Configuración de un túnel IPSec entre un concentrador VPN 3000 de Cisco y un firewall NG de punto de control

Contenido

Introducción

Este documento muestra cómo configurar un túnel IPsec con claves previamente compartidas para comunicarse entre dos redes privadas. En este ejemplo, las redes comunicantes son la red privada 192.168.10.x dentro del Cisco VPN 3000 Concentrator y la red privada 10.32.x.x dentro del firewall Checkpoint Next Generation (NG).

Prerequisites

Requirements

- El tráfico desde el interior del concentrador VPN y dentro del punto de control NG a Internet —representado aquí por las redes 172.18.124.x— debe fluir antes de comenzar esta configuración.
- Los usuarios deben estar familiarizados con la negociación IPSec. Este proceso se puede

dividir en cinco pasos, incluidas dos fases de intercambio de claves de Internet (IKE).Un túnel IPSec es iniciado por un tráfico interesado. Se considera que el tráfico es interesante cuando se transmite entre los pares IPSec.En la Fase 1 IKE, las entidades pares IPSec negocian la política establecida de la Asociación de seguridad (SA) IKE. Una vez que se autentican los pares, se crea un túnel seguro con la Asociación de seguridad de Internet y el protocolo de administración de claves (ISAKMP).En la Fase 2 de IKE, los peers IPSec utilizan el túnel autenticado y seguro para negociar las transformaciones de SA IPSec. La negociación de la política compartida determina el modo en que se establece el túnel IPSec.Se crea el túnel IPSec y los datos se transfieren entre los pares IPSec según los parámetros IPSec configurados en los conjuntos de transformación IPSec.El túnel IPSec termina cuando los IPSec SAs son borrados o cuando caduca su vigencia.

Componentes Utilizados

Esta configuración se desarrolló y aprobó con las siguientes versiones de software y hardware:

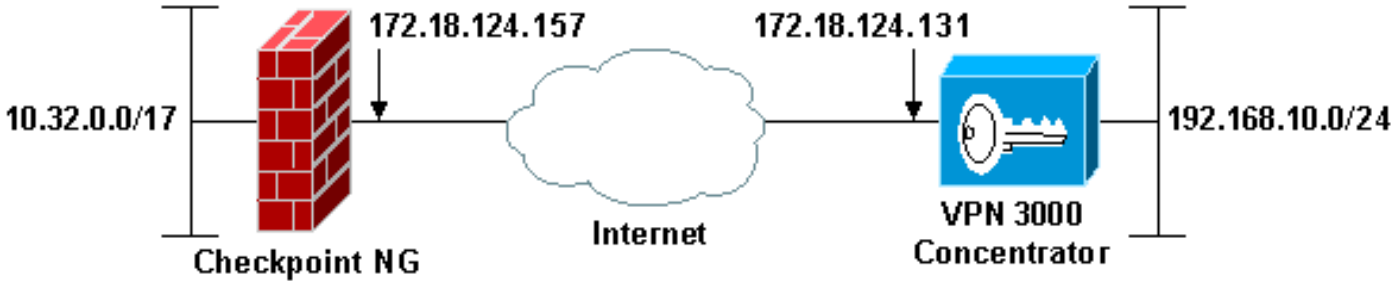
- Concentrador de la serie VPN 3000 3.5.2
- Firewall NG de punto de control

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Nota: El esquema de direccionamiento IP utilizado en esta configuración no es legalmente enrutable en Internet. Son direcciones RFC 1918, que se han utilizado en un entorno de laboratorio.

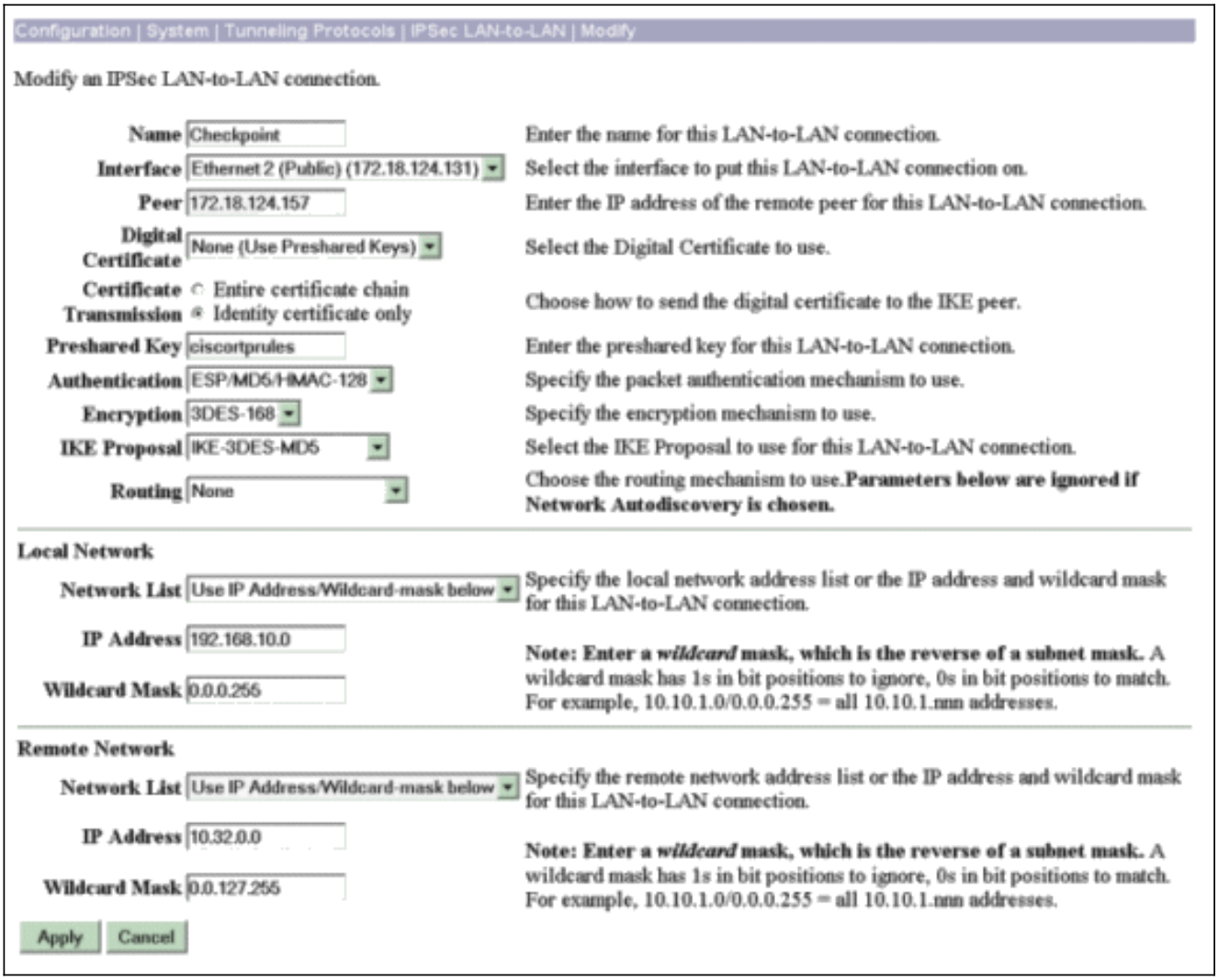
Configuraciones

Configurar el concentrador VPN 3000

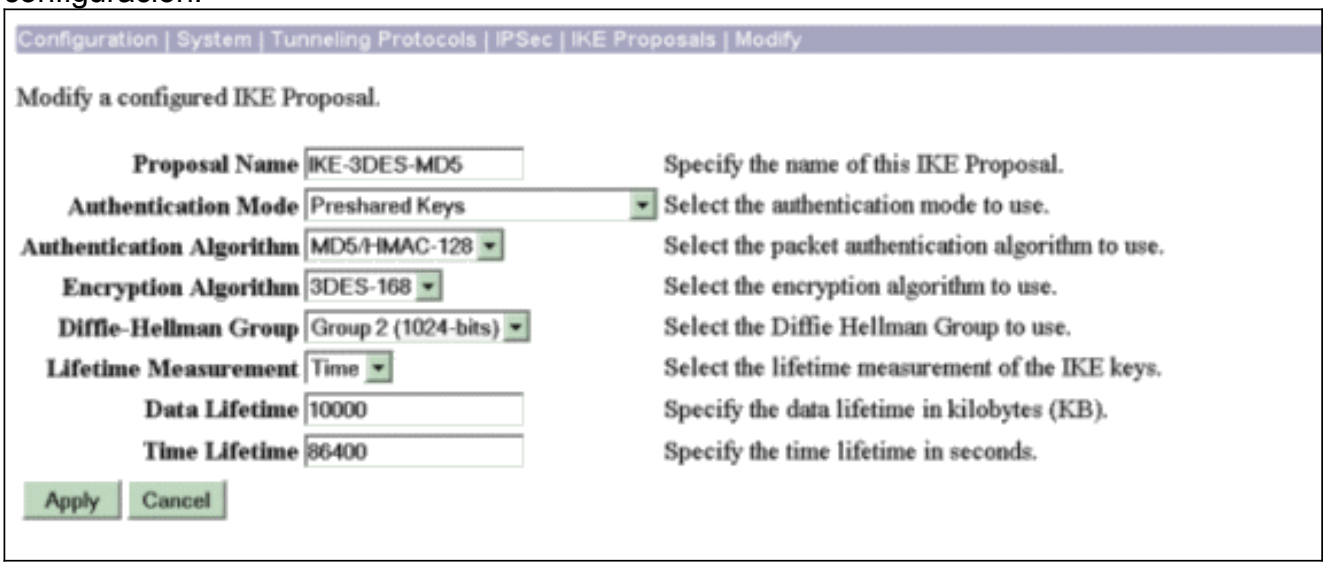
Complete estos pasos para configurar el VPN 3000 Concentrator:

1. Vaya a **Configuration > System > Tunneling Protocols > IPSec LAN a LAN** para configurar la sesión LAN a LAN. Establezca las opciones para los algoritmos de autenticación e IKE,

clave previamente compartida, dirección IP de peer y parámetros de red local y remota. Haga clic en Apply (Aplicar).En esta configuración, la autenticación se configuró como ESP-MD5-HMAC y el cifrado se configuró como
3DES.



