Configurando um túnel de IPsec entre um Cisco VPN 3000 Concentrator e um Firewall do NG ponto de verificação

Índice

Introdução

Este documento demonstra como configurar um túnel de IPsec com chaves pré-compartilhada para comunicar-se entre duas redes privadas. Neste exemplo, as redes de comunicação são a rede privada 192.168.10.x dentro do Cisco VPN 3000 Concentrator e a rede privada 10.32.x.x dentro do Firewall da próxima geração do ponto de verificação (NG).

Pré-requisitos

Requisitos

- Tráfego do interior do concentrador VPN e do interior o NG ponto de verificação ao Internet — representado aqui pelas redes 172.18.124.x — deve fluir antes de começar esta configuração.
- Os usuários devem ser familiares com a negociação de IPSec. Este processo pode ser

dividido em cinco etapas, incluindo duas fases de intercâmbio de chave de Internet (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. Uma vez que os pares são autenticados, um túnel seguro está criado com o Internet Security Association and Key Management Protocol (ISAKMP).Na fase 2 IKE, os ipsec peer usam o túnel seguro e autenticado a fim negociar IPsec SA transformam. 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 os ipsec peer baseados nos parâmetros IPSec configurados no IPsec transformam grupos.O túnel de IPSec finaliza quando os IPSec SAs são excluídos ou quando sua vida útil expira.

Componentes Utilizados

Esta configuração foi desenvolvida e testada com estes a versão de software e hardware:

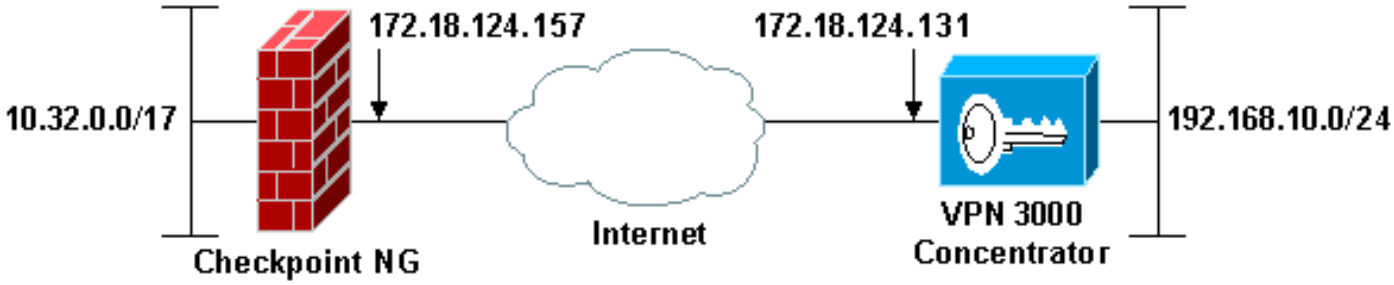
- VPN 3000 series concentrator 3.5.2
- Firewall do NG ponto de verificação

Convenções

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

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



Note: O esquema de endereçamento de IP usado nesta configuração não é legalmente roteável no Internet. São os endereços do RFC 1918, que foram usados em um ambiente de laboratório.

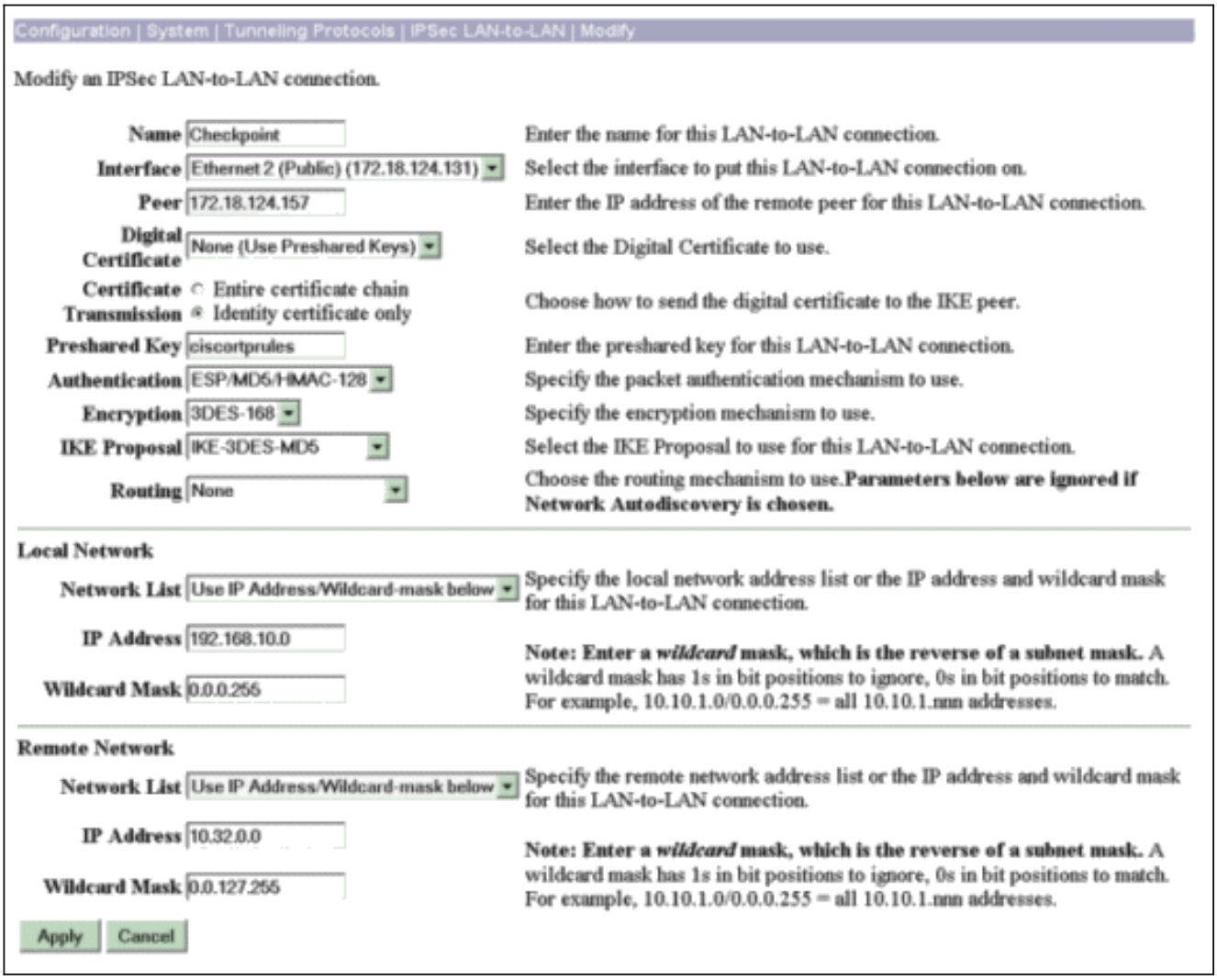
Configurações

Configurar o VPN 3000 Concentrator

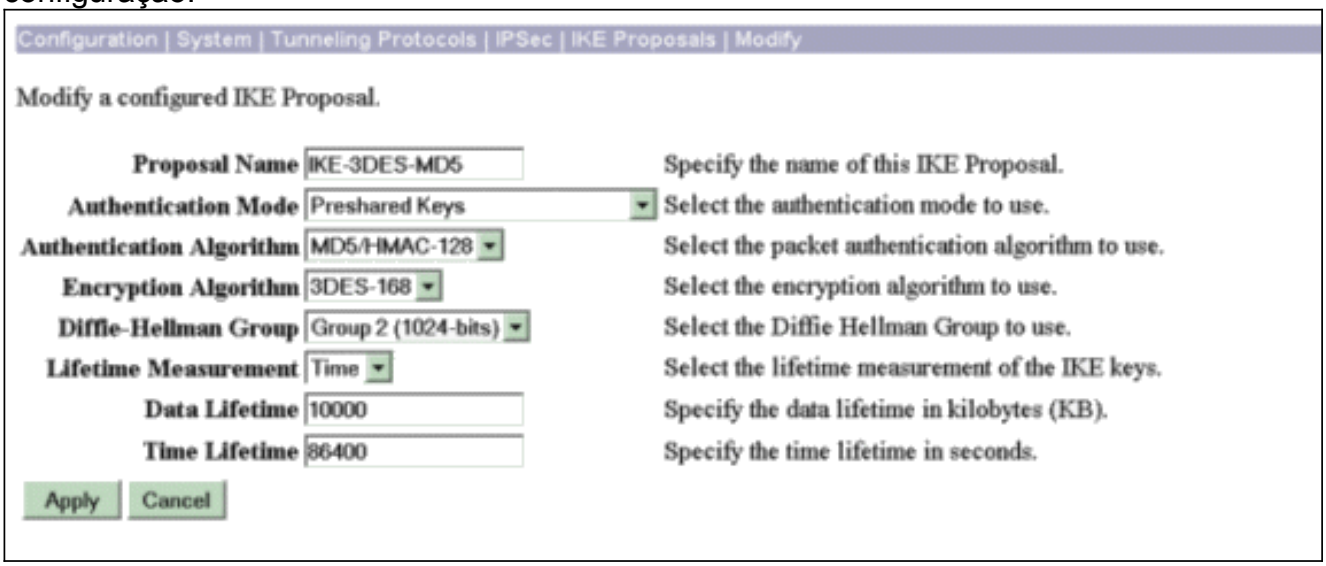
Termine estas etapas a fim configurar o VPN 3000 concentrator:

1. Vai ao **Configuration > System > Tunneling Protocols > o LAN para LAN do IPsec** a fim configurar a sessão de LAN a LAN. Ajuste as opções de autenticação e os algoritmos IKE, chave pré-compartilhada, endereço IP do peer, e parâmetros de rede remota e local. Clique

em Apply.Nesta configuração, a autenticação foi ajustada enquanto o ESP-MD5-HMAC e a criptografia foram ajustados como o
3DES.



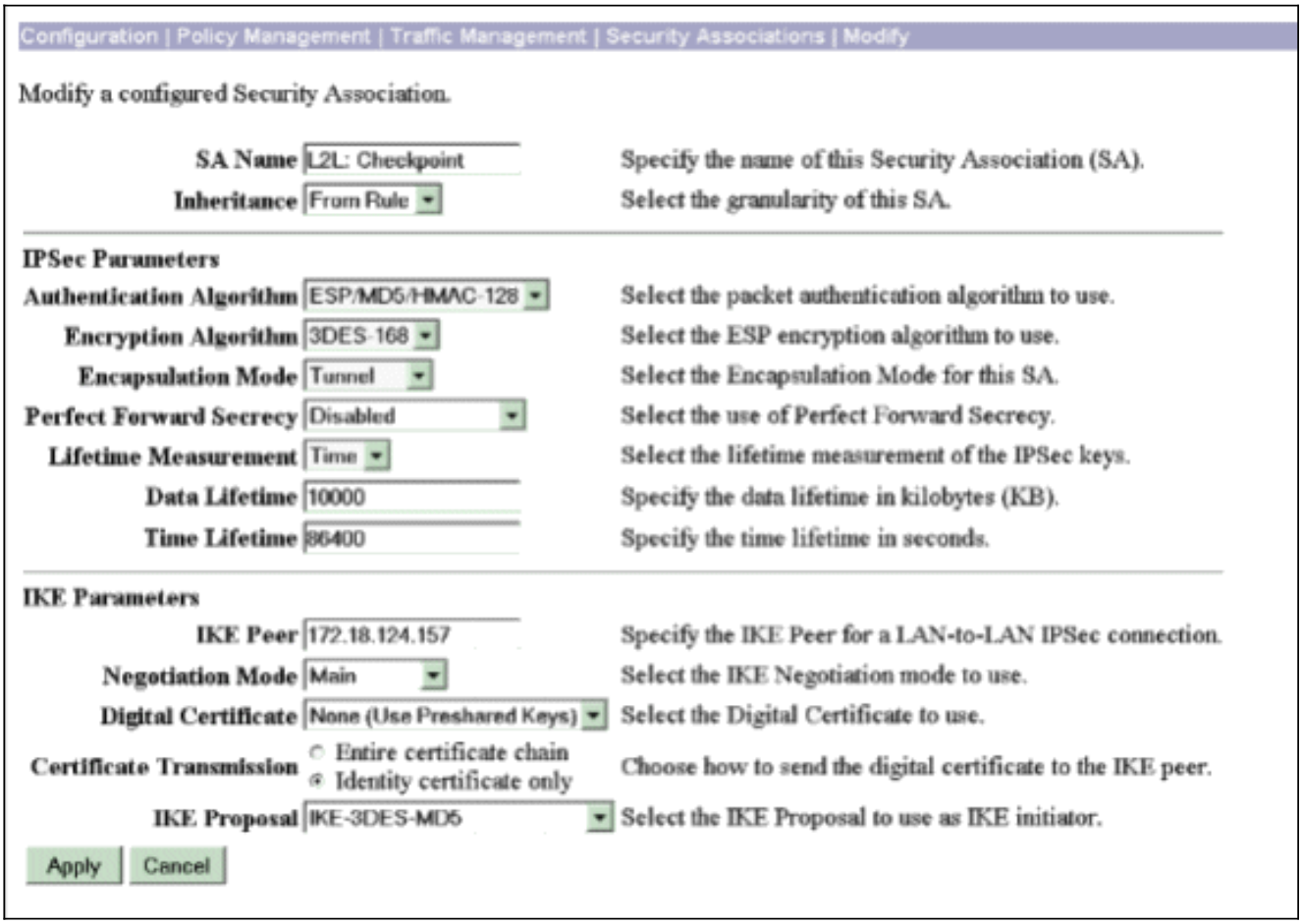
2. Vá ao **configuração > sistema > protocolos de tunelamento > IPSEC > propostas de IKE** e ajuste os parâmetros requerido.Selecione a proposta IKE IKE-3DES-MD5 e verifique os parâmetros selecionados para a proposta. O clique **aplica-se** a fim configurar a sessão de LAN a LAN.Estes são os parâmetros para esta
configuração:



3. Vá ao **Configuração > Gerenciamento de Política > Gerenciamento de Tráfego > Associações de Segurança**, selecione IPsec SA criado para a sessão, e verifique os

parâmetros IPsec SA escolhidos para a sessão de LAN a LAN.Nesta configuração o nome da sessão de LAN a LAN era “ponto de verificação, “assim que IPsec SA foi criado automaticamente como "L2L: Ponto de verificação.”

