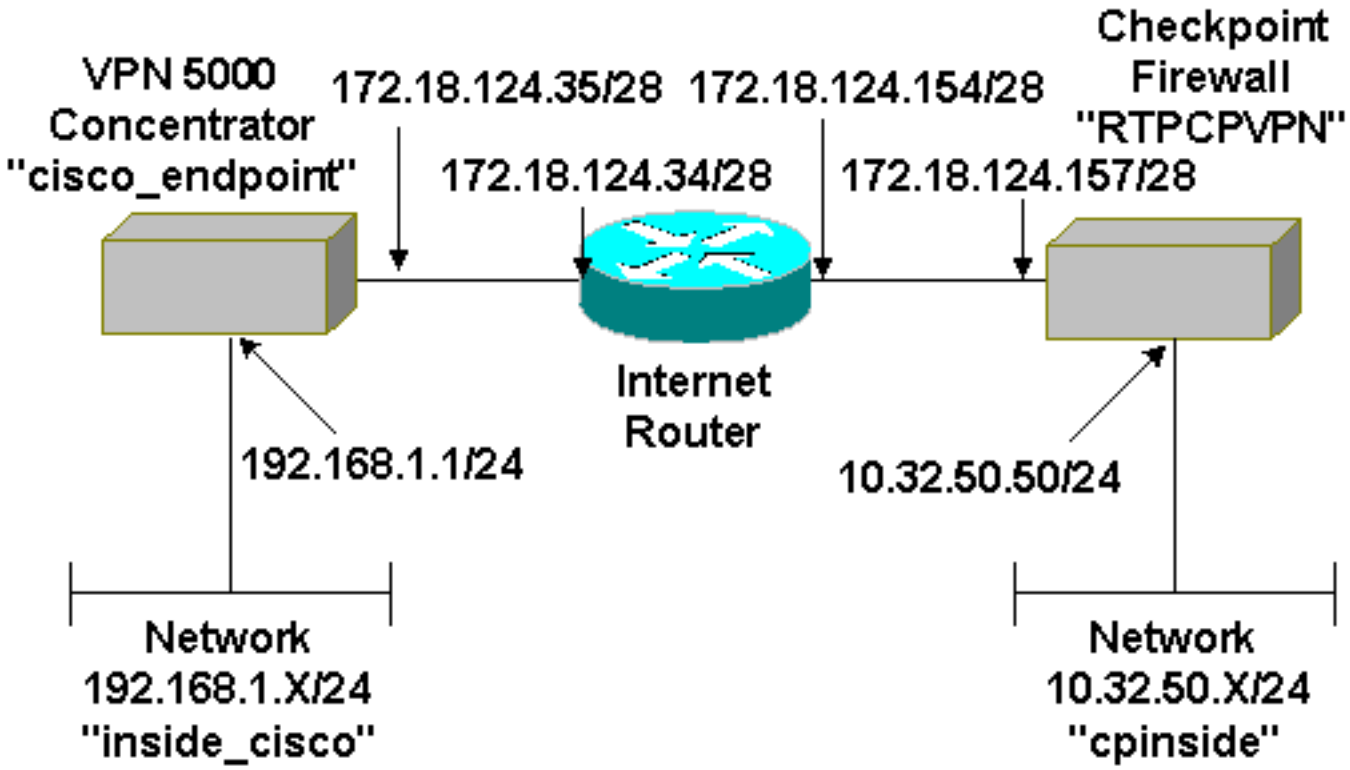
Configurar

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

Nota:Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados neste documento.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



Configurações

Este documento utiliza esta configuração.

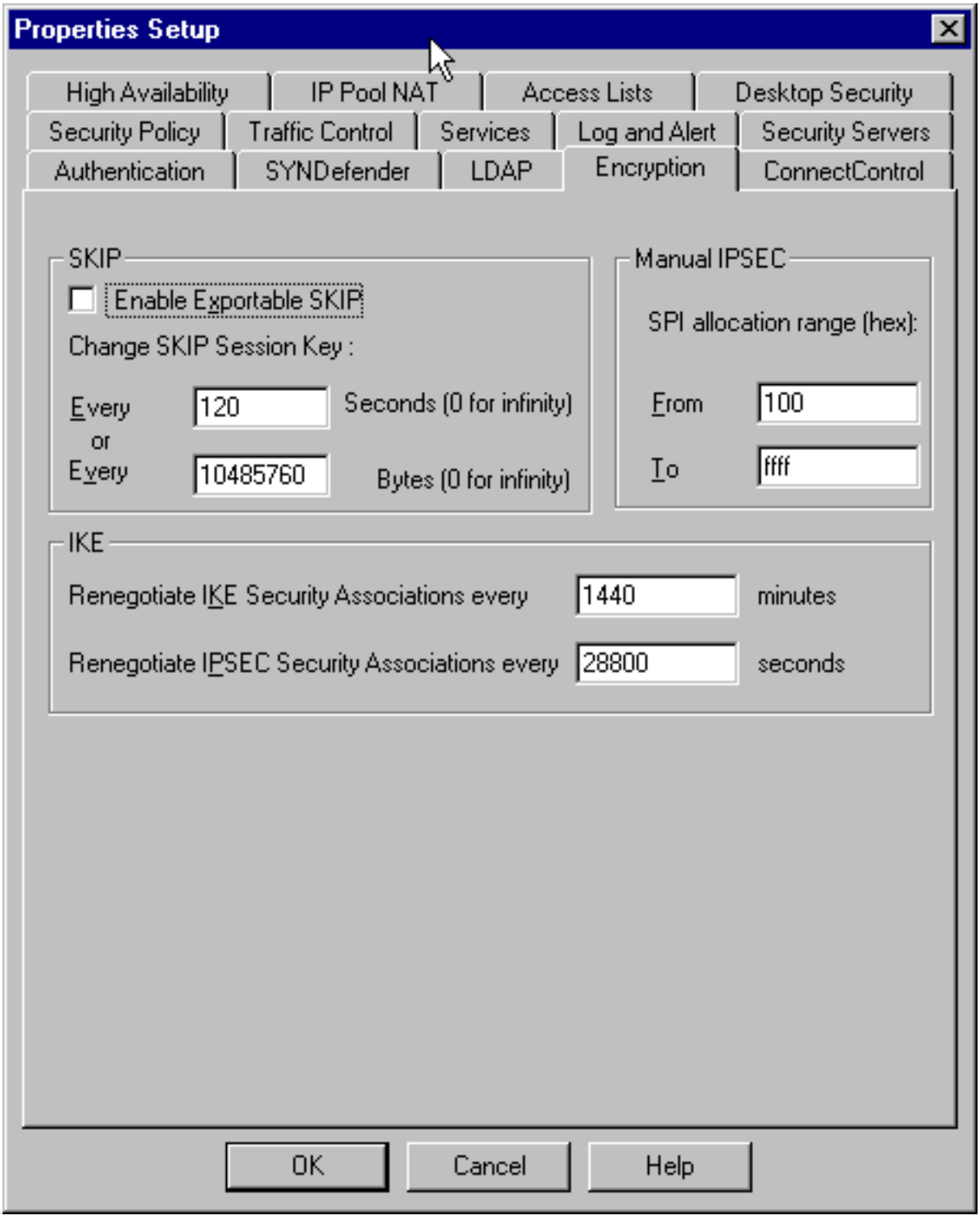
Cisco VPN 5000 Concentrator

```
[ IP Ethernet 0:0 ]
Mode                    = Routed
SubnetMask              = 255.255.255.0
IPAddress               = 192.168.1.1

[ General ]
EthernetAddress         = 00:00:a5:e9:c8:00
DeviceType              = VPN 5002/8 Concentrator
ConfiguredOn            = Timeserver not configured
ConfiguredFrom          = Command Line, from Console
DeviceName              = "cisco_endpoint"
IPSecGateway            = 172.18.124.34

[ IKE Policy ]
Protection              = SHA_DES_G2

[ Tunnel Partner VPN 1 ]
KeyLifeSecs             = 28800
LocalAccess             = "192.168.1.0/24"
Peer                    = "10.32.50.0/24"
BindTo                  = "ethernet 1:0"
SharedKey               = "ciscorules"
KeyManage               = Auto
Transform               = esp(sha,des)
Partner                 = 172.18.124.157
Mode                    = Main

[ IP VPN 1 ]
Numbered                = Off
Mode                    = Routed

[ IP Ethernet 1:0 ]
IPAddress               = 172.18.124.35
SubnetMask              = 255.255.255.240
Mode                    = Routed

[ IP Static ]
10.32.50.0 255.255.255.0 VPN 1 1

Configuration size is 1131 out of 65500 bytes.
```