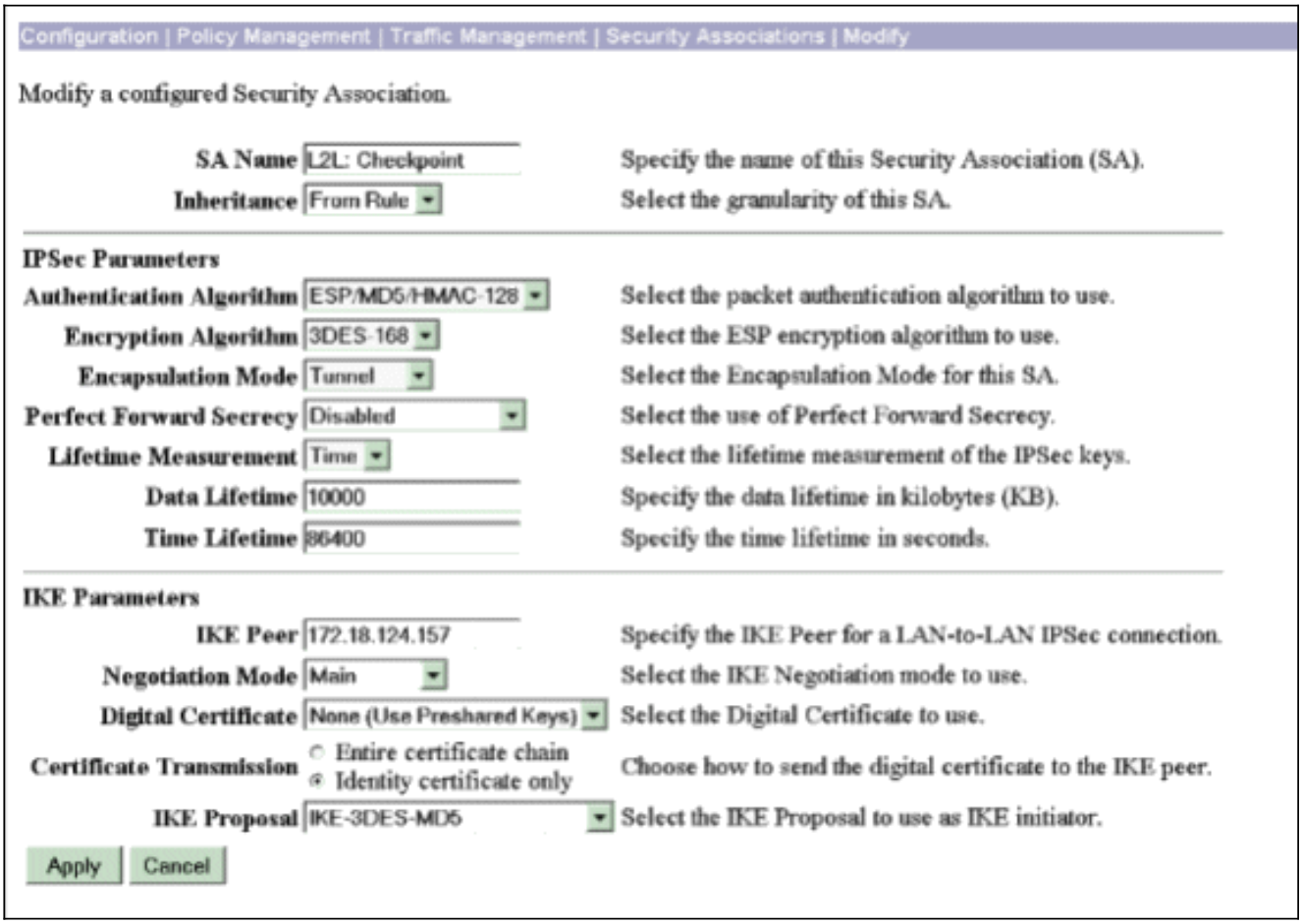
2. Vaya a **Configuration > System > Tunneling Protocols > IPSec > IKE Proposale** y establezca los parámetros requeridos.Seleccione la propuesta IKE IKE-3DES-MD5 y verifique los parámetros seleccionados para la propuesta. Haga clic en **Aplicar** para configurar la sesión de LAN a LAN.Estos son los parámetros para esta
configuración:



3. Vaya a **Configuration > Policy Management > Traffic Management > Security Associations**,

seleccione la SA IPSec creada para la sesión y verifique los parámetros SA IPSec elegidos para la sesión LAN a LAN.En esta configuración, el nombre de la sesión LAN a LAN era "Checkpoint", por lo que la SA IPSec se creó automáticamente como "L2L: Punto de control".

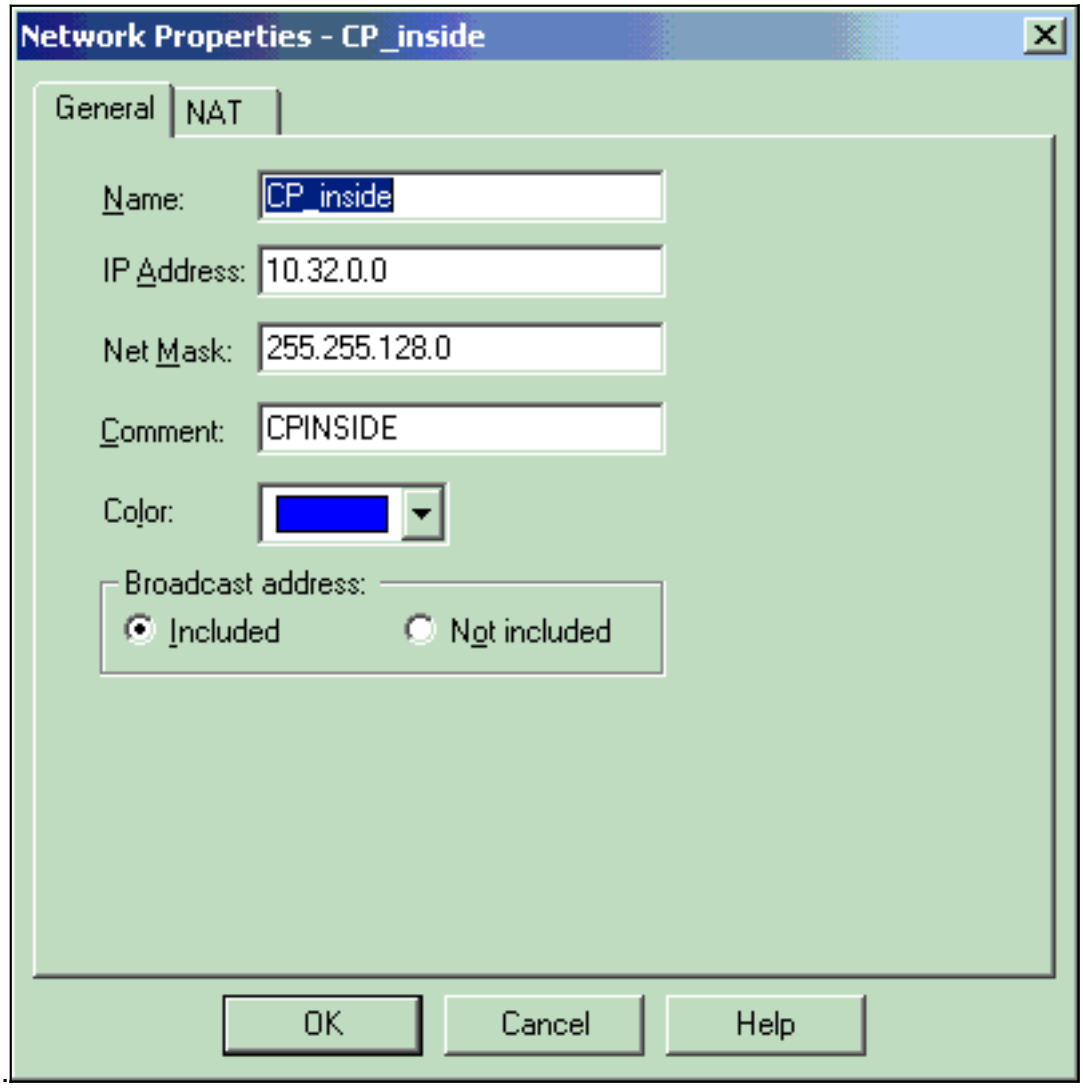
Estos son los parámetros para esta SA:

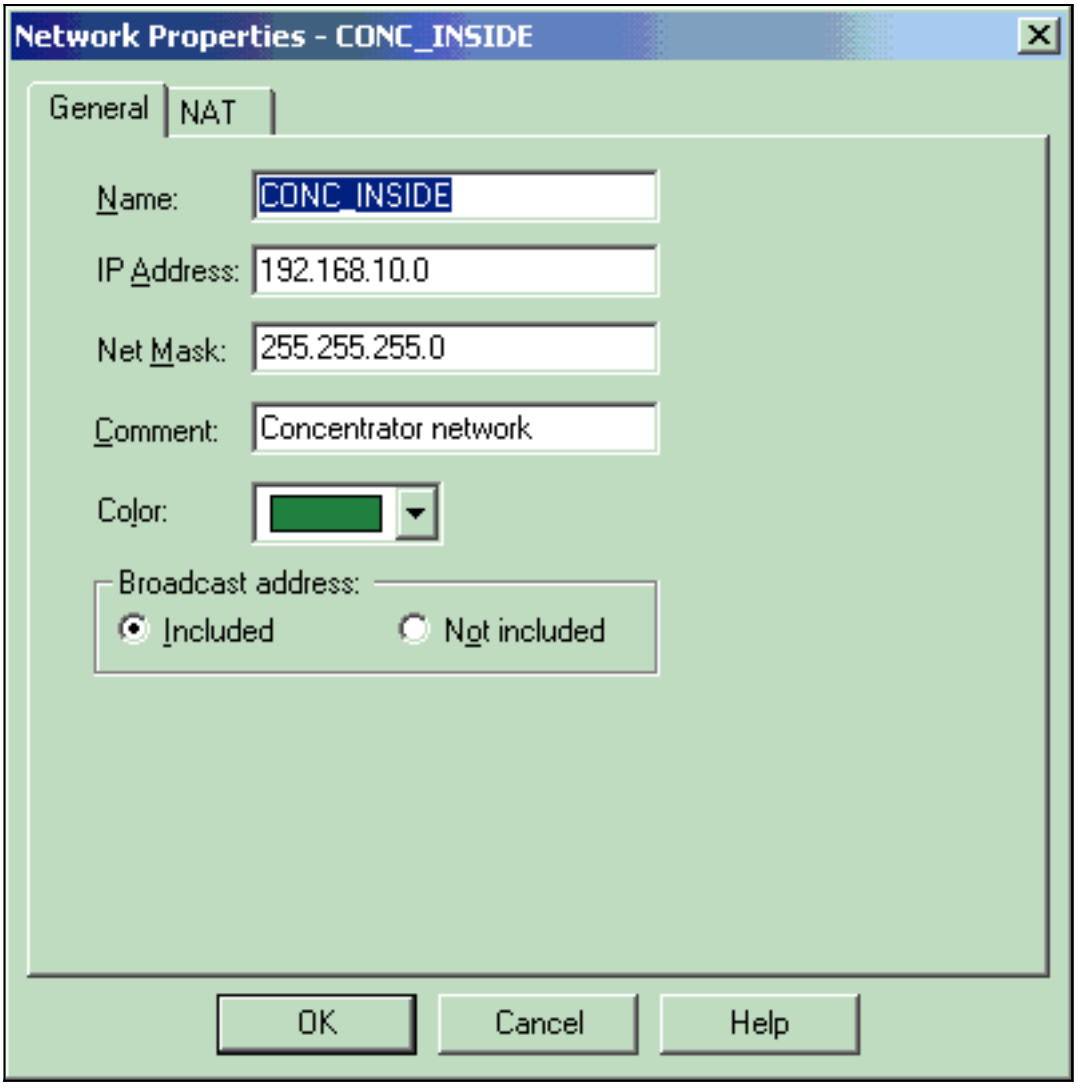


Configuración del punto de control NG

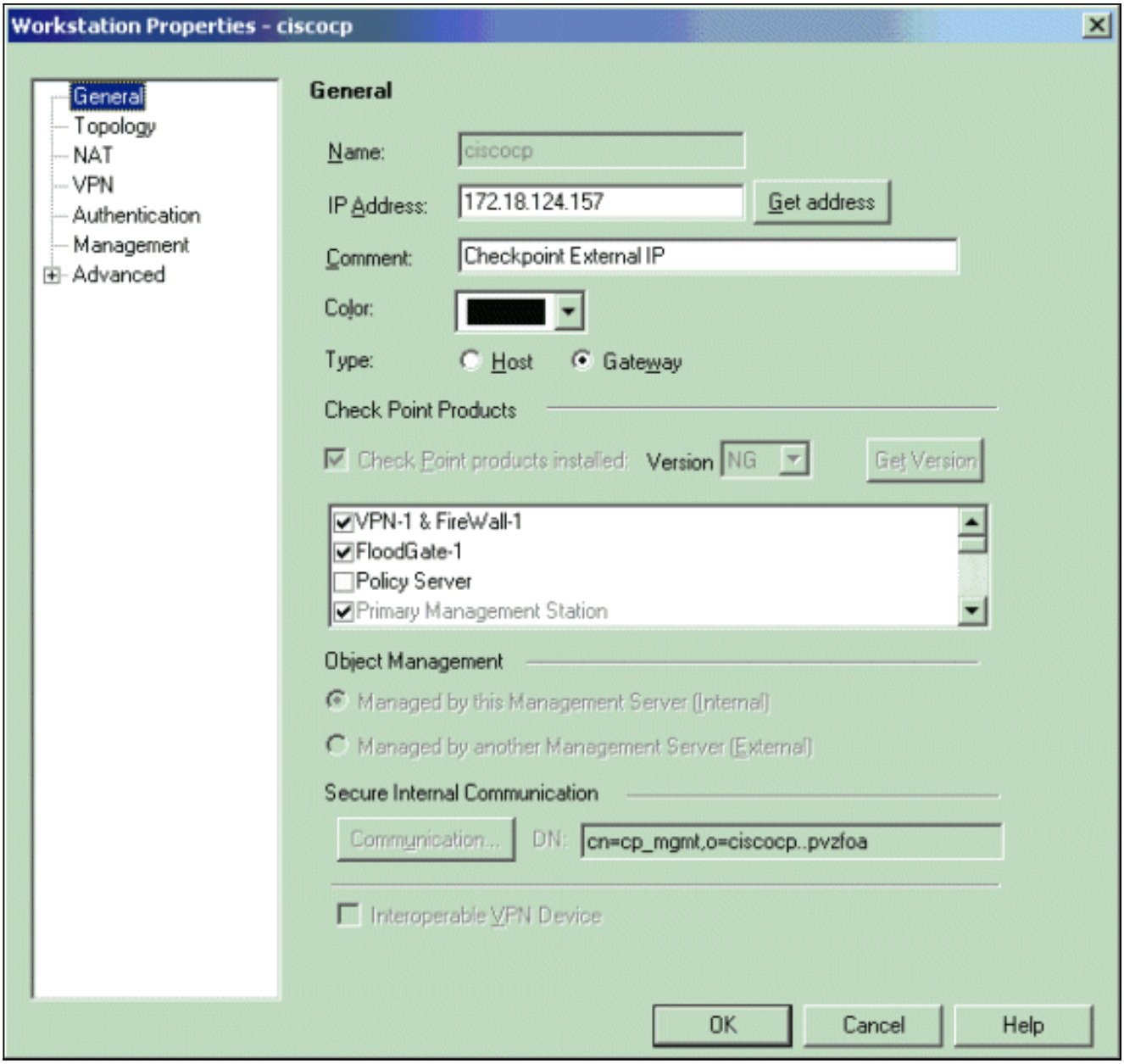
Los objetos de red y las reglas se definen en el NG del punto de control para formar la política que pertenece a la configuración de VPN que se va a configurar. A continuación, esta política se instala con el Editor de políticas de NG de punto de control para completar el lado NG de punto de control de la configuración.

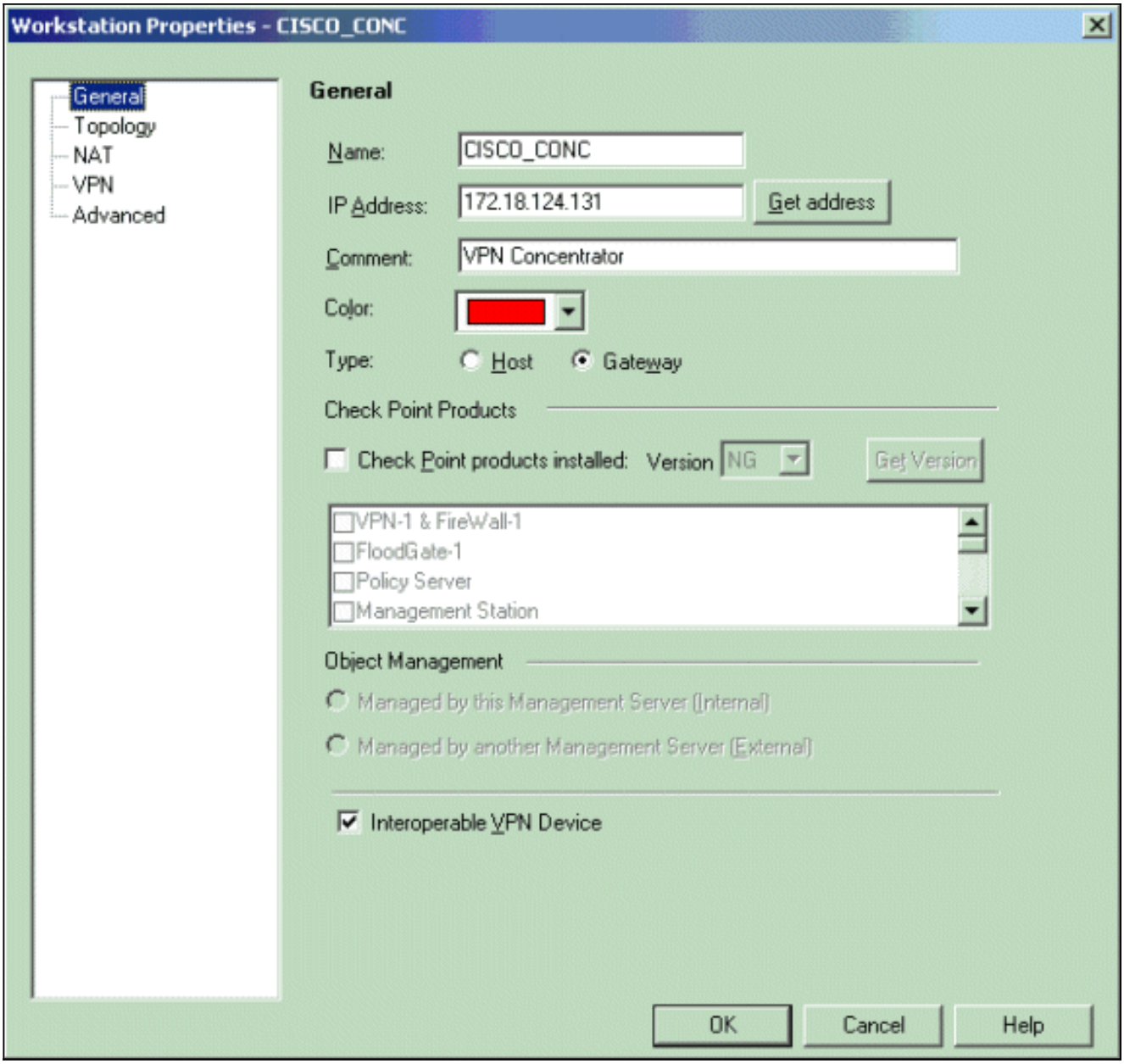
1. Cree los dos objetos de red para la red NG de punto de control y la red VPN Concentrator que cifrarán el tráfico interesante.para crear objetos, seleccione **Administrar > Objetos de red** y, a continuación, seleccione **Nuevo > Red**. Introduzca la información de red adecuada y, a continuación, haga clic en Aceptar.Estos ejemplos muestran la configuración de los objetos de red denominados CP_inside (la red interna del punto de control NG) y CONC_INSIDE (la red interna del concentrador VPN).



