Configurando um túnel IPSec - Cisco VPN 3000 Concentrator para Checkpoint 4.1 Firewall

Índice

Introdução

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

- Uma rede privada dentro do Cisco VPN 3000 Concentrator (192.168.1.x).
- 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 esta configuração comece.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

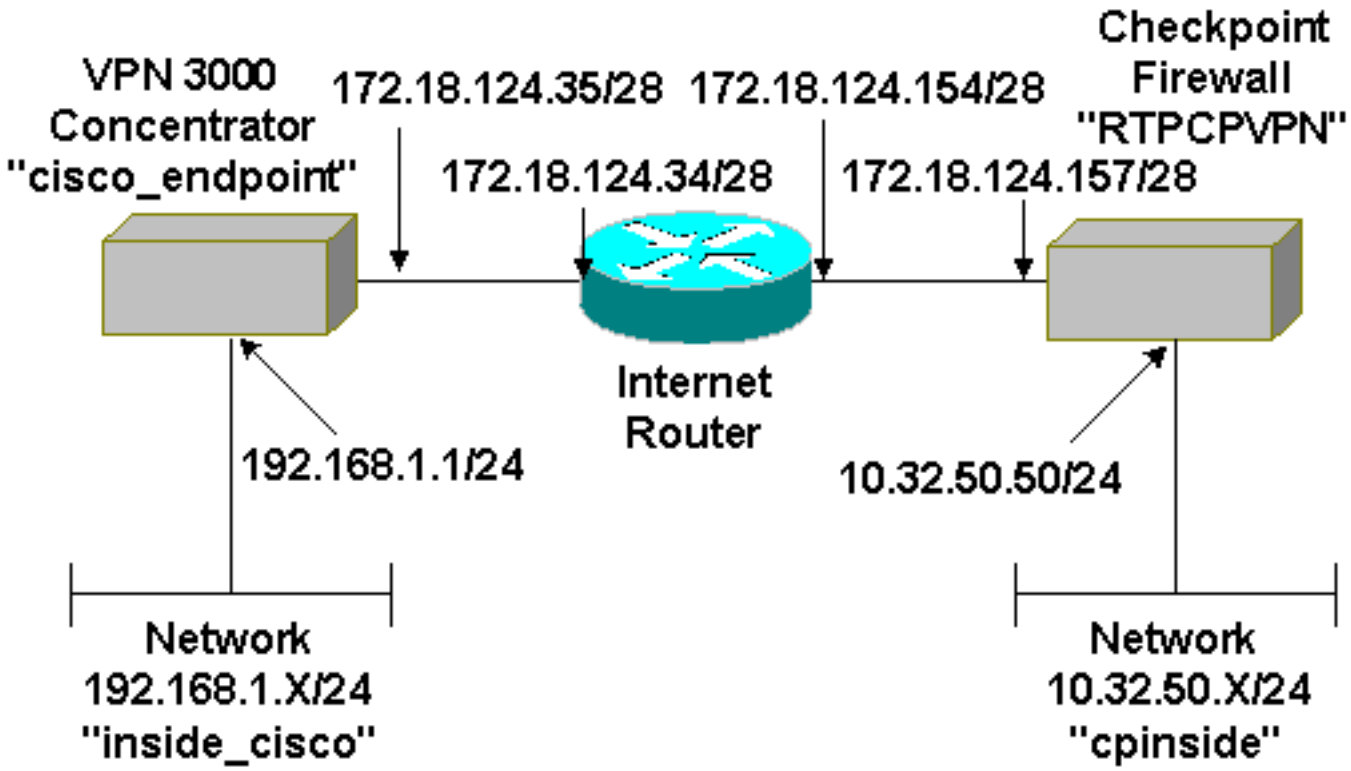
As informações neste documento são baseadas nestas versões de software e hardware:

- VPN 3000 Concentrator
- Software Release 2.5.2.F do VPN 3000 concentrator
- 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.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



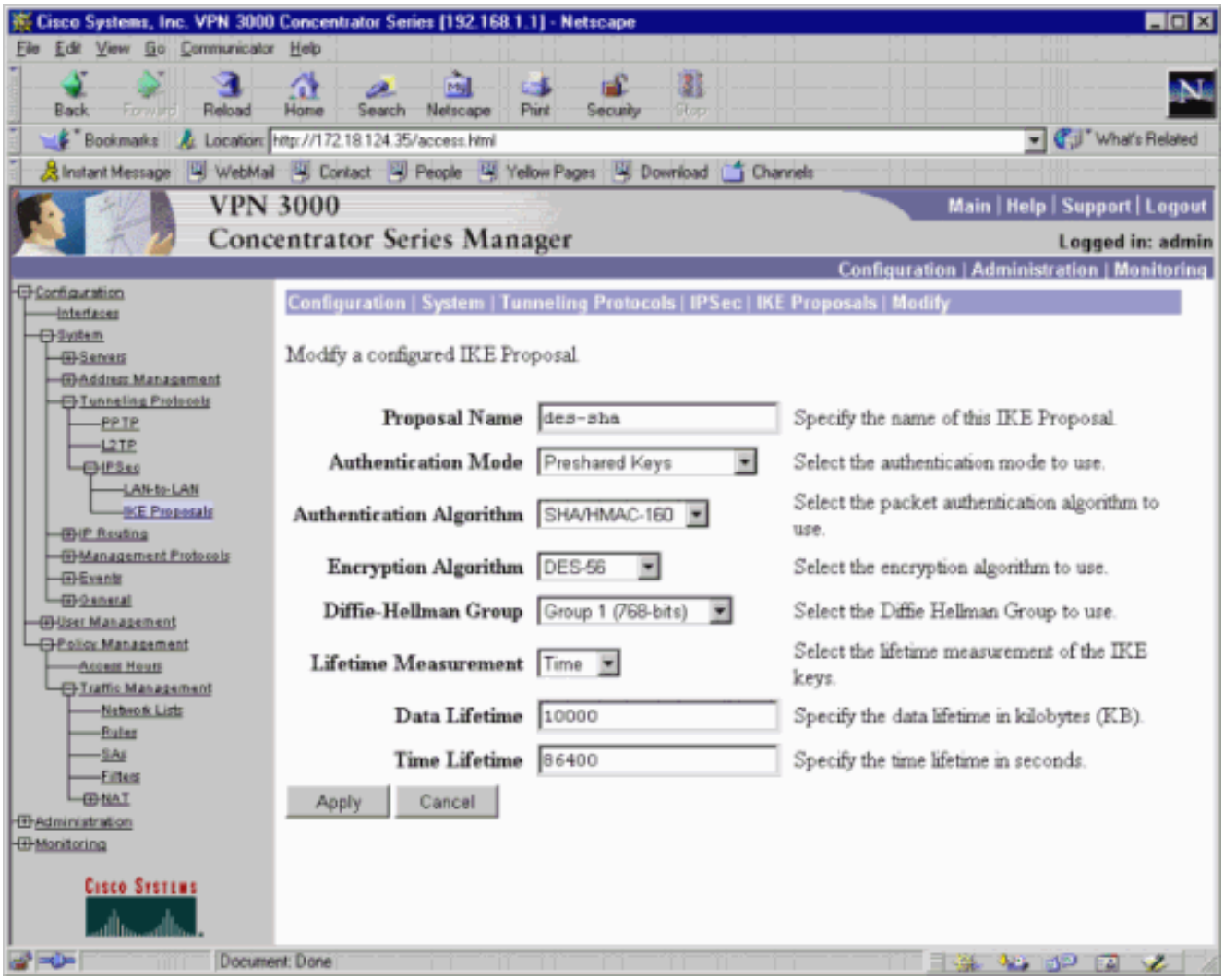
Convenções

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

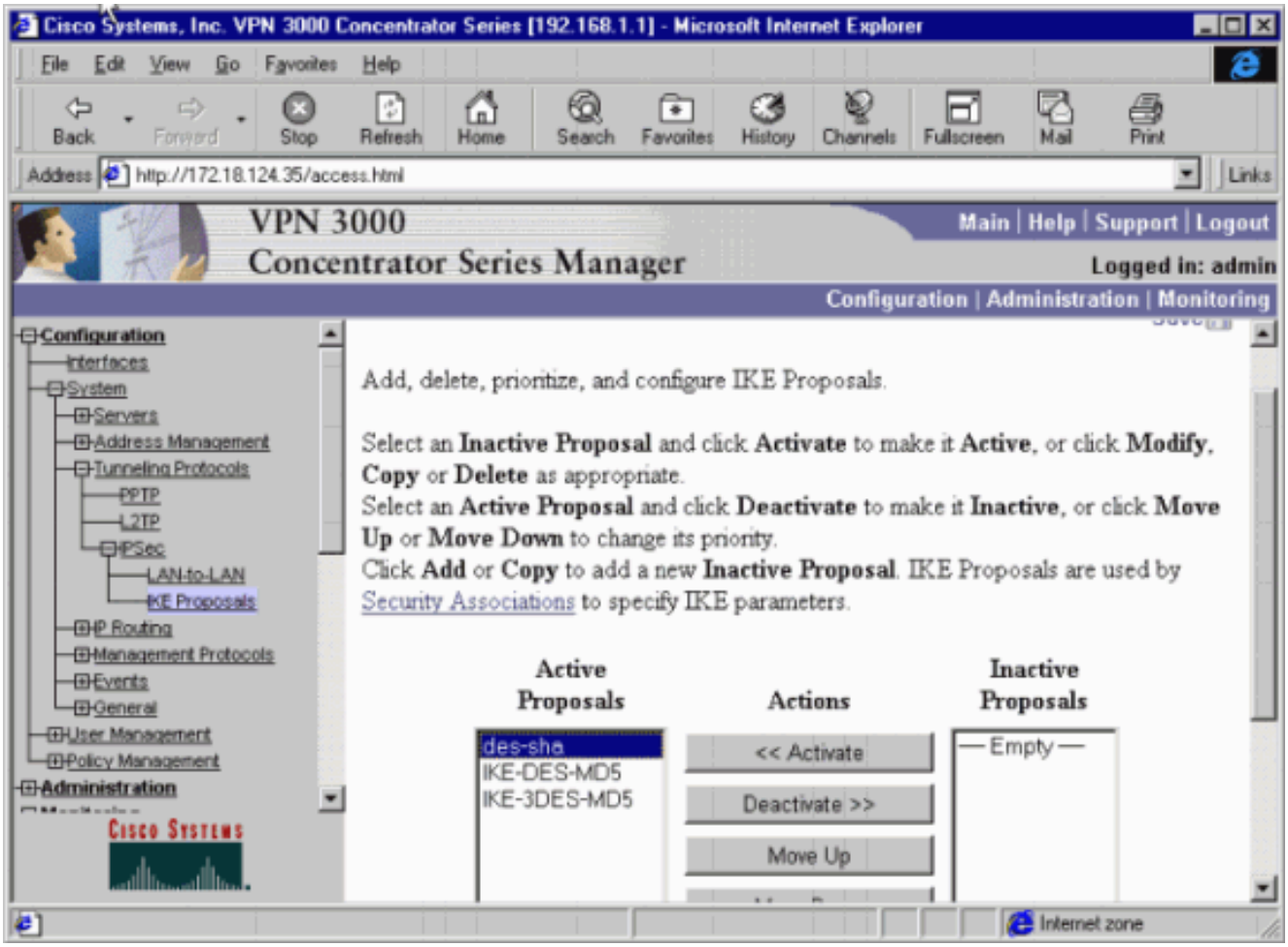
Configurar o VPN 3000 Concentrator

Termine estas etapas para configurar o VPN 3000 concentrator.