Checkpoint 4.1 Firewall

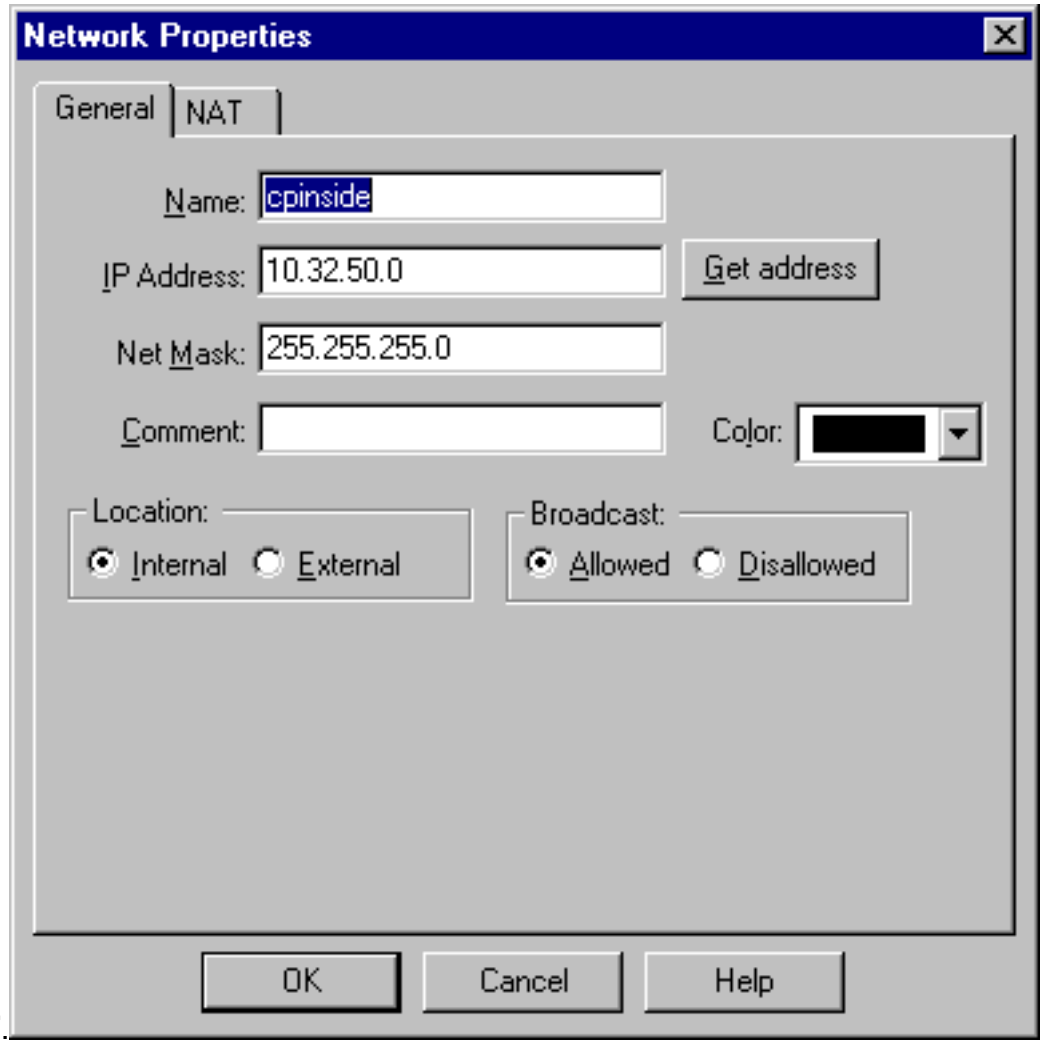
Conclua estes passos para configurar o Firewall do Ponto de Verificação 4.1.

1. Selecione **Propriedades > Criptografia** para definir as vidas do ponto de verificação IPsec para concordar com o comando **KeyLifeSecs = 28800** VPN Concentrator.**Observação:** deixe a vida útil do IKE (Internet Key Exchange) do ponto de controle no



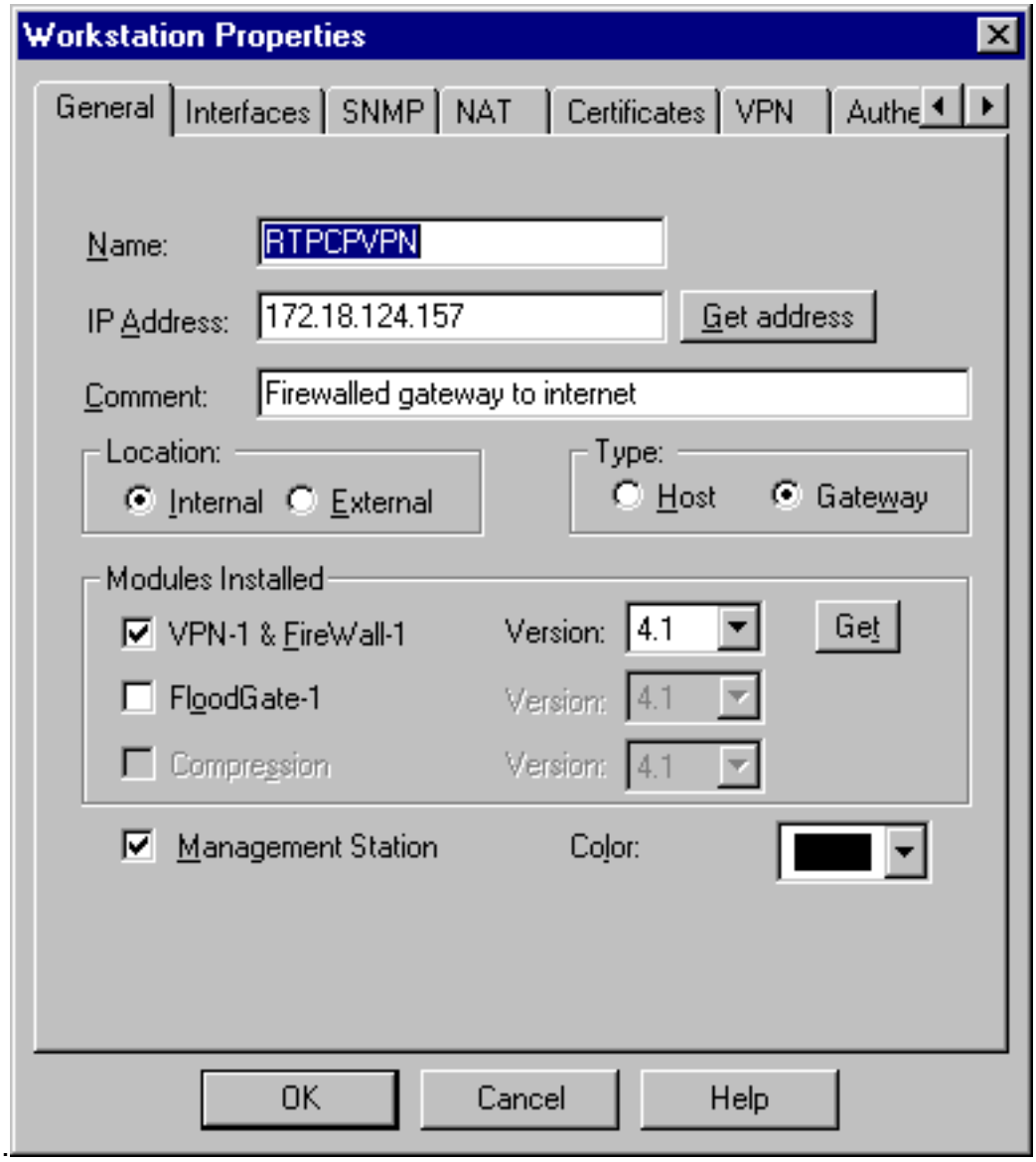
padrão.