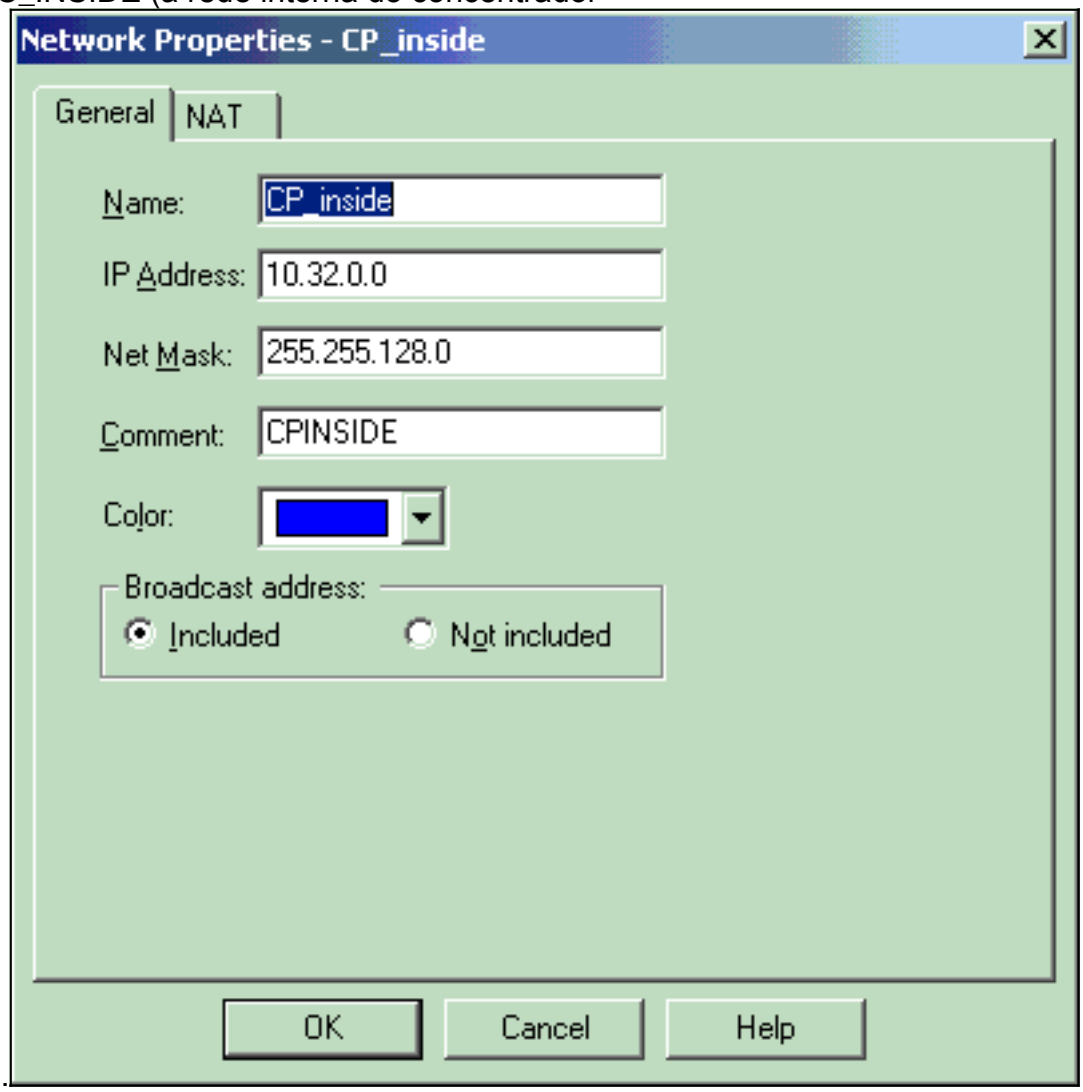
Estes são os parâmetros para este SA:

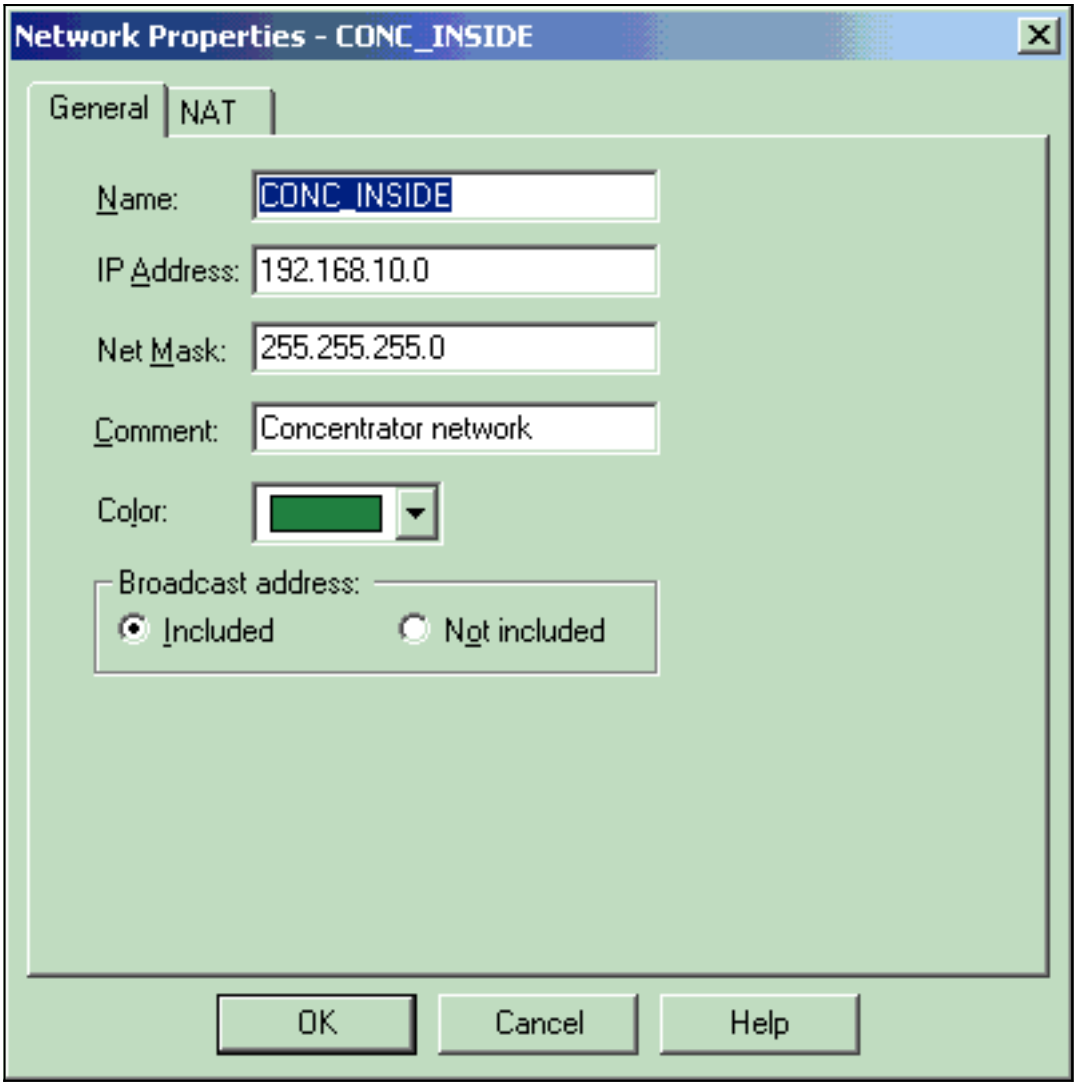


Configurar o NG ponto de verificação

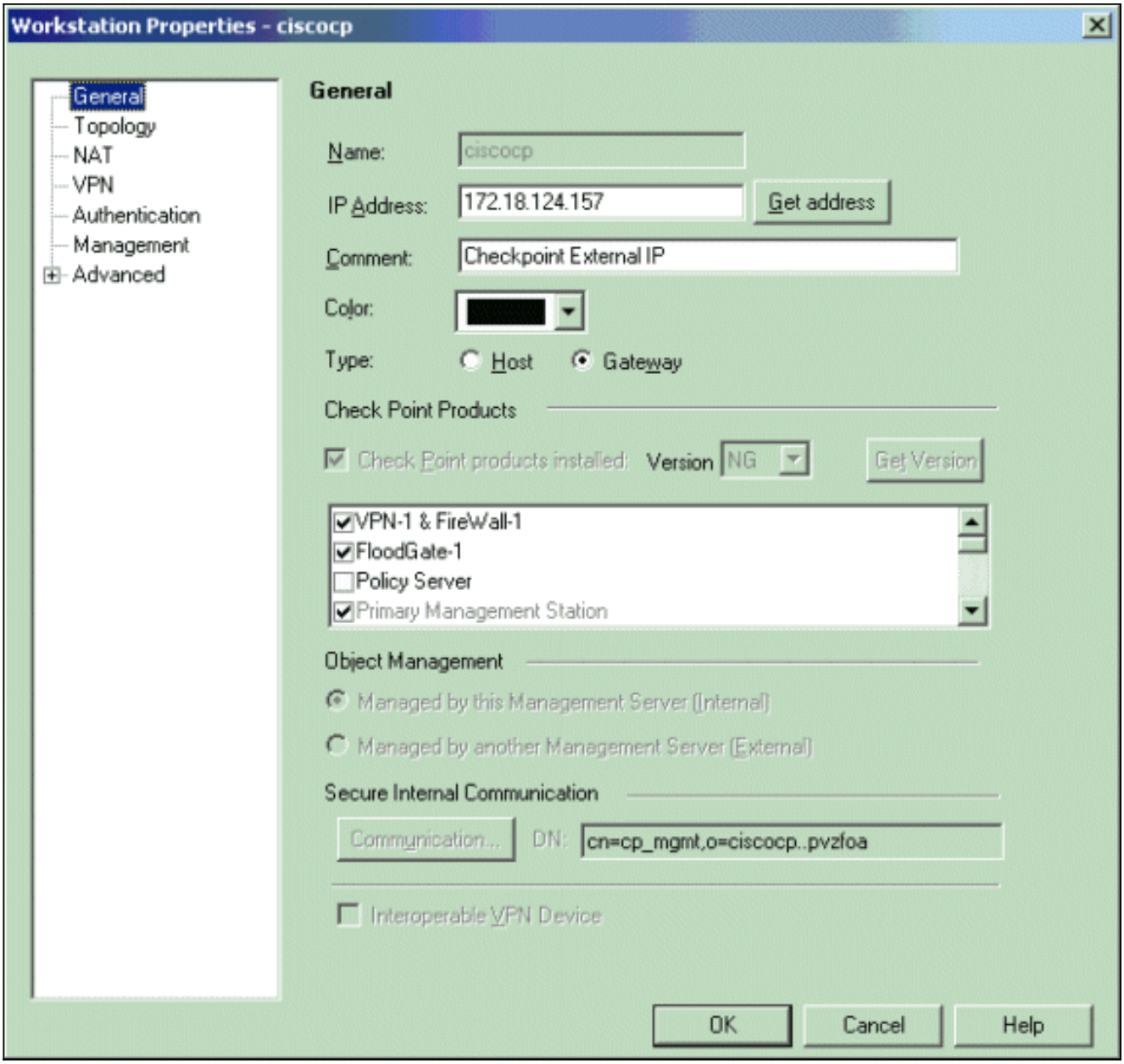
Os objetos de rede e as regras são definidos no NG ponto de verificação a fim compor a política que se refere a configuração de VPN a se estabelecer. Esta política é instalada então com o editor de política do NG ponto de verificação para terminar o lado do NG ponto de verificação da configuração.

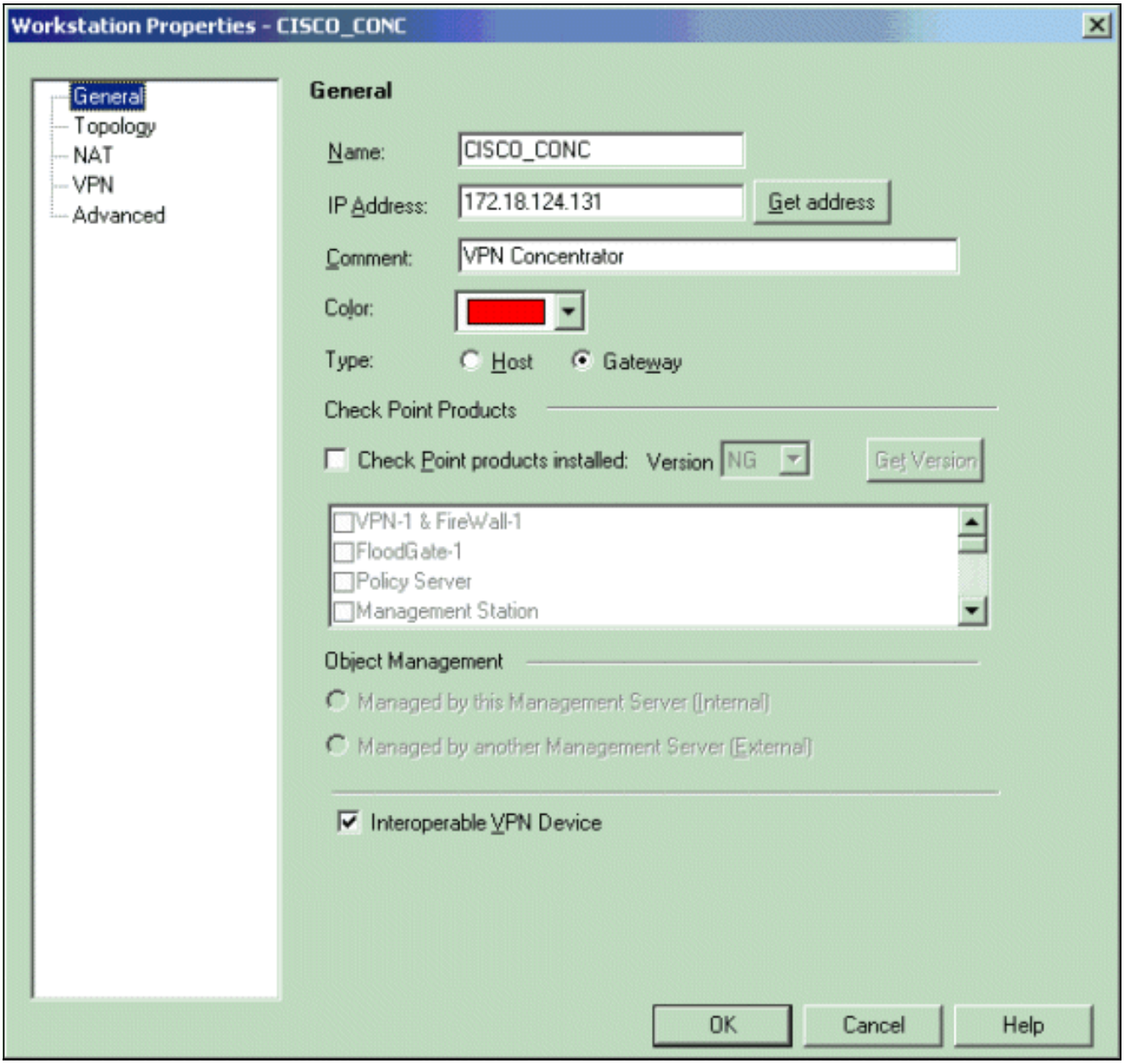
1. Crie os dois objetos de rede para a rede do NG ponto de verificação e a rede do concentrador VPN que cifrarão o tráfego interessante.a fim criar objetos, selecione **Manage > Network Objects**, a seguir selecione **New > Network**. Incorpore a informação de rede apropriada, a seguir clique a APROVAÇÃO.Estes exemplos mostram estabelecido dos objetos de rede chamados CP_inside (a rede interna do NG ponto de verificação) e CONC_INSIDE (a rede interna do concentrador VPN).



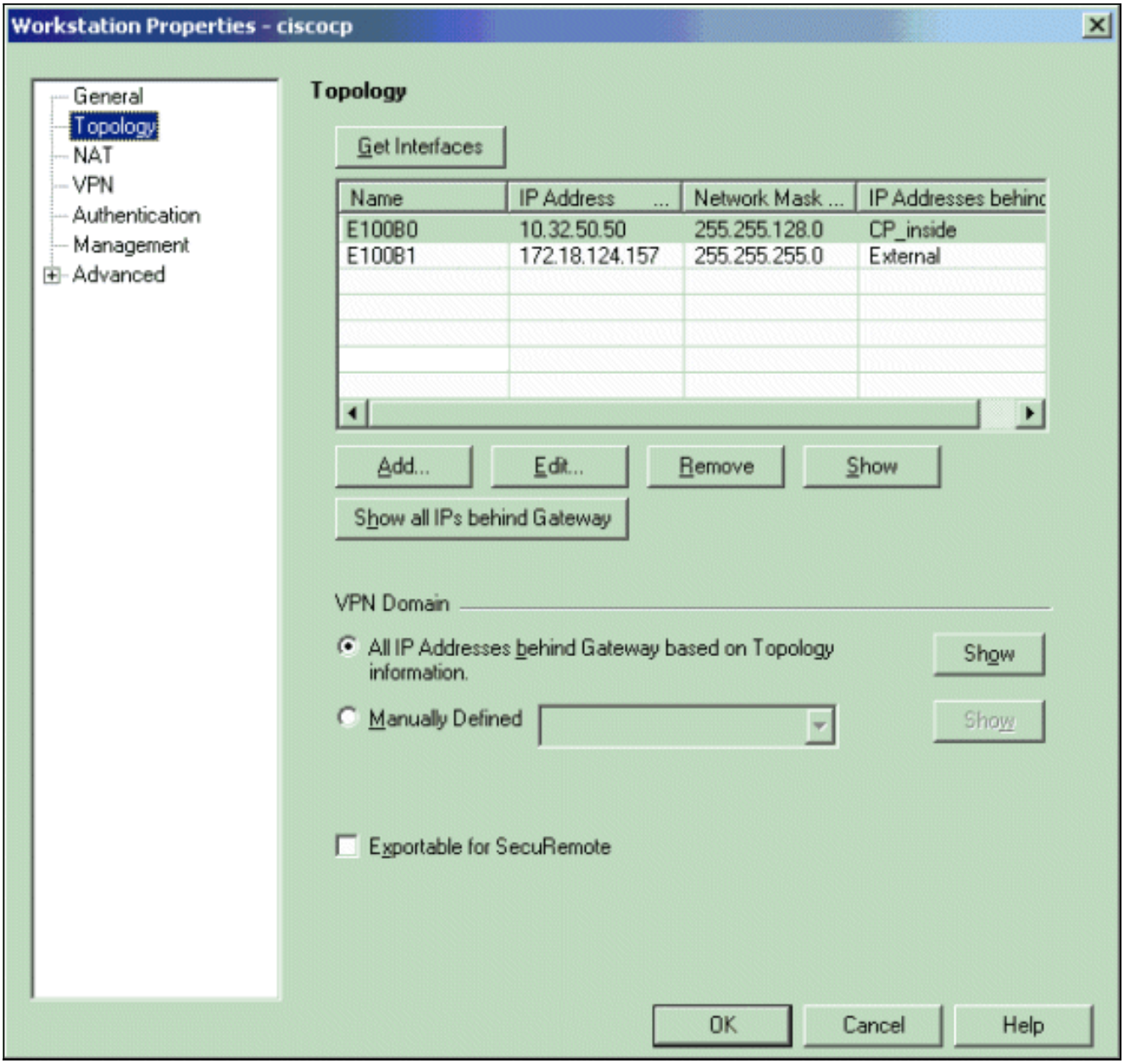


2. Vá a **Manage > Network Objects** e selecionando **New > Workstation** a fim criar objetos da estação de trabalho para os dispositivos, o NG ponto de verificação e o concentrador VPN VPN.**Note**: Você pode usar o objeto da estação de trabalho do NG ponto de verificação criado durante a instalação do ponto de verificação inicial NG. Selecione as opções para ajustar a estação de trabalho como o gateway e o dispositivo interoperáveis VPN, a seguir clique a **APROVAÇÃO**.Estes exemplos mostram estabelecido dos objetos chamados ciscocp (NG ponto de verificação) e CISCO_CONC (VPN 3000 concentrator):