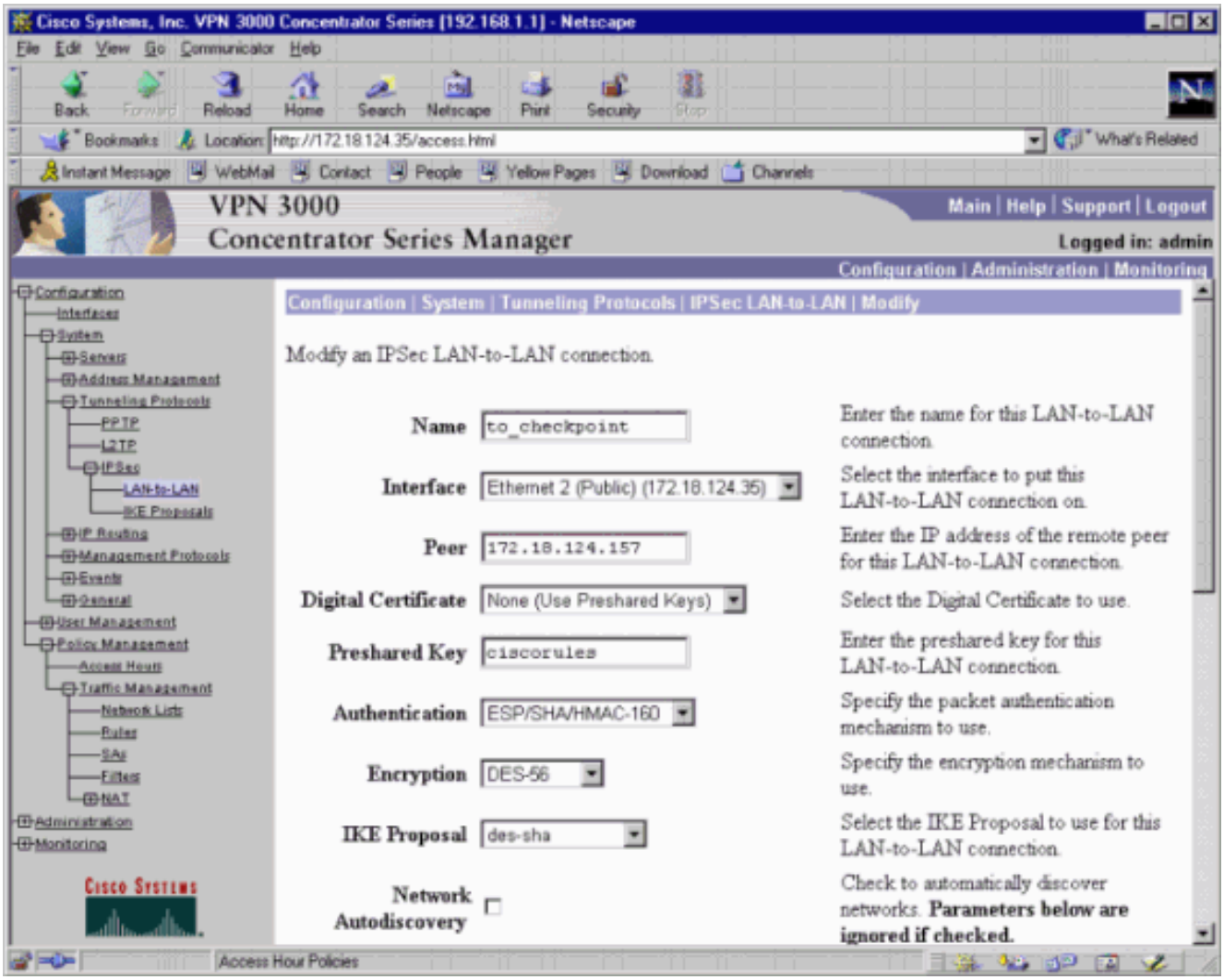
1. Selecione Configuration > System > Tunneling Protocols > IPSec > IKE Proposals > Modify para criar uma proposta do IKE (Internet Key Exchange) chamada "des-sha", com SHA (Algoritmo de hash seguro), DES (Criptografia de dados padrão) e Diffie-Hellman Grupo 1. Deixe a opção Time Lifetime definida com o valor padrão de 86400 segundos.**Note**: O intervalo válido para a duração de IKE do concentrador VPN é 60-2147483647 segundos.

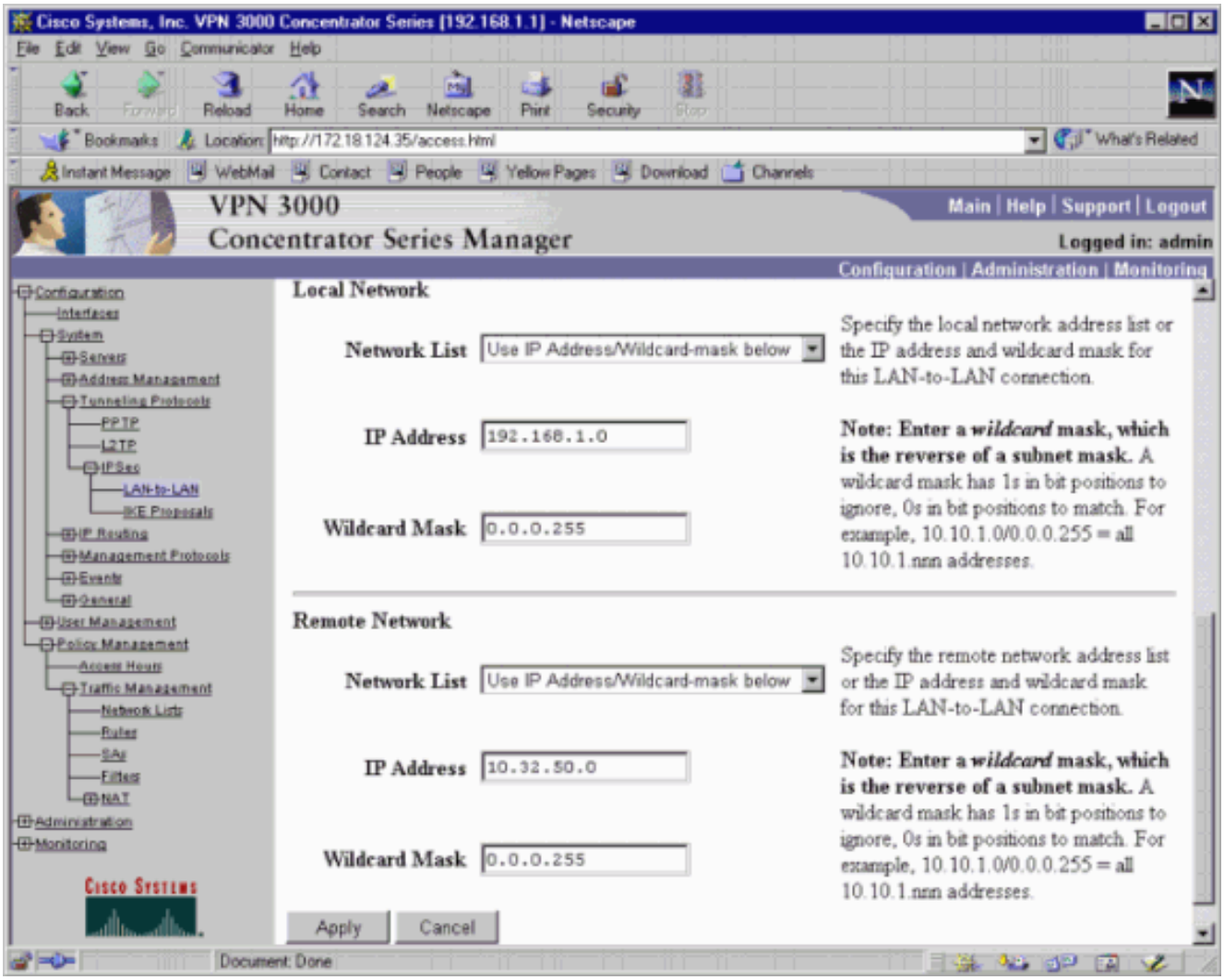


2. Selecione Configuration (Configuração) > System (Sistema) > Tunneling Protocols (Protocolos de Tunelamento) > IPSec > IKE Proposals (Propostas IKE). Selecione "des-sha" e clique em Activate para ativar a proposta
IKE.