2. Selecione Gerenciar > Objetos de rede > Novo (ou Editar) > Rede para configurar o objeto para a rede interna ("cpinside") por trás do ponto de controle. Isso deve concordar com o comando VPN Concentrator **Peer =**



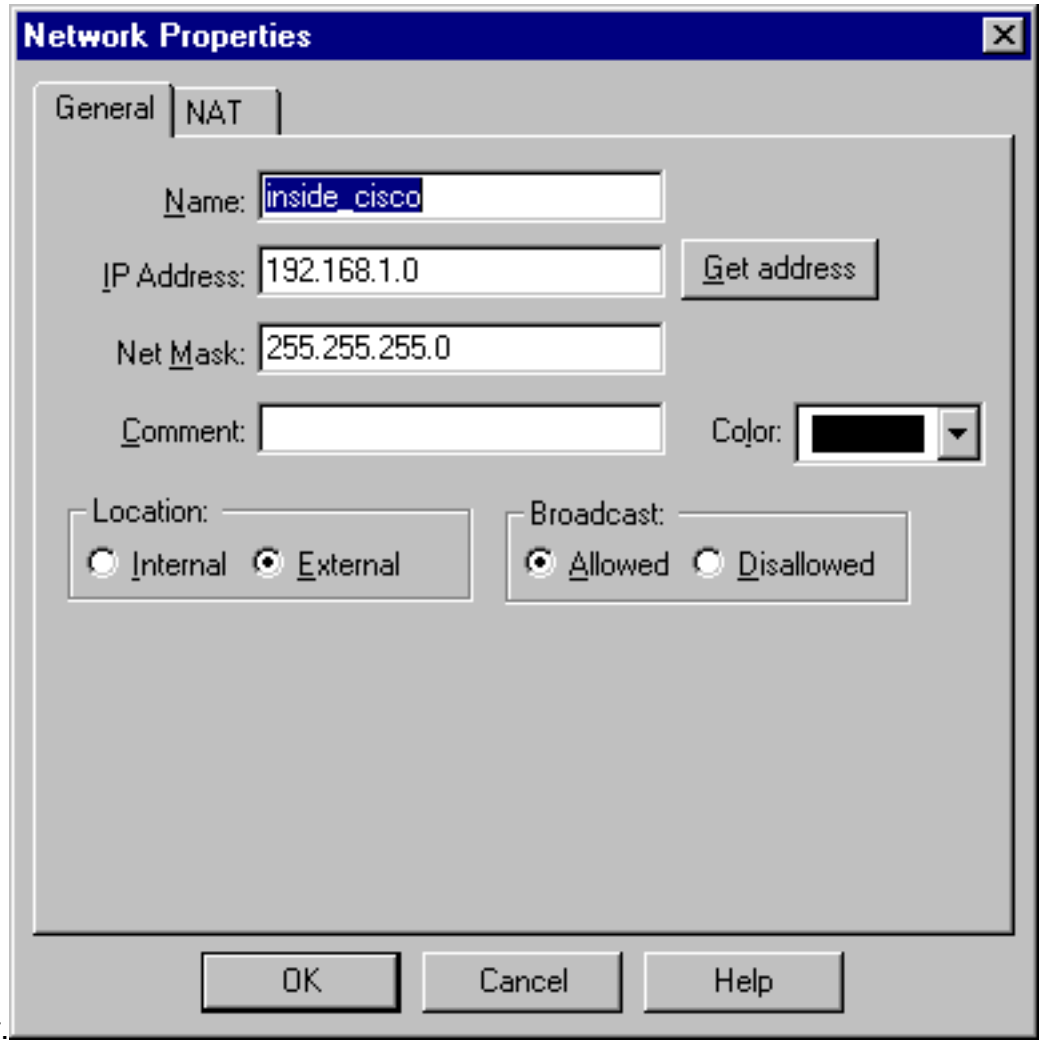
"10.32.50.0/24".

3. Selecione **Gerenciar > Objetos de rede > Editar** para editar o objeto do ponto de extremidade do gateway ("RTPCPVPN" Checkpoint) para o qual o VPN Concentrator aponta no comando **Partner = <ip>**.Selecione **Interno** em Local.Selecione **Gateway** para Tipo.Verifique **VPN-1 e FireWall-1** e **Management Station** em Modules Installed (Módulos



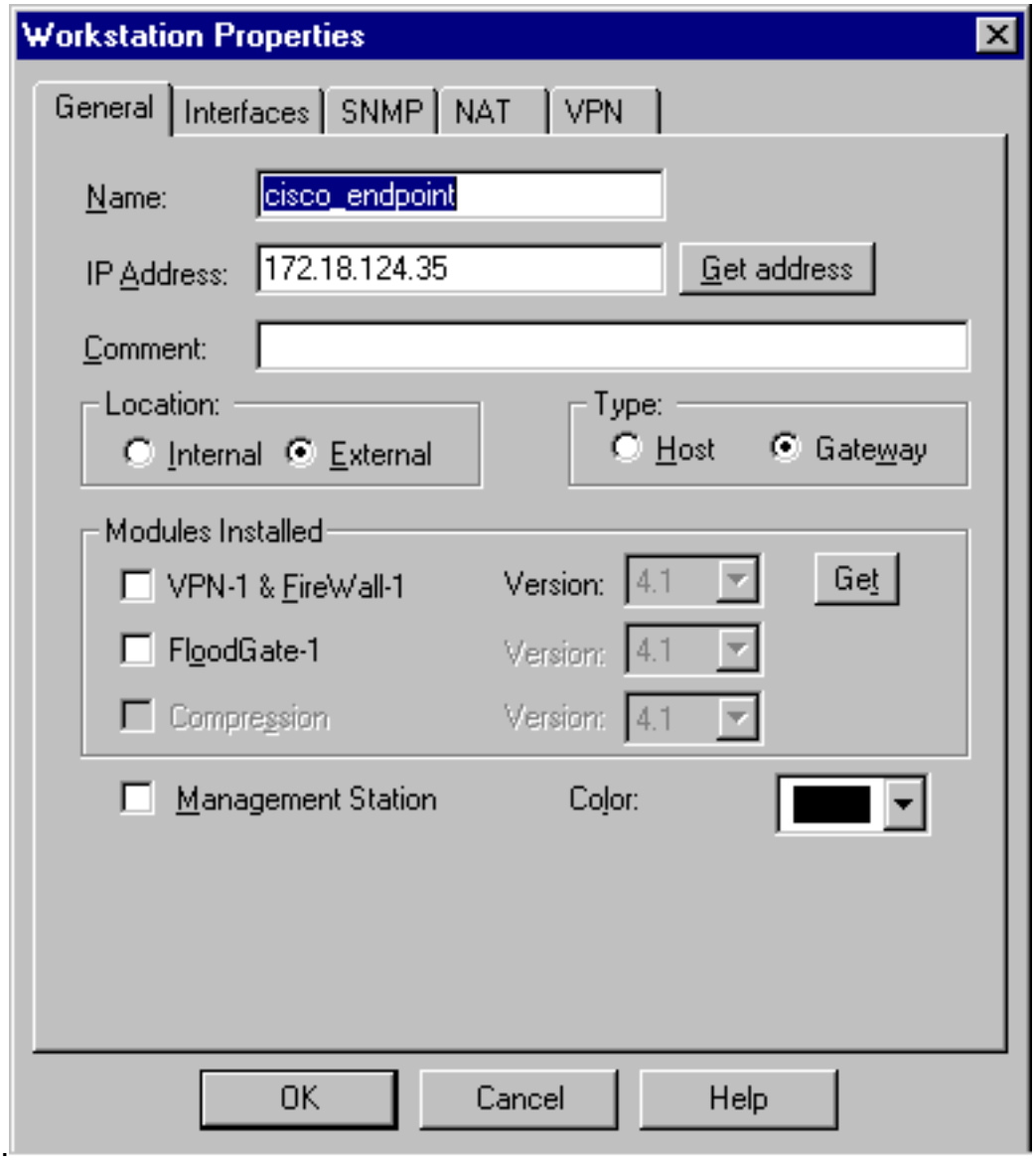
instalados).