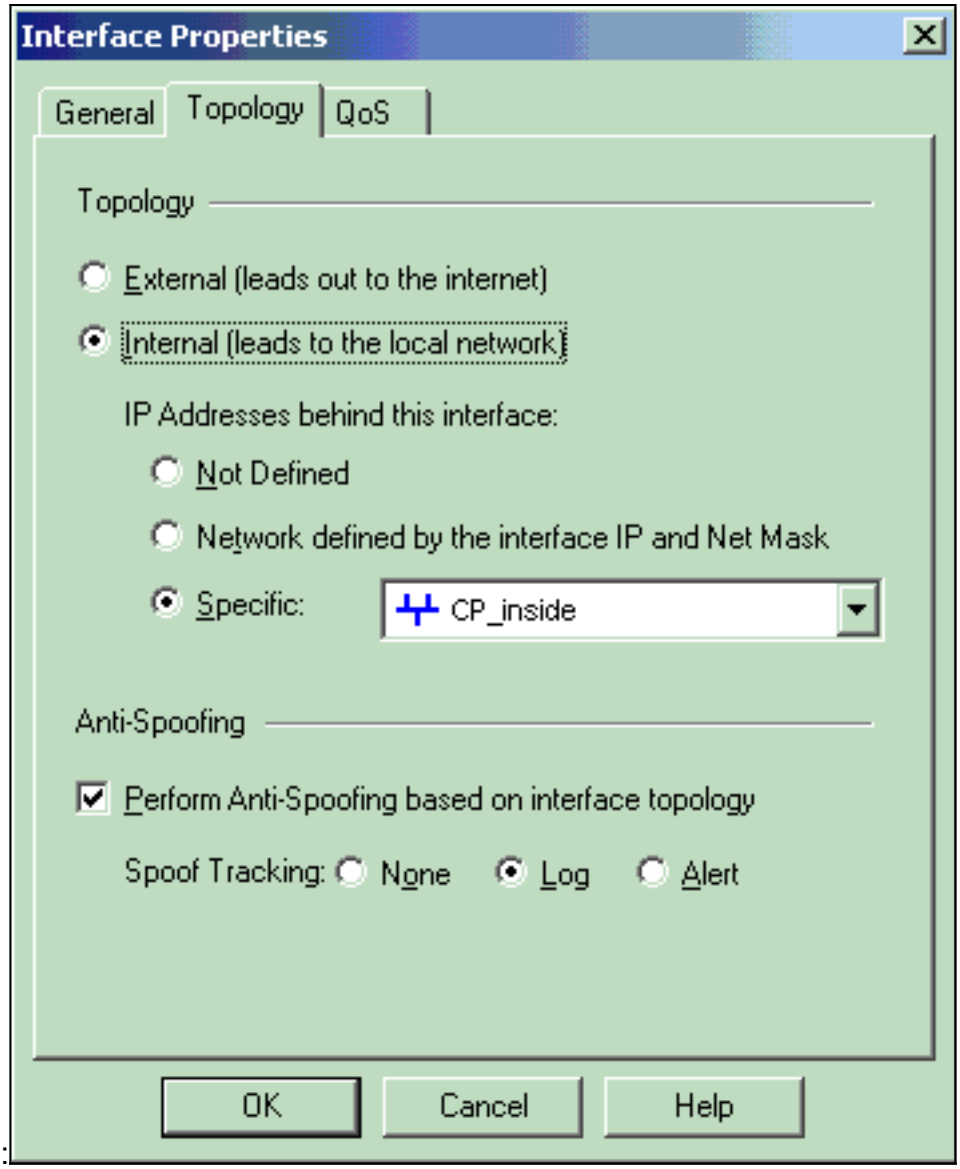

Workstation Properties - ciscocp
General
Topology
NAT
VPN
Authentication
Management
Advanced
General
Name:
ciscocp
IP Address:
172.18.124.157
Get address
Comment:
Checkpoint External IP
Color:
Type:
Host
Gateway
Check Point Products
Check Point products installed:
Version
NG
Get Version
VPN-1 & FireWall-1
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=ciscocp..pvzfoa
Interoperable VPN Device
OK
Cancel
Help



3. Vá a **Manage > Network Objects > Edit** a fim abrir a janela Propriedades de estação de trabalho para a estação de trabalho do NG ponto de verificação (ciscocp neste exemplo). Selecione a **topologia das** escolhas no lado esquerdo do indicador, a seguir selecione a rede para ser cifrado. O clique **edita** a fim ajustar as propriedades da relação.Neste exemplo, a CP_inside é a rede interna do NG ponto de verificação.

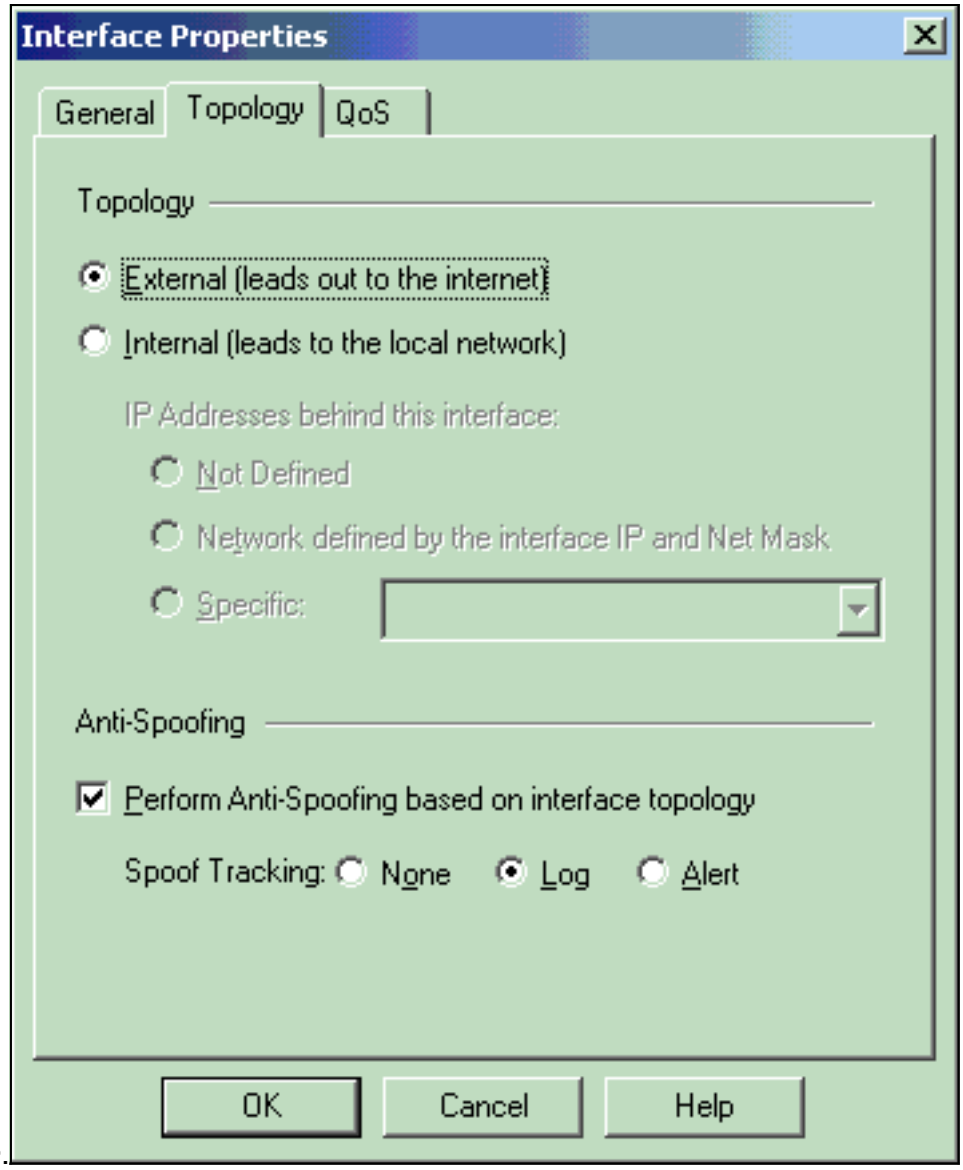


4. Na janela de propriedades da relação, selecione a opção para designar a estação de trabalho como interna, a seguir especifique o endereço IP de Um ou Mais Servidores Cisco ICM NT apropriado. Click **OK**.As seleções de topologia mostradas designam a estação de trabalho como interno e especificam endereços IP de Um ou Mais Servidores Cisco ICM NT atrás da relação da



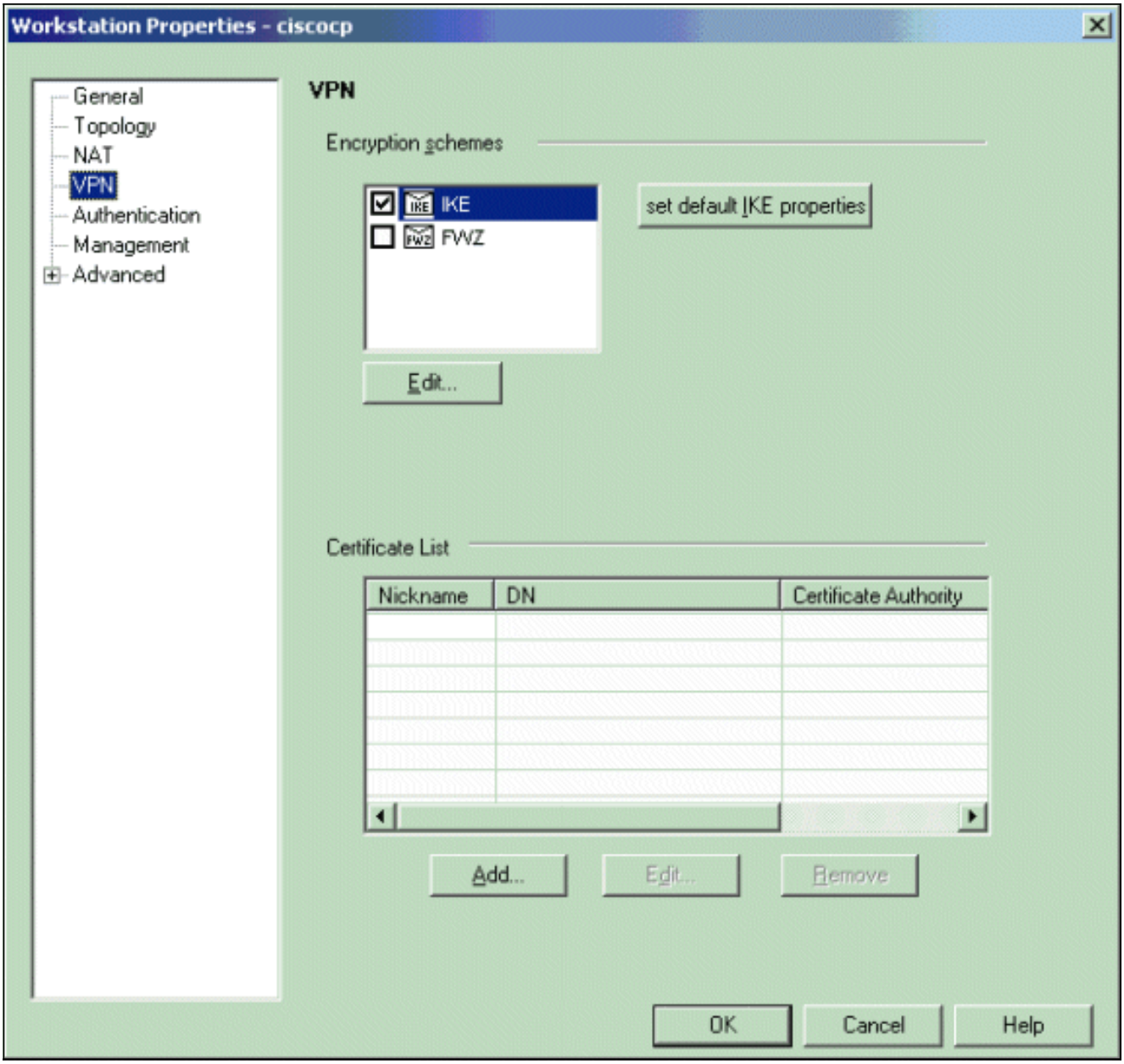
CP_inside:

5. Da janela Propriedades de estação de trabalho, selecione a interface externa no NG ponto de verificação que isso conduz para fora ao Internet, a seguir clique-a **editam** a fim ajustar as propriedades da relação. Selecione a opção para designar a topologia como externo, a seguir clique a

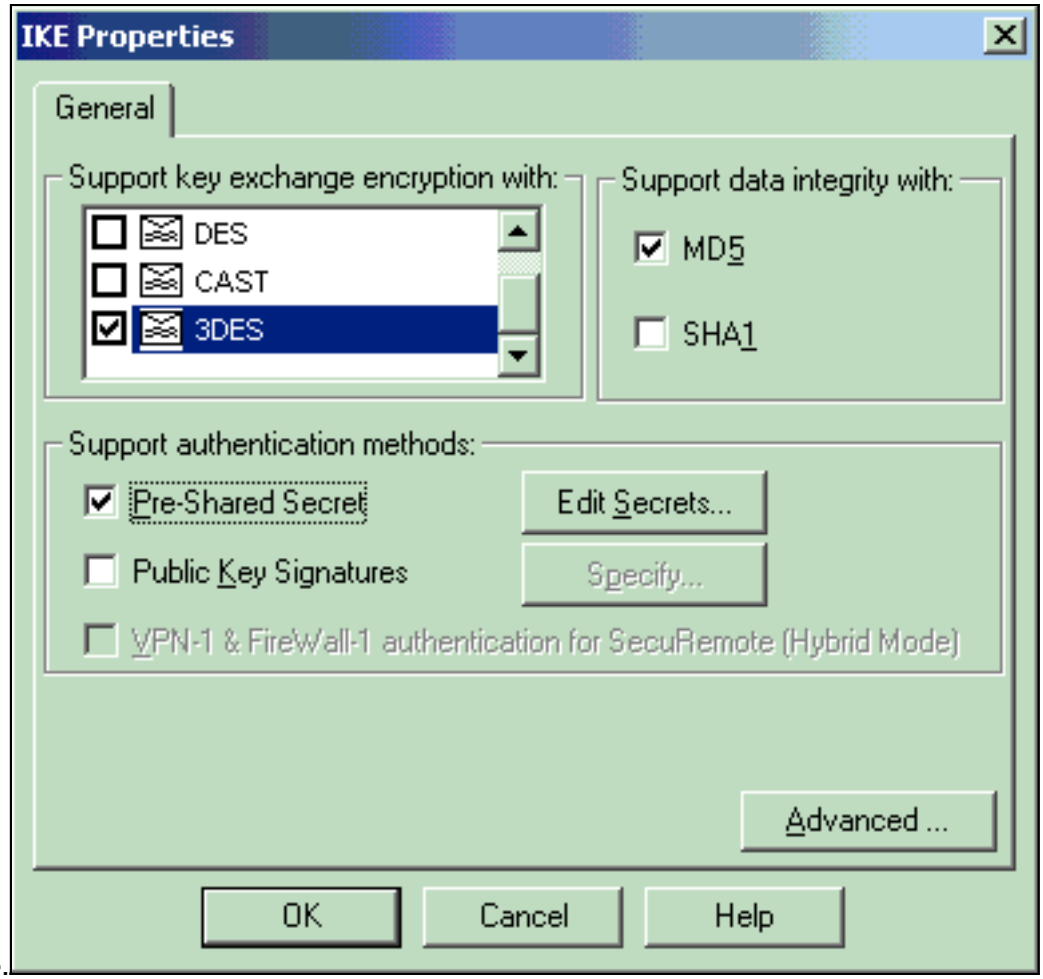


APROVAÇÃO.

