Configurando um túnel de IPsec - Concentrador do Cisco VPN 5000 ao Firewall do ponto de verificação 4.1

Índice

Introdução

Este documento demonstra como formar um túnel de IPsec com chaves pré-compartilhada para juntar-se a duas redes privadas. Junta-se a uma rede privada dentro do concentrador do Cisco VPN 5000 (192.168.1.x) a uma rede privada dentro do Firewall do ponto de verificação 4.1 (10.32.50.x). Supõe-se que o tráfego do interior do concentrador VPN e do interior o ponto de verificação ao Internet (representado neste documento pelas redes 172.18.124.x) flui antes que você comece esta configuração.

Pré-requisitos

Requisitos

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
- Versão de software do concentrador 5.2.19.0001 do Cisco VPN 5000
- Checkpoint 4.1 Firewall

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

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

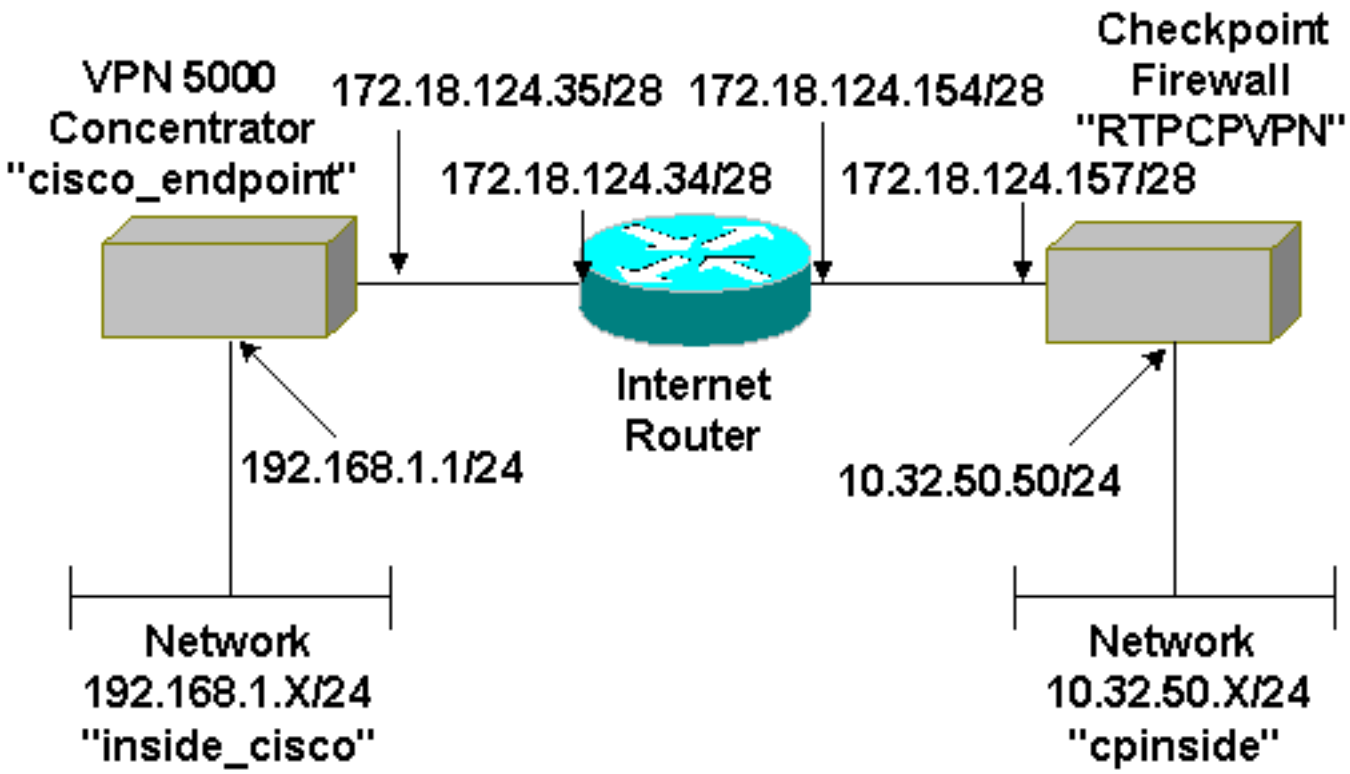
Configurar

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

Note: Use a ferramenta Command Lookup Tool (apenas para 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 usa esta configuração.

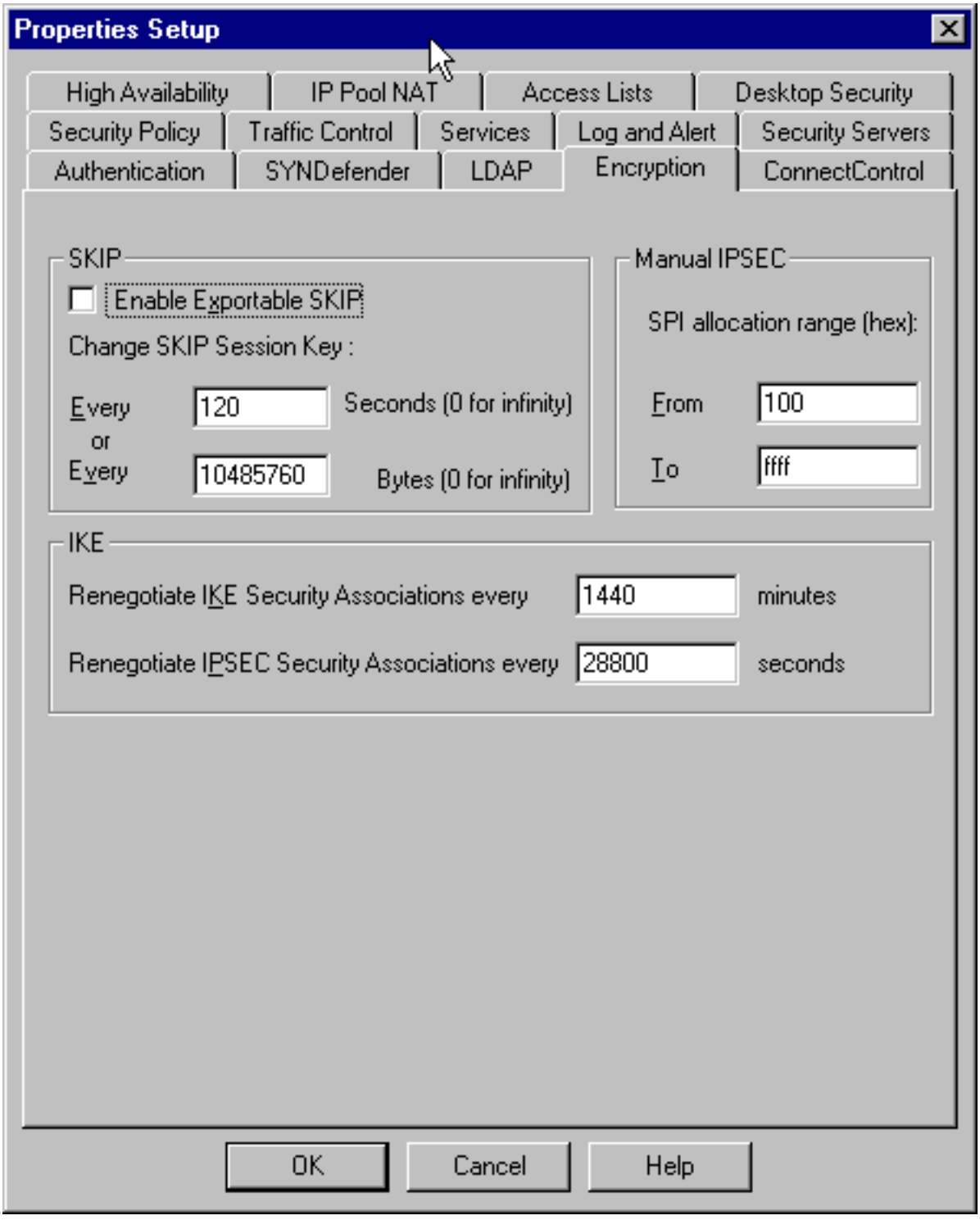
Cisco VPN 5000 Concentrator

```
[ 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

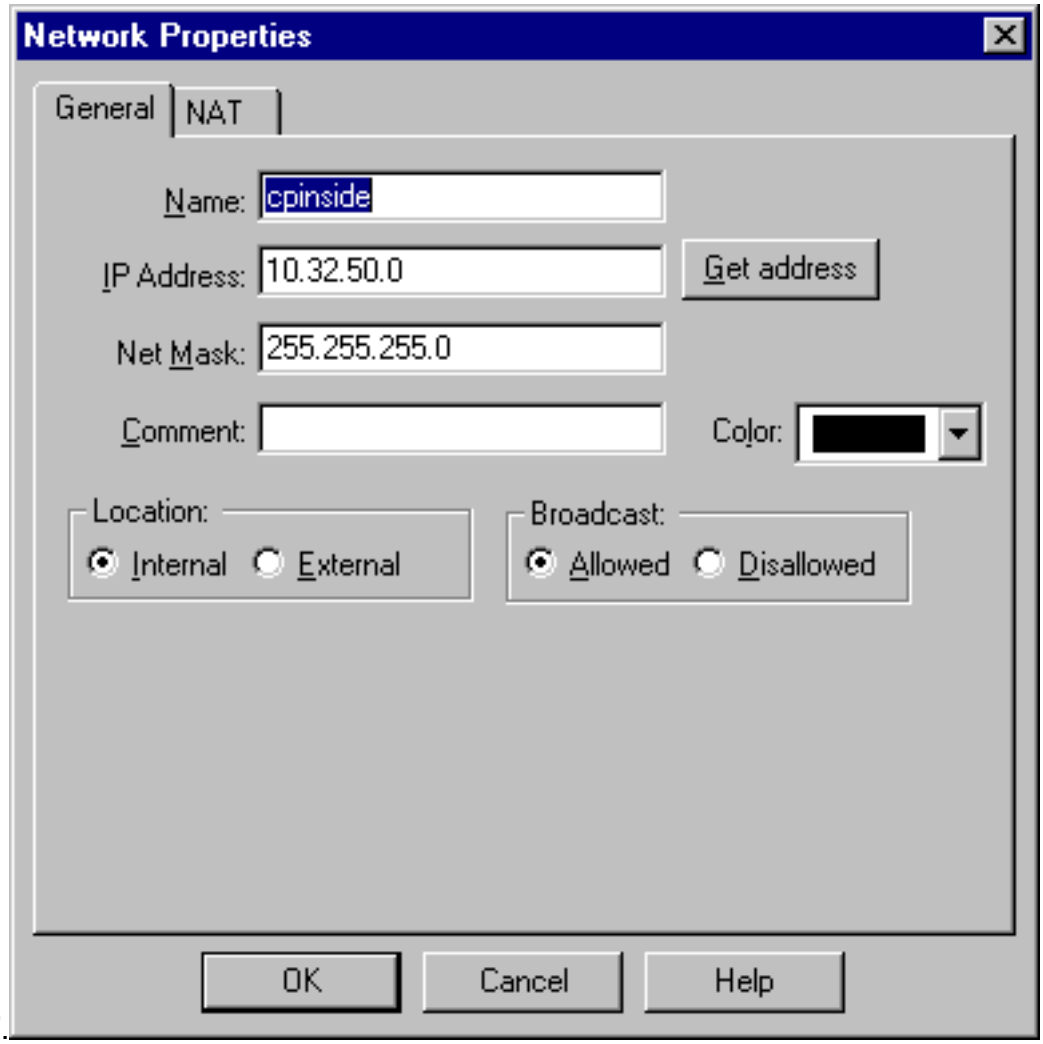
Termine estas etapas para configurar o Firewall do ponto de verificação 4.1.

1. Selecione o **Propriedades > Criptografia** para ajustar as durações de IPSec do ponto de verificação para concordar com o **KeyLifeSecs = o** comando vpn concentrator **28800**.**Note**: Deixe as vidas do Internet Key Exchange (IKE) do ponto de verificação no



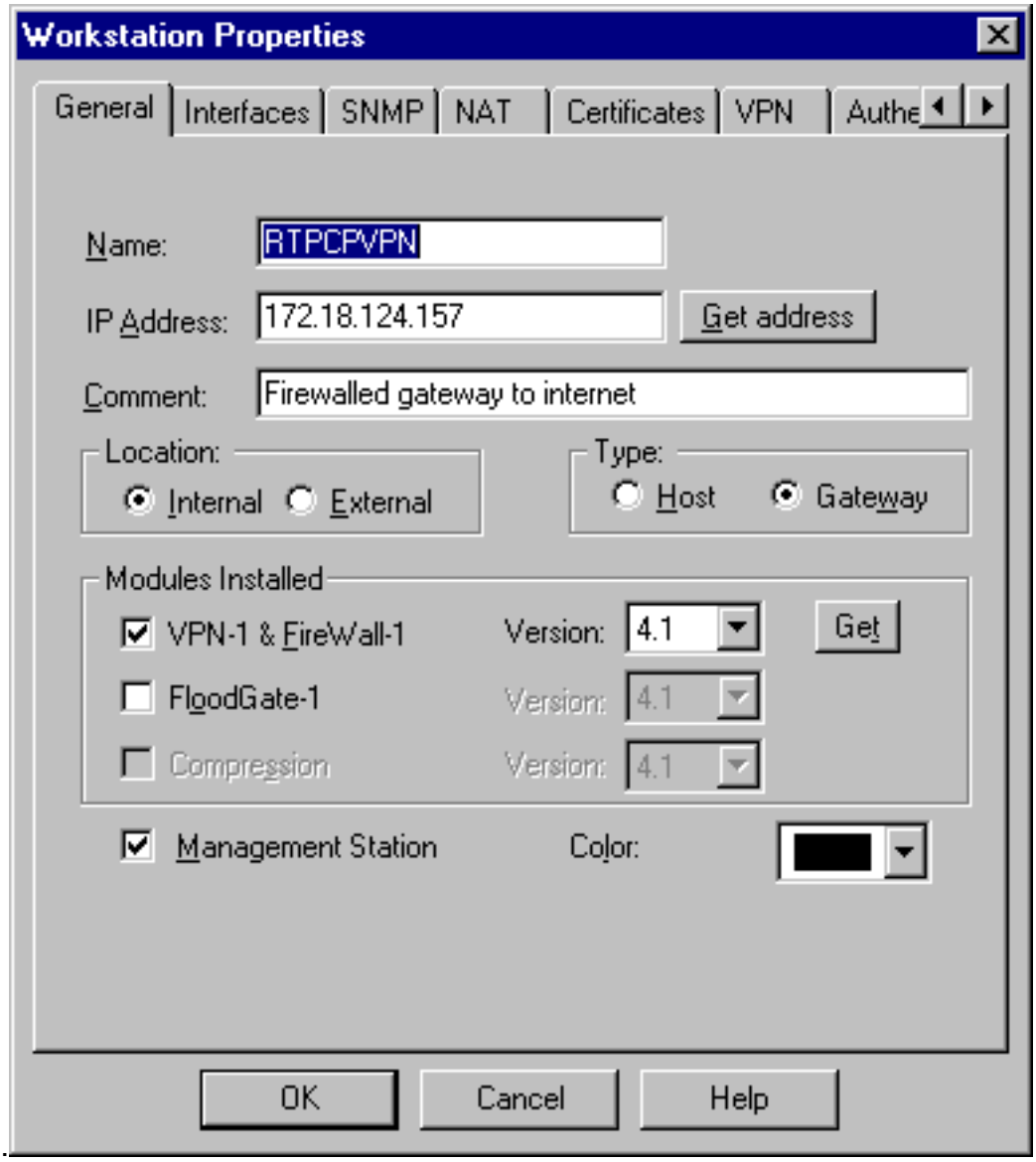
padrão.