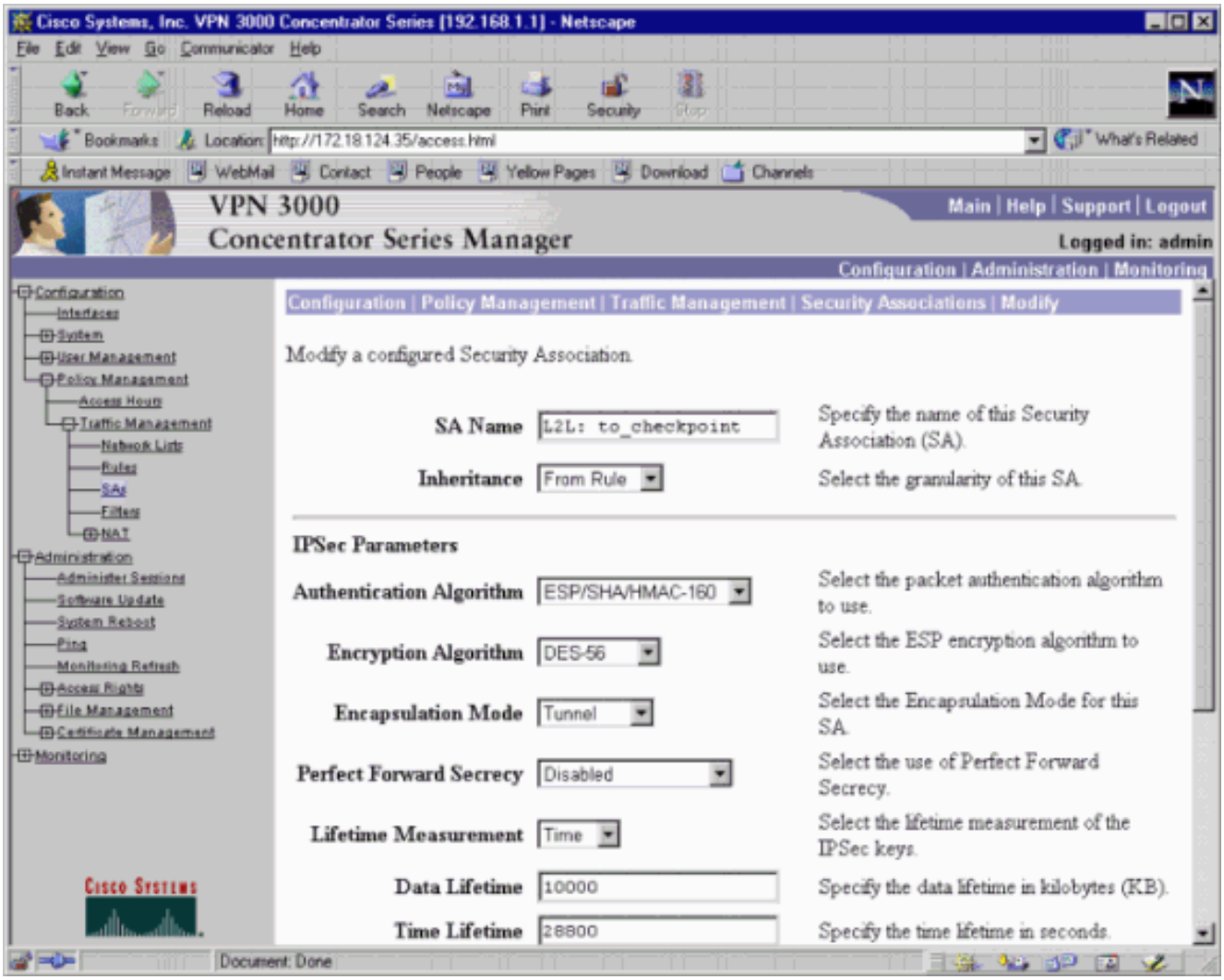


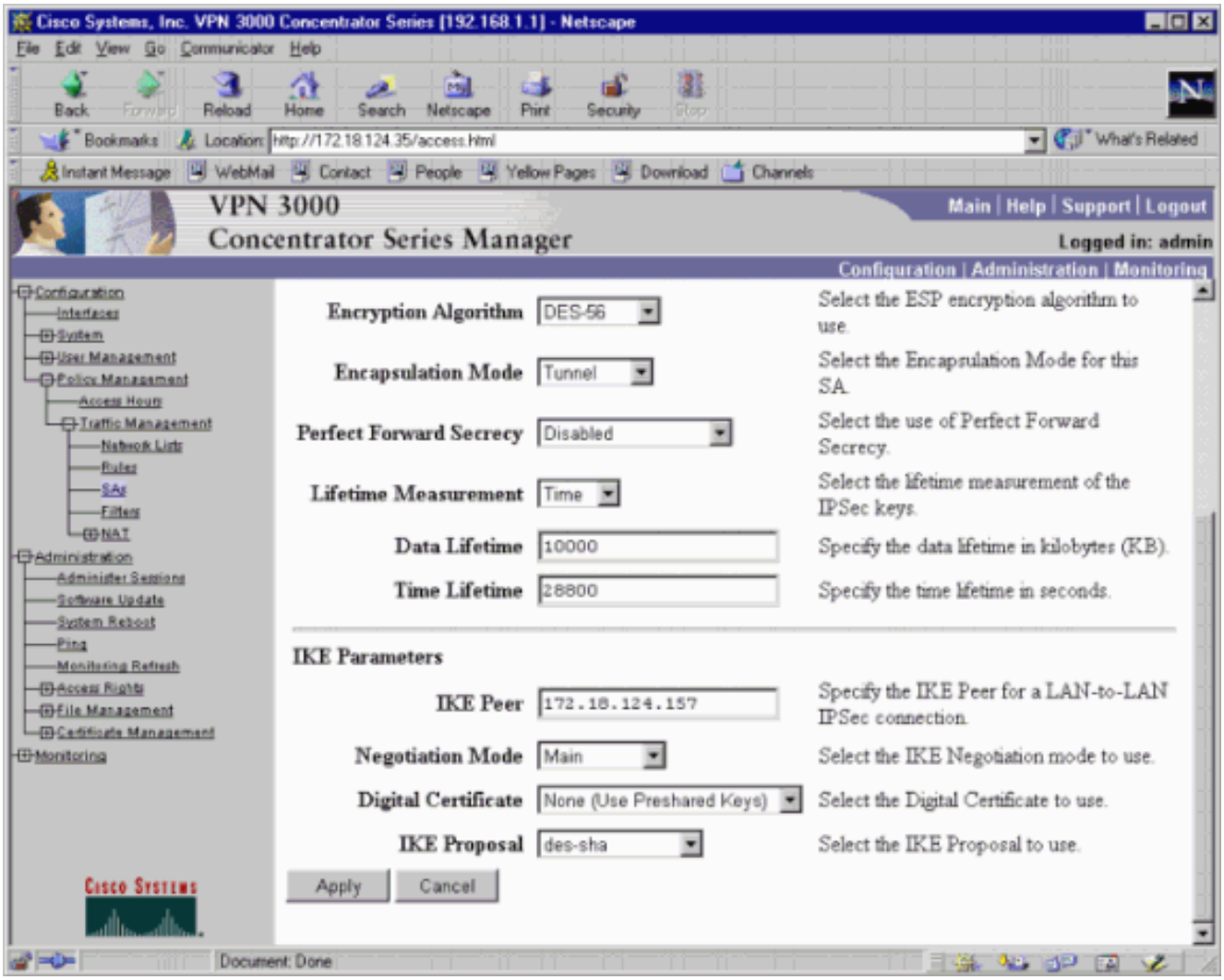
3. Selecione Configuration > System > Tunneling Protocols > IPSec LAN-to-LAN > Add (Configuração > Sistema > Protocolos de Canalização > IPSec LAN para LAN > Adicionar).Estabelecer um túnel de IPsec chamado “to_checkpoint” com o endereço do ponto de verificação como o par. Para a chave pré-compartilhadas, insira a chave real. Sob a autenticação, o ESP/SHA/HMAC-160 seleto, e o DES-56 seleto para a criptografia. Insira a proposta IKE (“des-sha” neste exemplo) e as redes local e remota.


Cisco Systems, Inc. VPN 3000 Concentrator Series [192.168.1.1] - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Stop
Bookmarks Location: http://172.18.124.35/access.html What's Related
Instant Message WebMail Contact People Yellow Pages Download Channels
VPN 3000
Concentrator Series Manager
Main | Help | Support | Logout
Logged in: admin
Configuration | Administration | Monitoring
Configuration
Interfaces
System
Servers
Address Management
Tunneling Protocols
PPTP
L2TP
IPSec
LAN-to-LAN
IKE Proposals
IP Routing
Management Protocols
Events
General
User Management
Policy Management
Access Hours
Traffic Management
Network Lists
Rules
SAs
Filters
NAT
Administration
Monitoring
Cisco Systems
Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN | Modify
Modify an IPSec LAN-to-LAN connection.
Name
to_checkpoint
Enter the name for this LAN-to-LAN connection.
Interface
Ethernet 2 (Public) (172.18.124.35)
Select the interface to put this LAN-to-LAN connection on.
Peer
172.18.124.157
Enter the IP address of the remote peer for this LAN-to-LAN connection.
Digital Certificate
None (Use Preshared Keys)
Select the Digital Certificate to use.
Preshared Key
ciscorules
Enter the preshared key for this LAN-to-LAN connection.
Authentication
ESP/SHA/HMAC-160
Specify the packet authentication mechanism to use.
Encryption
DES-56
Specify the encryption mechanism to use.
IKE Proposal
des-sha
Select the IKE Proposal to use for this LAN-to-LAN connection.
Network Autodiscovery
Check to automatically discover networks. Parameters below are ignored if checked.
Access Hour Policies



4. Selecione Configuração > Gerenciamento de Política > Gerenciamento de Tráfego > Associações de Segurança > Modificar. Verifique que o discrição perfeita adiante **está desabilitado** e deixe à duração de período do IPsec no padrão **28800** segundos.**Note**: O intervalo válido para a duração de IPSec do concentrador VPN é 60-2147483647 segundos.


Cisco Systems, Inc. VPN 3000 Concentrator Series [192.168.1.1] - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Stop
Bookmarks Location: http://172.18.124.35/access.html What's Related
Instant Message WebMail Contact People Yellow Pages Download Channels
VPN 3000
Concentrator Series Manager
Main | Help | Support | Logout
Logged in: admin
Configuration | Administration | Monitoring
Configuration
Interfaces
System
User Management
Policy Management
Access Hours
Traffic Management
Network Lists
Rules
SAs
Filters
NAT
Administration
Administer Sessions
Software Update
System Reboot
Ping
Monitoring Refresh
Access Rights
File Management
Certificate Management
Monitoring
Cisco Systems
Configuration | Policy Management | Traffic Management | Security Associations | Modify
Modify a configured Security Association.
SA Name L2L: to_checkpoint Specify the name of this Security Association (SA).
Inheritance From Rule Select the granularity of this SA.
IPSec Parameters
Authentication Algorithm ESP/SHA/HMAC-160 Select the packet authentication algorithm to use.
Encryption Algorithm DES-56 Select the ESP encryption algorithm to use.
Encapsulation Mode Tunnel Select the Encapsulation Mode for this SA.
Perfect Forward Secrecy Disabled Select the use of Perfect Forward Secrecy.
Lifetime Measurement Time Select the lifetime measurement of the IPSec keys.
Data Lifetime 10000 Specify the data lifetime in kilobytes (KB).
Time Lifetime 28800 Specify the time lifetime in seconds.
Document: Done