6. Da janela Propriedades de estação de trabalho no NG ponto de verificação, o **VPN** seleto das escolhas no lado esquerdo do indicador, seleciona então os parâmetros IKE para criptografia e os algoritmos de autenticação. O clique **edita** a fim configurar as propriedades IKE.

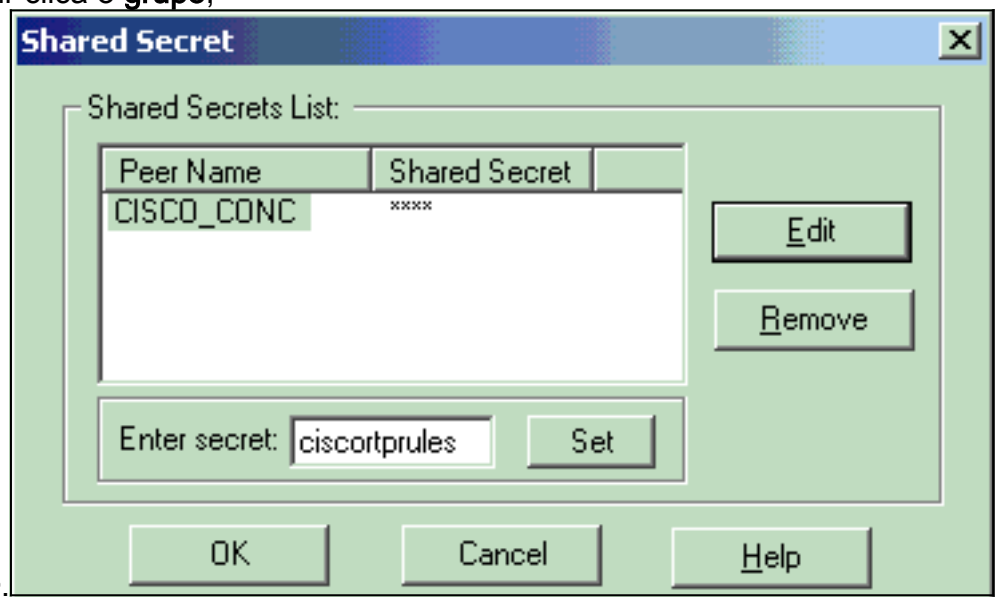


7. Ajuste as propriedades IKE para combinar as propriedades no concentrador VPN.Neste exemplo, selecione a opção de criptografia para o **3DES** e a opção do hashing para o



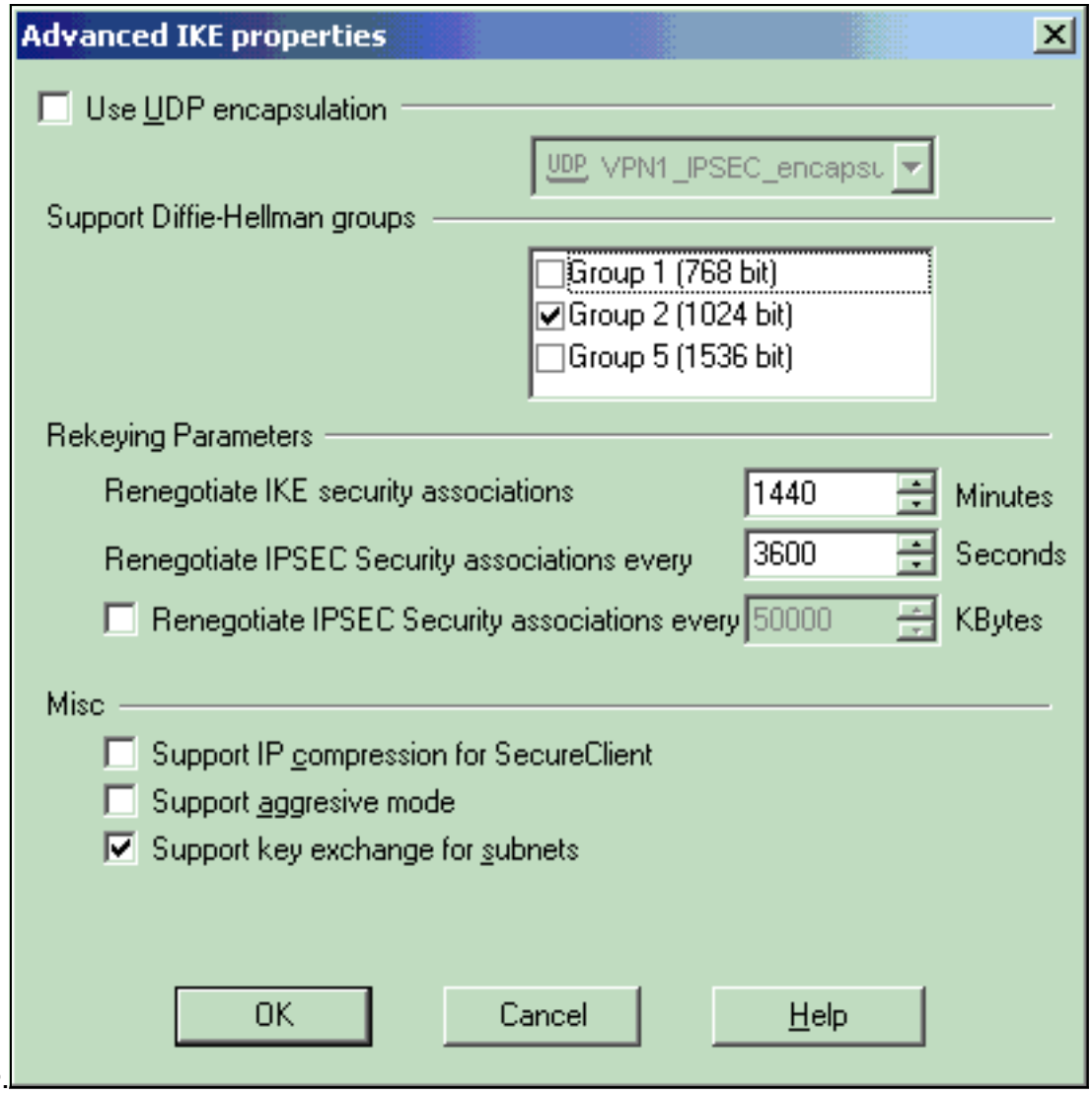
MD5.

8. Selecione a opção de autenticação para **segredos pré-compartilhados**, a seguir clique-a **editam segredos** para ajustar a chave pré-compartilhada para ser compatível com a chave pré-compartilhada no concentrador VPN. O clique **edita** a fim incorporar como mostrado sua chave, a seguir clica o **grupo**,



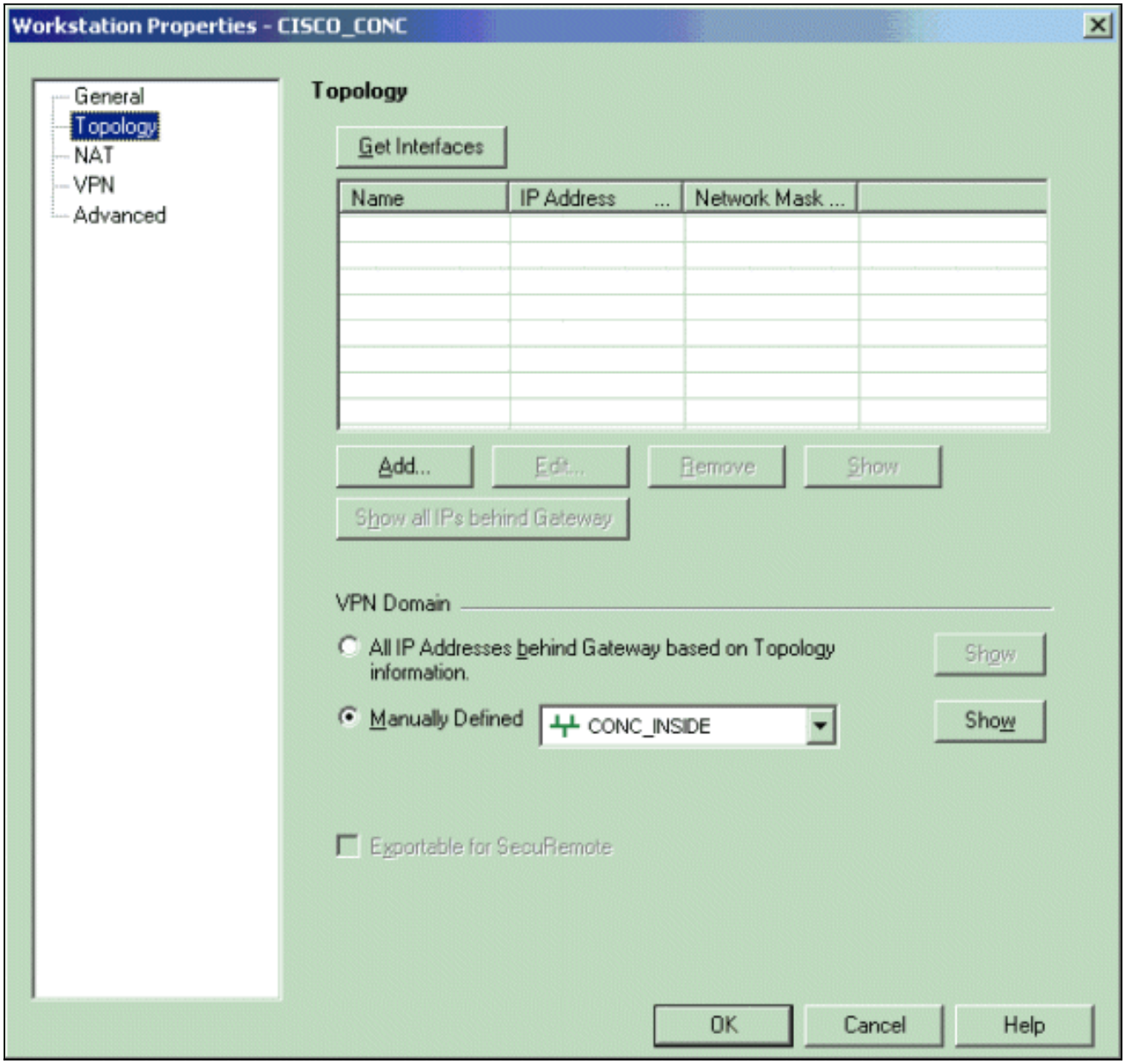
APROVAÇÃO.

9. Do indicador das propriedades IKE, clique **avançado…** e mude estes ajustes:Deselect a opção para o **modo assertivo de suporte**.Selecione a opção para **trocas de chave do apoio para sub-redes**.Quando você for terminado, **APROVAÇÃO do** clique,

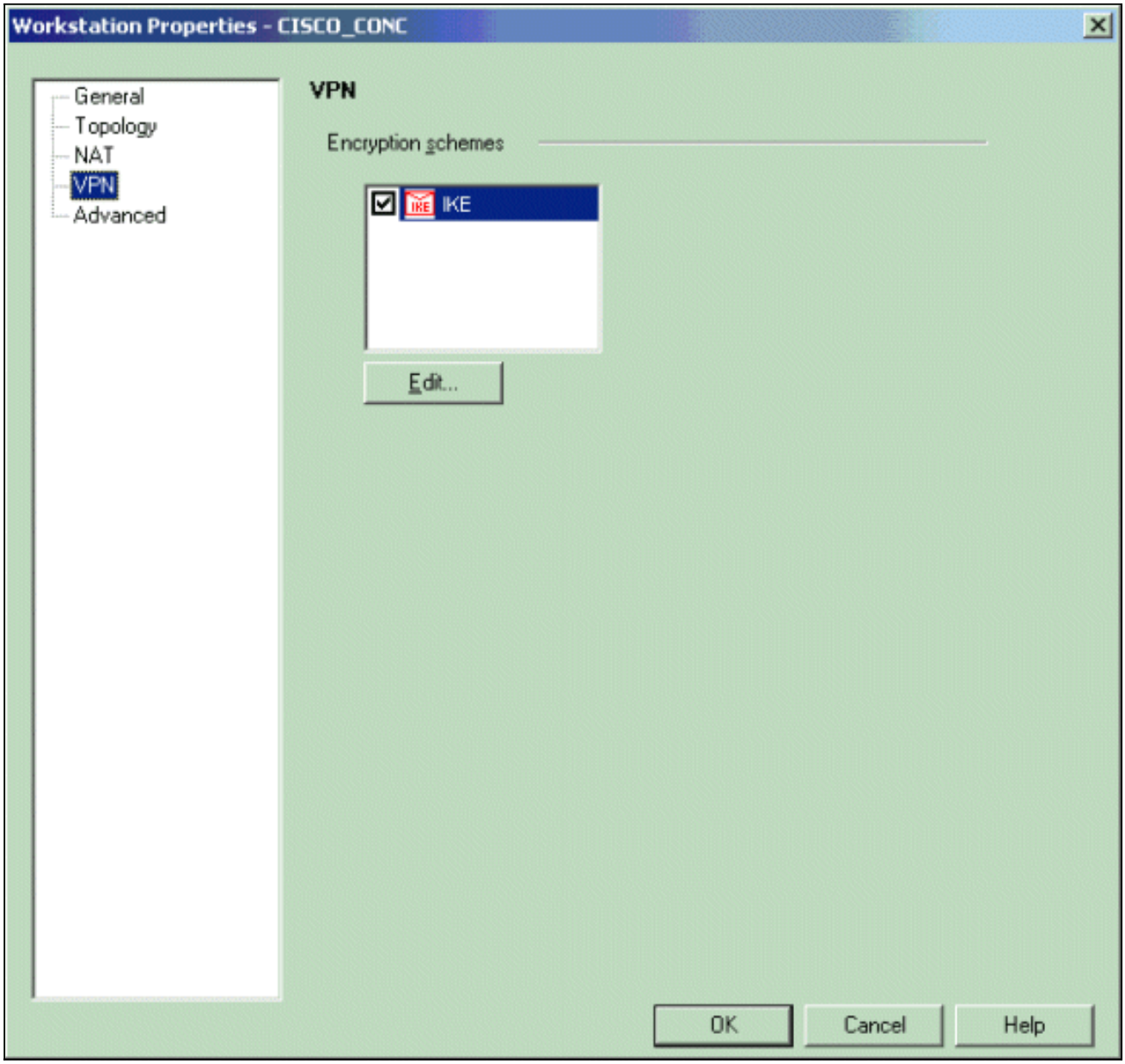


APROVAÇÃO.

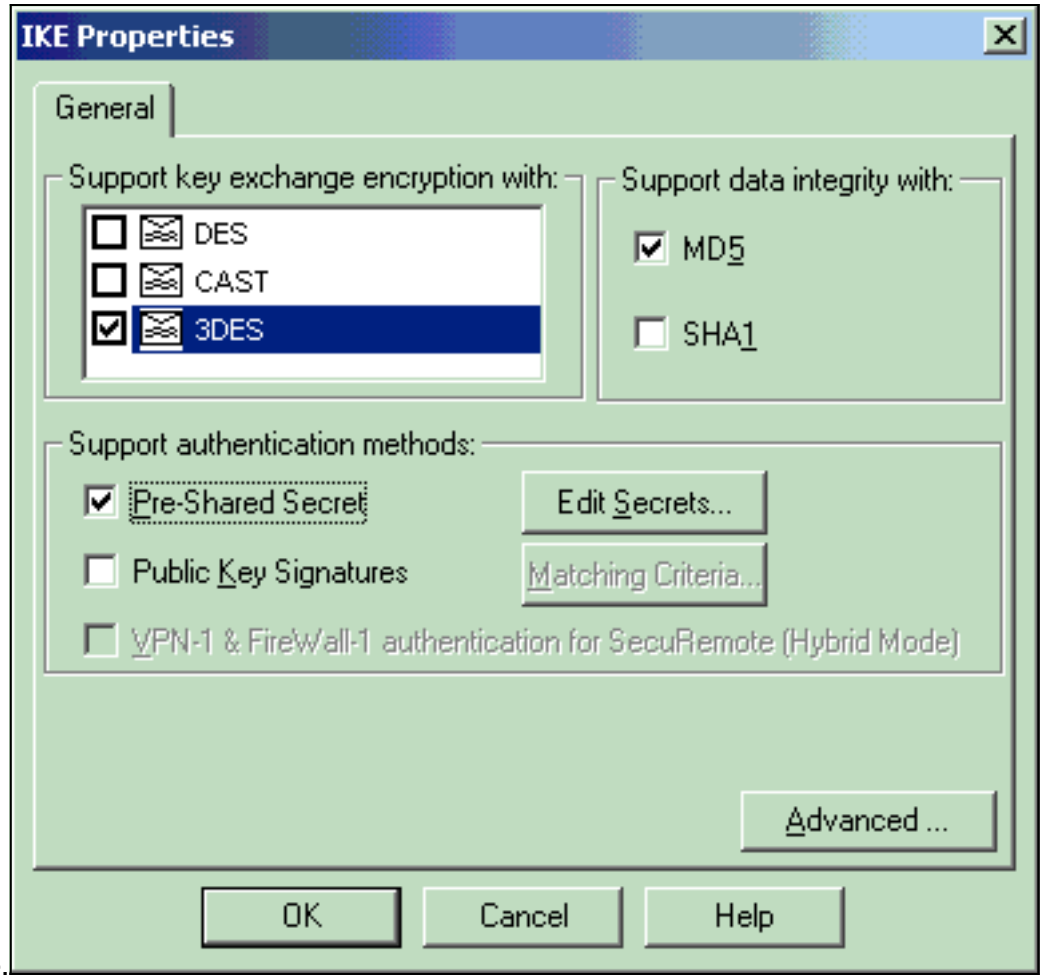
10. Vá a **Manage > Network Objects > Edit** a fim abrir a janela Propriedades de estação de trabalho para o concentrador VPN. **Topologia** seleta das escolhas no lado esquerdo do indicador a fim definir manualmente o domínio de VPN.Neste exemplo, o CONC_INSIDE (a rede interna do concentrador VPN) é definido como o domínio de VPN.