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. Isto deve concordar com o **par =** comando vpn concentrator de



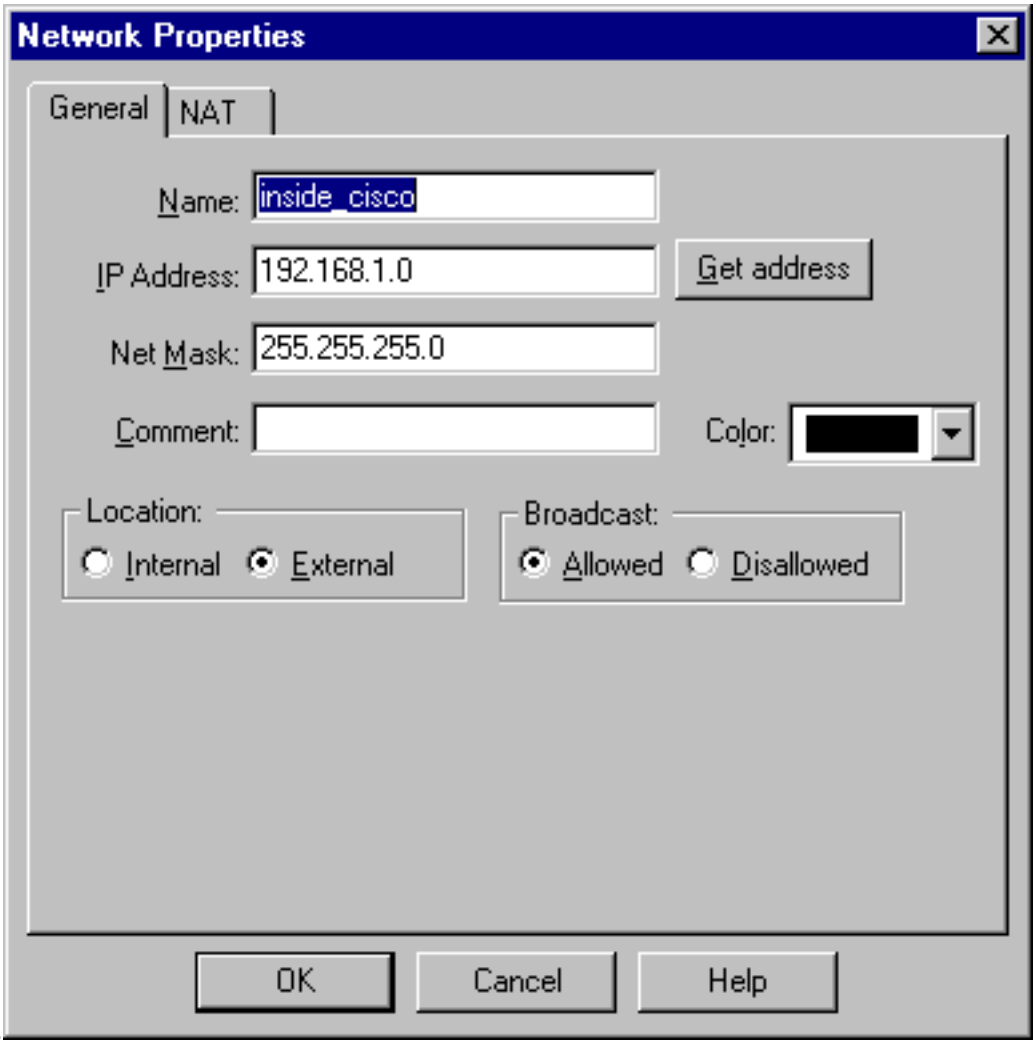
"10.32.50.0/24".

3. Selecione **Manage > Network Objects > Edit** para editar o objeto para o valor-limite do gateway (ponto de verificação “RTPCPVPN”) esse os pontos do concentrador VPN no **comando Partner = <ip>**.Selecione o lugar inferior **interno**.Selecione o **gateway** para o tipo.Verifique o **VPN-1 & o FireWall-1** e a **estação de gerenciamento** sob os módulos



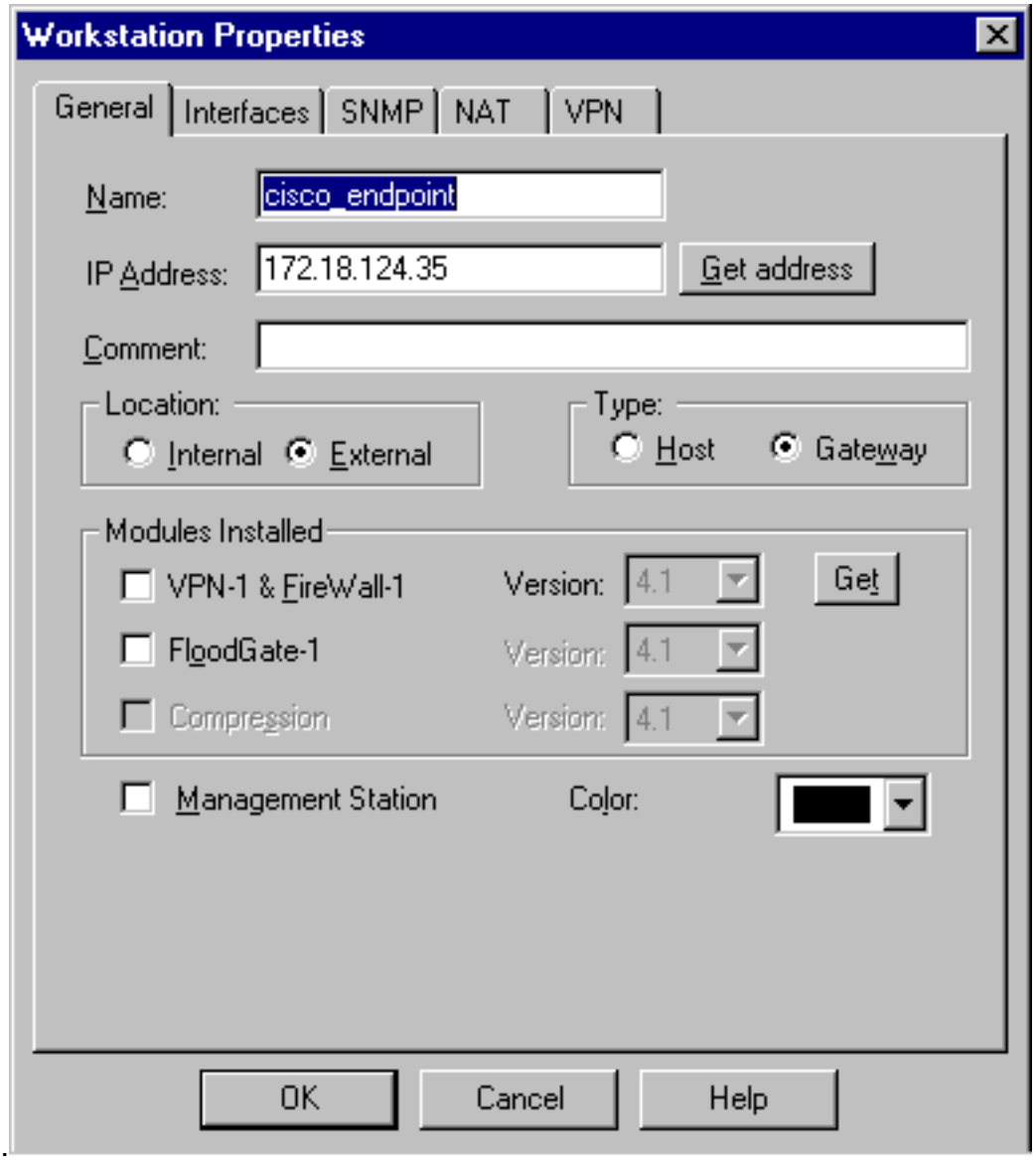
instalados.