4. Selecione **Gerenciar > Objetos de rede > Novo (ou Editar) > Rede** para configurar o objeto para a rede externa ("inside_cisco") atrás do VPN Concentrator.Isso deve concordar com o comando **LocalAccess = <192.168.1.0/24>** VPN

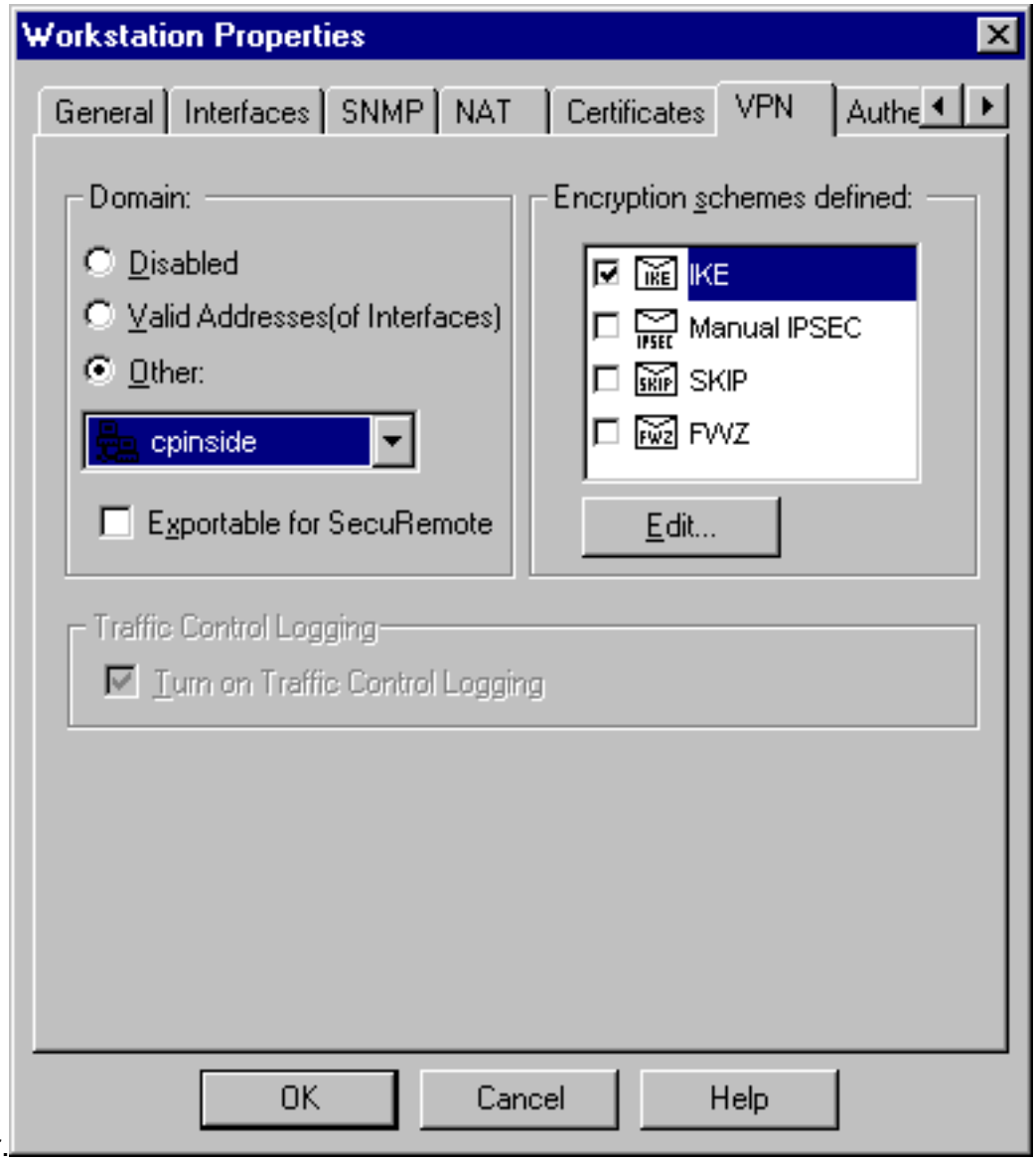


Concentrator.

5. Selecione **Gerenciar > Objetos de rede > Novo > Estação de trabalho** para adicionar um objeto ao gateway do VPN Concentrator externo ("cisco_endpoint").Esta é a interface "externa" do VPN Concentrator com conectividade com o Checkpoint (neste documento, 172.18.124.35 é o endereço IP no comando **IPAaddress = <ip>**).Selecione **Externo** em Local. Selecione **Gateway** para Tipo.**Observação:** não verifique VPN-1/FireWall-

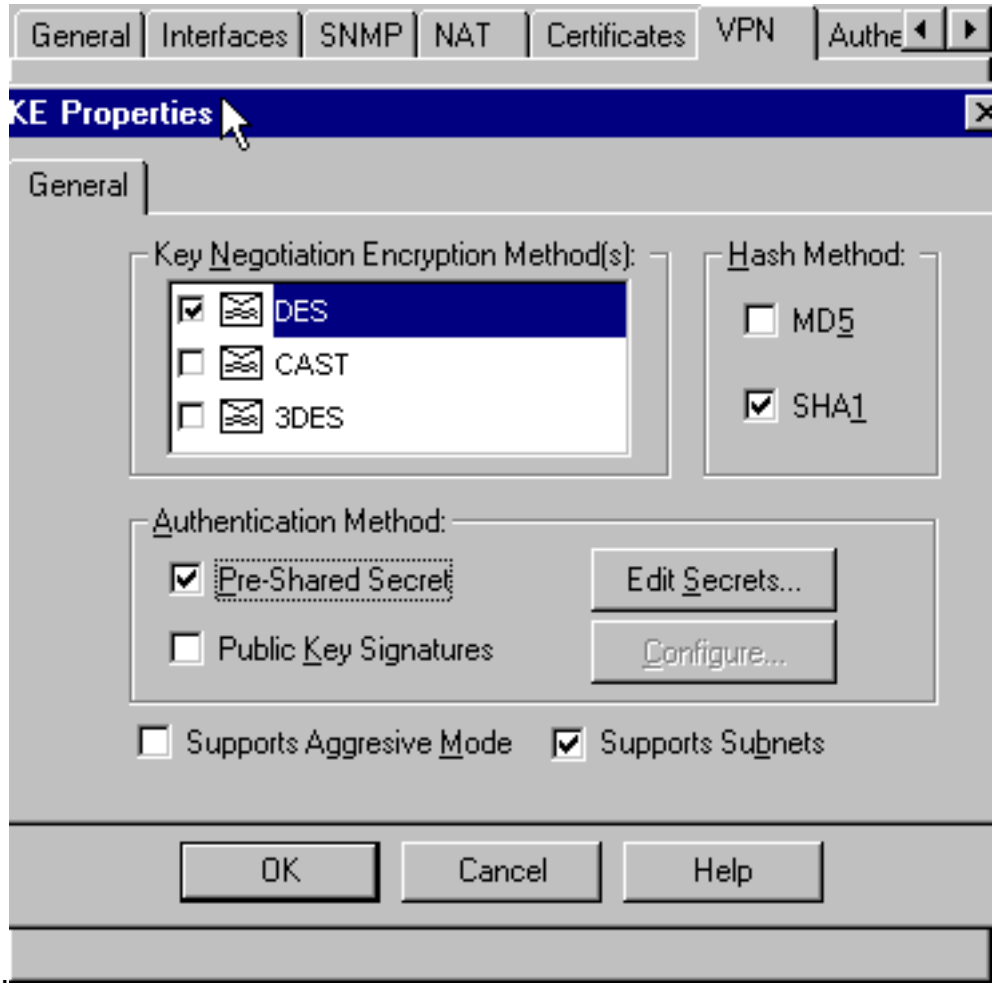
1. 