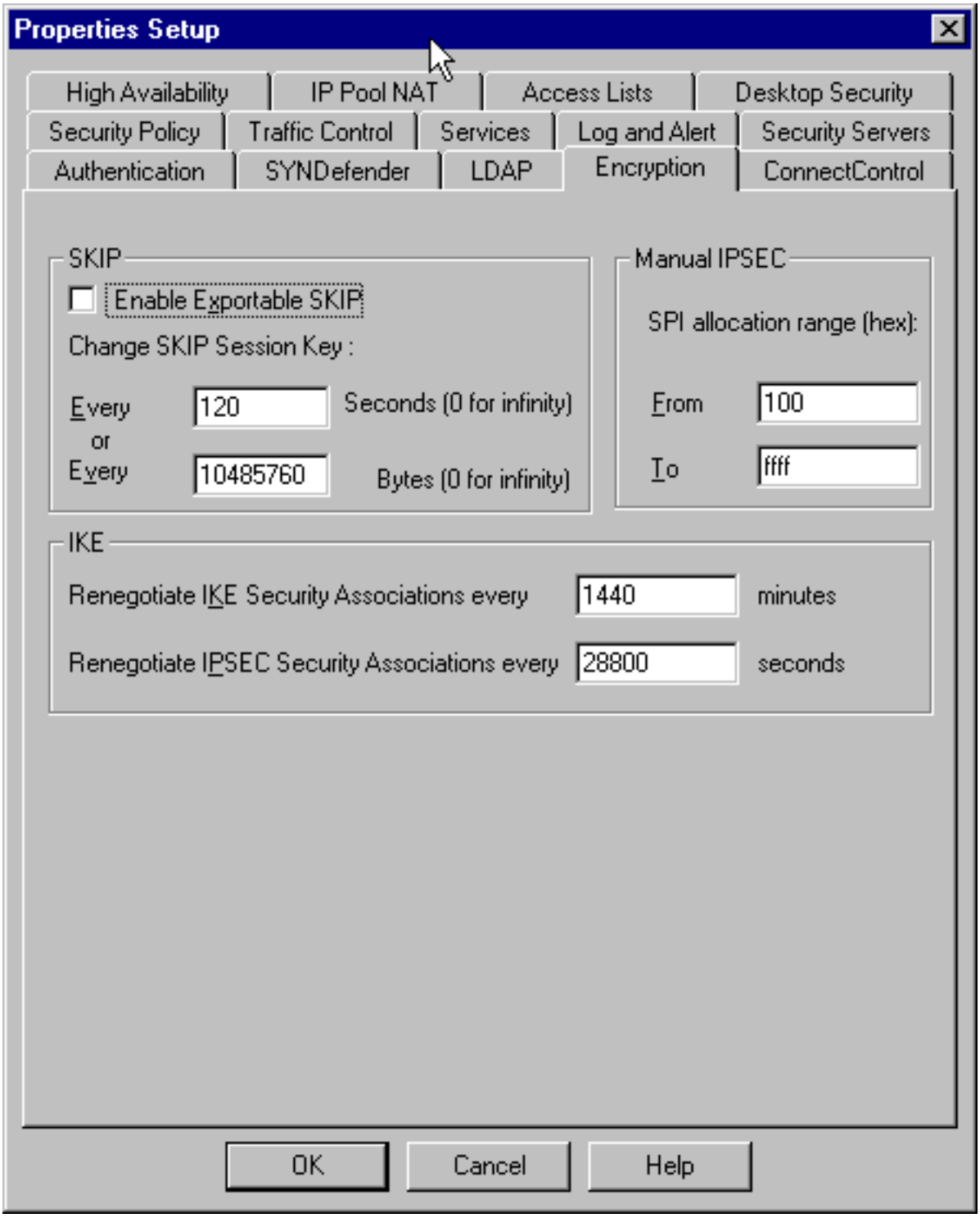


5. Salve a configuração.

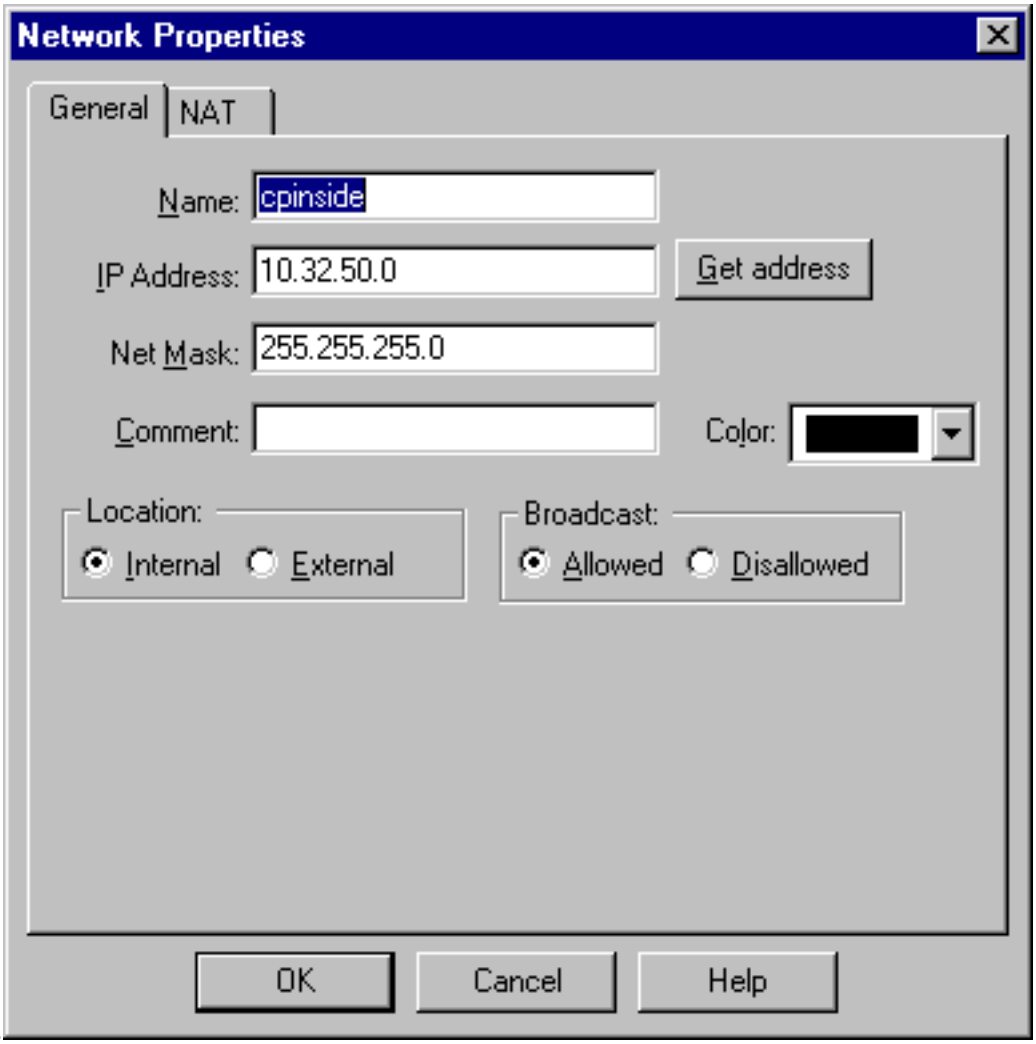
Configurar o Firewall do ponto de verificação 4.1

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

1. Desde que o IKE e as durações padrão IPSec diferem entre vendedores, selecione o **Propriedades > Criptografia** para ajustar as durações do ponto de controle para concordar com os padrões do concentrador VPN.A duração de IKE do padrão do concentrador VPN é 86400 segundos (minutos =1440).A duração padrão de IPSec do concentrador VPN é 28800 segundos.

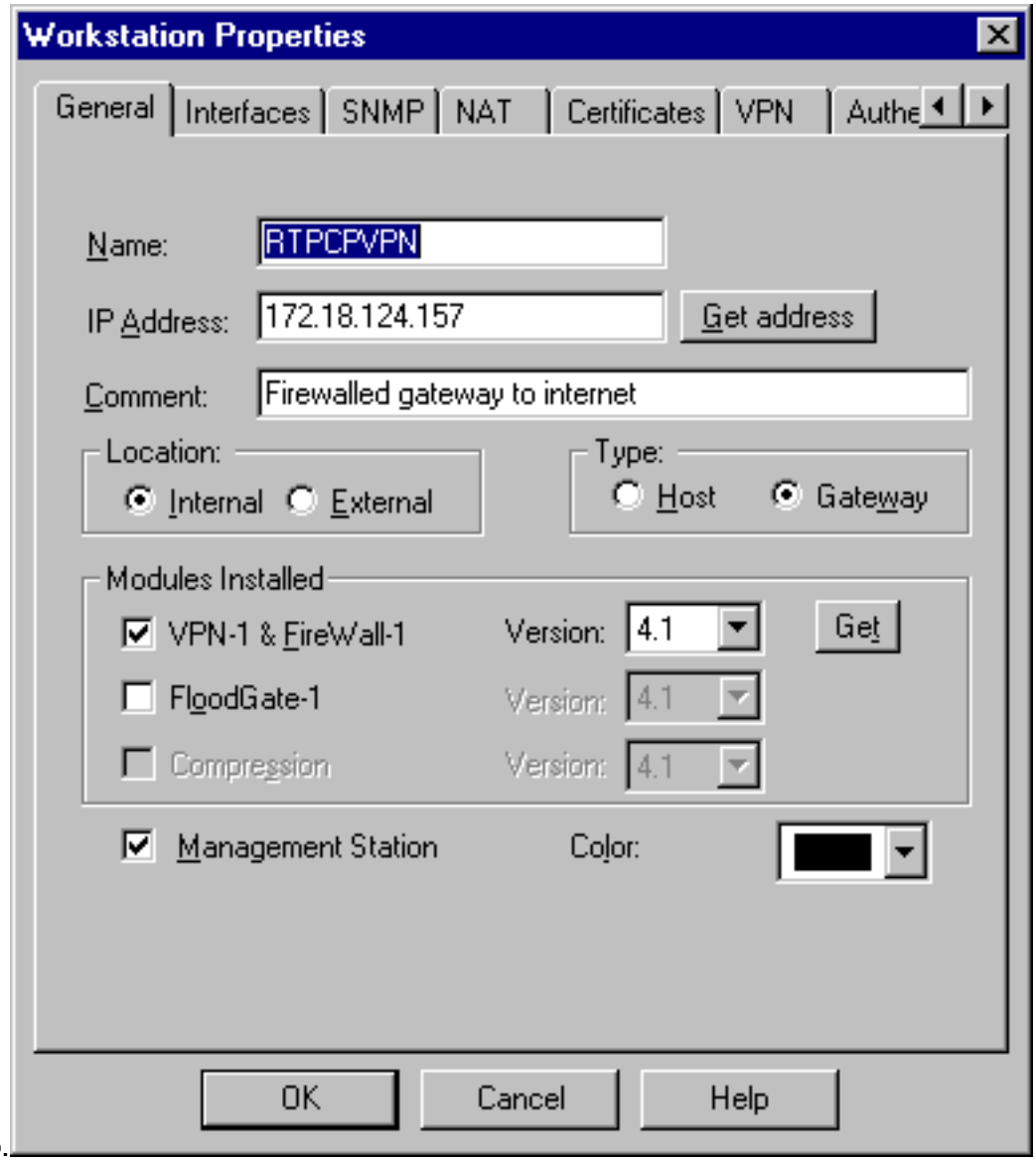


2. Selecione Gerenciar > Objetos de rede > Novo (ou Editar) > Rede para configurar o objeto para a rede interna ("cpinside") por trás do ponto de controle. Isto deve concordar com a “rede remota” no concentrador



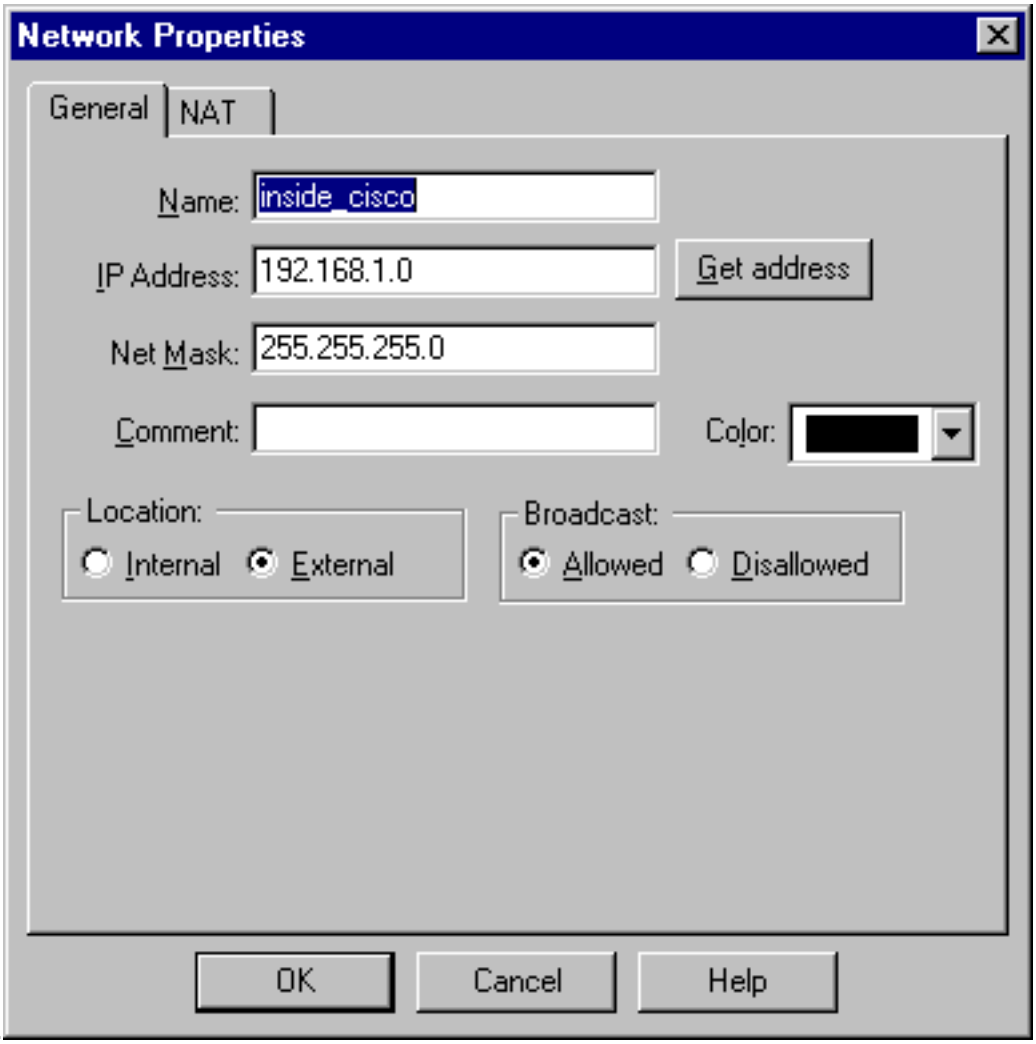
VPN.