4. Selecione **Manage > Network Objects o > New (Or Edit) > Network** para configurar o objeto para (“inside_cisco”) a rede externo atrás do concentrador VPN.Isto deve concordar com o **LocalAccess = o** comando vpn concentrator

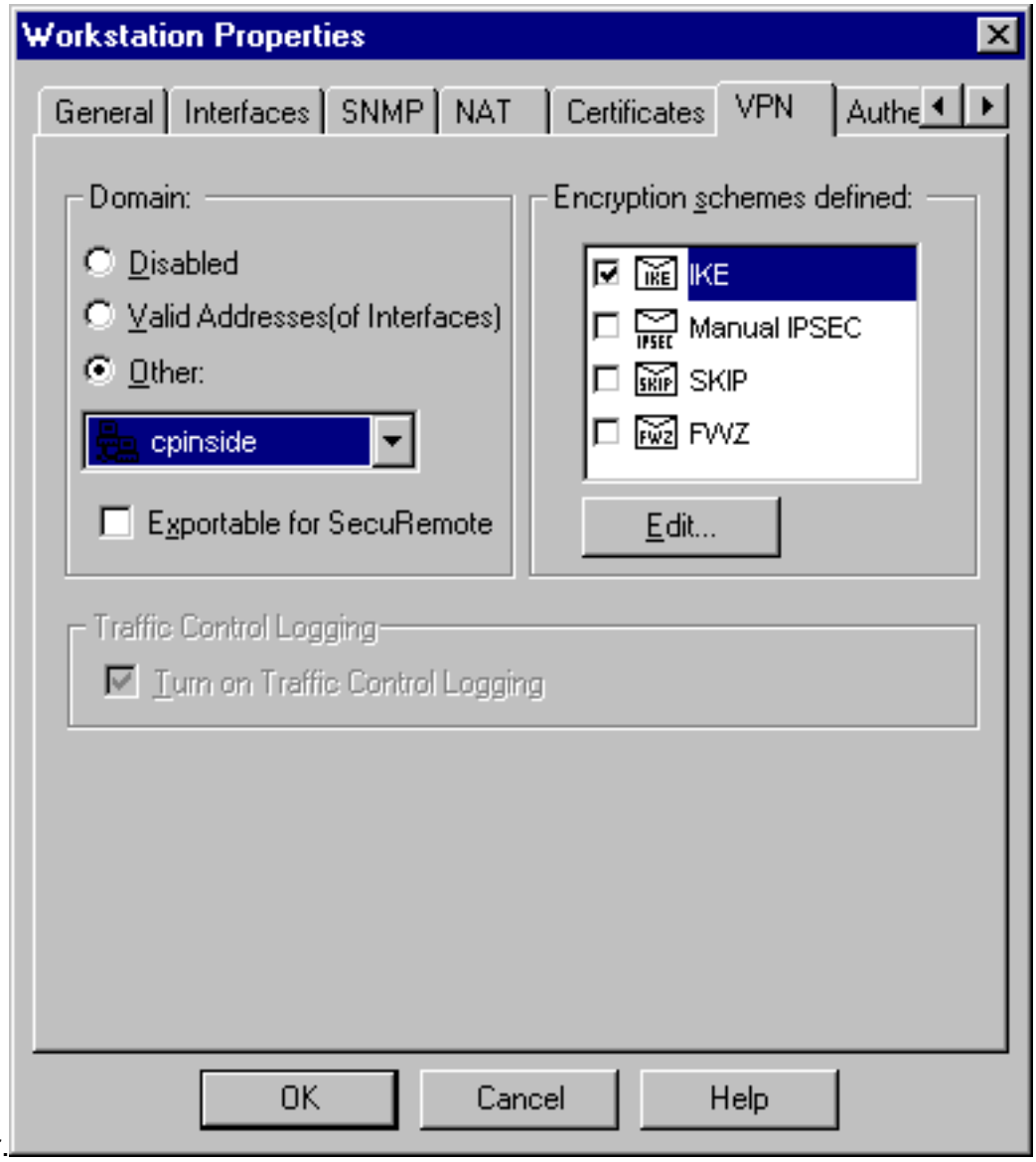


<192.168.1.0/24>.