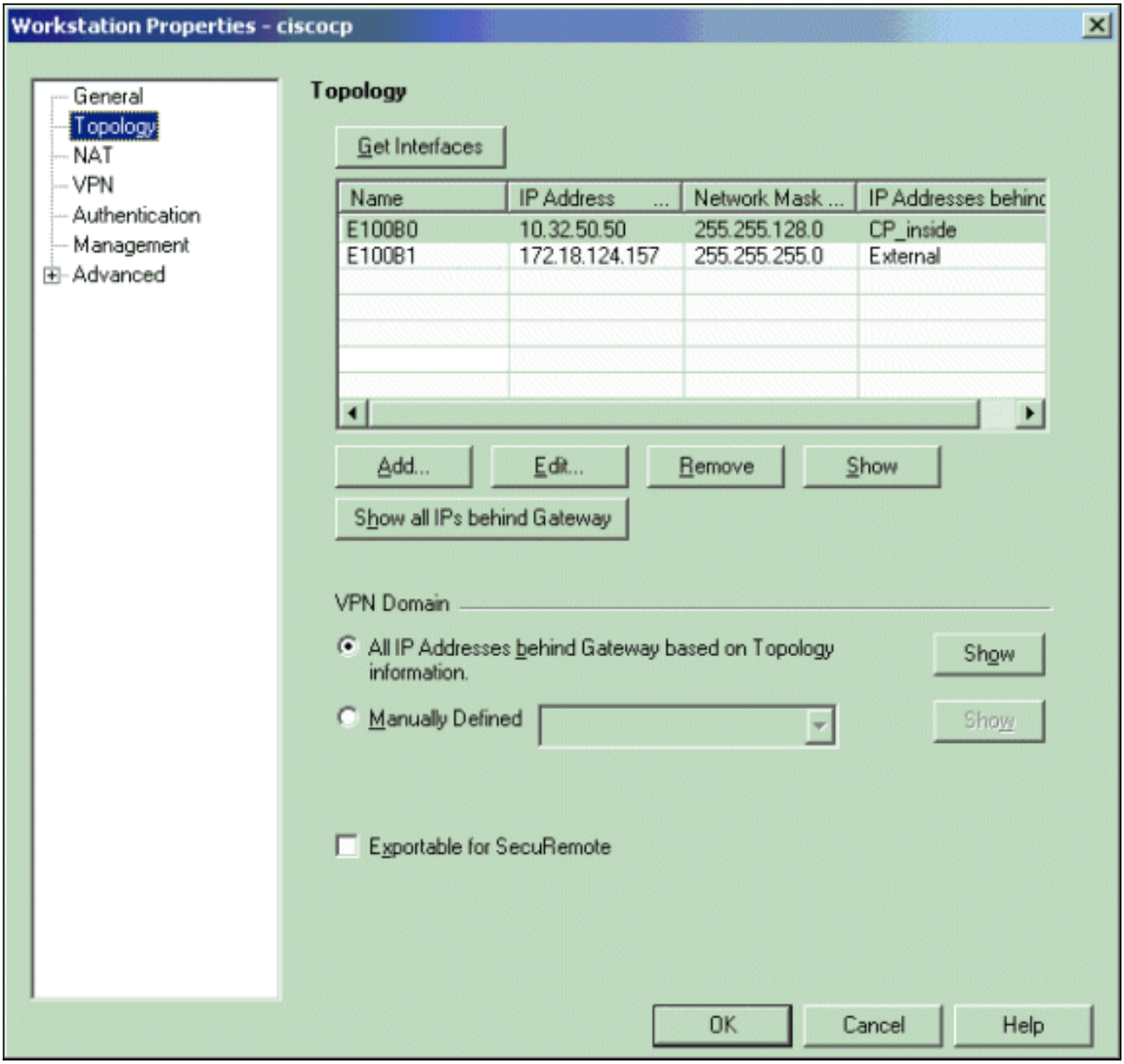


2. Vaya a **Manage > Network Objects** y seleccione **New > Workstation** para crear objetos de estación de trabajo para los dispositivos VPN, Checkpoint NG y VPN Concentrator.**Nota:** Puede utilizar el objeto de estación de trabajo NG de punto de control creado durante la configuración inicial de NG de punto de control. Seleccione las opciones para configurar la estación de trabajo como Gateway y dispositivo VPN interoperable y, a continuación, haga clic en **Aceptar**.Estos ejemplos muestran la configuración de objetos llamados ciscocp (Checkpoint NG) y CISCO_CONC (VPN 3000
Concentrator):

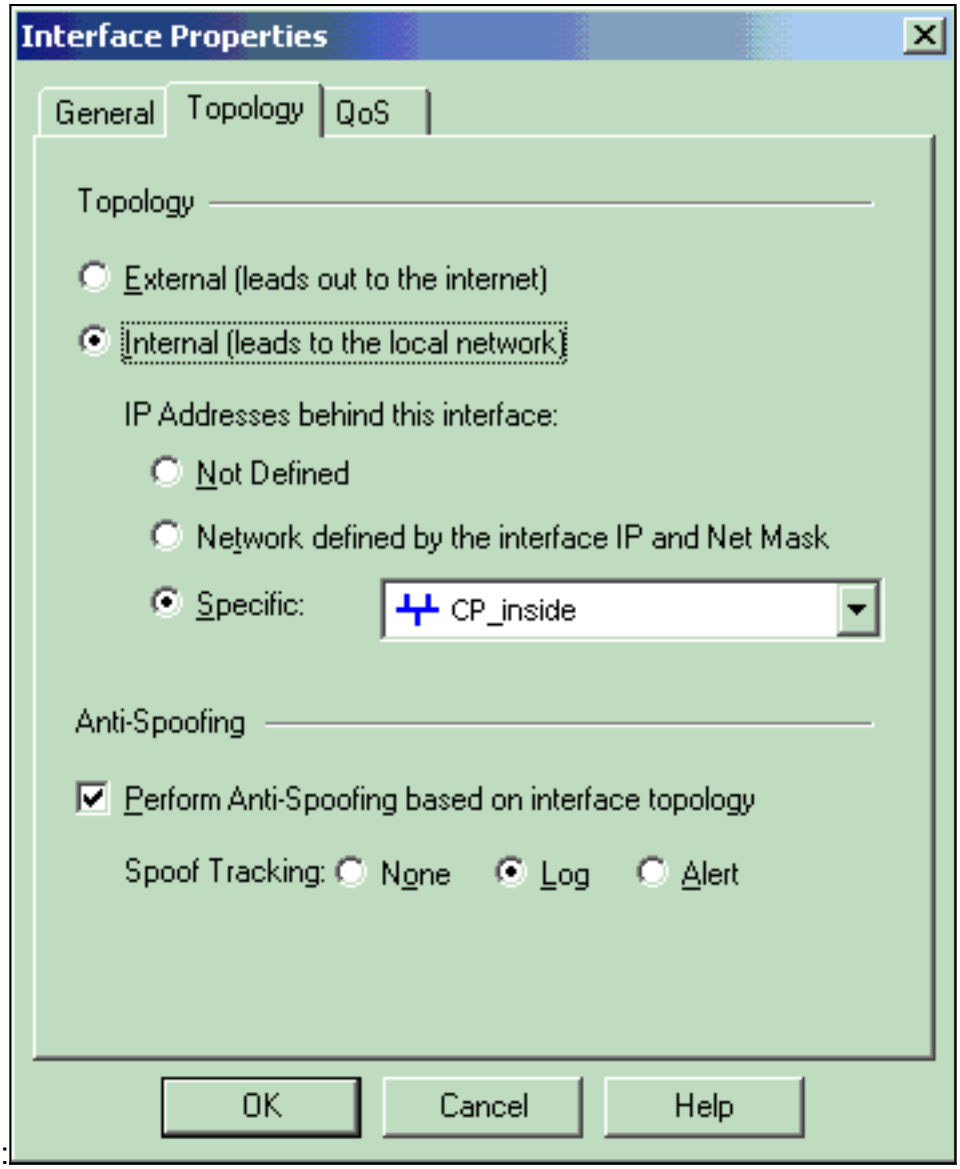

Workstation Properties - ciscocp
General
Topology
NAT
VPN
Authentication
Management
Advanced
General
Name:
ciscocp
IP Address:
172.18.124.157
Get address
Comment:
Checkpoint External IP
Color:
Type:
Host
Gateway
Check Point Products
Check Point products installed:
Version
NG
Get Version
VPN-1 & FireWall-1
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. Vaya a **Administrar > Objetos de Red > Editar** para abrir la ventana Propiedades de la Estación de Trabajo para la estación de trabajo NG de punto de control (ciscocp en este ejemplo). Seleccione **Topology** en las opciones del lado izquierdo de la ventana y luego seleccione la red que desea cifrar. Haga clic en **Editar** para establecer las propiedades de la interfaz.En este ejemplo, CP_inside es la red interna del punto de control NG.

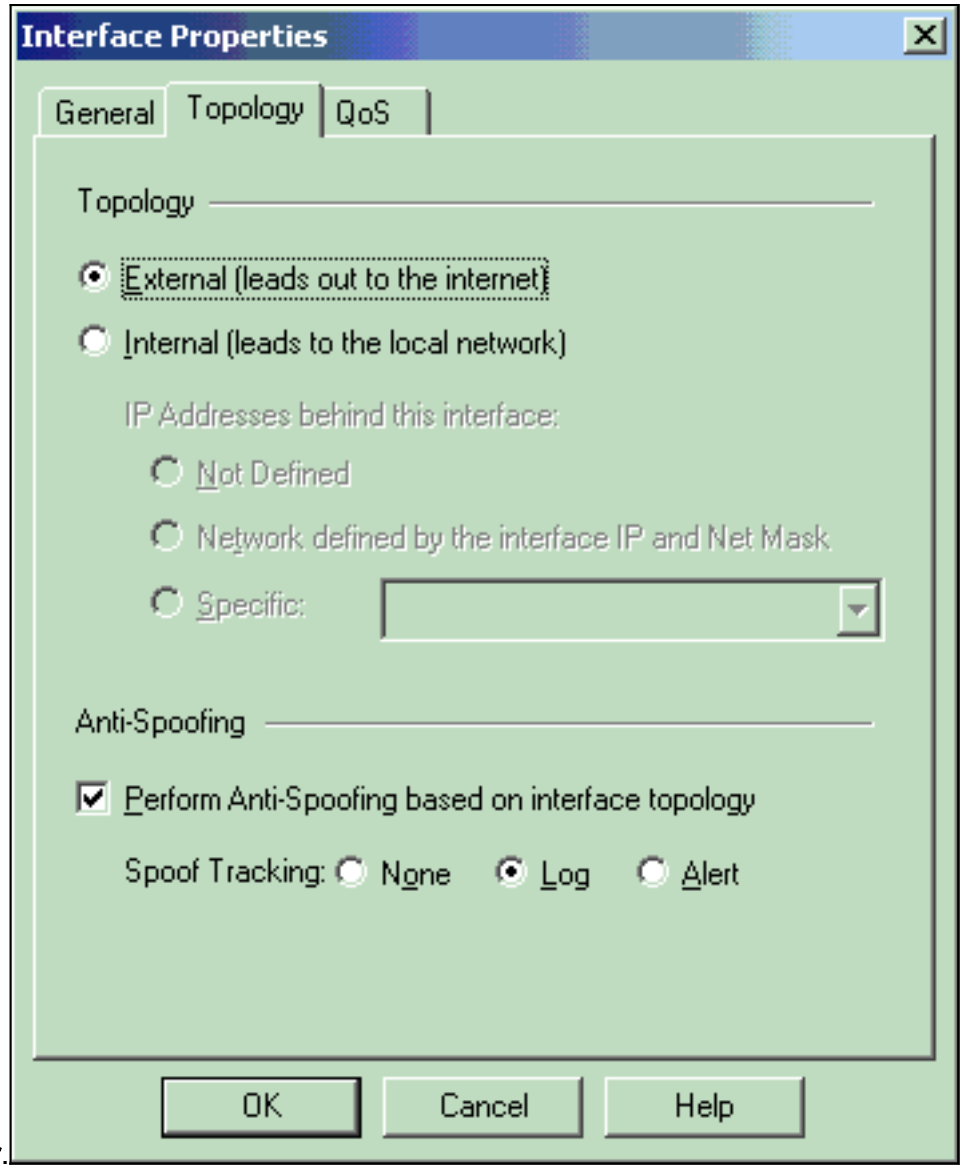


4. En la ventana Propiedades de la interfaz, seleccione la opción para designar la estación de trabajo como interna y, a continuación, especifique la dirección IP adecuada. Click OK.Las selecciones de topología mostradas designan la estación de trabajo como interna y especifican las direcciones IP detrás de la interfaz