3. Selecione **Manage > Network Objects > Edit** para editar o objeto para o valor-limite do gateway (ponto de verificação “RTPCPVPN”) que o concentrador VPN tem em seu parâmetro do par.Em Local, selecione Interno. Para Tipo, selecione Gateway. Sob os módulos instalados, verifique o **VPN-1 & o FireWall-1** e verifique a **estação de**



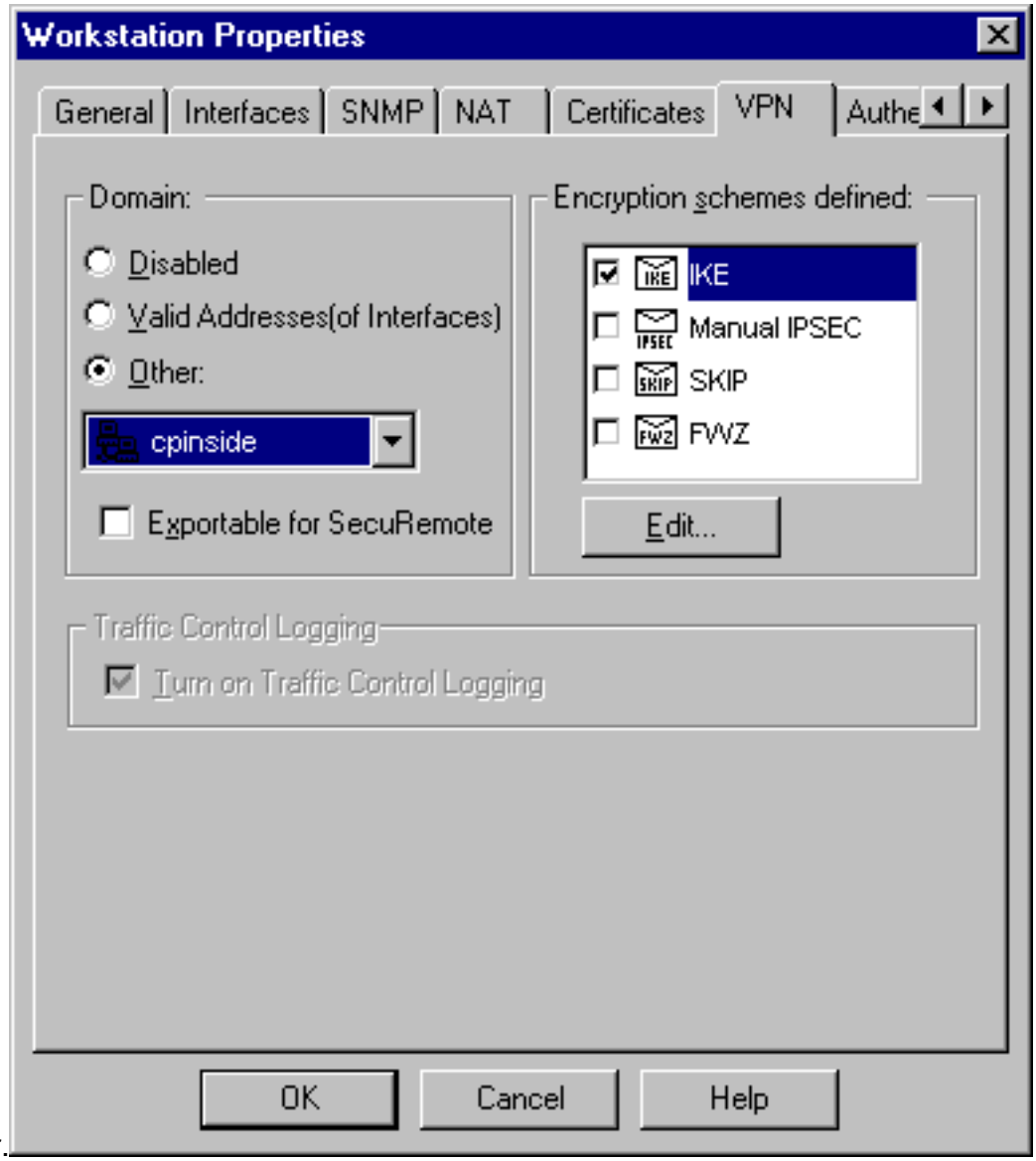
gerenciamento.

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 a rede “local” no concentrador



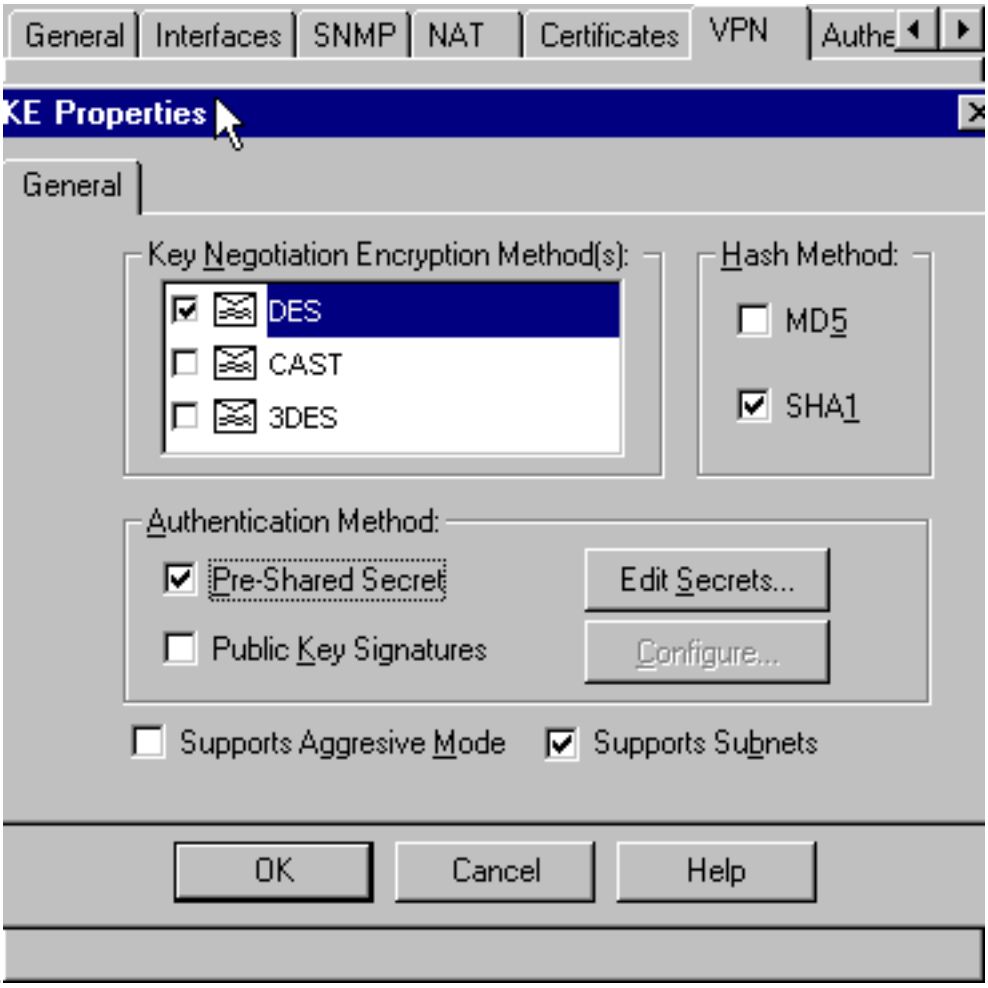
VPN.

5. Selecione **Manage > Network Objects > New > Workstation** para adicionar um objeto para (“cisco_endpoint”) o gateway externo do concentrador VPN. Esta é a relação “pública” do concentrador VPN.Em Local, selecione Externo. Para Tipo, selecione Gateway.**Note**: Não selecione a caixa de seleção 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



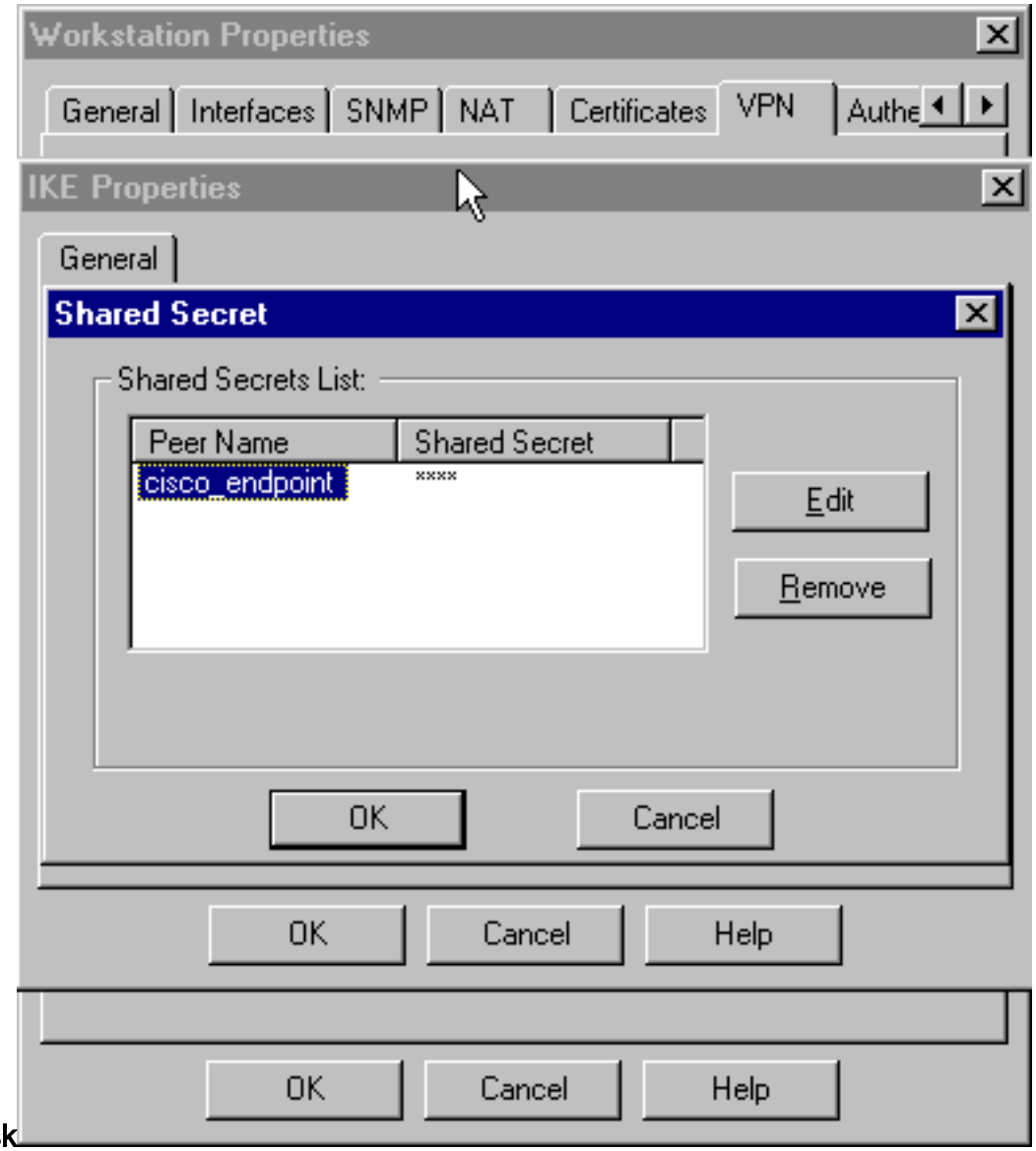
Editar.