5. Selecione **Manage > Network Objects > New > Workstation** para adicionar um objeto para (“cisco_endpoint”) o gateway externo do concentrador VPN.Esta é a relação da “parte externa” do concentrador VPN com Conectividade ao ponto de verificação (neste documento, 172.18.124.35 é o endereço IP de Um ou Mais Servidores Cisco ICM NT no **comando IPAddress = <ip>**).Selecione o lugar inferior **externo**. Selecione o **gateway** para o tipo.**Note**: Não verifique VPN-1/FireWall-

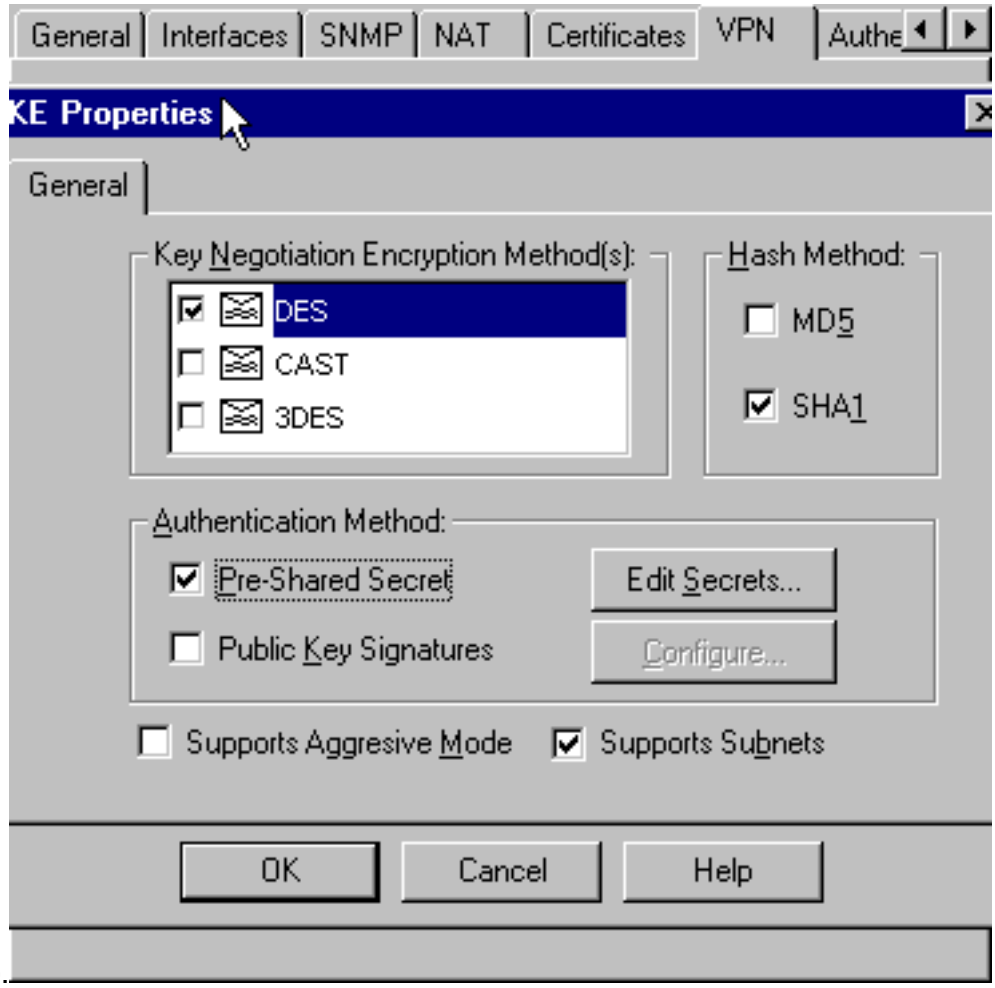
1. 

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



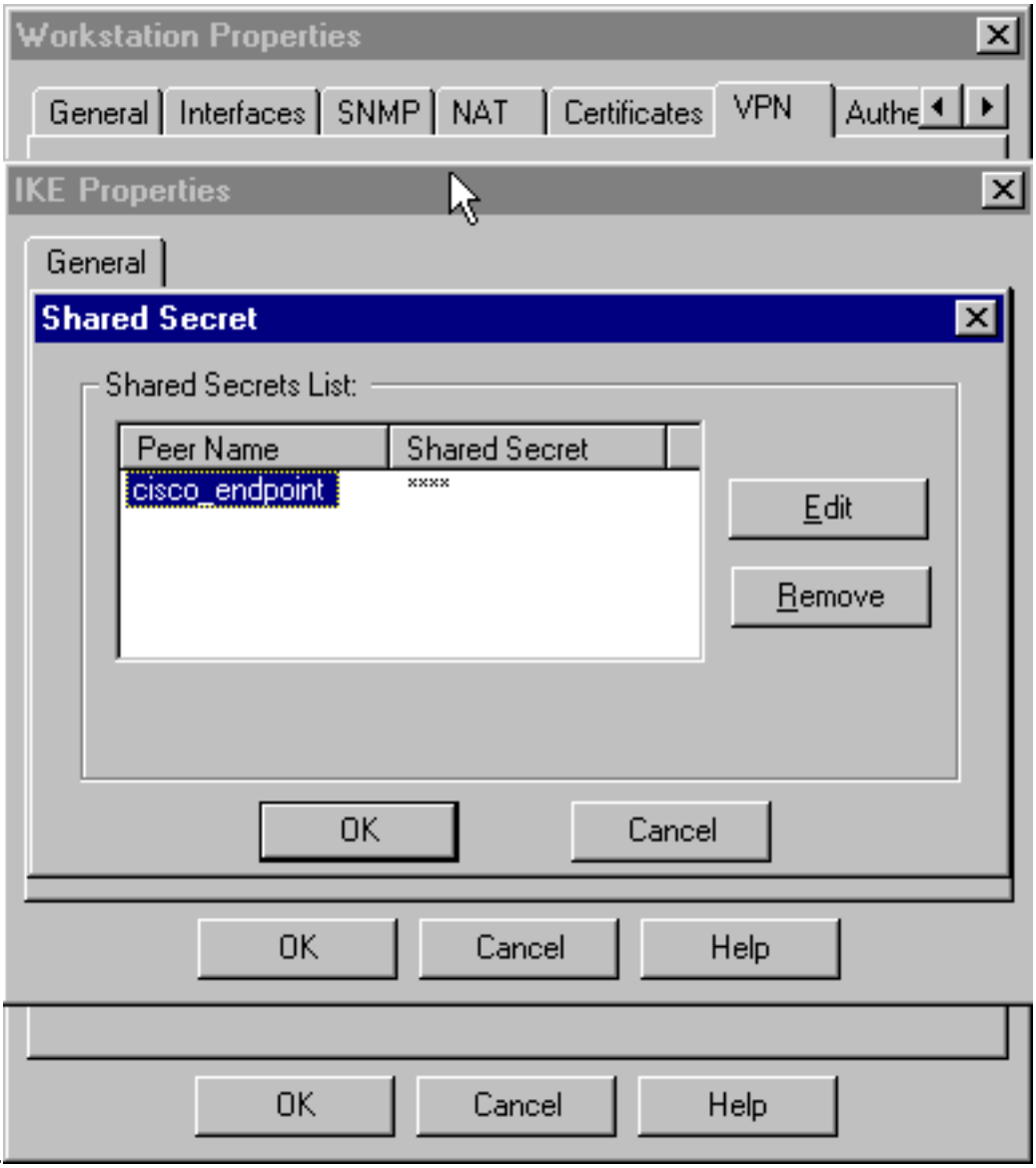
Editar.