6. Selecionar Manage > Network objetct > Edit para editar o ponto final do gateway do ponto de controle (chamado "RTPCPVPN") na guia VPN. Em Domain, selecione Other e, em seguida, selecione o lado interno da rede de ponto de controle (chamado “cpinside”) a partir da lista suspensa. Sob esquemas de criptografia definidos, selecione IKE e clique em



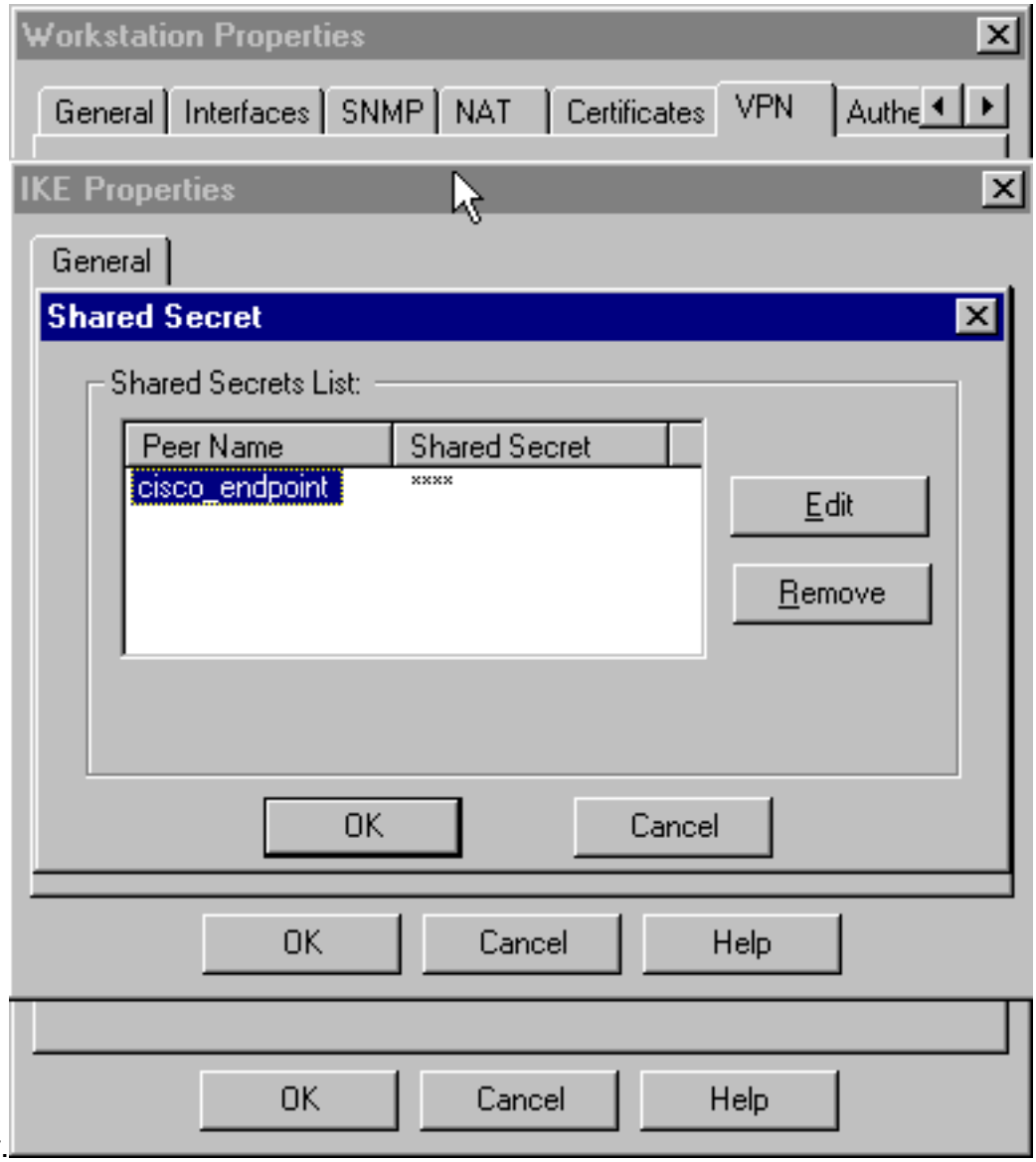
Editar.

7. Altere as propriedades de IKE para a criptografia **DES** e o **hashing SHA1** para concordar com o comando do VPN Concentrator **SHA_DES_G2**.**Nota:** O "G2" refere-se ao grupo Diffie-Hellman 1 ou 2. No teste, descobriu-se que o Checkpoint aceita "G2" ou "G1".Altere estas configurações:Desative o Modo assertivo.Verifique **Suporta Sub-Redes**.Marque **Pre-Shared Secret** em Authentication Method (Método de



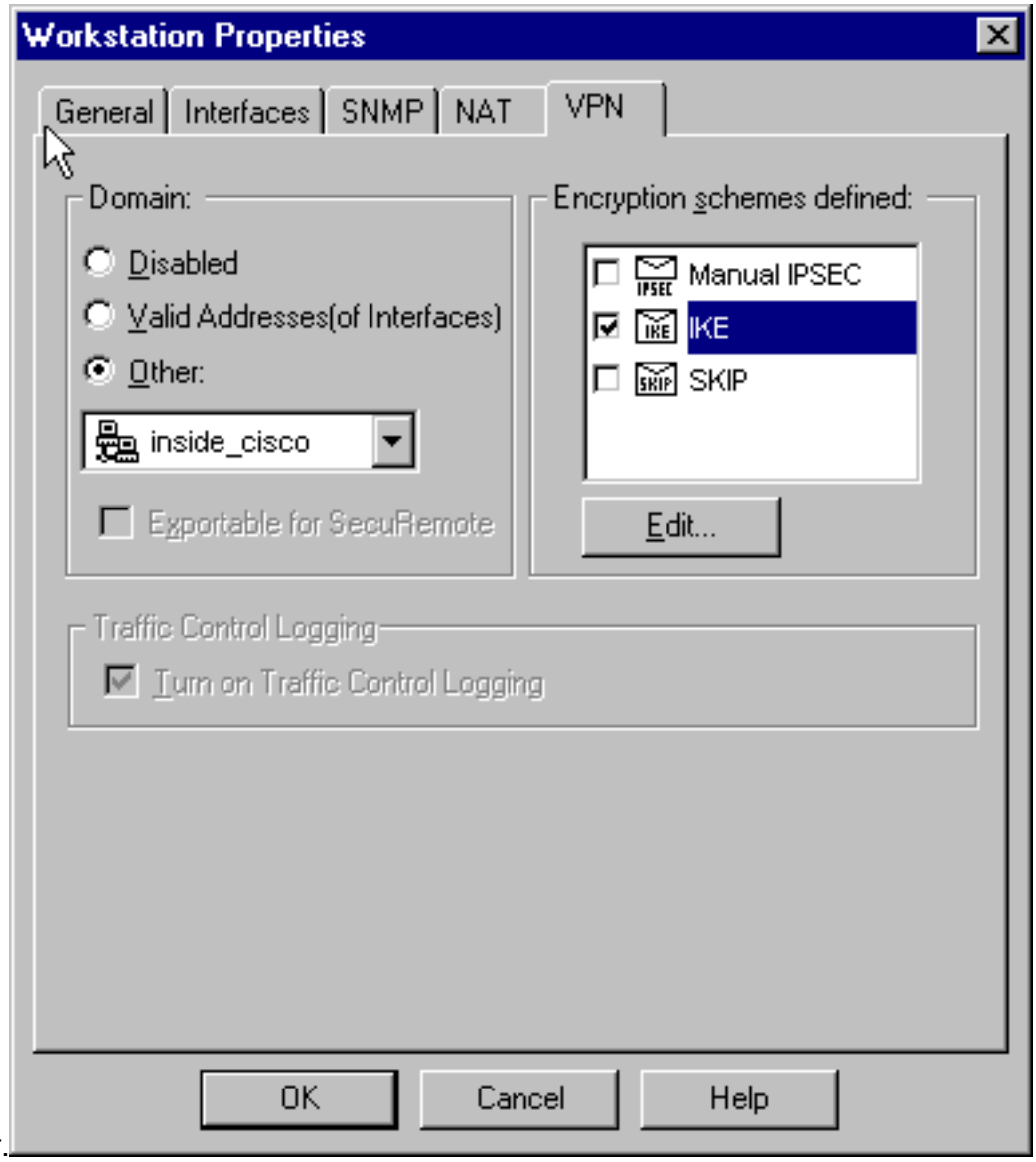
autenticação).