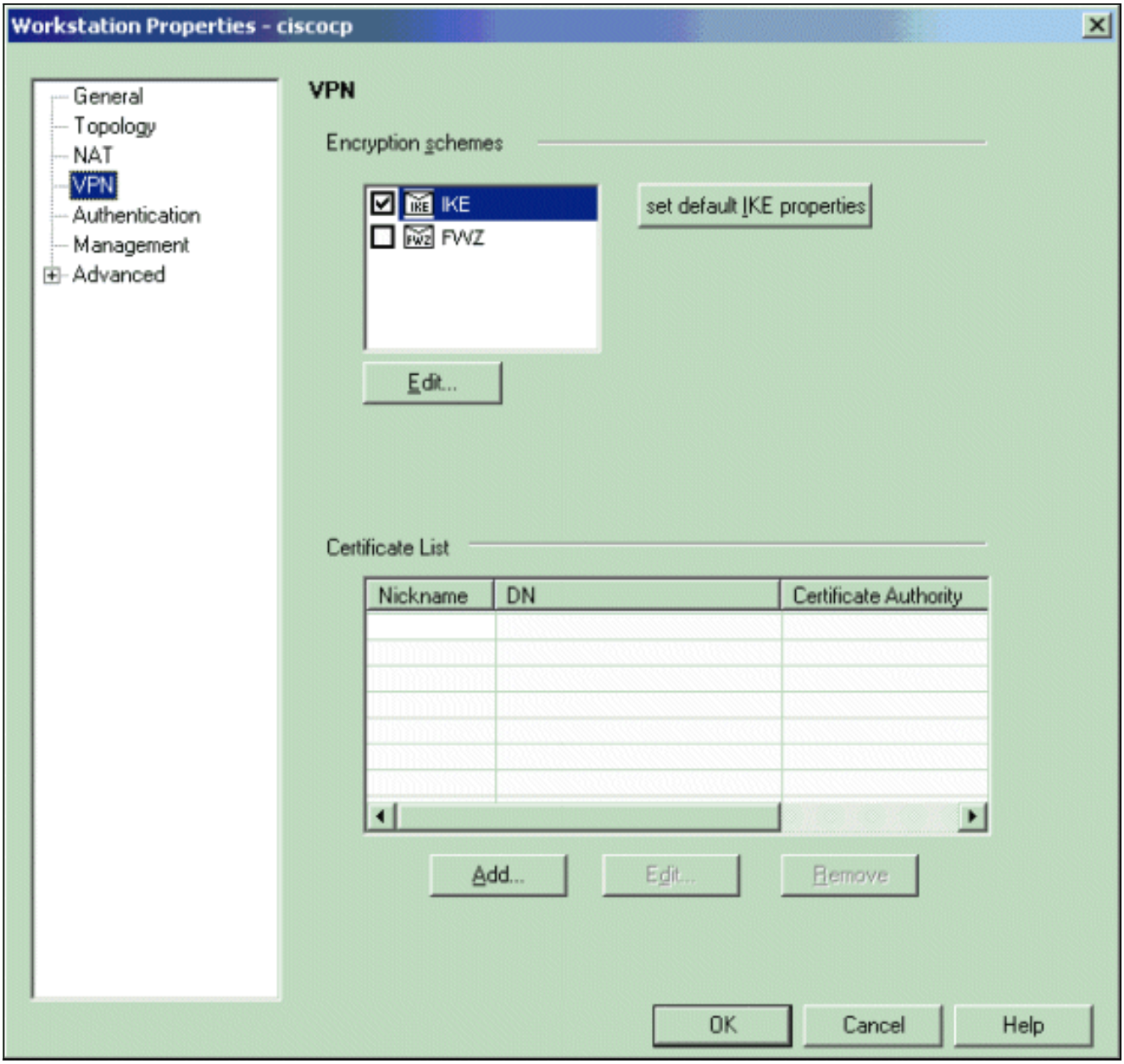
CP_inside:

5. En la ventana Propiedades de la estación de trabajo, seleccione la interfaz exterior en el Checkpoint NG que lleva a Internet y luego haga clic en **Editar** para establecer las propiedades de la interfaz. Seleccione la opción para designar la topología como externa y luego haga clic en

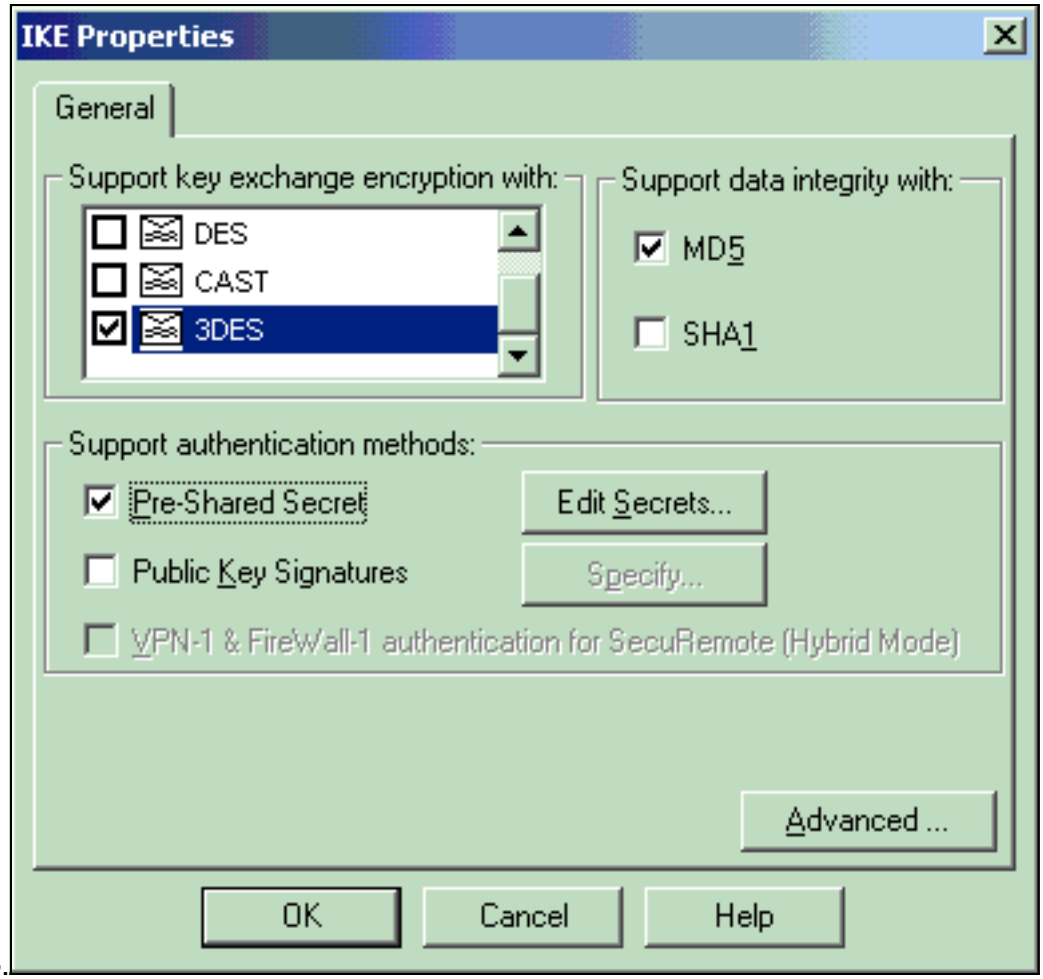


Aceptar.

6. En la ventana Propiedades de la estación de trabajo en el Checkpoint NG, seleccione **VPN** de las opciones del lado izquierdo de la ventana y, a continuación, seleccione los parámetros IKE para los algoritmos de cifrado y autenticación. Haga clic en **Edit** para configurar las propiedades
IKE.

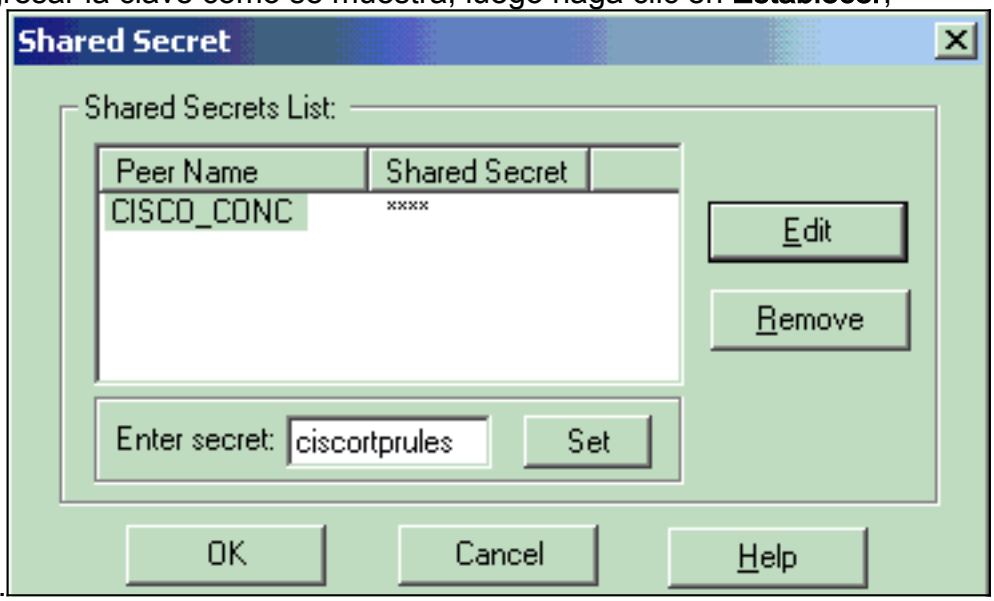


7. Establezca las propiedades IKE para que coincidan con las propiedades del concentrador VPN.En este ejemplo, seleccione la opción de cifrado para **3DES** y la opción de hash para