7. Mude as propriedades IKE à **criptografia DES** e ao hashing **SHA1** para concordar com o comando vpn concentrator **SHA_DES_G2**.**Note**: O "G2" refere o grupo Diffie-Hellman 1 ou 2. Nos testes, descobriu-se que o ponto de verificação aceita "G2" ou "G1."Mude estes ajustes:Desative o Modo assertivo.A verificação **apoia sub-redes**.Verifique o **segredo pré-compartilhado** sob o método de



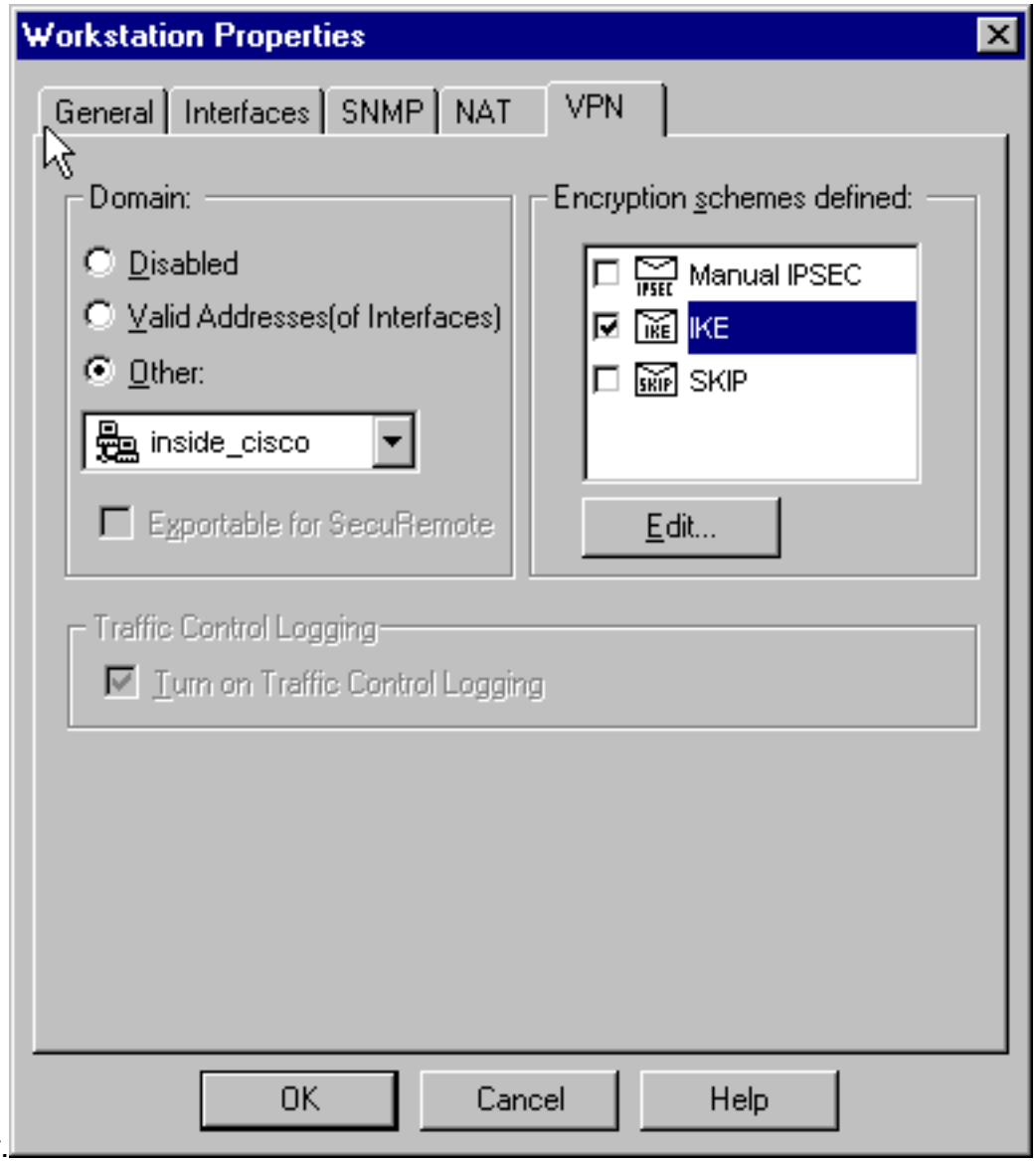
autenticação.

8. O clique **edita segredos** para ajustar a chave pré-compartilhada para concordar com a **Chave compartilhada = o** comando vpn concentrator do



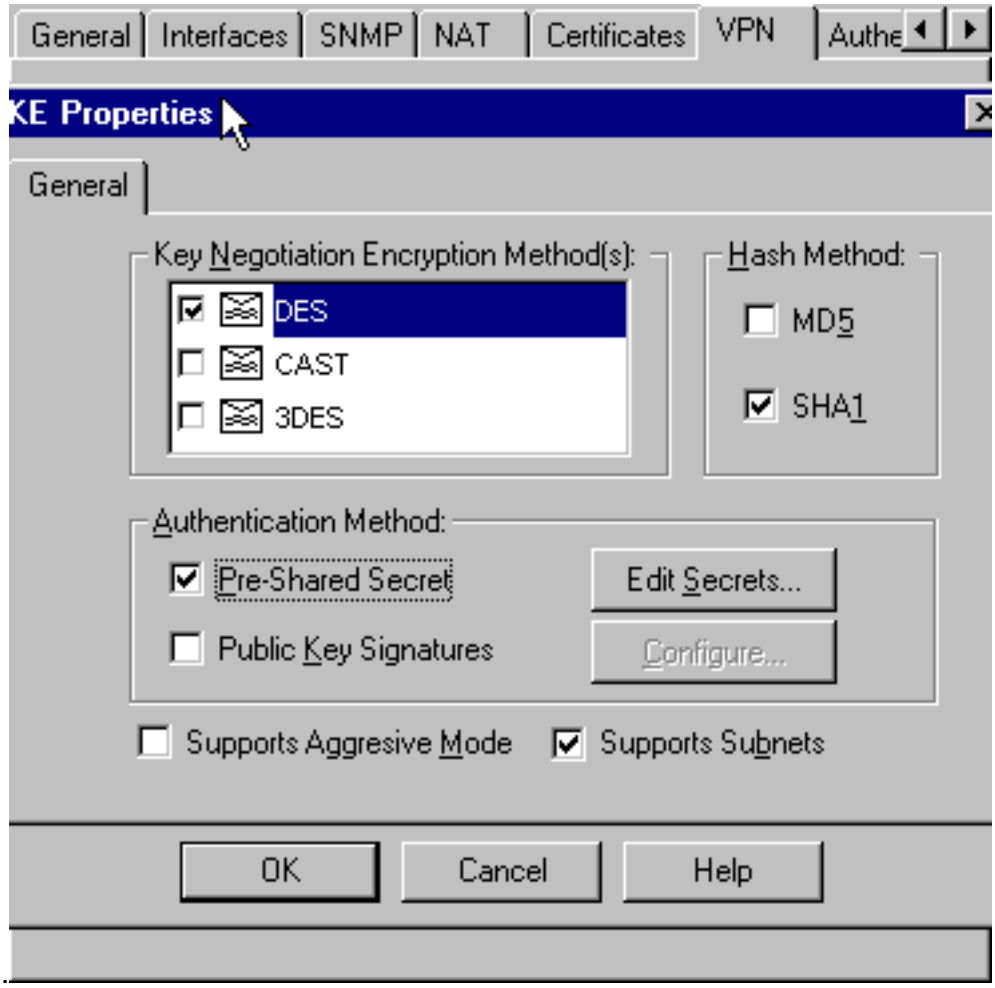
<key>.