7. Mude as propriedades IKE para a criptografia DES para concordar com o **DES-56** e o **algoritmo de criptografia** com o concentrador VPN.
8. Mude as propriedades IKE ao hashing SHA1 para concordar com o algoritmo **SHA/HMAC-160 no** concentrador VPN.Desative o Modo assertivo.A verificação **apoia sub-redes**.Verifique o **segredo pré-compartilhado** sob o método de autenticação. Isto concorda com o modo de autenticação do concentrador VPN, chaves



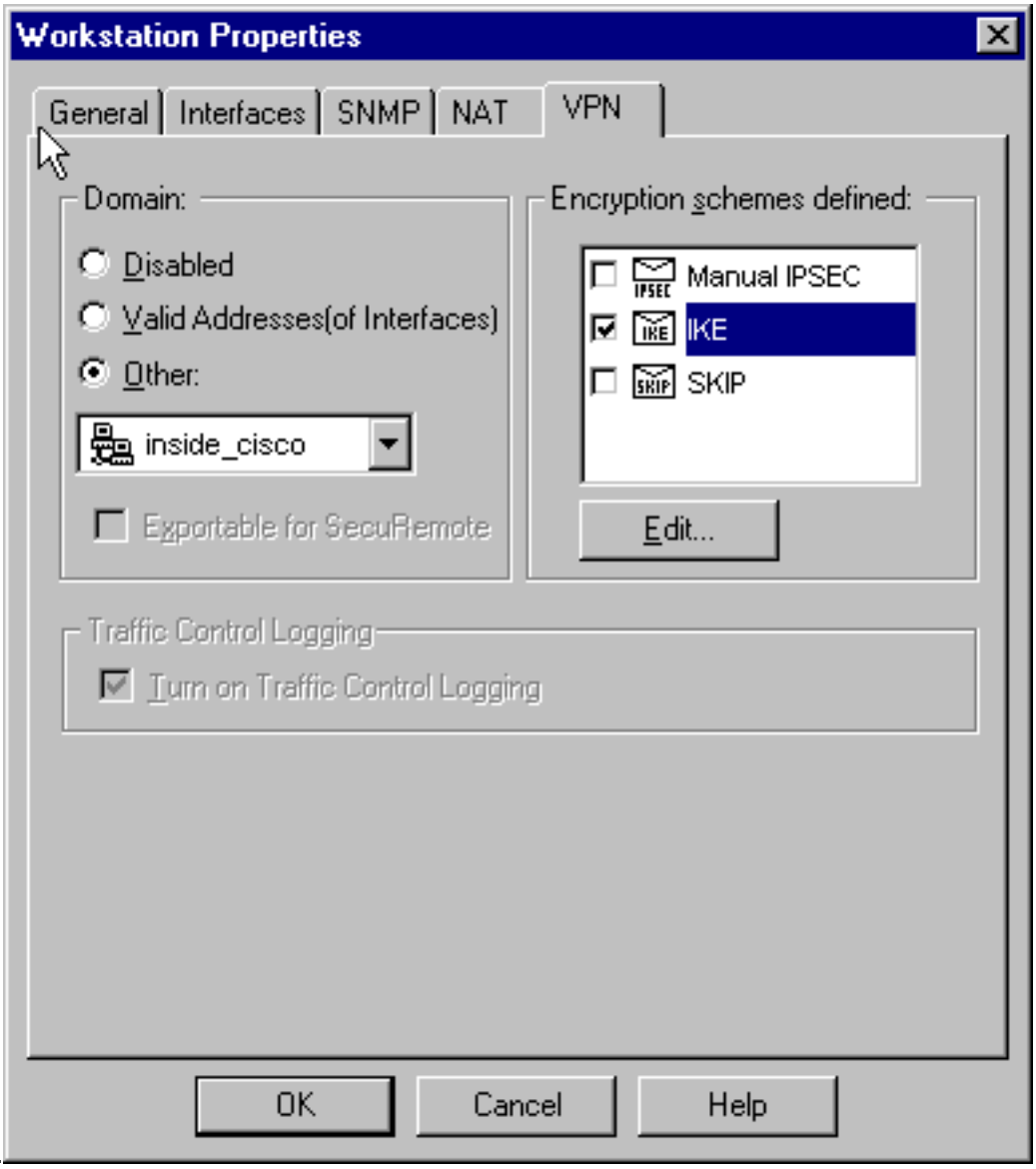
Preshared.

9. O clique **edita segredos** para ajustar a chave pré-compartilhada para concordar com a **chave Preshared do** concentrador VPN real.**isakmp key key address address netmask**



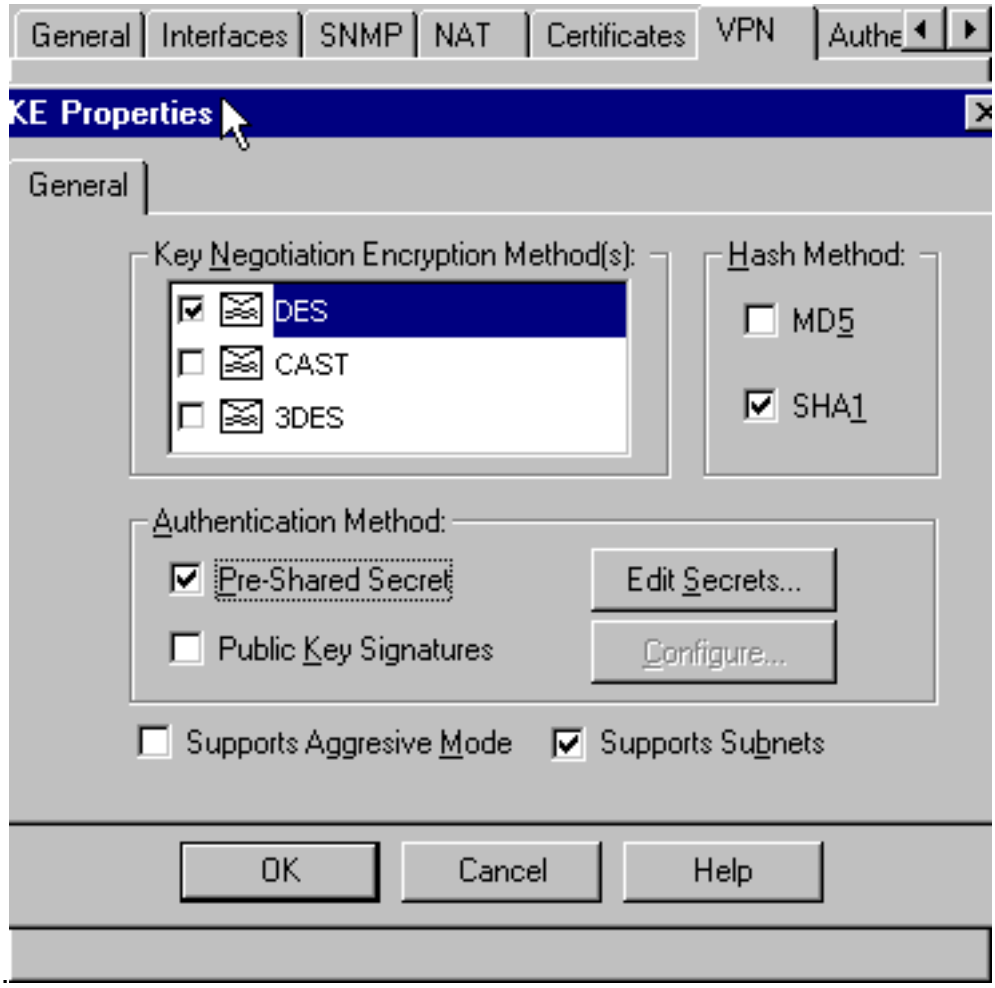
netmask

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



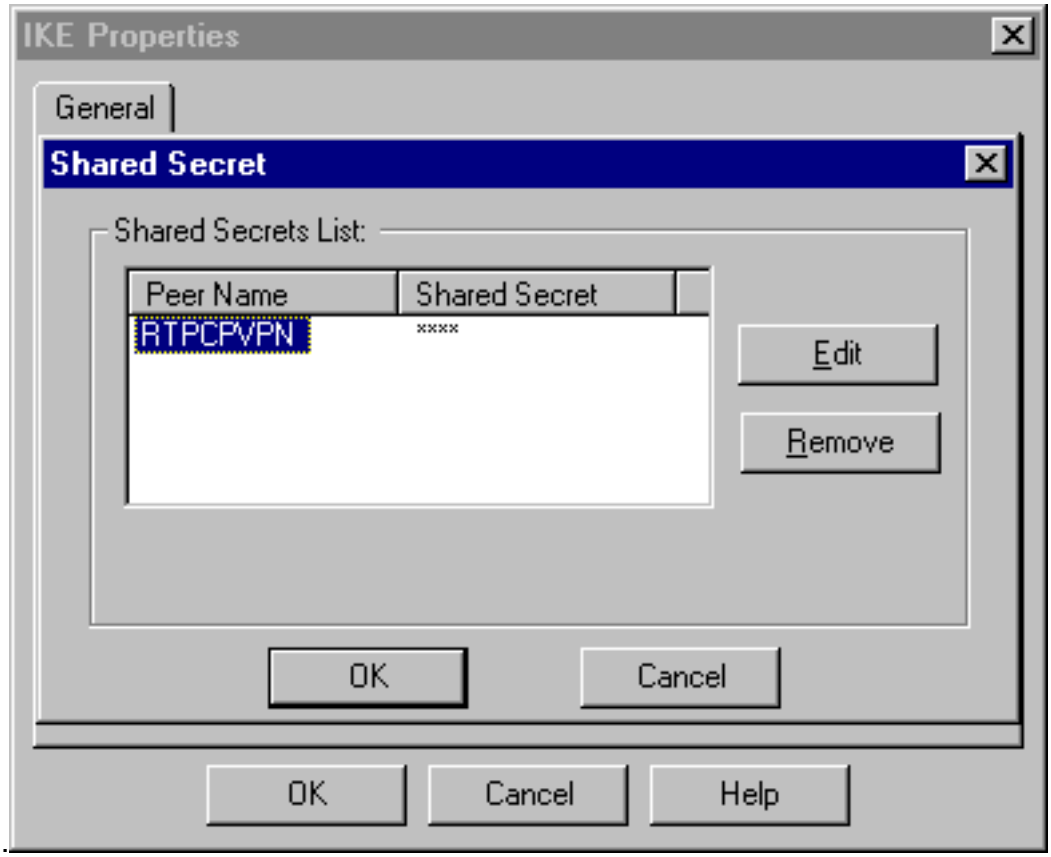
Editar.

11. Mude a criptografia DES das propriedades IKE para concordar com o **DES-56, algoritmo de criptografia** com o concentrador VPN.
12. Mude as propriedades IKE ao hashing SHA1 para concordar com o algoritmo **SHA/HMAC-160 no** concentrador VPN.Mude estes ajustes:Modo DeselectAggressive.A verificação **apoia sub-redes**.Verifique o **segredo pré-compartilhado** sob o método de autenticação. Isto concorda com o modo de autenticação do concentrador VPN de chaves



Preshared.