11. **O VPN** seleto das escolhas no lado esquerdo do indicador, seleciona então o **IKE** como o esquema de criptografia. O clique **edita** a fim configurar as propriedades IKE.

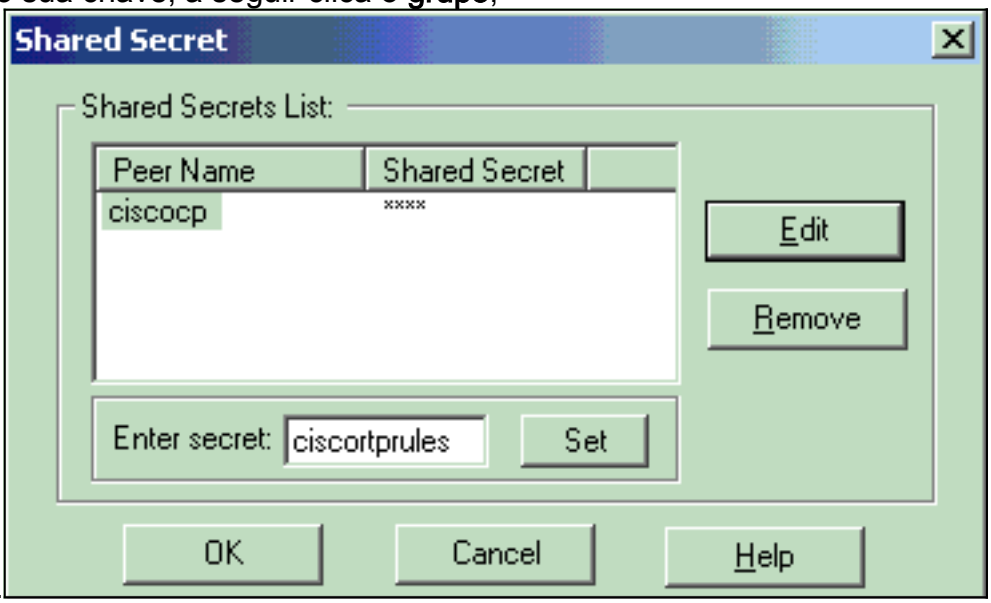


12. Ajuste as propriedades IKE para refletir a configuração atual no concentrador VPN.Neste exemplo, ajuste a opção de criptografia para o **3DES** e a opção do hashing para o



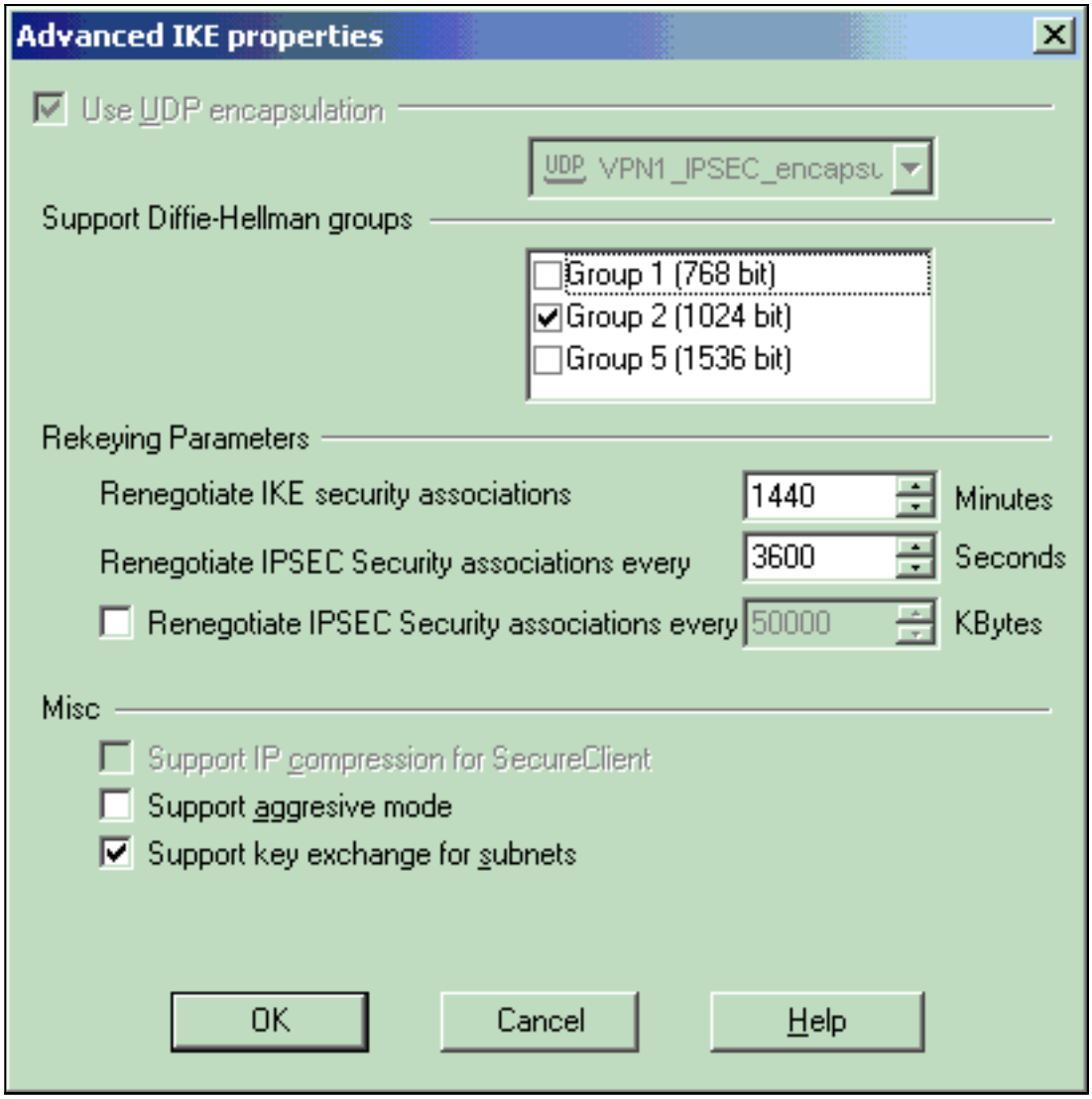
MD5.

13. Selecione a opção de autenticação para **segredos pré-compartilhados**, a seguir clique-a **editam segredos** a fim ajustar a chave pré-compartilhada. O clique **edita** a fim incorporar como mostrado sua chave, a seguir clica o **grupo**,

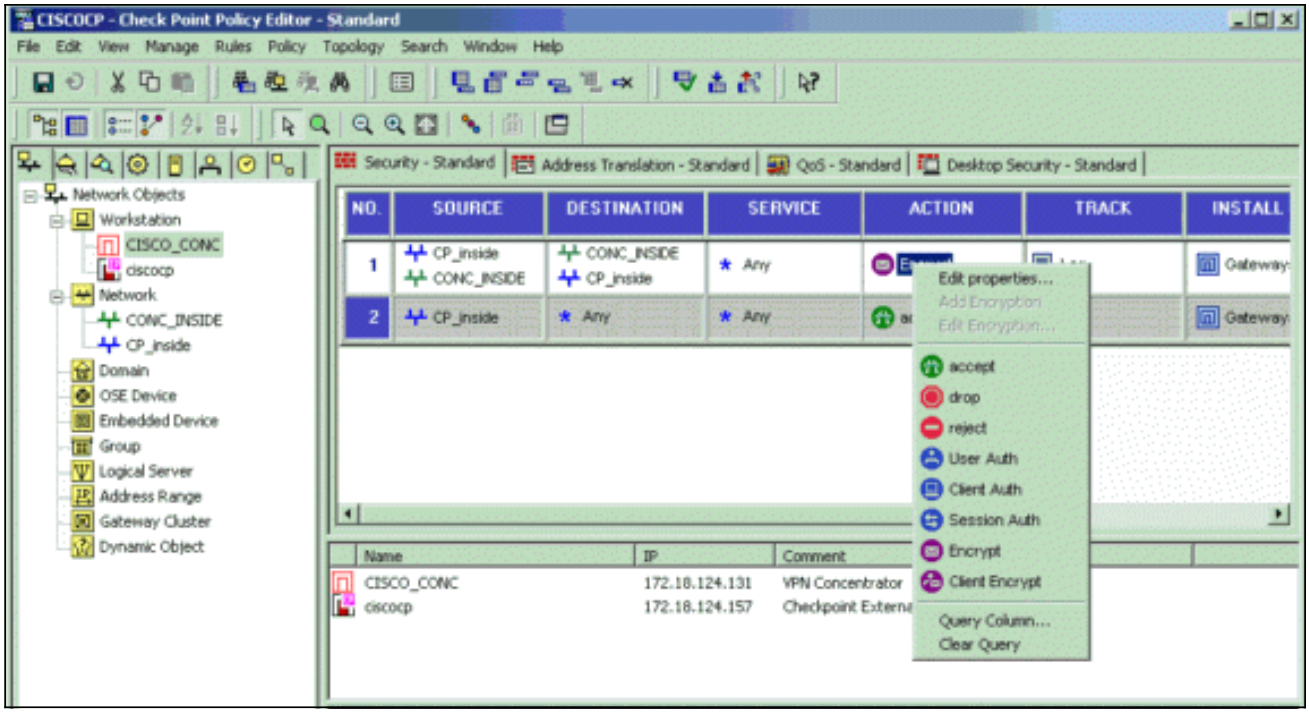


APROVAÇÃO.

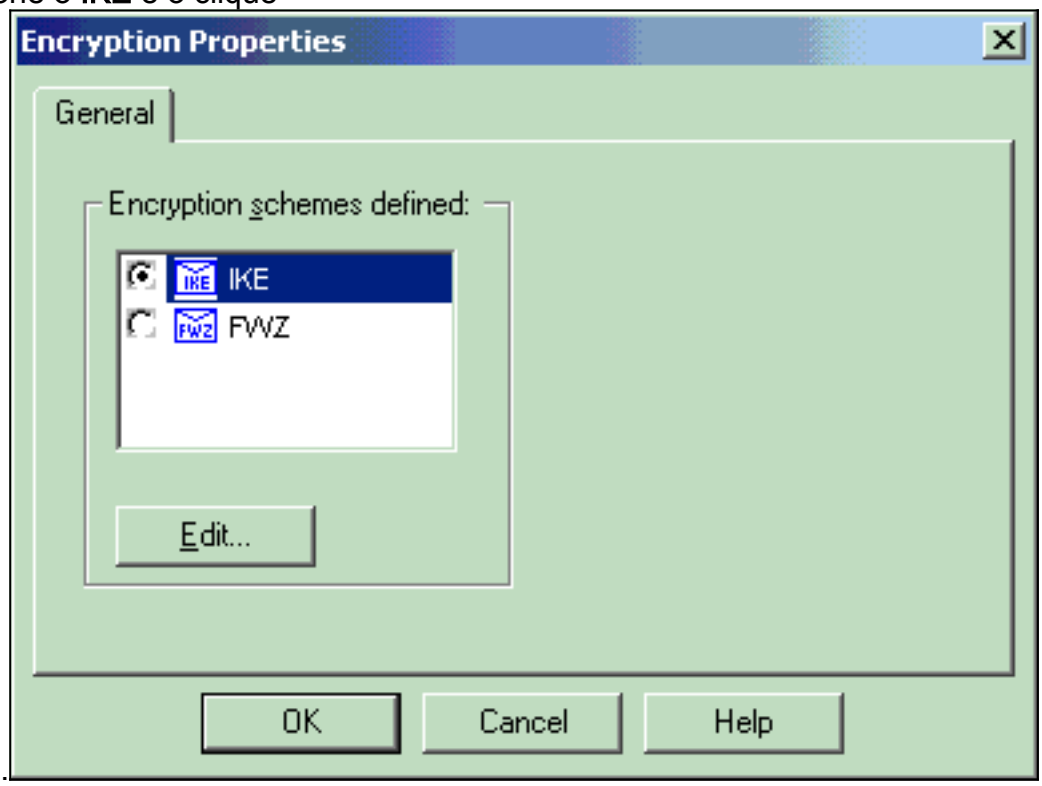
14. Do indicador das propriedades IKE, clique **avançado…** e mude estes ajustes:Selecione o grupo Diffie-Hellman apropriado para as propriedades IKE.Deselect a opção para o **modo assertivo de suporte**.Selecione a opção para **trocas de chave do apoio para sub-redes**.Quando você for terminado, **APROVAÇÃO do** clique, **APROVAÇÃO**.



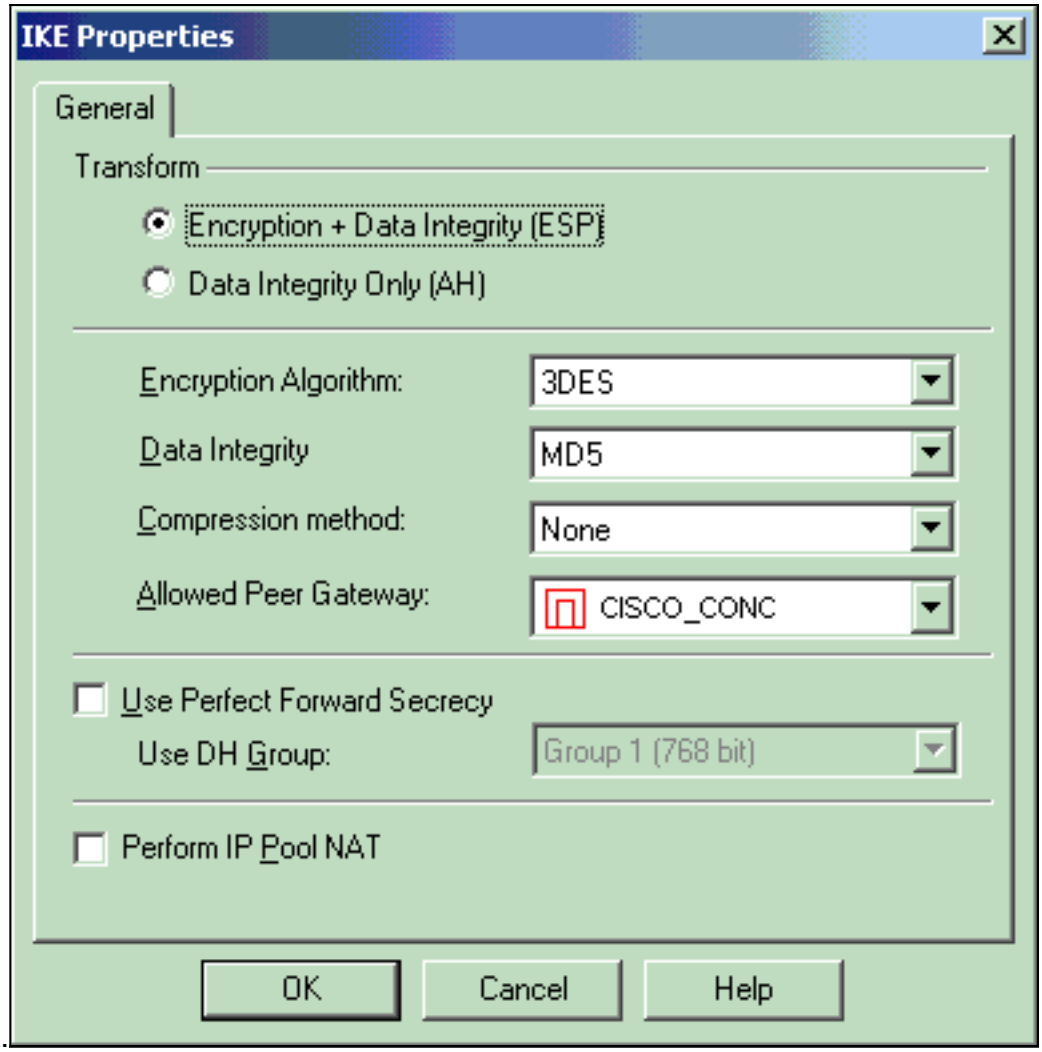
15. Selecione o **Regras > Adicionar Regras > Parte Superior** a fim configurar as regras de criptografia para a política. Na janela de editor de política, introduza uma regra com fonte como a CP_inside (rede interna do NG ponto de verificação) e o destino como CONC_INSIDE (rede interna do concentrador VPN). Os valores determinados para o **serviço = alguns**, **ação = cifram**, e **trilha = log**. Quando você adicionou a seção da ação da criptografia da regra, clicar com o botão direito a **ação** e selecione-a **Edit Properties**.