9. Selecione Gerenciar > Objetos de rede > Editar para editar a guia VPN “cisco_endpoint”. Sob o domínio, selecione **outro**, e selecione então o interior da rede do concentrador VPN (chamada “inside_cisco”). Sob esquemas de criptografia definidos, selecione IKE e clique



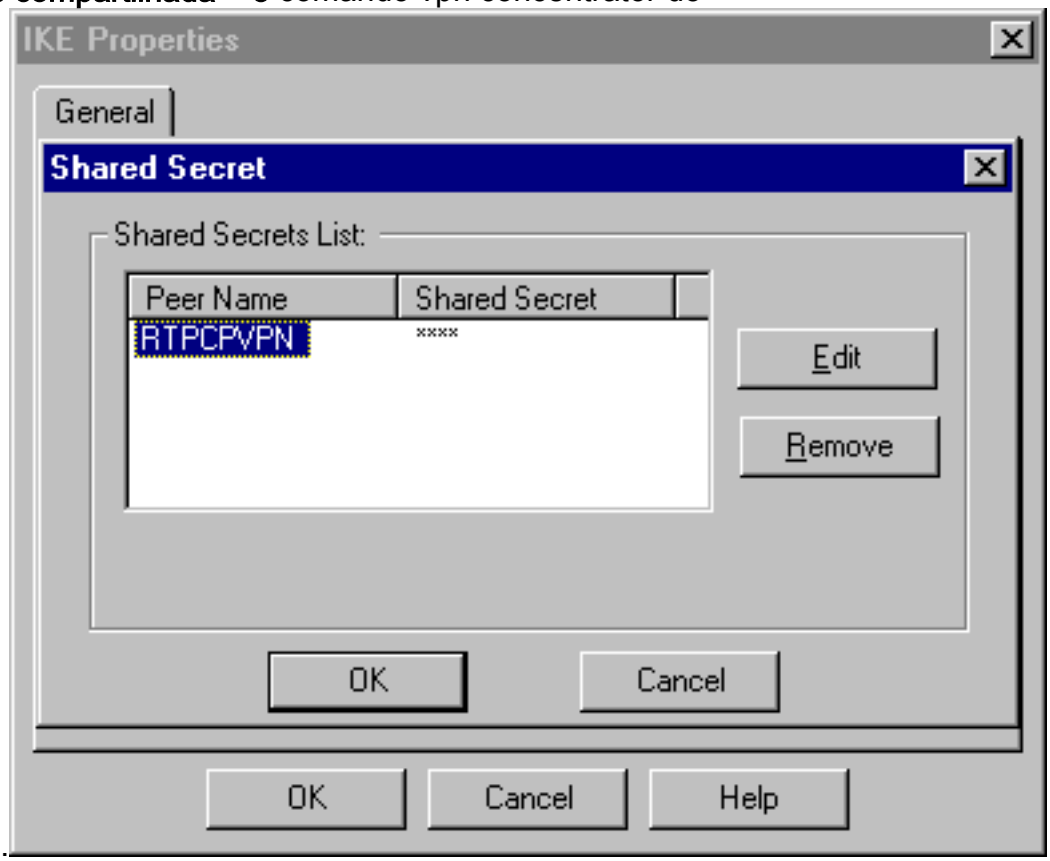
em Editar.

10. Mude as propriedades IKE à **criptografia DES** e ao hashing **SHA1** para concordar com o comando vpn concentrator **SHA_DES_G2**.**Note**: O "G2" refere o grupo Diffie-Hellman 1 ou 2. Nos testes, encontrou-se que o ponto de verificação aceita "G2" ou "G1."Mude estes ajustes:Desative o Modo assertivo.A verificação **apoia sub-redes**.Verifique o **segredo pré-compartilhado** sob o método de



autenticação.

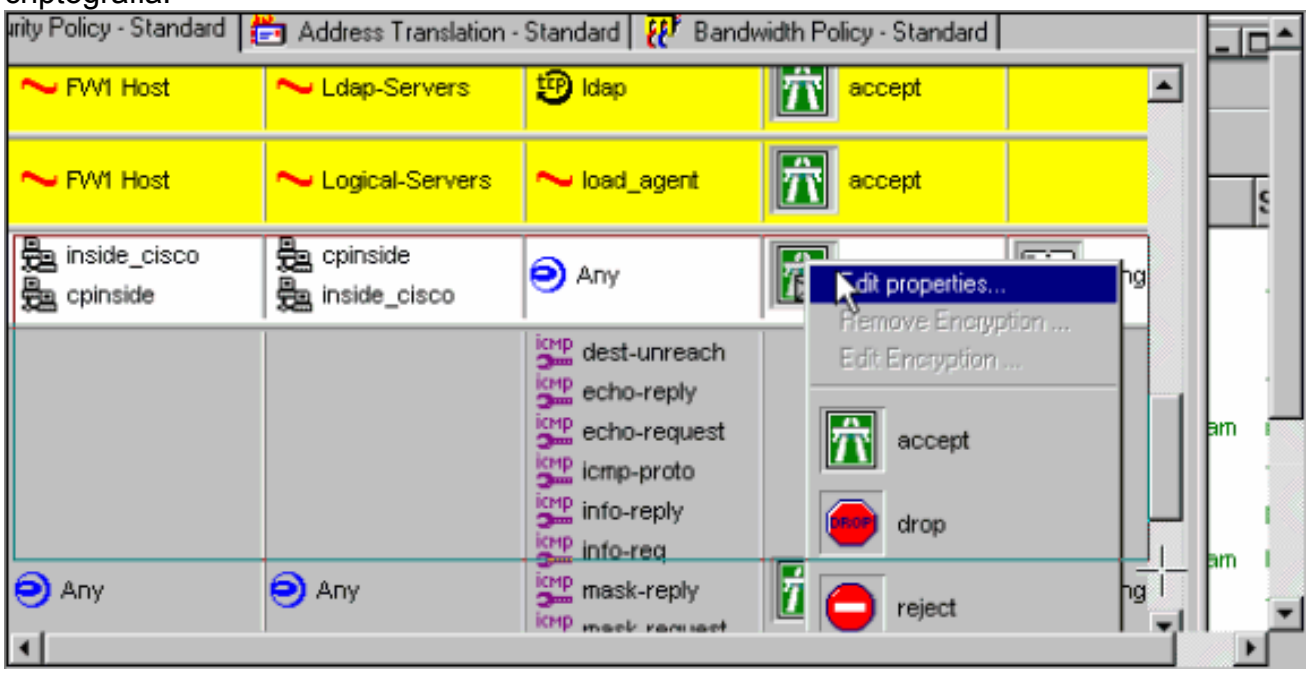
11. O clique **edita segredos** para ajustar a chave pré-compartilhada para concordar com a **Chave compartilhada = o** comando vpn concentrator do



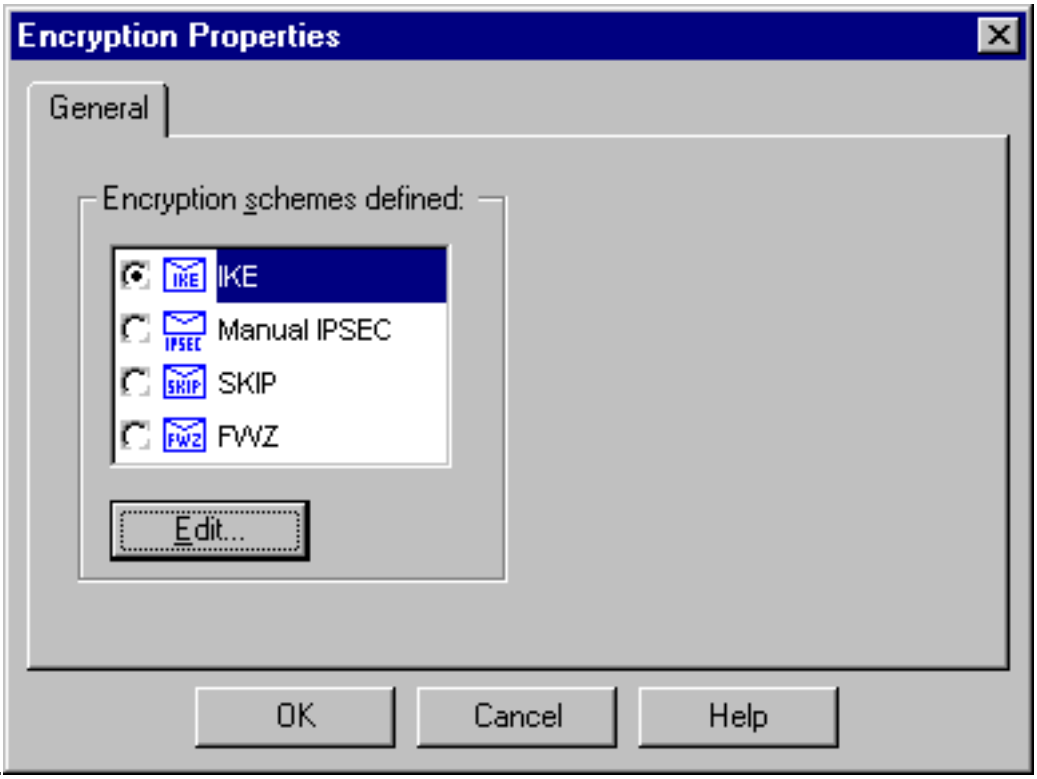
<key>.