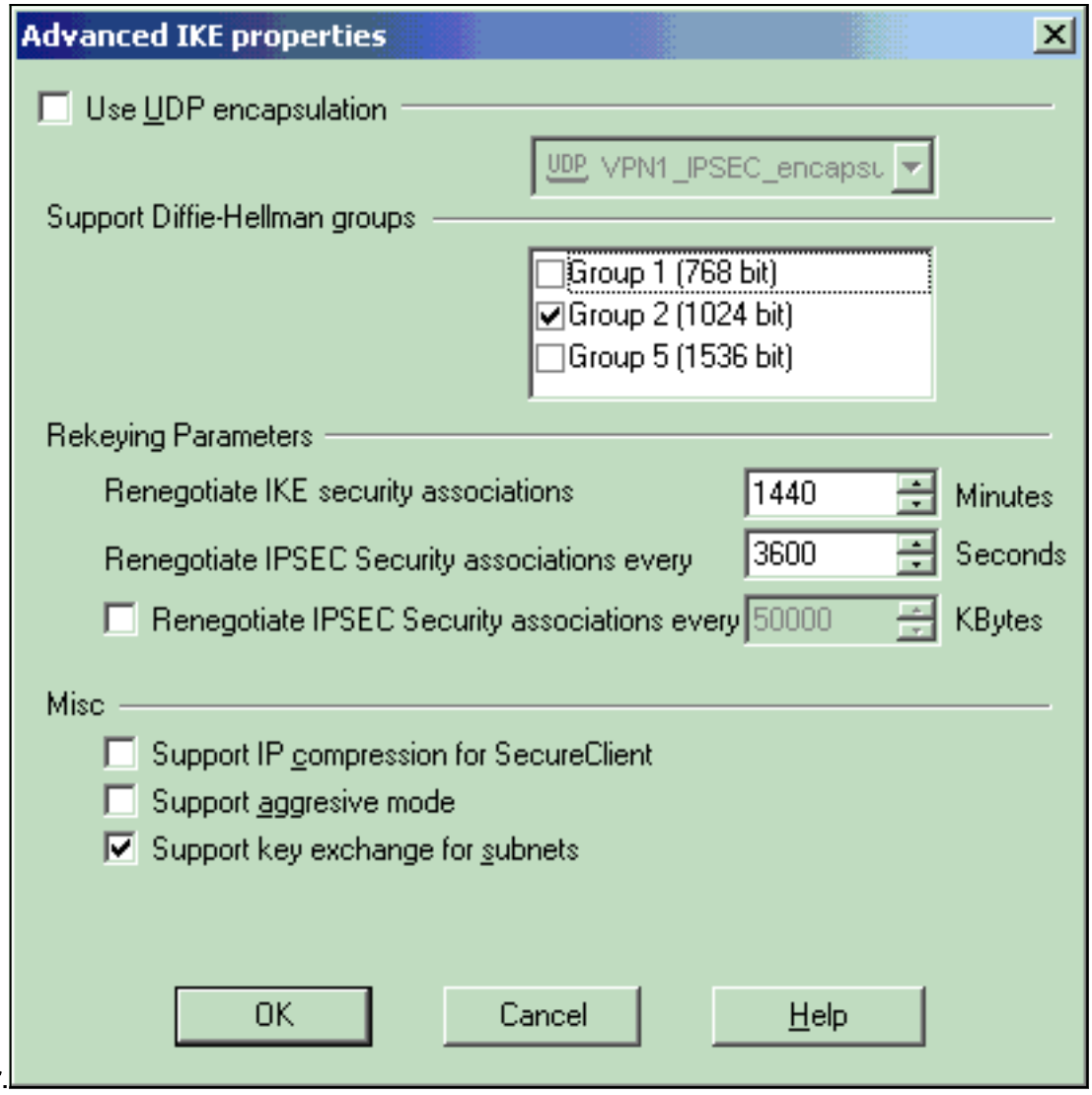
MD5.

8. Seleccione la opción de autenticación para **Secretos Previamente Compartidos** y luego haga clic en **Editar Secretos** para establecer la clave previamente compartida para que sea compatible con la clave previamente compartida en el concentrador VPN. Haga clic en **Editar** para ingresar la clave como se muestra, luego haga clic en **Establecer**,



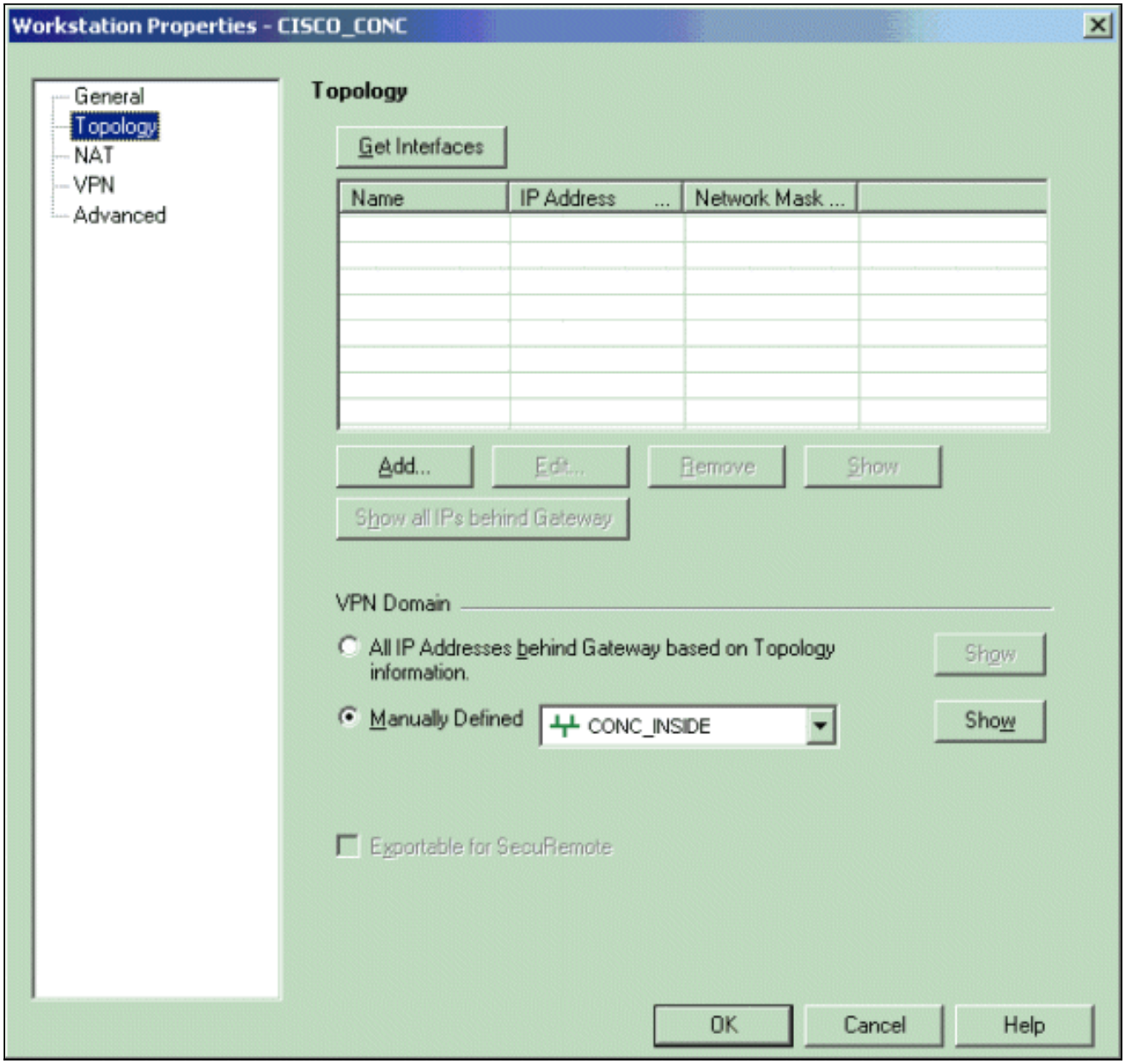
Aceptar.

9. En la ventana de propiedades IKE, haga clic en **Avanzadas...** y cambie estos parámetros:Anule la selección de la opción **Support agresive mode**.Seleccione la opción para el **intercambio de claves Support para subredes**.Cuando haya terminado, haga clic en **Aceptar**,

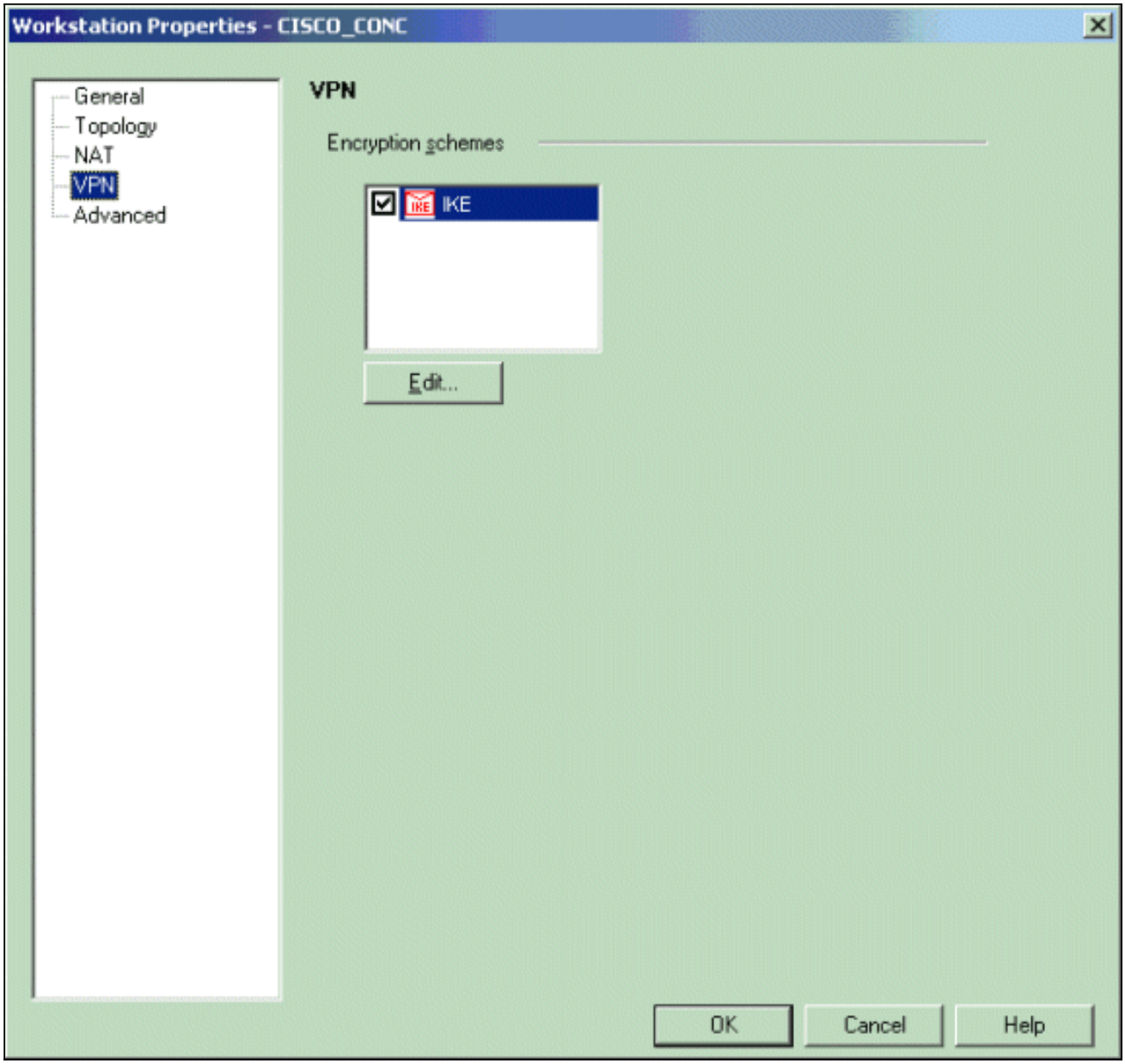


Aceptar.