16. Selecione o **IKE** e o clique **editam**.

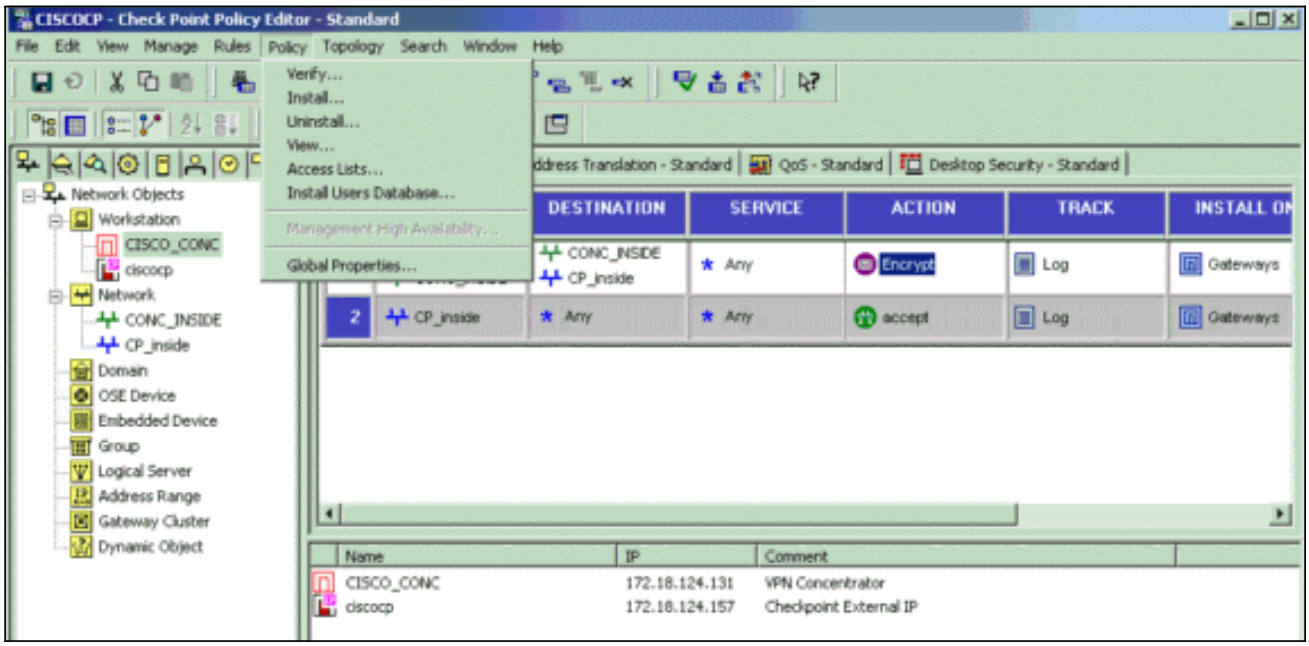


17. No indicador das propriedades IKE, mude as propriedades para concordar com o concentrador VPN transformam.Ajuste a opção da transformação ao **Encryption + Data Integrity (ESP)**.Ajuste o algoritmo de criptografia ao **3DES**.Ajuste a integridade de dados ao **MD5**.Ajuste o gateway de peer permitido para combinar o concentrador VPN (CISCO_CONC).Quando terminar, clique em

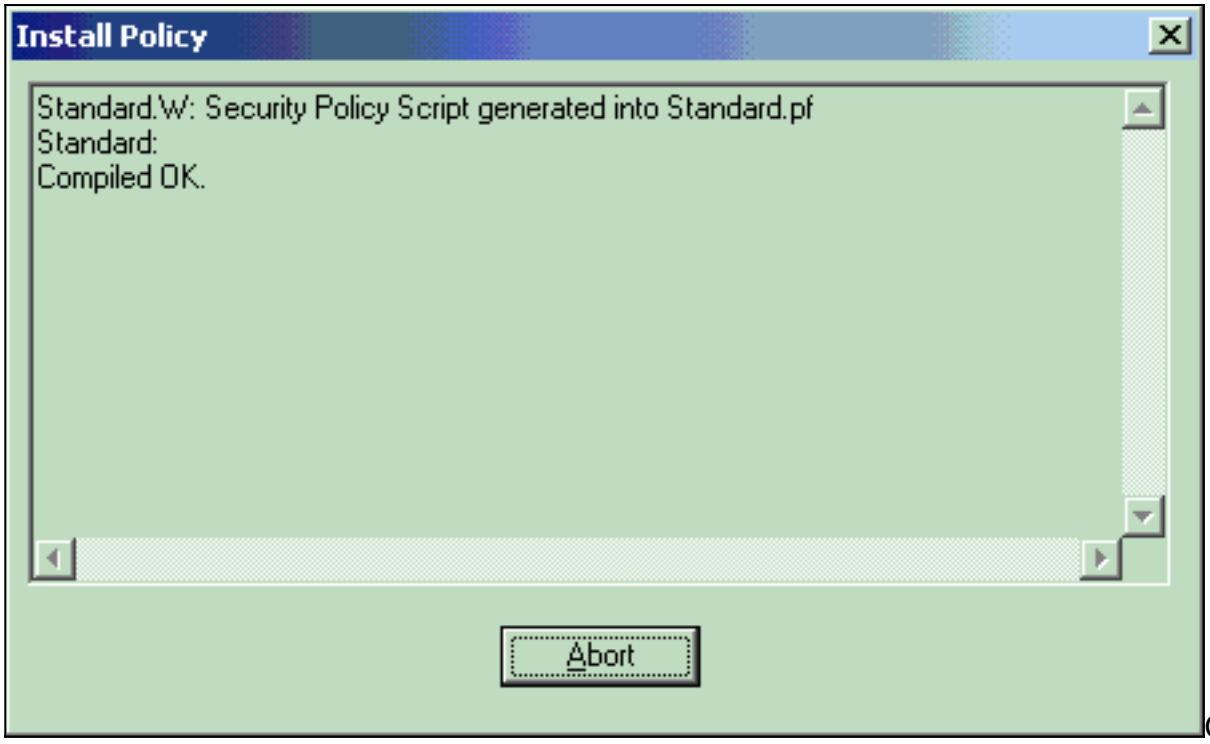


OK.

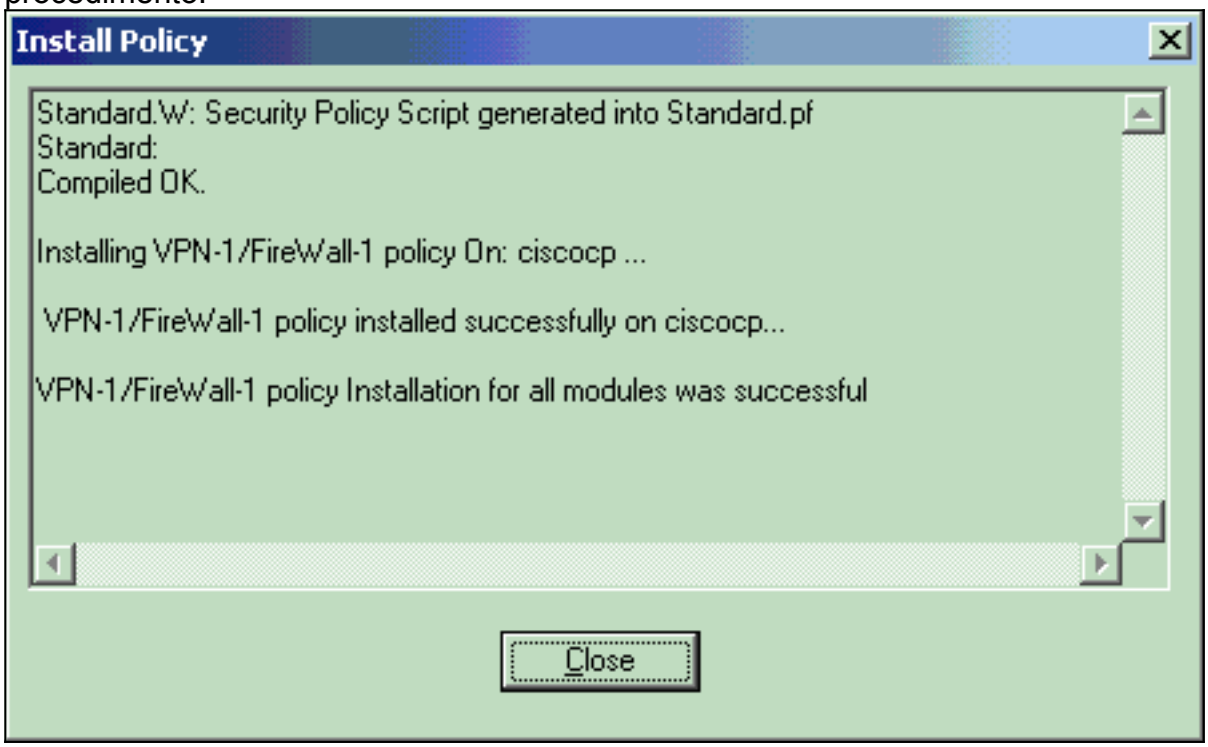
18. Depois que o NG ponto de verificação é configurado, salvar a política e a **política** seleta **> instala** a fim permiti-
la.



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



Quando a janela de instalação indicar que a instalação de política está completa, clique **próximo** a fim terminar o procedimento.

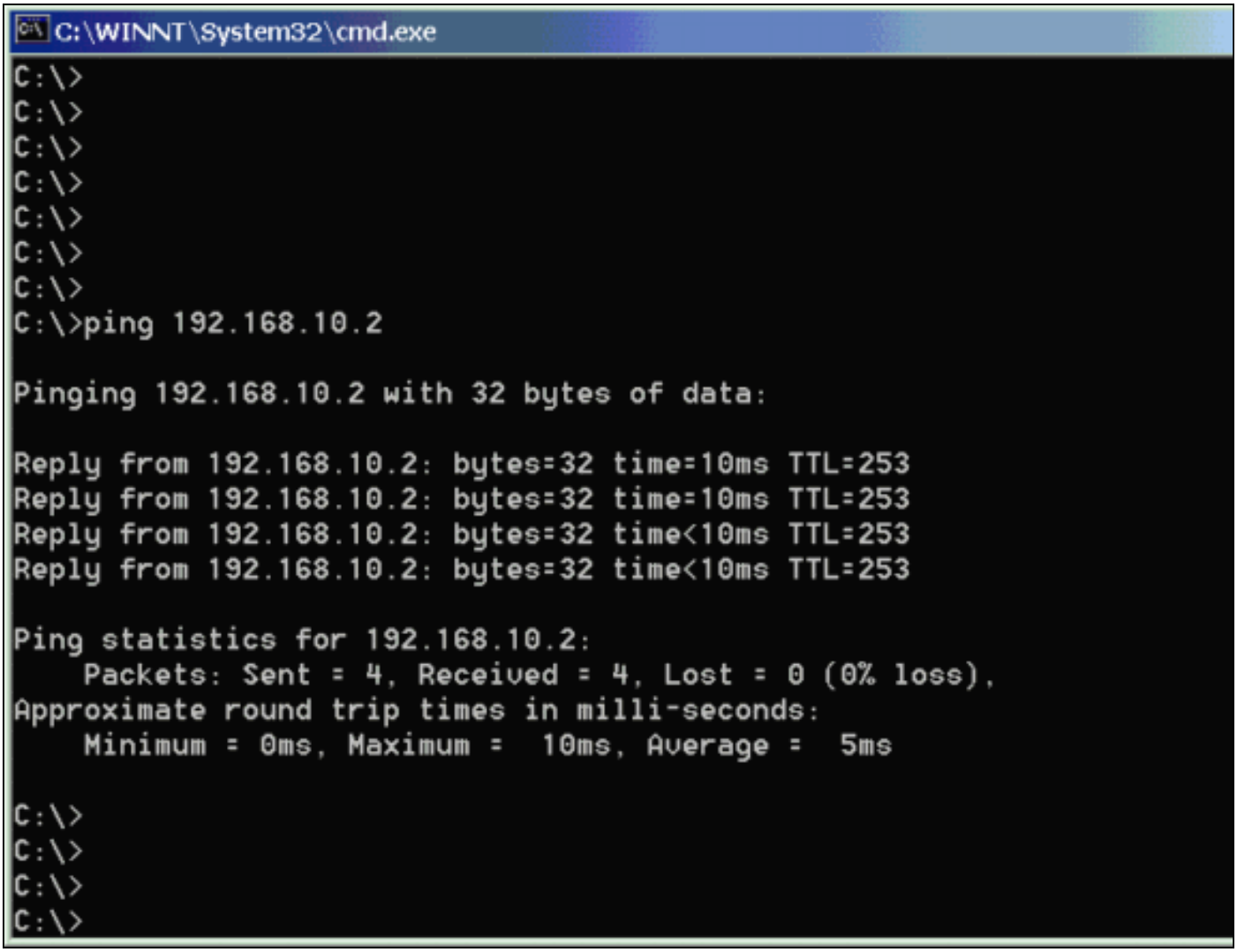


Verificar

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

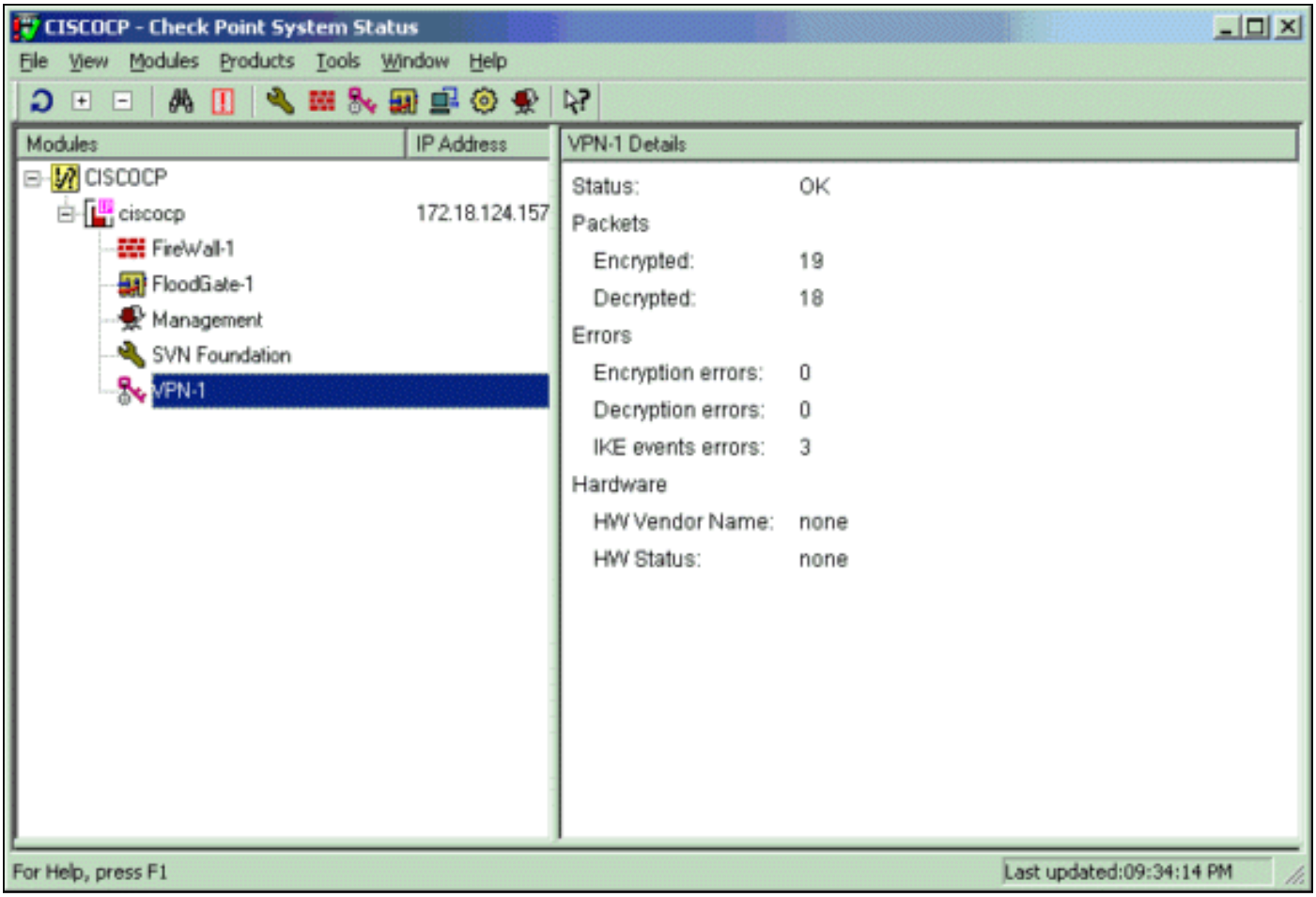
Verifique a comunicação de rede

A fim testar uma comunicação entre as duas redes privadas, você pode iniciar um sibilo de uma das redes privadas à outra rede privada. Nesta configuração, um sibilo foi enviado do lado do NG ponto de verificação (10.32.50.51) à rede do concentrador VPN (192.168.10.2).