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. Sob o título da ação, clique o ícone verde de criptografia e selecione-o **Edit Properties** para configurar políticas de criptografia.

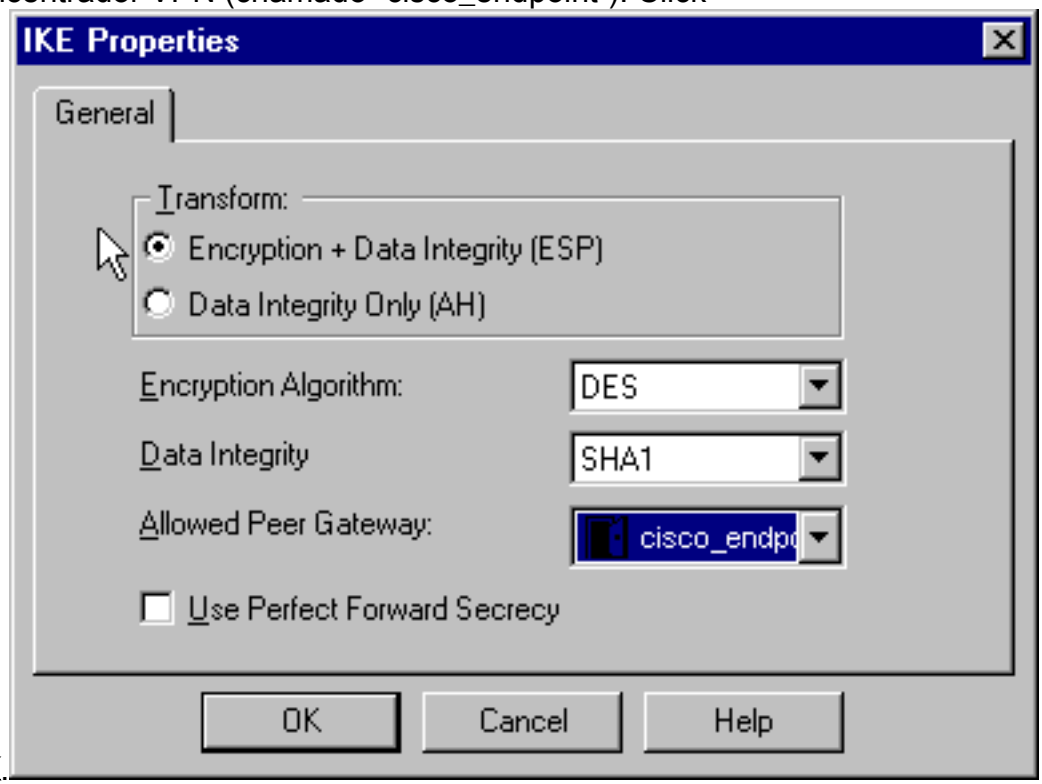


14. Selecione o **IKE**, e o clique



edita.

15. No indicador das propriedades IKE, mude estas propriedades para concordar com a **transformação = esp (sha, DES)** comando vpn concentrator.Em Transform, selecione Encryption + Data Integrity (ESP). O algoritmo de criptografia deve ser **DES**, integridade de dados deve ser **SHA1**, e o gateway de peer permitido deve ser o gateway externo do concentrador VPN (chamado “cisco_endpoint”). Click



OK.

16. Depois que você configura o ponto de verificação, a **política** seleta **> instala no** menu do ponto de controle para mandar as mudanças tomar o efeito.

Verificar

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

Troubleshooting

Comandos de Troubleshooting do VPN 5000 Concentrator

A Output Interpreter Tool (apenas para clientes registrados) (OIT) suporta determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

Note: 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 o horário, o número VPN, o endereço IP real do correspondente, quais scripts foram executadas e, em caso de erro, a rotina e o número da linha do código do software em que ocorrreu o erro.
- **Show System Log Buffer** — Mostra os índices do buffer de registro interno.
- **show vpn statistics** — Mostra esta informação para usuários, Parceiros, e o total para ambos. (Para modelos modulares, o indicador inclui uma seção para cada slot de módulo. Refira a seção do exemplo de debug.)Current Active - As conexões ativas no momento.Em negociação - As conexões em negociação no momento.Nível alto – O maior número de conexões ativas desde a última reinicialização.Total em execução – O número total de conexões bem-sucedidas desde a última reinicialização.Túnel OK – O número de túneis que não apresentaram erros.Inicialização do túnel – O número do túnel é iniciado.Tunnel Error – O número de túneis com erros.
- show vpn statistics verbose - Mostra estatísticas de negociação de ISAKMP e muitas outras estatísticas de conexão.

Sumarização da rede

Quando as redes internas adjacentes do múltiplo são configuradas no domínio da criptografia no ponto de verificação, o dispositivo pôde automaticamente resumi-las no que diz respeito ao tráfego interessante. Se o concentrador VPN não é configurado para combinar, o túnel é provável falhar. Por exemplo, se as redes internas de 10.0.0.0 /24 e de 10.0.1.0 /24 são configuradas para ser incluídas no túnel, puderam ser resumidas a 10.0.0.0 /23.

Debug de Checkpoint 4.1 Firewall

Esta era uma instalação de Microsoft Windows NT. Porque o seguimento foi ajustado para `por muito tempo` dentro a janela de editor de política (como visto em etapa 12), o tráfego negado deve aparecer no vermelho no Log Viewer. Mais verboso debugar pode ser obtido 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 cancelar as associações de segurança (SA) 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
```

A resposta **sim no** `é você certo?` prompt.

Exemplo de debug

```
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 End-of-Life de concentradores do Cisco VPN 5000 Series
- Negociação IPsec/Protocolos IKE
- Suporte Técnico e Documentação - Cisco Systems