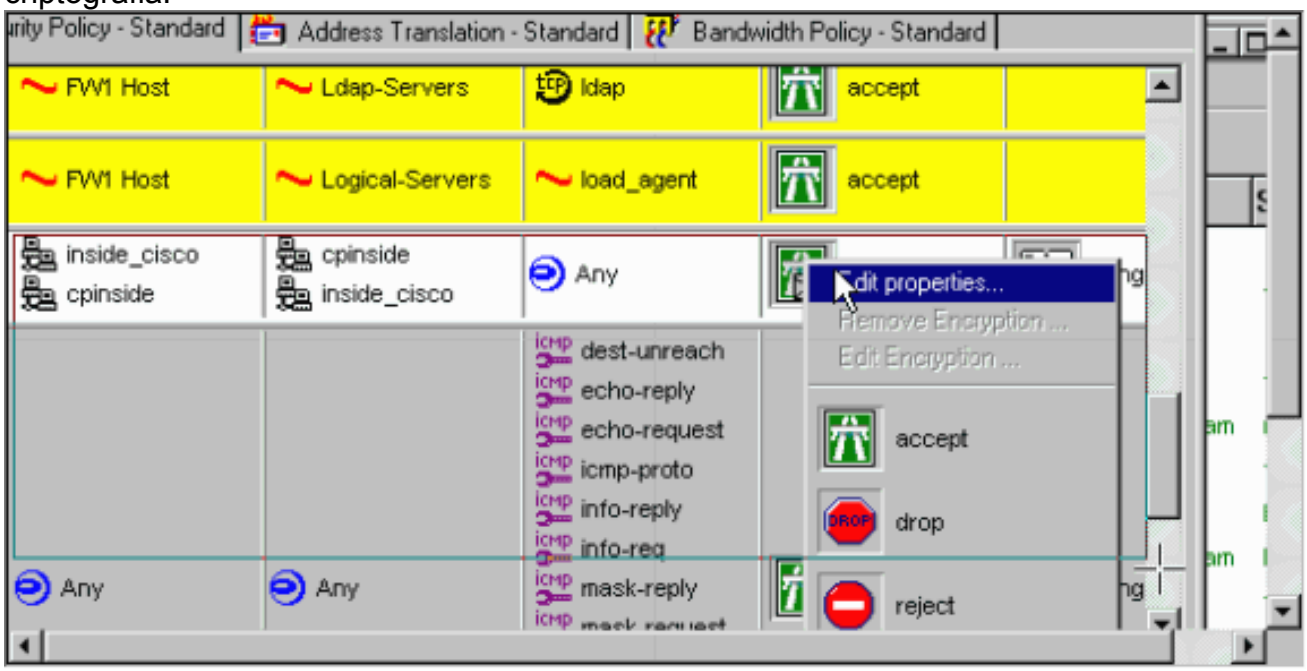
13. O clique **edita segredos** para ajustar a chave pré-compartilhada para concordar com a chave Preshared do concentrador VPN



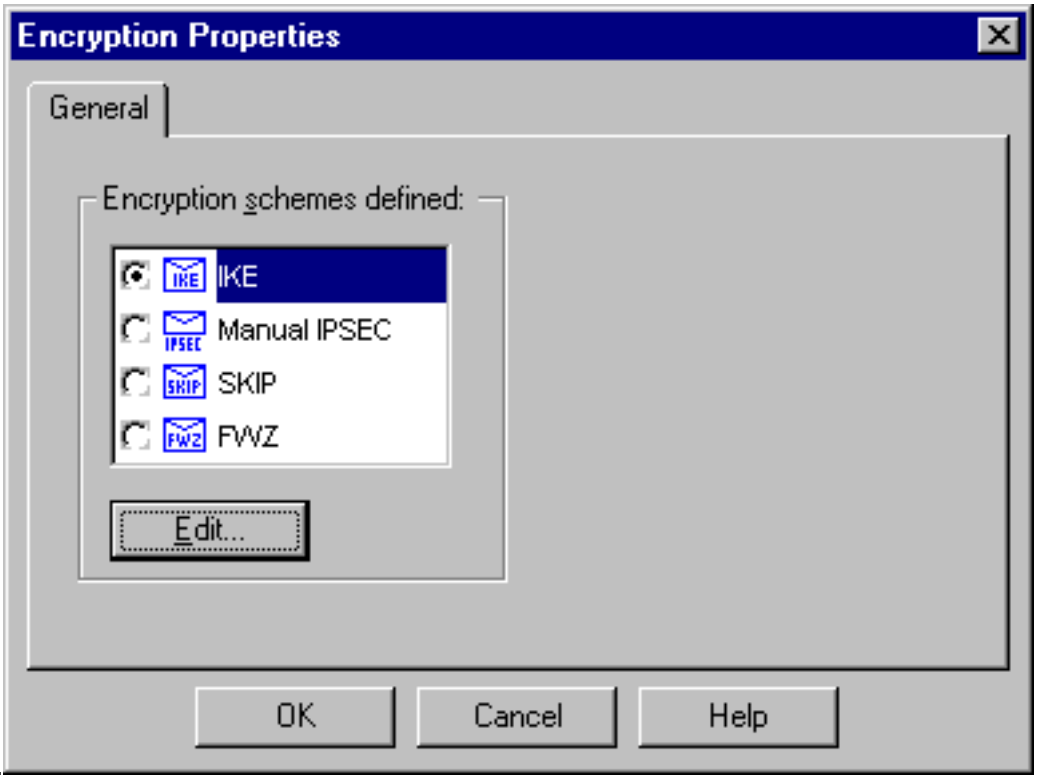
real.

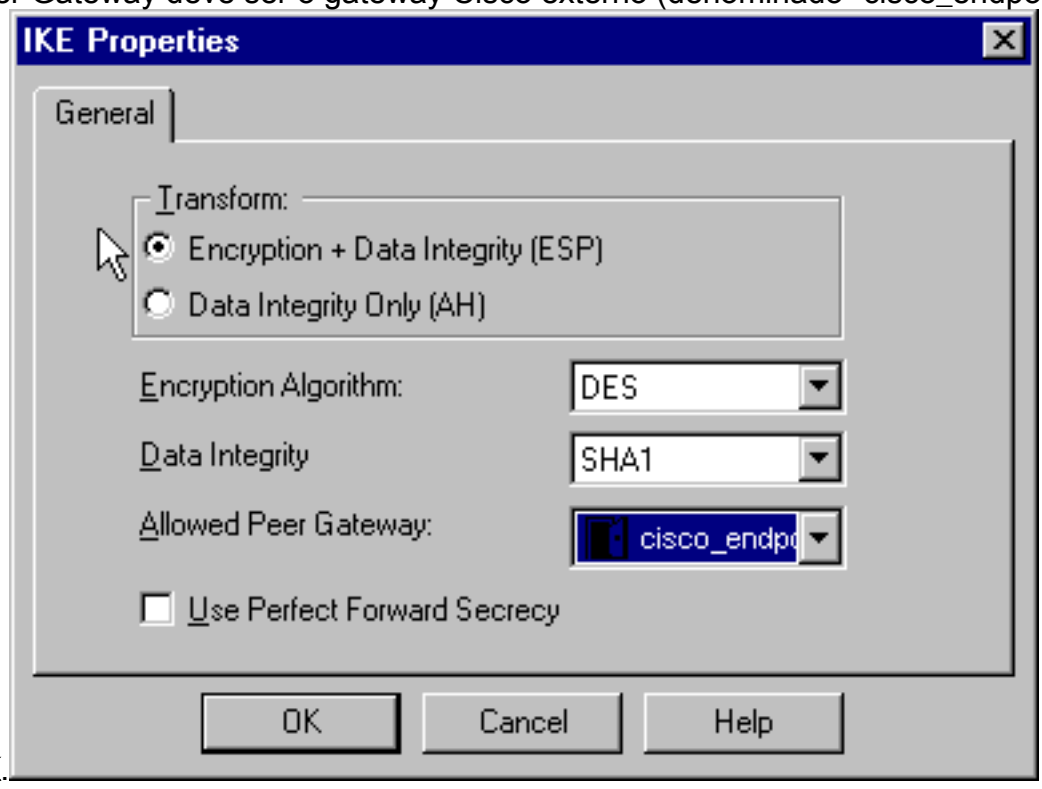
14. Na janela Policy Editor, insira uma regra com Source e Destination como "inside_cisco" e "cpinside" (bidirecional). Ajustar Serviço=Qualquer, Ação=Criptografar e Rastreio=Longo.

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



16. Selecione IKE e, em seguida, clique em

Editar. 

17. No indicador das propriedades IKE, mude estas propriedades para concordar com o IPsec do concentrador VPN transforma.Em Transform, selecione Encryption + Data Integrity (ESP). O Encryption Algorithm deve ser DES, Data Integrity deve ser SHA1 e o Allowed Peer Gateway deve ser o gateway Cisco externo (denominado "cisco_endpoint"). Click OK. 

18. 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

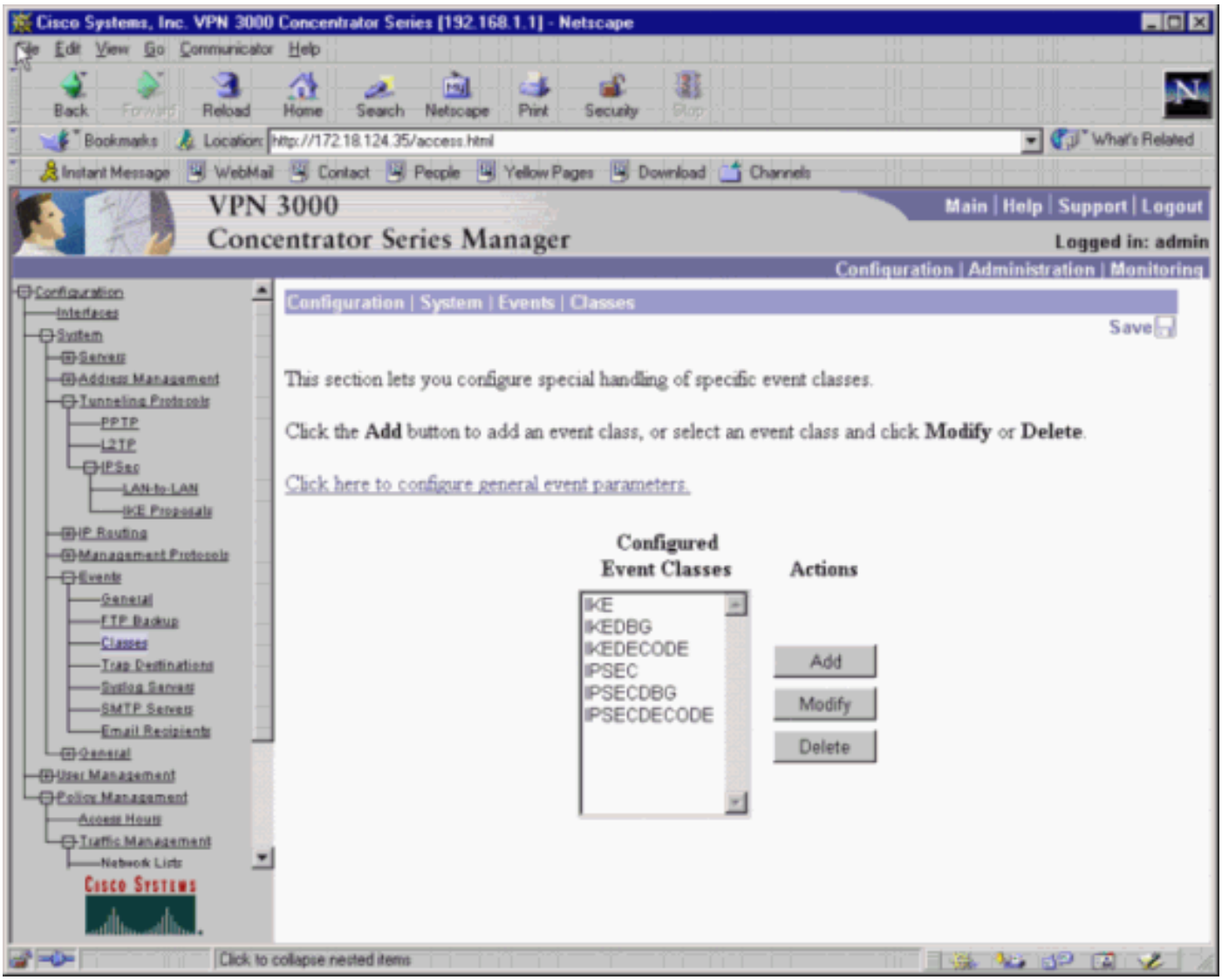
Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