8. Clique em **Editar segredos** para definir a chave pré-compartilhada de acordo com o comando **SharedKey = <key>** VPN



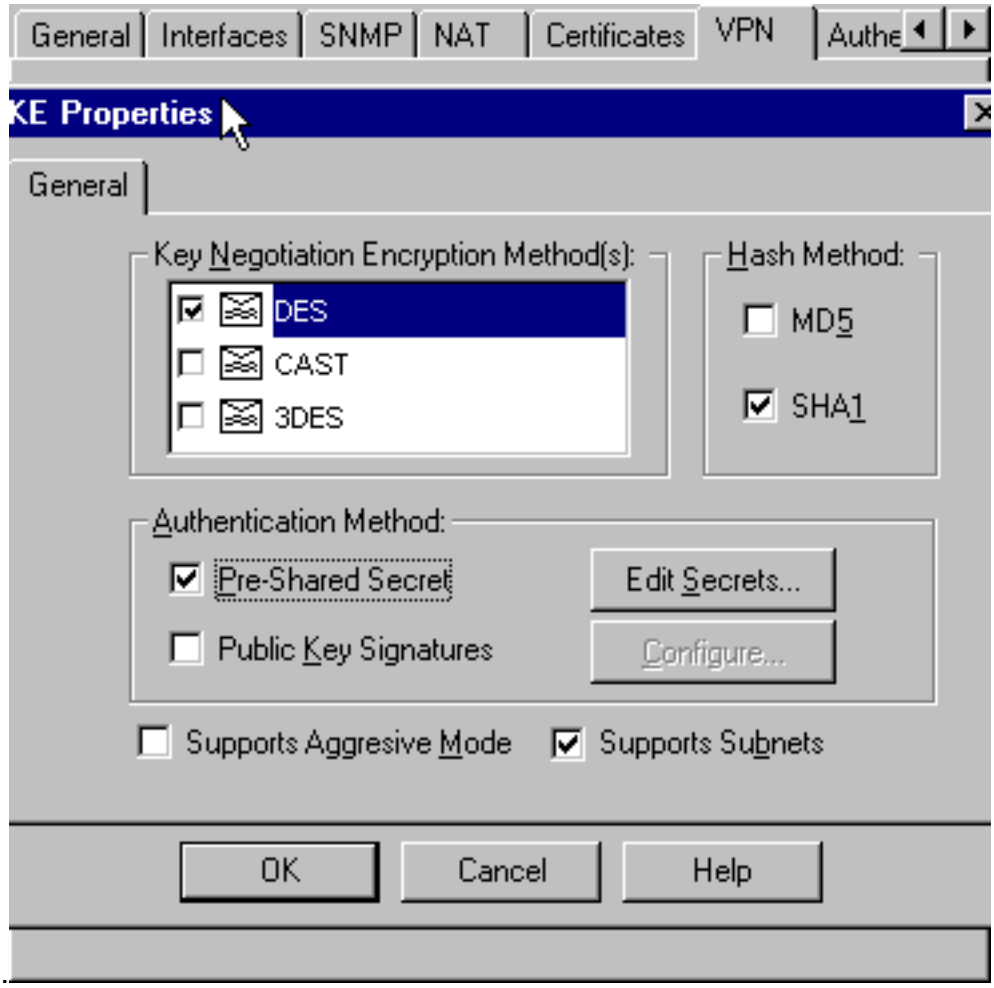
Concentrator.

9. Selecione Gerenciar > Objetos de rede > Editar para editar a guia VPN “cisco_endpoint”. Em Domain, selecione **Other** e selecione o interior da rede VPN Concentrator (chamada "inside_cisco"). Sob esquemas de criptografia definidos, selecione IKE e clique em



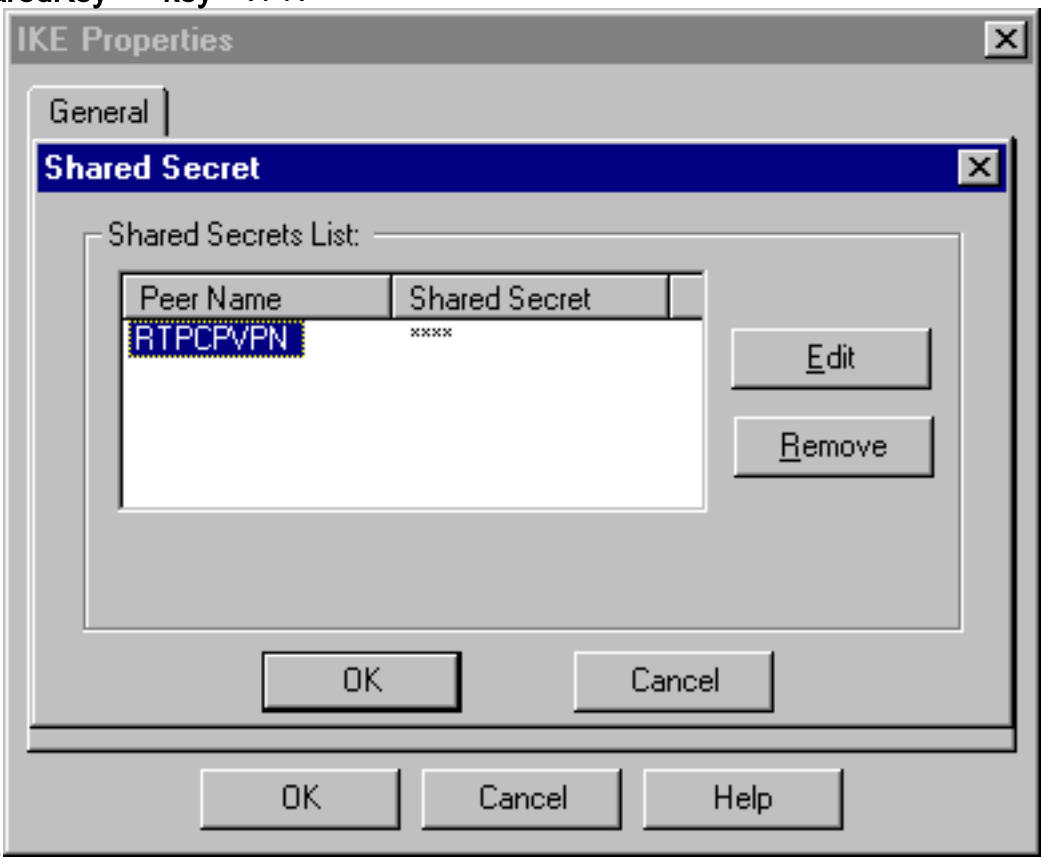
Editar.

10. Altere as propriedades de IKE para a criptografia **DES** e o **hashing SHA1** para concordar com o comando do VPN Concentrator **SHA_DES_G2**.**Nota:** O "G2" refere-se ao grupo Diffie-Hellman 1 ou 2. No teste, descobriu-se que o ponto de verificação aceita "G2" ou "G1".Altere estas configurações:Desative o Modo assertivo.Verifique **Suporta Sub-Redes**.Marque **Pre-Shared Secret** em Authentication Method (Método de



autenticação).

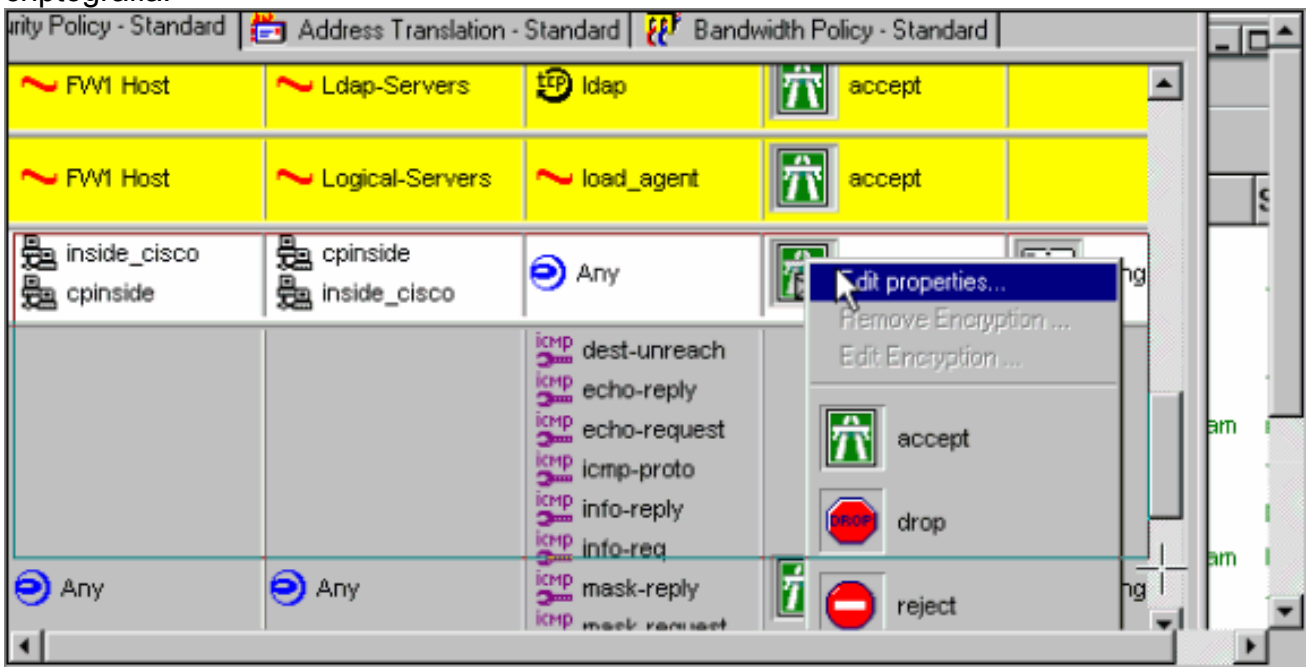
11. Clique em **Editar segredos** para definir a chave pré-compartilhada de acordo com o comando **SharedKey = <key>** VPN