10. Vaya a **Administrar > Objetos de Red > Editar** para abrir la ventana Propiedades de la Estación de Trabajo para el Concentrador VPN. Seleccione **Topology** en las opciones del lado izquierdo de la ventana para definir manualmente el dominio VPN.En este ejemplo, CONC_INSIDE (la red interna del concentrador VPN) se define como el dominio VPN.

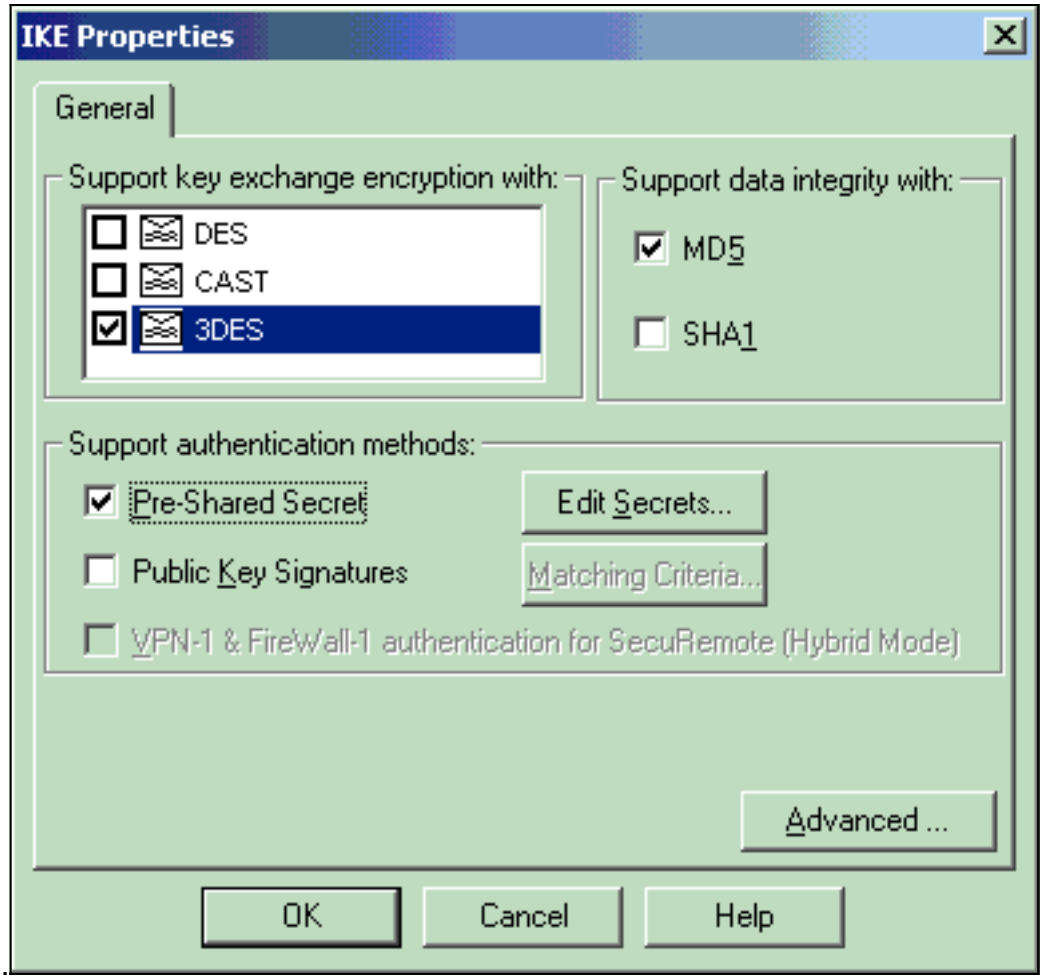


11. Seleccione **VPN** de las opciones del lado izquierdo de la ventana y luego seleccione **IKE** como esquema de encriptación. Haga clic en **Edit** para configurar las propiedades IKE.

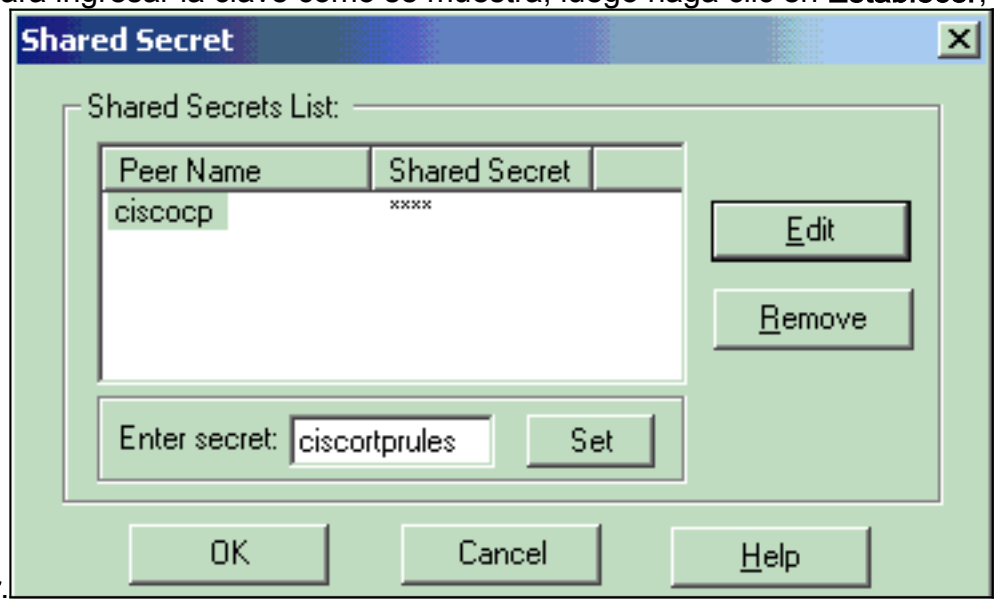


12. Establezca las propiedades IKE para reflejar la configuración actual en el concentrador VPN.En este ejemplo, establezca la opción de encripción para **3DES** y la opción de

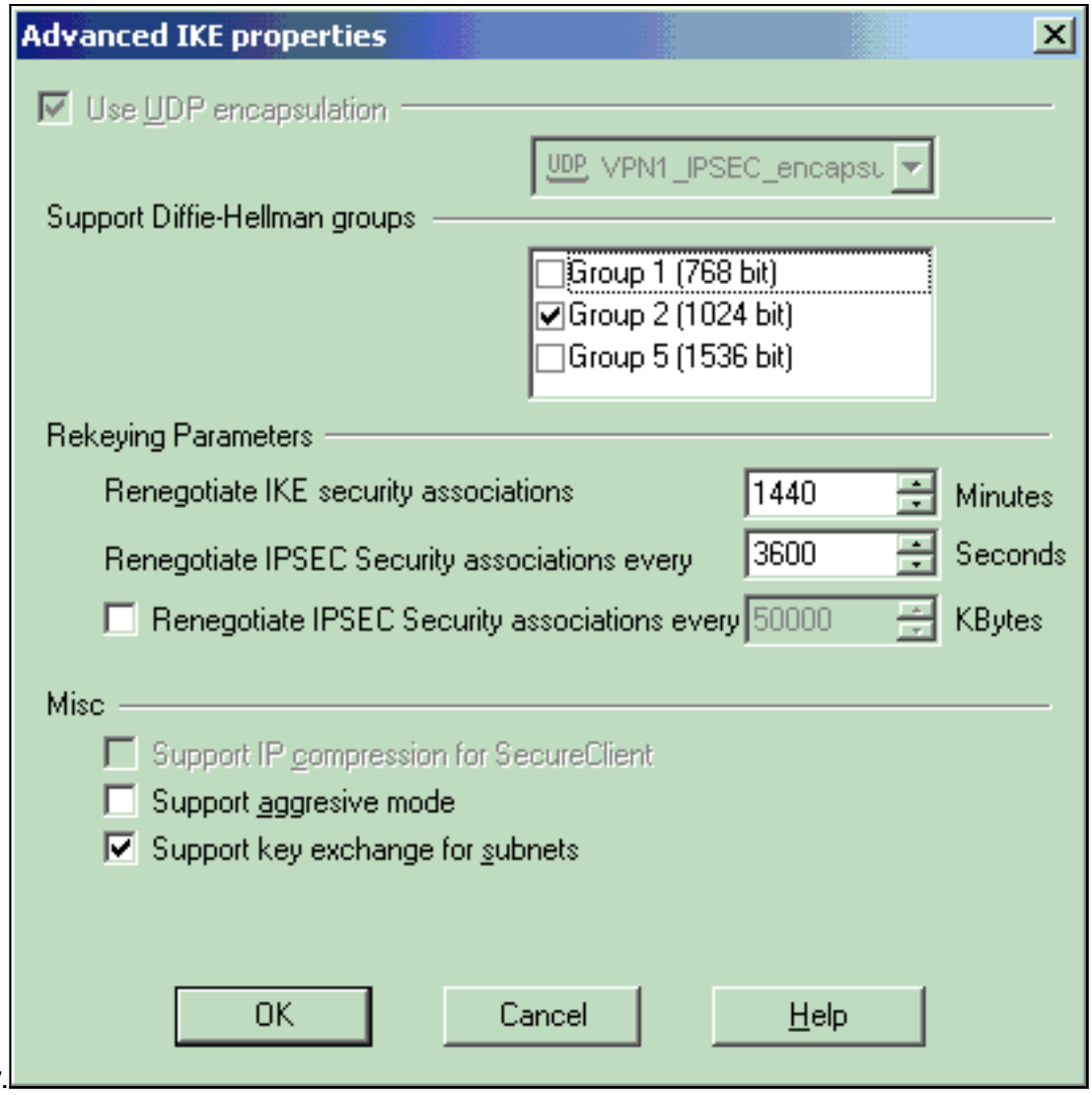
hashing para **MD5**.