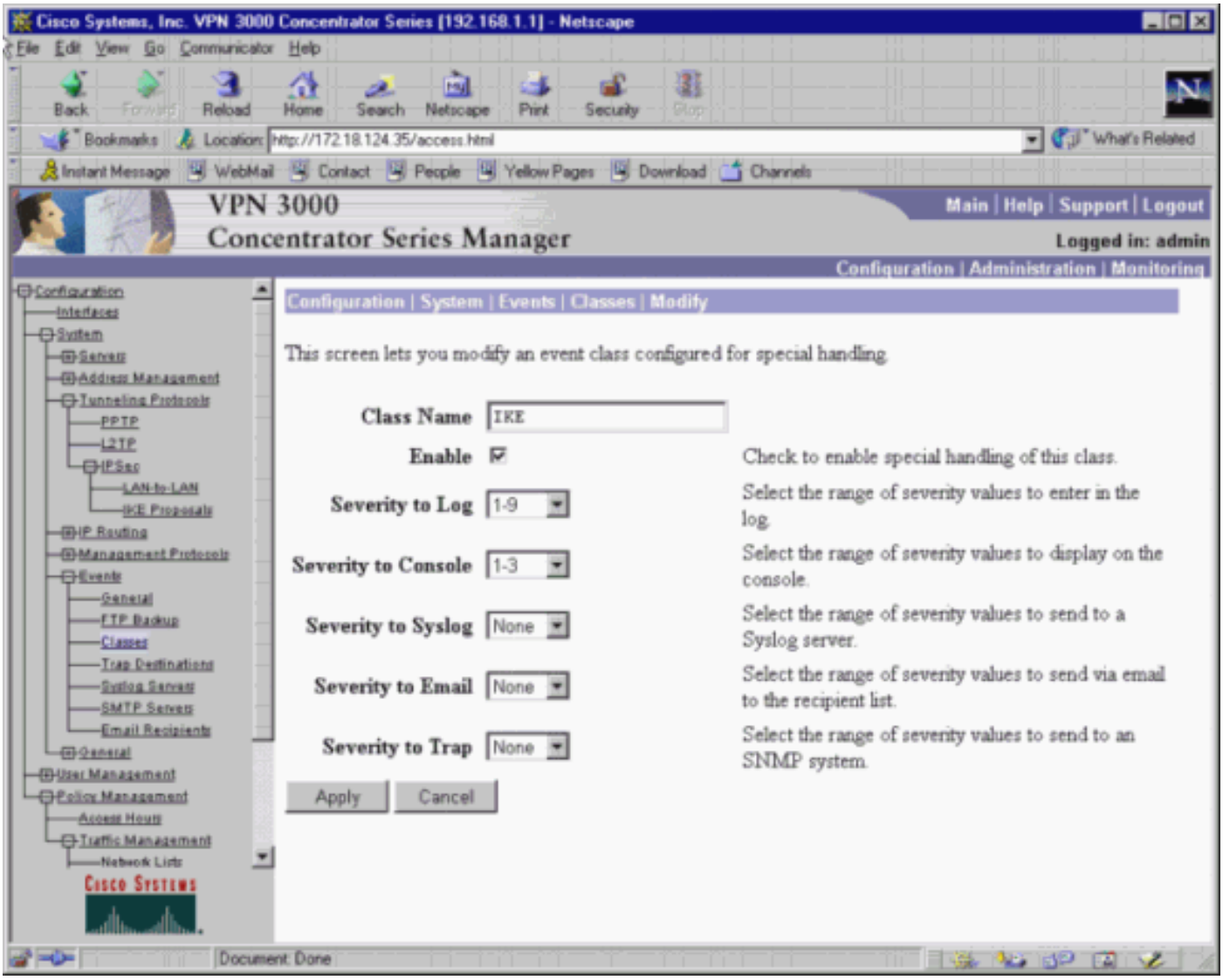
Sumarização da rede

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.

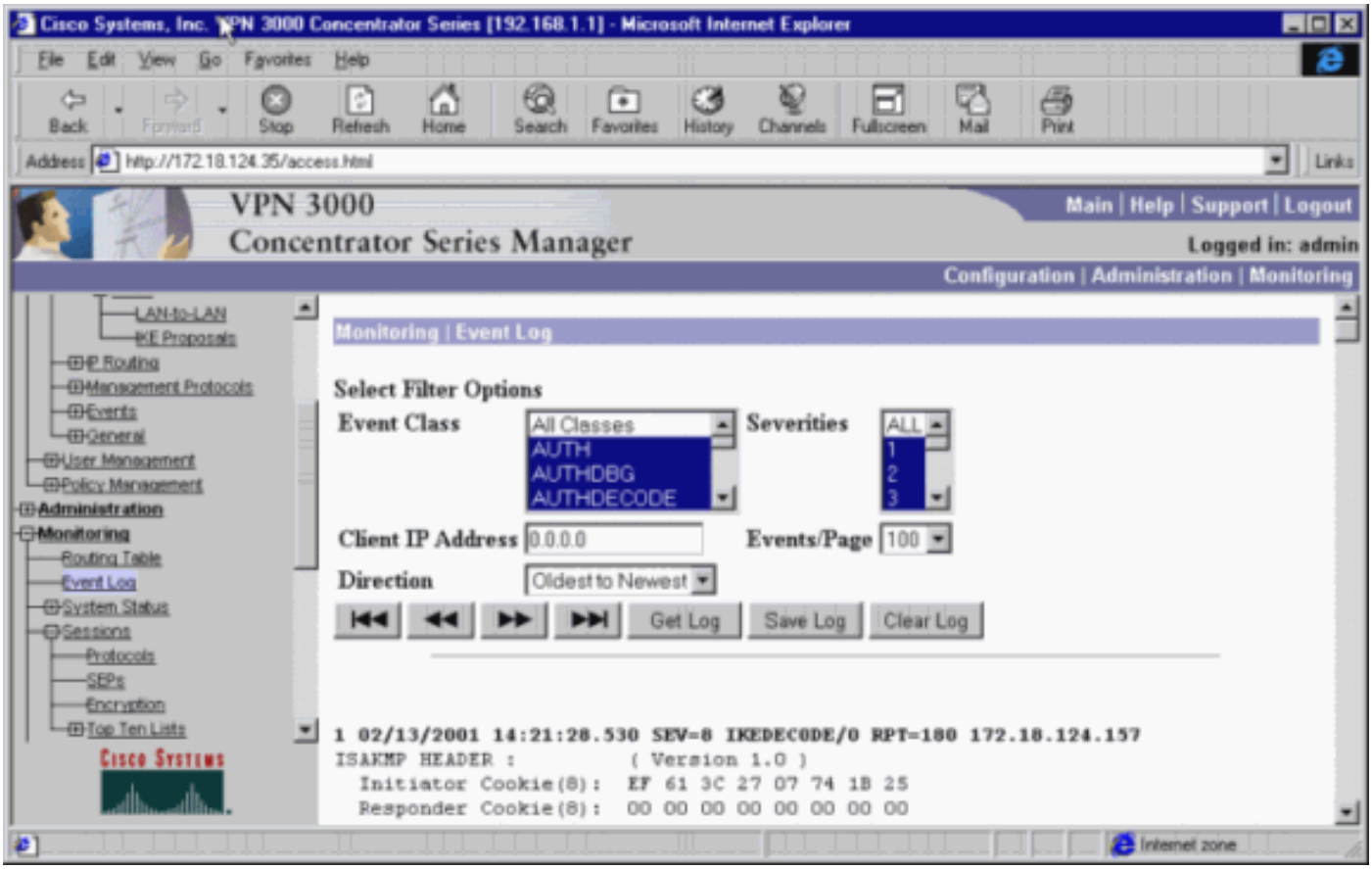
Debug de VPN 3000 Concentrator

O concentrador VPN possível debuga inclui o IKE, IKEDBG, IKEDECODE, IPSEC, IPSECDBG, IPSECDECODE. É configurado em Configuration > System > Events > Classes.

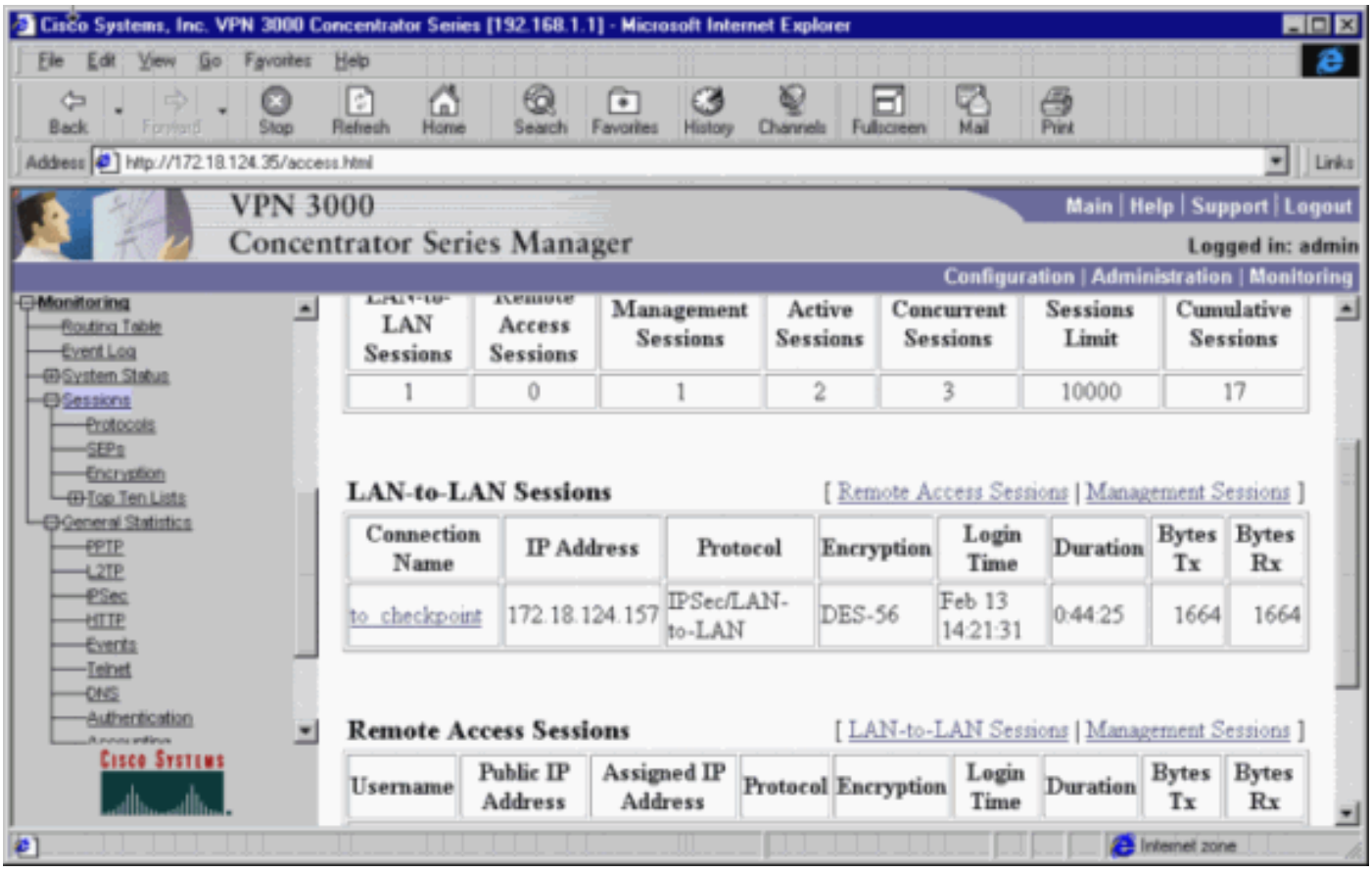




Épossível exibir depurações em Monitoring > Event log > Get Log.



Selecione o **monitoramento > sessões** para monitorar o tráfego de túnel do LAN para LAN.



Selecione o **administração > sessões de administrador > as sessões de LAN a LAN > ações - desconexão** para cancelar o túnel.

Debug de Checkpoint 4.1 Firewall

Note: Esta era uma instalação de Microsoft Windows NT. Como o rastreamento foi definido para Long na janela Policy Editor, o tráfego negado deve aparecer em vermelho em Log Viewer. Mais verboso debugar pode ser obtido com:

```
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 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 VPN 3000 Concentrator

```
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
```

Informações Relacionadas

- Negociação IPsec/Protocolos IKE
- Suporte Técnico e Documentação - Cisco Systems