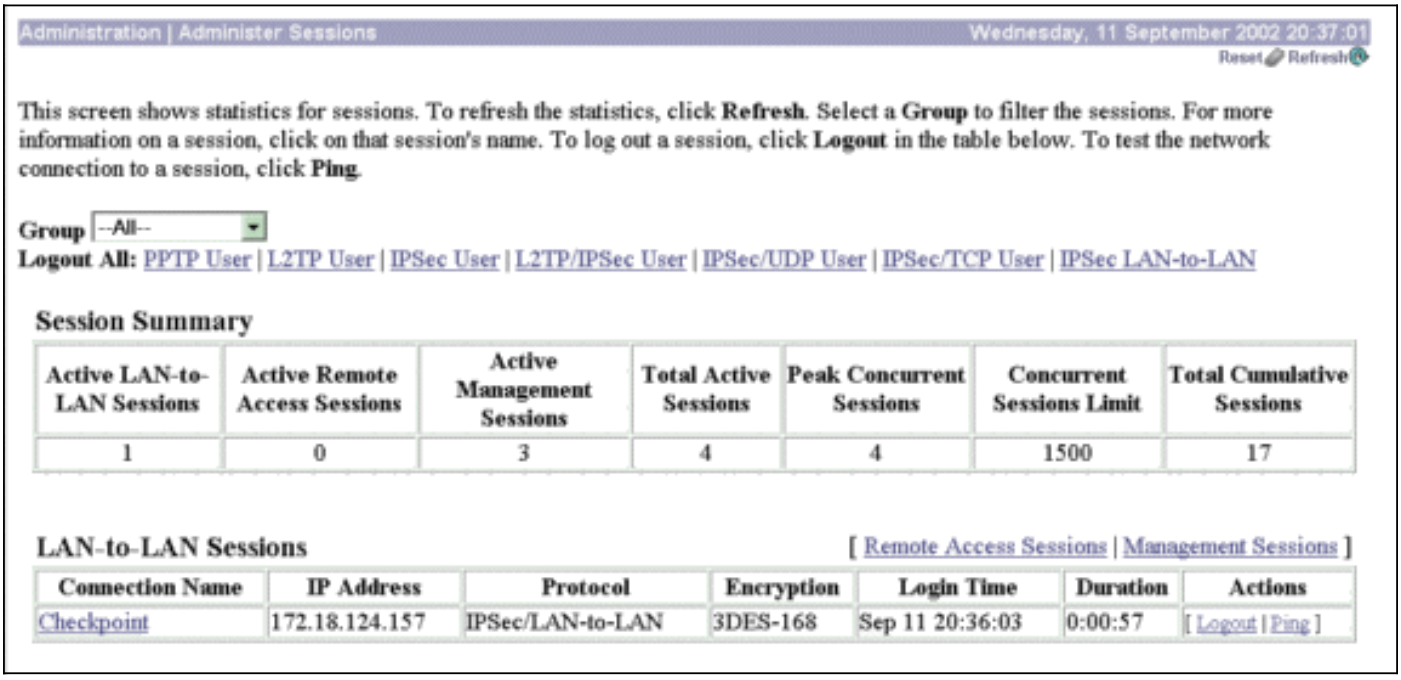
Status de túnel da vista no NG ponto de verificação

A fim ver o status de túnel, vá ao editor de política e selecione o **Janela > Status de Sistema**.

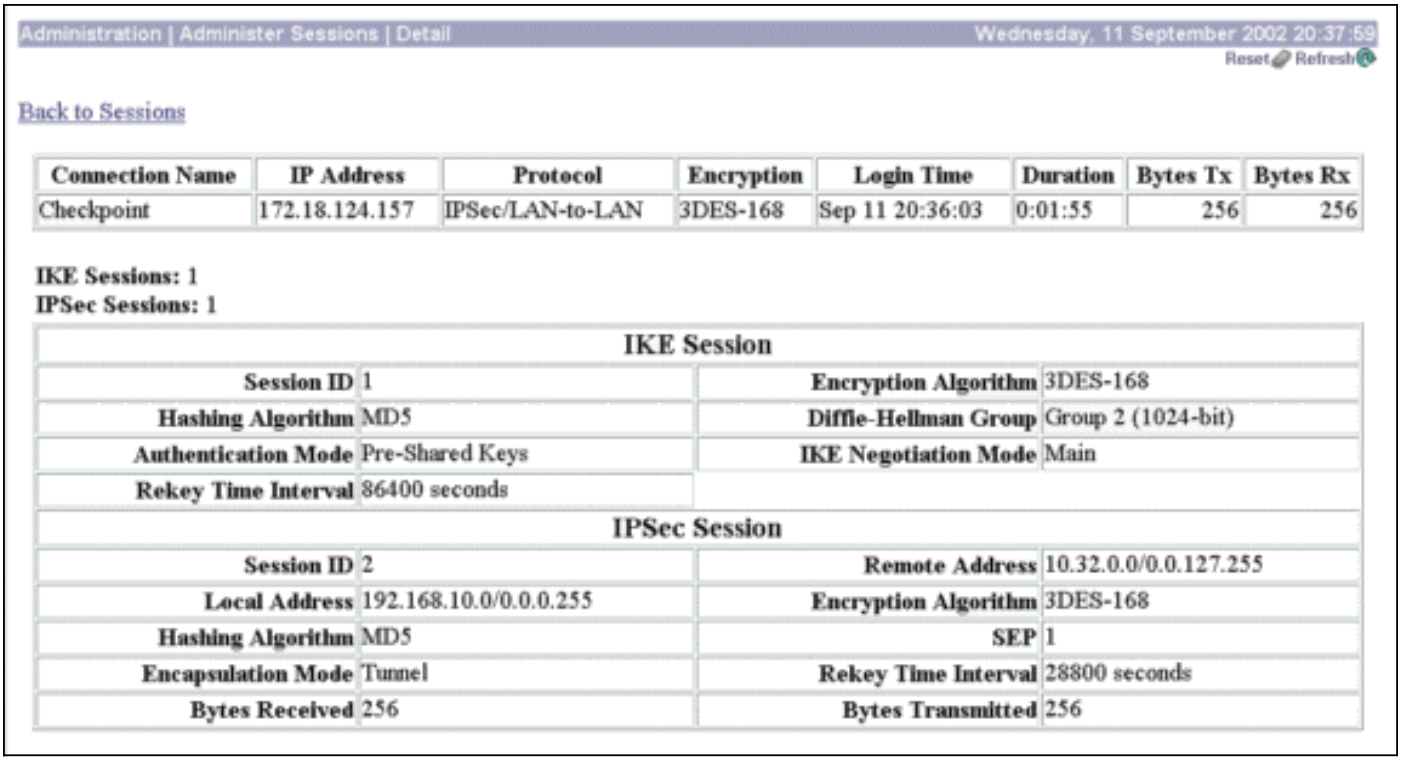


Veja o status de túnel no concentrador VPN

A fim verificar o status de túnel no concentrador VPN, vá ao **administração > sessões de administrador**.



Sob sessões de LAN a LAN, selecione o nome de conexão para que o ponto de verificação ver detalhes nos SA criados e o número de pacotes transmitidos/recebidos.



Administration | Administer Sessions | Detail — Wednesday, 11 September 2002 20:37:59

Reset Refresh

Back to Sessions

Connection Name	IP Address	Protocol	Encryption	Login Time	Duration	Bytes Tx	Bytes Rx
Checkpoint	172.18.124.157	IPSec/LAN-to-LAN	3DES-168	Sep 11 20:36:03	0:01:55	256	256

IKE Sessions: 1
IPSec Sessions: 1

IKE Session			
Session ID	1	**Encryption Algorithm**	3DES-168
Hashing Algorithm	MD5	**Diffie-Hellman Group**	Group 2 (1024-bit)
Authentication Mode	Pre-Shared Keys	**IKE Negotiation Mode**	Main
Rekey Time Interval	86400 seconds		
IPSec Session			
Session ID	2	**Remote Address**	10.32.0.0/0.0.127.255
Local Address	192.168.10.0/0.0.0.255	**Encryption Algorithm**	3DES-168
Hashing Algorithm	MD5	**SEP**	1
Encapsulation Mode	Tunnel	**Rekey Time Interval**	28800 seconds
Bytes Received	256	**Bytes Transmitted**	256

Troubleshooting

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

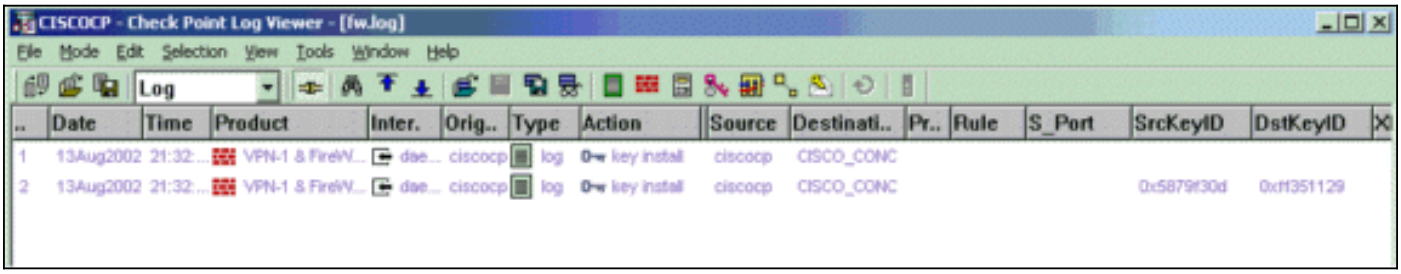
Note: O tráfego não deve ser PATed através do túnel de IPsec usando o endereço IP público do concentrador VPN (interface externa). Se não, o túnel falha. Assim, o endereço IP de Um ou Mais Servidores Cisco ICM NT usado para PATing deve ser um endereço a não ser o endereço configurado na interface externa.

Sumarização da rede

Quando o múltiplo adjacente, redes internas é configurado no domínio da criptografia no ponto de verificação, o dispositivo pode automaticamente resumir as redes 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, estas redes podem ser resumidas a 10.0.0.0 /23.