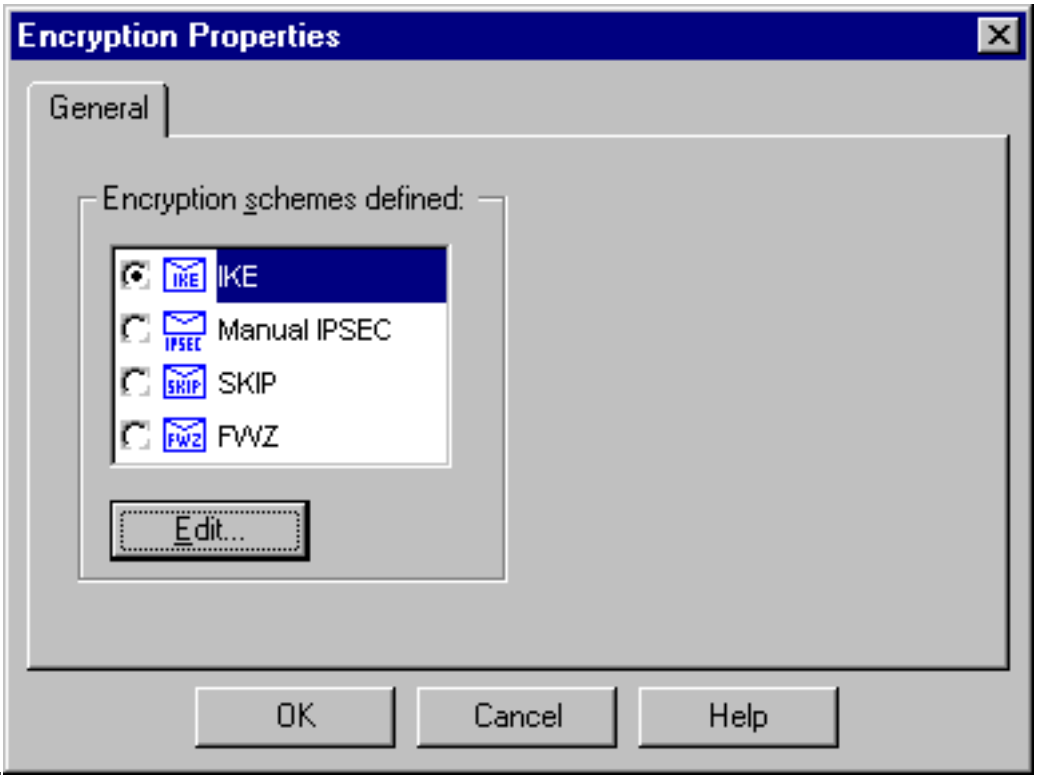
Concentrator.

12. Na janela Policy Editor, insira uma regra com Source e Destination como "inside_cisco" e "cpinside" (bidirecional). Ajustar Serviço=Qualquer, Ação=Criptografar e Rastreio=Longo.

13. No título Ação, clique no ícone **Criptografar** verde e selecione **Editar propriedades** para configurar políticas de criptografia.

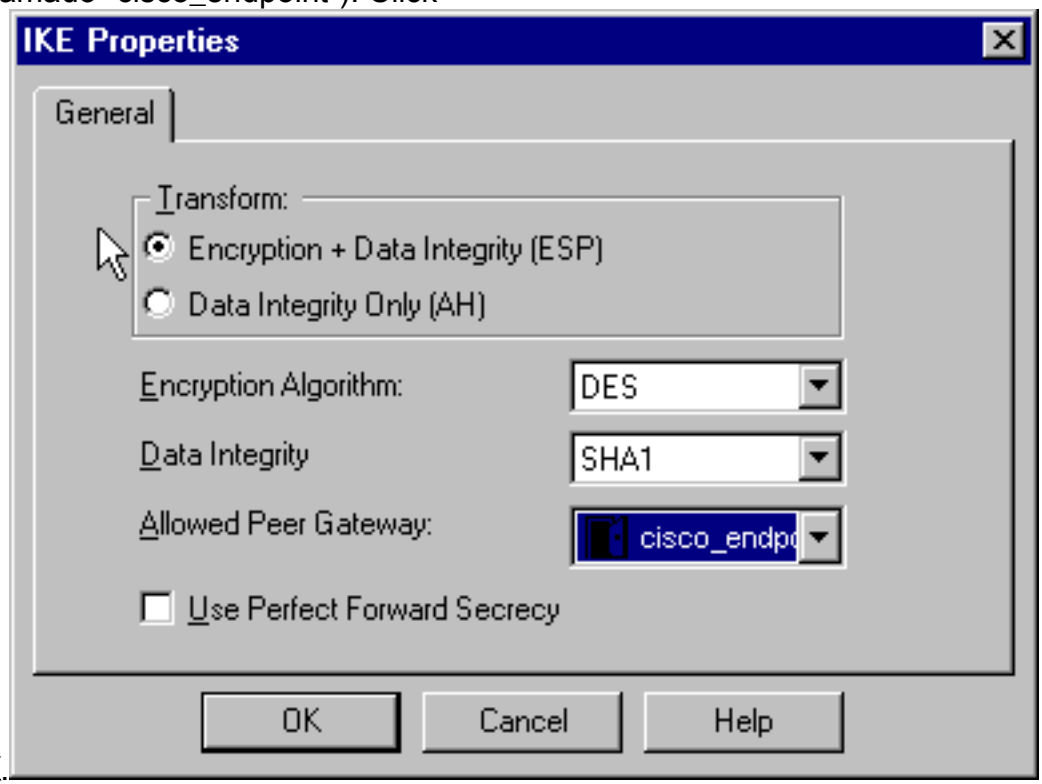


14. Selecione **IKE** e clique em



Editar.

15. Na janela Propriedades de IKE, altere essas propriedades para concordar com o **comando Transform = esp(sha,des)** VPN Concentrator.Em Transform, selecione Encryption + Data Integrity (ESP). O algoritmo de criptografia deve ser **DES**, a integridade dos dados deve ser **SHA1**, e o gateway de peer permitido deve ser o gateway do VPN Concentrator externo (chamado "cisco_endpoint"). Click



OK.

16. Depois de configurar o ponto de verificação, selecione **Política > Instalar** no menu Ponto de verificação para que as alterações entrem em vigor.

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshoot

Comandos de Troubleshooting do VPN 5000 Concentrator

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.

- **vpn trace dump all** — Mostra informações sobre todas as conexões VPN correspondentes, incluindo informações sobre a hora, o número VPN, o endereço IP real do peer, quais scripts foram executados e, em caso de erro, o número de linha e de rotina do código de software em que ocorreu o erro.
- **show system log buffer** — Mostra o conteúdo do buffer de log interno.
- **show vpn statistics** — Mostra essas informações para usuários, parceiros e o total para ambos. (Para modelos modulares, a tela inclui uma seção para cada slot de módulo. Consulte a seção Exemplo de Saída de Depuração.)`Ativo Atual` — As conexões ativas atuais.`Em Negot` — As conexões em negociação no momento.`High Water` — O maior número de conexões ativas simultâneas desde a última reinicialização.`Total em execução` — O número total de conexões bem-sucedidas desde a última reinicialização.`Túnel OK` — O número de túneis para os quais não houve erros.`Túnel é iniciado` — O número de túneis é iniciado.`Erro de túnel` — O número de túneis com erros.
- **show vpn statistics verbose** — Mostra as estatísticas de negociação de ISAKMP e muitas outras estatísticas de conexão ativas.

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 o VPN Concentrator não estiver configurado 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.