Depurações para ponto de controle NG

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



Debugs para concentrador de VPN

A fim permitir debuga no concentrador VPN, vão ao **configuração > sistema > eventos > classes**. Permita o AUTH, o AUTHDBG, o IKE, o IKEDBG, o IPSEC, e o IPSECDBG para que a severidade registre como 1 - 13. A fim ver debuga, selecionam a **monitoração > o log filtrável de eventos**.

```
1 09/11/2002 20:36:03.610 SEV=8 IKEDBG/0 RPT=506 172.18.124.157
RECEIVED Message (msgid=0) with payloads :
HDR + SA (1) + VENDOR (13) + NONE (0) ... total length : 128

3 09/11/2002 20:36:03.610 SEV=9 IKEDBG/0 RPT=507 172.18.124.157
processing SA payload

4 09/11/2002 20:36:03.610 SEV=8 IKEDBG/0 RPT=508
Proposal # 1, Transform # 1, Type ISAKMP, Id IKE
Parsing received transform:
Phase 1 failure against global IKE proposal # 1:
Mismatched attr types for class Auth Method:
Rcv'd: Preshared Key
Cfg'd: XAUTH with Preshared Key (Initiator authenticated)

10 09/11/2002 20:36:03.610 SEV=8 IKEDBG/0 RPT=509
Phase 1 failure against global IKE proposal # 2:
Mismatched attr types for class DH Group:
Rcv'd: Oakley Group 2
Cfg'd: Oakley Group 1

13 09/11/2002 20:36:03.610 SEV=7 IKEDBG/0 RPT=510 172.18.124.157
Oakley proposal is acceptable

14 09/11/2002 20:36:03.610 SEV=9 IKEDBG/47 RPT=9 172.18.124.157
processing VID payload

15 09/11/2002 20:36:03.610 SEV=9 IKEDBG/0 RPT=511 172.18.124.157
processing IKE SA

16 09/11/2002 20:36:03.610 SEV=8 IKEDBG/0 RPT=512
Proposal # 1, Transform # 1, Type ISAKMP, Id IKE
Parsing received transform:
Phase 1 failure against global IKE proposal # 1:
Mismatched attr types for class Auth Method:
Rcv'd: Preshared Key
Cfg'd: XAUTH with Preshared Key (Initiator authenticated)

22 09/11/2002 20:36:03.610 SEV=8 IKEDBG/0 RPT=513
Phase 1 failure against global IKE proposal # 2:
Mismatched attr types for class DH Group:
Rcv'd: Oakley Group 2
Cfg'd: Oakley Group 1

25 09/11/2002 20:36:03.610 SEV=7 IKEDBG/28 RPT=9 172.18.124.157
IKE SA Proposal # 1, Transform # 1 acceptable
Matches global IKE entry # 3

26 09/11/2002 20:36:03.610 SEV=9 IKEDBG/0 RPT=514 172.18.124.157
constructing ISA_SA for isakmp

27 09/11/2002 20:36:03.610 SEV=8 IKEDBG/0 RPT=515 172.18.124.157
SENDING Message (msgid=0) with payloads :
HDR + SA (1) + NONE (0) ... total length : 84

29 09/11/2002 20:36:03.630 SEV=8 IKEDBG/0 RPT=516 172.18.124.157
```

```
RECEIVED Message (msgid=0) with payloads :
HDR + KE (4) + NONCE (10) + NONE (0) ... total length : 184

31 09/11/2002 20:36:03.630 SEV=8 IKEDBG/0 RPT=517 172.18.124.157
RECEIVED Message (msgid=0) with payloads :
HDR + KE (4) + NONCE (10) + NONE (0) ... total length : 184

33 09/11/2002 20:36:03.630 SEV=9 IKEDBG/0 RPT=518 172.18.124.157
processing ke payload

34 09/11/2002 20:36:03.630 SEV=9 IKEDBG/0 RPT=519 172.18.124.157
processing ISA_KE

35 09/11/2002 20:36:03.630 SEV=9 IKEDBG/1 RPT=91 172.18.124.157
processing nonce payload

36 09/11/2002 20:36:03.660 SEV=9 IKEDBG/0 RPT=520 172.18.124.157
constructing ke payload

37 09/11/2002 20:36:03.660 SEV=9 IKEDBG/1 RPT=92 172.18.124.157
constructing nonce payload

38 09/11/2002 20:36:03.660 SEV=9 IKEDBG/46 RPT=37 172.18.124.157
constructing Cisco Unity VID payload

39 09/11/2002 20:36:03.660 SEV=9 IKEDBG/46 RPT=38 172.18.124.157
constructing xauth V6 VID payload

40 09/11/2002 20:36:03.660 SEV=9 IKEDBG/48 RPT=19 172.18.124.157
Send IOS VID

41 09/11/2002 20:36:03.660 SEV=9 IKEDBG/38 RPT=10 172.18.124.157
Constructing VPN 3000 spoofing IOS Vendor ID payload (version: 1.0.0,
capabilities: 20000001)

43 09/11/2002 20:36:03.660 SEV=9 IKEDBG/46 RPT=39 172.18.124.157
constructing VID payload

44 09/11/2002 20:36:03.660 SEV=9 IKEDBG/48 RPT=20 172.18.124.157
Send Altiga GW VID

45 09/11/2002 20:36:03.660 SEV=9 IKEDBG/0 RPT=521 172.18.124.157
Generating keys for Responder...

46 09/11/2002 20:36:03.670 SEV=8 IKEDBG/0 RPT=522 172.18.124.157
SENDING Message (msgid=0) with payloads :
HDR + KE (4) + NONCE (10) ... total length : 256

48 09/11/2002 20:36:03.690 SEV=8 IKEDBG/0 RPT=523 172.18.124.157
RECEIVED Message (msgid=0) with payloads :
HDR + ID (5) + HASH (8) + NONE (0) ... total length : 60

50 09/11/2002 20:36:03.690 SEV=9 IKEDBG/1 RPT=93 172.18.124.157
Group [172.18.124.157]
Processing ID

51 09/11/2002 20:36:03.690 SEV=9 IKEDBG/0 RPT=524 172.18.124.157
Group [172.18.124.157]
processing hash

52 09/11/2002 20:36:03.690 SEV=9 IKEDBG/0 RPT=525 172.18.124.157
Group [172.18.124.157]
computing hash
```

```
53 09/11/2002 20:36:03.690 SEV=9 IKEDBG/23 RPT=10 172.18.124.157
Group [172.18.124.157]
Starting group lookup for peer 172.18.124.157

54 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/1 RPT=10
AUTH_Open() returns 9

55 09/11/2002 20:36:03.690 SEV=7 AUTH/12 RPT=10
Authentication session opened: handle = 9

56 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/3 RPT=10
AUTH_PutAttrTable(9, 748174)

57 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/6 RPT=10
AUTH_GroupAuthenticate(9, 2f1b19c, 49c648)

58 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/59 RPT=10
AUTH_BindServer(51a6b48, 0, 0)

59 09/11/2002 20:36:03.690 SEV=9 AUTHDBG/69 RPT=10
Auth Server e054d4 has been bound to ACB 51a6b48, sessions = 1

60 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/65 RPT=10
AUTH_CreateTimer(51a6b48, 0, 0)

61 09/11/2002 20:36:03.690 SEV=9 AUTHDBG/72 RPT=10
Reply timer created: handle = 4B0018

62 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/61 RPT=10
AUTH_BuildMsg(51a6b48, 0, 0)

63 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/64 RPT=10
AUTH_StartTimer(51a6b48, 0, 0)

64 09/11/2002 20:36:03.690 SEV=9 AUTHDBG/73 RPT=10
Reply timer started: handle = 4B0018, timestamp = 1163319,
timeout = 30000

65 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/62 RPT=10
AUTH_SndRequest(51a6b48, 0, 0)

66 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/50 RPT=19
IntDB_Decode(3825300, 156)

67 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/47 RPT=19
IntDB_Xmt(51a6b48)

68 09/11/2002 20:36:03.690 SEV=9 AUTHDBG/71 RPT=10
xmit_cnt = 1

69 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/47 RPT=20
IntDB_Xmt(51a6b48)

70 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/49 RPT=10
IntDB_Match(51a6b48, 3eb7ab0)

71 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/63 RPT=10
AUTH_RcvReply(51a6b48, 0, 0)

72 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/50 RPT=20
IntDB_Decode(3eb7ab0, 298)

73 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/48 RPT=10
IntDB_Rcv(51a6b48)
```

```
74 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/66 RPT=10
AUTH_DeleteTimer(51a6b48, 0, 0)

75 09/11/2002 20:36:03.790 SEV=9 AUTHDBG/74 RPT=10
Reply timer stopped: handle = 4B0018, timestamp = 1163329

76 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/58 RPT=10
AUTH_Callback(51a6b48, 0, 0)

77 09/11/2002 20:36:03.790 SEV=6 AUTH/41 RPT=10 172.18.124.157
Authentication successful: handle = 9, server = Internal,
group = 172.18.124.157

78 09/11/2002 20:36:03.790 SEV=7 IKEDBG/0 RPT=526 172.18.124.157
Group [172.18.124.157]
Found Phase 1 Group (172.18.124.157)

79 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/4 RPT=10
AUTH_GetAttrTable(9, 748420)

80 09/11/2002 20:36:03.790 SEV=7 IKEDBG/14 RPT=10 172.18.124.157
Group [172.18.124.157]
Authentication configured for Internal

81 09/11/2002 20:36:03.790 SEV=9 IKEDBG/19 RPT=19 172.18.124.157
Group [172.18.124.157]
IKEGetUserAttributes: IP Compression = disabled

82 09/11/2002 20:36:03.790 SEV=9 IKEDBG/19 RPT=20 172.18.124.157
Group [172.18.124.157]
IKEGetUserAttributes: Split Tunneling Policy = Disabled

83 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/2 RPT=10
AUTH_Close(9)

84 09/11/2002 20:36:03.790 SEV=9 IKEDBG/1 RPT=94 172.18.124.157
Group [172.18.124.157]
constructing ID

85 09/11/2002 20:36:03.790 SEV=9 IKEDBG/0 RPT=527
Group [172.18.124.157]
construct hash payload

86 09/11/2002 20:36:03.790 SEV=9 IKEDBG/0 RPT=528 172.18.124.157
Group [172.18.124.157]
computing hash

87 09/11/2002 20:36:03.790 SEV=9 IKEDBG/46 RPT=40 172.18.124.157
Group [172.18.124.157]
constructing dpd vid payload

88 09/11/2002 20:36:03.790 SEV=8 IKEDBG/0 RPT=529 172.18.124.157
SENDING Message (msgid=0) with payloads :
HDR + ID (5) + HASH (8) ... total length : 80

90 09/11/2002 20:36:03.790 SEV=4 IKE/119 RPT=10 172.18.124.157
Group [172.18.124.157]
PHASE 1 COMPLETED

91 09/11/2002 20:36:03.790 SEV=6 IKE/121 RPT=10 172.18.124.157
Keep-alive type for this connection: None

92 09/11/2002 20:36:03.790 SEV=6 IKE/122 RPT=10 172.18.124.157
```

```
Keep-alives configured on but peer does not
support keep-alives (type = None)

93 09/11/2002 20:36:03.790 SEV=7 IKEDBG/0 RPT=530 172.18.124.157
Group [172.18.124.157]
Starting phase 1 rekey timer: 64800000 (ms)

94 09/11/2002 20:36:03.790 SEV=4 AUTH/22 RPT=16
User 172.18.124.157 connected

95 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/60 RPT=10
AUTH_UnbindServer(51a6b48, 0, 0)

96 09/11/2002 20:36:03.790 SEV=9 AUTHDBG/70 RPT=10
Auth Server e054d4 has been unbound from ACB 51a6b48, sessions = 0

97 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/10 RPT=10
AUTH_Int_FreeAuthCB(51a6b48)

98 09/11/2002 20:36:03.790 SEV=7 AUTH/13 RPT=10
Authentication session closed: handle = 9

99 09/11/2002 20:36:03.790 SEV=8 IKEDBG/0 RPT=531 172.18.124.157
RECEIVED Message (msgid=54796f76) with payloads :
HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0)
... total length : 156

102 09/11/2002 20:36:03.790 SEV=9 IKEDBG/0 RPT=532 172.18.124.157
Group [172.18.124.157]
processing hash

103 09/11/2002 20:36:03.790 SEV=9 IKEDBG/0 RPT=533 172.18.124.157
Group [172.18.124.157]
processing SA payload

104 09/11/2002 20:36:03.790 SEV=9 IKEDBG/1 RPT=95 172.18.124.157
Group [172.18.124.157]
processing nonce payload

105 09/11/2002 20:36:03.790 SEV=9 IKEDBG/1 RPT=96 172.18.124.157
Group [172.18.124.157]
Processing ID

106 09/11/2002 20:36:03.790 SEV=5 IKE/35 RPT=6 172.18.124.157
Group [172.18.124.157]
Received remote IP Proxy Subnet data in ID Payload:
Address 10.32.0.0, Mask 255.255.128.0, Protocol 0, Port 0

109 09/11/2002 20:36:03.790 SEV=9 IKEDBG/1 RPT=97 172.18.124.157
Group [172.18.124.157]
Processing ID

110 09/11/2002 20:36:03.790 SEV=5 IKE/34 RPT=6 172.18.124.157
Group [172.18.124.157]
Received local IP Proxy Subnet data in ID Payload:
Address 192.168.10.0, Mask 255.255.255.0, Protocol 0, Port 0

113 09/11/2002 20:36:03.790 SEV=8 IKEDBG/0 RPT=534
QM IsRekeyed old sa not found by addr

114 09/11/2002 20:36:03.790 SEV=5 IKE/66 RPT=8 172.18.124.157
Group [172.18.124.157]
IKE Remote Peer configured for SA: L2L: Checkpoint
```

```
115 09/11/2002 20:36:03.790 SEV=9 IKEDBG/0 RPT=535 172.18.124.157
Group [172.18.124.157]
processing IPSEC SA

116 09/11/2002 20:36:03.790 SEV=7 IKEDBG/27 RPT=8 172.18.124.157
Group [172.18.124.157]
IPSec SA Proposal # 1, Transform # 1 acceptable

117 09/11/2002 20:36:03.790 SEV=7 IKEDBG/0 RPT=536 172.18.124.157
Group [172.18.124.157]
IKE: requesting SPI!

118 09/11/2002 20:36:03.790 SEV=9 IPSECDBG/6 RPT=39
IPSEC key message parse - msgtype 6, len 200, vers 1, pid 00000000,
seq 10, err 0, type 2, mode 0, state 32, label 0, pad 0,
spi 00000000, encrKeyLen 0, hashKeyLen 0, ivlen 0, alg 0, hmacAlg 0,
lifetype 0, lifetime1 17248580, lifetime2 0, dsId 300

122 09/11/2002 20:36:03.790 SEV=9 IPSECDBG/1 RPT=139
Processing KEY_GETSPI msg!

123 09/11/2002 20:36:03.790 SEV=7 IPSECDBG/13 RPT=10
Reserved SPI 305440147

124 09/11/2002 20:36:03.790 SEV=8 IKEDBG/6 RPT=10
IKE got SPI from key engine: SPI = 0x1234a593

125 09/11/2002 20:36:03.790 SEV=9 IKEDBG/0 RPT=537 172.18.124.157
Group [172.18.124.157]
oakley constucting quick mode

126 09/11/2002 20:36:03.800 SEV=9 IKEDBG/0 RPT=538 172.18.124.157
Group [172.18.124.157]
constructing blank hash

127 09/11/2002 20:36:03.800 SEV=9 IKEDBG/0 RPT=539 172.18.124.157
Group [172.18.124.157]
constructing ISA_SA for ipsec

128 09/11/2002 20:36:03.800 SEV=9 IKEDBG/1 RPT=98 172.18.124.157
Group [172.18.124.157]
constructing ipsec nonce payload

129 09/11/2002 20:36:03.800 SEV=9 IKEDBG/1 RPT=99 172.18.124.157
Group [172.18.124.157]
constructing proxy ID

130 09/11/2002 20:36:03.800 SEV=7 IKEDBG/0 RPT=540 172.18.124.157
Group [172.18.124.157]
Transmitting Proxy Id:
Remote subnet: 10.32.0.0 Mask 255.255.128.0 Protocol 0 Port 0
Local subnet: 192.168.10.0 mask 255.255.255.0 Protocol 0 Port 0

134 09/11/2002 20:36:03.800 SEV=9 IKEDBG/0 RPT=541 172.18.124.157
Group [172.18.124.157]
constructing qm hash

135 09/11/2002 20:36:03.800 SEV=8 IKEDBG/0 RPT=542 172.18.124.157
SENDING Message (msgid=54796f76) with payloads :
HDR + HASH (8) + SA (1) ... total length : 152

137 09/11/2002 20:36:03.800 SEV=8 IKEDBG/0 RPT=543 172.18.124.157
RECEIVED Message (msgid=54796f76) with payloads :
HDR + HASH (8) + NONE (0) ... total length : 48
```

```
139 09/11/2002 20:36:03.800 SEV=9 IKEDBG/0 RPT=544 172.18.124.157
Group [172.18.124.157]
processing hash

140 09/11/2002 20:36:03.800 SEV=9 IKEDBG/0 RPT=545 172.18.124.157
Group [172.18.124.157]
loading all IPSEC SAs

141 09/11/2002 20:36:03.800 SEV=9 IKEDBG/1 RPT=100 172.18.124.157
Group [172.18.124.157]
Generating Quick Mode Key!

142 09/11/2002 20:36:03.800 SEV=9 IKEDBG/1 RPT=101 172.18.124.157
Group [172.18.124.157]
Generating Quick Mode Key!

143 09/11/2002 20:36:03.800 SEV=7 IKEDBG/0 RPT=546 172.18.124.157
Group [172.18.124.157]
Loading subnet:
Dst: 192.168.10.0 mask: 255.255.255.0
Src: 10.32.0.0 mask: 255.255.128.0

146 09/11/2002 20:36:03.800 SEV=4 IKE/49 RPT=7 172.18.124.157
Group [172.18.124.157]
Security negotiation complete for LAN-to-LAN Group (172.18.124.157)
Responder, Inbound SPI = 0x1234a593, Outbound SPI = 0x0df37959

149 09/11/2002 20:36:03.800 SEV=9 IPSECDBG/6 RPT=40
IPSEC key message parse - msgtype 1, len 606, vers 1, pid 00000000,
seq 0, err 0, type 2, mode 1, state 64, label 0, pad 0,
spi 0df37959, encrKeyLen 24, hashKeyLen 16, ivlen 8, alg 2, hmacAlg 3,
lifetype 0, lifetime1 17248580, lifetime2 0, dsId 0

153 09/11/2002 20:36:03.800 SEV=9 IPSECDBG/1 RPT=140
Processing KEY_ADD msg!

154 09/11/2002 20:36:03.800 SEV=9 IPSECDBG/1 RPT=141
key_msghdr2secassoc(): Enter

155 09/11/2002 20:36:03.800 SEV=7 IPSECDBG/1 RPT=142
No USER filter configured

156 09/11/2002 20:36:03.800 SEV=9 IPSECDBG/1 RPT=143
KeyProcessAdd: Enter

157 09/11/2002 20:36:03.800 SEV=8 IPSECDBG/1 RPT=144
KeyProcessAdd: Adding outbound SA

158 09/11/2002 20:36:03.800 SEV=8 IPSECDBG/1 RPT=145
KeyProcessAdd: src 192.168.10.0 mask 0.0.0.255,
dst 10.32.0.0 mask 0.0.127.255

159 09/11/2002 20:36:03.810 SEV=8 IPSECDBG/1 RPT=146
KeyProcessAdd: FilterIpsecAddIkeSa success

160 09/11/2002 20:36:03.810 SEV=9 IPSECDBG/6 RPT=41
IPSEC key message parse - msgtype 3, len 327, vers 1, pid 00000000,
seq 0, err 0, type 2, mode 1, state 32, label 0, pad 0,
spi 1234a593, encrKeyLen 24, hashKeyLen 16, ivlen 8, alg 2, hmacAlg 3,
lifetype 0, lifetime1 17248580, lifetime2 0, dsId 0

164 09/11/2002 20:36:03.810 SEV=9 IPSECDBG/1 RPT=147
Processing KEY_UPDATE msg!
```

```
165 09/11/2002 20:36:03.810 SEV=9 IPSECDBG/1 RPT=148
Update inbound SA addresses

166 09/11/2002 20:36:03.810 SEV=9 IPSECDBG/1 RPT=149
key_msghdr2secassoc(): Enter

167 09/11/2002 20:36:03.810 SEV=7 IPSECDBG/1 RPT=150
No USER filter configured

168 09/11/2002 20:36:03.810 SEV=9 IPSECDBG/1 RPT=151
KeyProcessUpdate: Enter

169 09/11/2002 20:36:03.810 SEV=8 IPSECDBG/1 RPT=152
KeyProcessUpdate: success

170 09/11/2002 20:36:03.810 SEV=8 IKEDBG/7 RPT=7
IKE got a KEY_ADD msg for SA: SPI = 0x0df37959

171 09/11/2002 20:36:03.810 SEV=8 IKEDBG/0 RPT=547
pitcher: rcv KEY_UPDATE, spi 0x1234a593

172 09/11/2002 20:36:03.810 SEV=4 IKE/120 RPT=7 172.18.124.157
Group [172.18.124.157]
PHASE 2 COMPLETED (msgid=54796f76)
```

Informações Relacionadas

- Página de suporte do Cisco VPN 3000 Series Concentrator
- Página de suporte ao cliente do Cisco VPN 3000 Series
- Página de suporte do IPSec
- Suporte Técnico - Cisco Systems