Debug de Checkpoint 4.1 Firewall

Esta foi uma instalação do Microsoft Windows NT. Como o rastreamento foi definido como `Longo` na janela do Editor de políticas (conforme visto na Etapa 12), o tráfego negado deve aparecer em vermelho no Visualizador de registros. Uma depuração mais detalhada pode ser obtida por:

```
C:\WINNT\FW1\4.1\fwstop
C:\WINNT\FW1\4.1\fw d -d
```

e em outra janela:

```
C:\WINNT\FW1\4.1\fwstart
```

Emita estes comandos para limpar as Associações de Segurança (SAs) no ponto de verificação:

```
fw tab -t IKE_SA_table -x
fw tab -t ISAKMP_ESP_table -x
fw tab -t inbound_SPI -x
fw tab -t ISAKMP_AH_table -x
```

Responda **sim** na `janela Tem certeza?` prompt.

Exemplo de saída de depuração

```
cisco_endpoint#vpn trac dump all
         4 seconds -- stepmngr trace enabled --
   new script: lan-lan primary initiator for <no id> (start)
manage @ 38 seconds :: lan-lan-VPN0:1:[172.18.124.157] (start)
         38 seconds doing l2lp_init, (0 @ 0)
         38 seconds doing l2lp_do_negotiation, (0 @ 0)
   new script: ISAKMP secondary Main for lan-lan-VPN0:1:[172.18.124.157] (start)
         38 seconds doing isa_i_main_init, (0 @ 0)
manage @ 38 seconds :: lan-lan-VPN0:1:[172.18.124.157] (done)
manage @ 38 seconds :: lan-lan-VPN0:1:[172.18.124.157] (start)
         38 seconds doing isa_i_main_process_pkt_2, (0 @ 0)
manage @ 38 seconds :: lan-lan-VPN0:1:[172.18.124.157] (done)
manage @ 38 seconds :: lan-lan-VPN0:1:[172.18.124.157] (start)
         38 seconds doing isa_i_main_process_pkt_4, (0 @ 0)
manage @ 38 seconds :: lan-lan-VPN0:1:[172.18.124.157] (done)
manage @ 39 seconds :: lan-lan-VPN0:1:[172.18.124.157] (start)
         39 seconds doing isa_i_main_process_pkt_6, (0 @ 0)
         39 seconds doing isa_i_main_last_op, (0 @ 0)
   end script: ISAKMP secondary Main for lan-lan-VPN0:1:[172.18.124.157], (0 @ 0)
   next script: lan-lan primary initiator for lan-lan-VPN0:1:[172.18.124.157], (0 @ 0)
         39 seconds doing l2lp_phase_1_done, (0 @ 0)
         39 seconds doing l2lp_start_phase_2, (0 @ 0)
   new script: phase 2 initiator for lan-lan-VPN0:1:[172.18.124.157] (start)
         39 seconds doing iph2_init, (0 @ 0)
         39 seconds doing iph2_build_pkt_1, (0 @ 0)
         39 seconds doing iph2_send_pkt_1, (0 @ 0)
manage @ 39 seconds :: lan-lan-VPN0:1:[172.18.124.157] (done)
manage @ 39 seconds :: lan-lan-VPN0:1:[172.18.124.157] (start)
         39 seconds doing iph2_pkt_2_wait, (0 @ 0)
         39 seconds doing ihp2_process_pkt_2, (0 @ 0)
         39 seconds doing iph2_build_pkt_3, (0 @ 0)
         39 seconds doing iph2_config_SAs, (0 @ 0)
         39 seconds doing iph2_send_pkt_3, (0 @ 0)
         39 seconds doing iph2_last_op, (0 @ 0)
   end script: phase 2 initiator for lan-lan-VPN0:1:[172.18.124.157], (0 @ 0)
   next script: lan-lan primary initiator for lan-lan-VPN0:1:[172.18.124.157], (0 @ 0)
         39 seconds doing l2lp_open_tunnel, (0 @ 0)
         39 seconds doing l2lp_start_i_maint, (0 @ 0)
   new script: initiator maintenance for lan-lan-VPN0:1:[172.18.124.157] (start)
         39 seconds doing imnt_init, (0 @ 0)
manage @ 39 seconds :: lan-lan-VPN0:1:[172.18.124.157] (done)


cisco_endpoint#show vpn stat

          Current  In       High     Running  Tunnel   Tunnel   Tunnel
          Active   Negot    Water    Total    Starts   OK       Error
          ----------------------------------------------------------
Users     0        0        0        0        0        0        0
Partners  1        0        1        1        1        0        0
Total     1        0        1        1        1        0        0
```

```
IOP slot 1:

          Current  In       High     Running  Tunnel   Tunnel   Tunnel
          Active   Negot    Water    Total    Starts   OK       Error
          -----------------------------------------------------------
Users     0        0        0        0        0        0        0
Partners  0        0        0        0        0        0        0
Total     0        0        0        0        0        0        0

cisco_endpoint#show vpn stat verb

          Current  In       High     Running  Tunnel   Tunnel   Tunnel
          Active   Negot    Water    Total    Starts   OK       Error
          -----------------------------------------------------------
Users     0        0        0        0        0        0        0
Partners  1        0        1        1        1        0        0
Total     1        0        1        1        1        0        0

Stats             VPN0:1
Wrapped               13
Unwrapped              9
BadEncap               0
BadAuth                0
BadEncrypt             0
rx IP                  9
rx IPX                 0
rx Other               0
tx IP                 13
tx IPX                 0
tx Other               0
IKE rekey              0

Input VPN pkts dropped due to no SA: 0

Input VPN pkts dropped due to no free queue entries: 0

ISAKMP Negotiation stats
Admin packets in        4
Fastswitch packets in   0
No cookie found         0
Can't insert cookie     0
Inserted cookie(L)      1
Inserted cookie(R)      0
Cookie not inserted(L)  0
Cookie not inserted(R)  0
Cookie conn changed     0
Cookie already inserted  0
Deleted cookie(L)       0
Deleted cookie(R)       0
Cookie not deleted(L)   0
Cookie not deleted(R)   0
Forwarded to RP         0
Forwarded to IOP        0
Bad UDP checksum        0
Not fastswitched        0
Bad Initiator cookie    0
Bad Responder cookie    0
Has Responder cookie    0
No Responder cookie     0
No SA                   0
Bad find conn           0
Admin queue full        0
Priority queue full     0
Bad IKE packet          0
```

```
No memory               0
Bad Admin Put           0
IKE pkt dropped         0
No UDP PBuf             0
No Manager              0
Mgr w/ no cookie        0
Cookie Scavenge Add     1
Cookie Scavenge Rem     0
Cookie Scavenged        0
Cookie has mgr err      0
New conn limited        0

IOP slot 1:

          Current  In       High     Running  Tunnel   Tunnel   Tunnel
          Active   Negot    Water    Total    Starts   OK       Error
          -------------------------------------------------------------
Users     0        0        0        0        0        0        0
Partners  0        0        0        0        0        0        0
Total     0        0        0        0        0        0        0

Stats
Wrapped
Unwrapped
BadEncap
BadAuth
BadEncrypt
rx IP
rx IPX
rx Other
tx IP
tx IPX
tx Other
IKE rekey

Input VPN pkts dropped due to no SA: 0

Input VPN pkts dropped due to no free queue entries: 0

ISAKMP Negotiation stats
Admin packets in        0
Fastswitch packets in   3
No cookie found         0
Can't insert cookie     0
Inserted cookie(L)      0
Inserted cookie(R)      1
Cookie not inserted(L)  0
Cookie not inserted(R)  0
Cookie conn changed     0
Cookie already inserted  0
Deleted cookie(L)       0
Deleted cookie(R)       0
Cookie not deleted(L)   0
Cookie not deleted(R)   0
Forwarded to RP         0
Forwarded to IOP        3
Bad UDP checksum        0
Not fastswitched        0
Bad Initiator cookie    0
Bad Responder cookie    0
Has Responder cookie    0
No Responder cookie     0
No SA                   0
Bad find conn           0
```

```
Admin queue full         0
Priority queue full      0
Bad IKE packet           0
No memory                0
Bad Admin Put            0
IKE pkt dropped          0
No UDP PBuf              0
No Manager               0
Mgr w/ no cookie         0
Cookie Scavenge Add      1
Cookie Scavenge Rem      0
Cookie Scavenged         0
Cookie has mgr err       0
New conn limited         0
```

Informações Relacionadas

- Anúncio do fim do ciclo de comercialização dos concentradores Cisco VPN 5000 Series
- Negociação IPsec/Protocolos IKE
- Suporte Técnico e Documentação - Cisco Systems