13. Seleccione la opción de autenticación para **Secretos Previamente Compartidos** y luego haga clic en **Editar Secretos** para establecer la clave previamente compartida. Haga clic en **Editar** para ingresar la clave como se muestra, luego haga clic en **Establecer**, **Aceptar**.

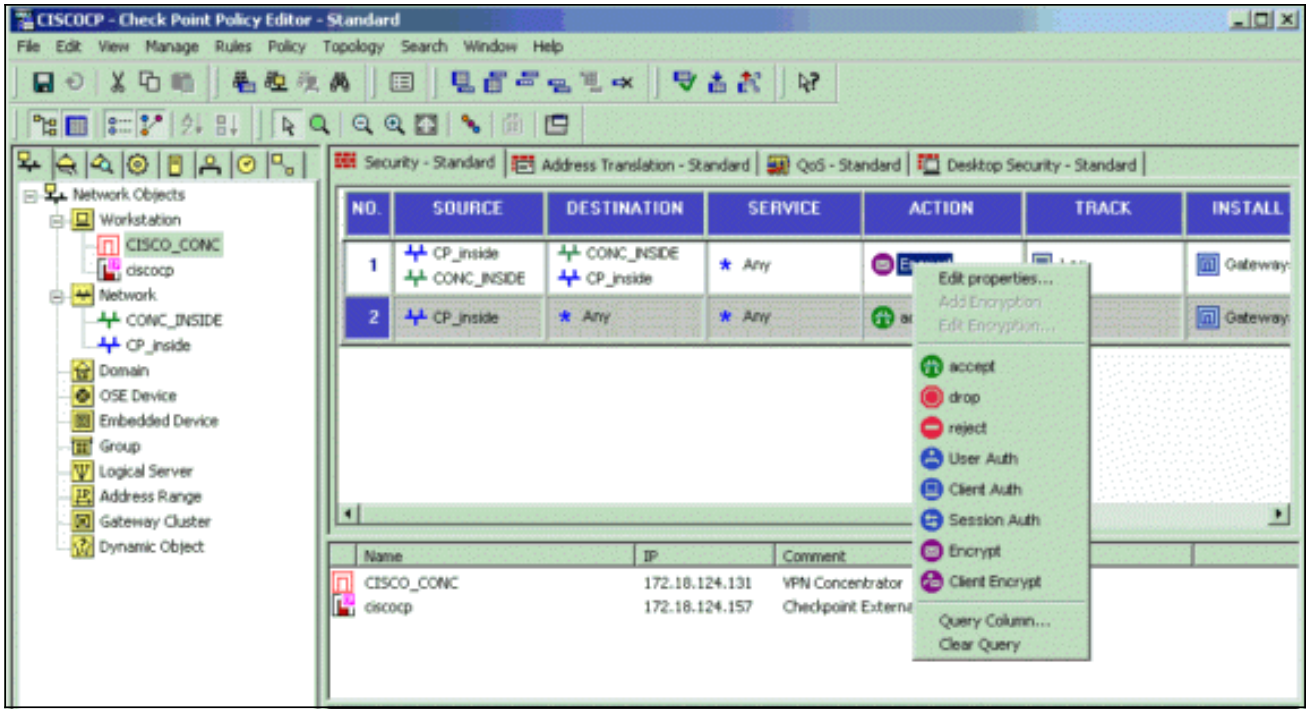


14. En la ventana de propiedades IKE, haga clic en **Avanzadas...** y cambie estos parámetros:Seleccione el grupo Diffie-Hellman adecuado para las propiedades IKE.Anule la selección de la opción **Support agresive mode**.Seleccione la opción para el **intercambio de claves Support para subredes**.Cuando haya terminado, haga clic en **Aceptar**,

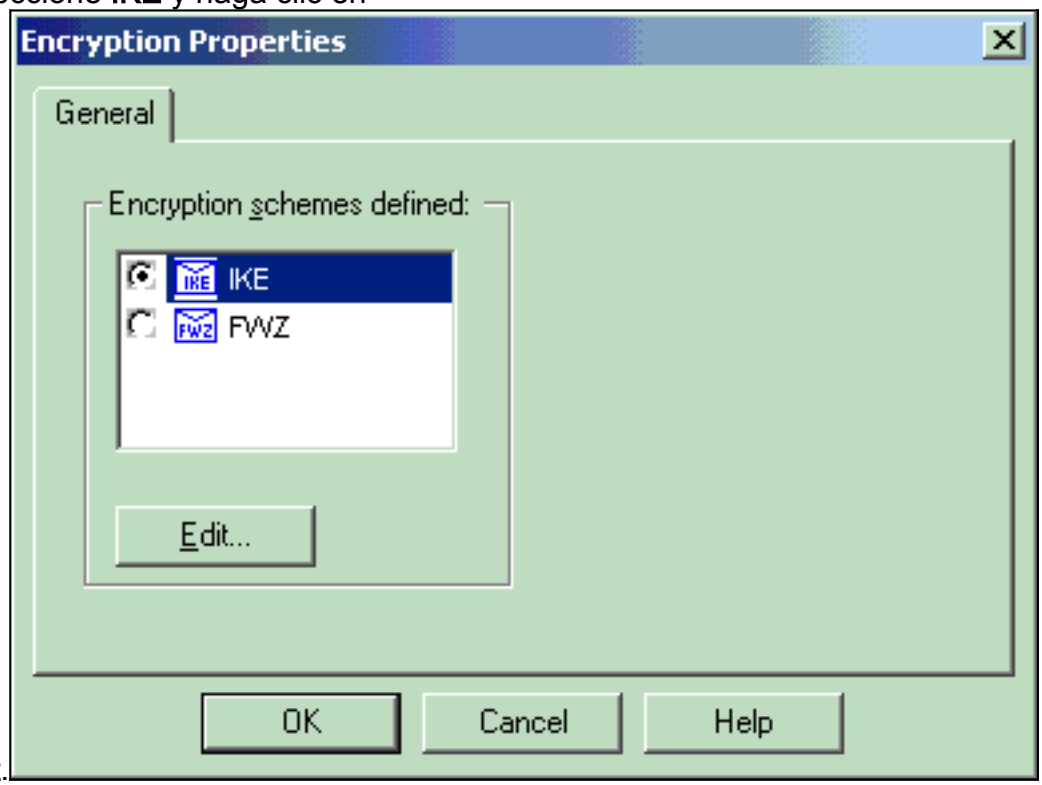


Aceptar.

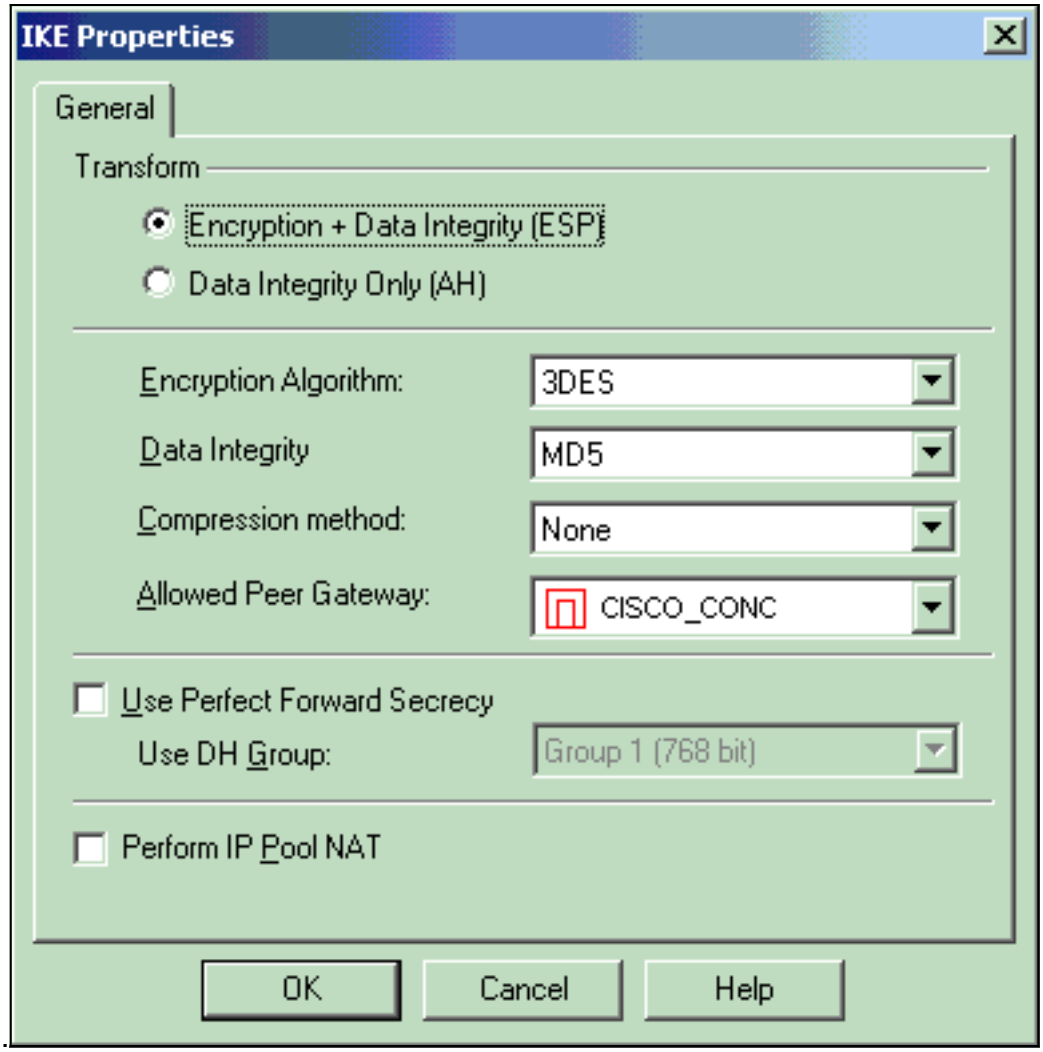
15. Seleccione **Reglas > Agregar reglas > Arriba** para configurar las reglas de cifrado para la política. En la ventana Policy Editor, inserte una regla con el origen como CP_inside (red interna del punto de control NG) y el destino como CONC_INSIDE (red interna del concentrador VPN). Establecer valores para **Servicio = Any** , **Action = Encrypt** y **Track = Log**. Cuando haya agregado la sección Acción de cifrado de la regla, haga clic con el botón derecho en **Acción** y seleccione **Editar propiedades**.



16. Seleccione **IKE** y haga clic en **Edit**.

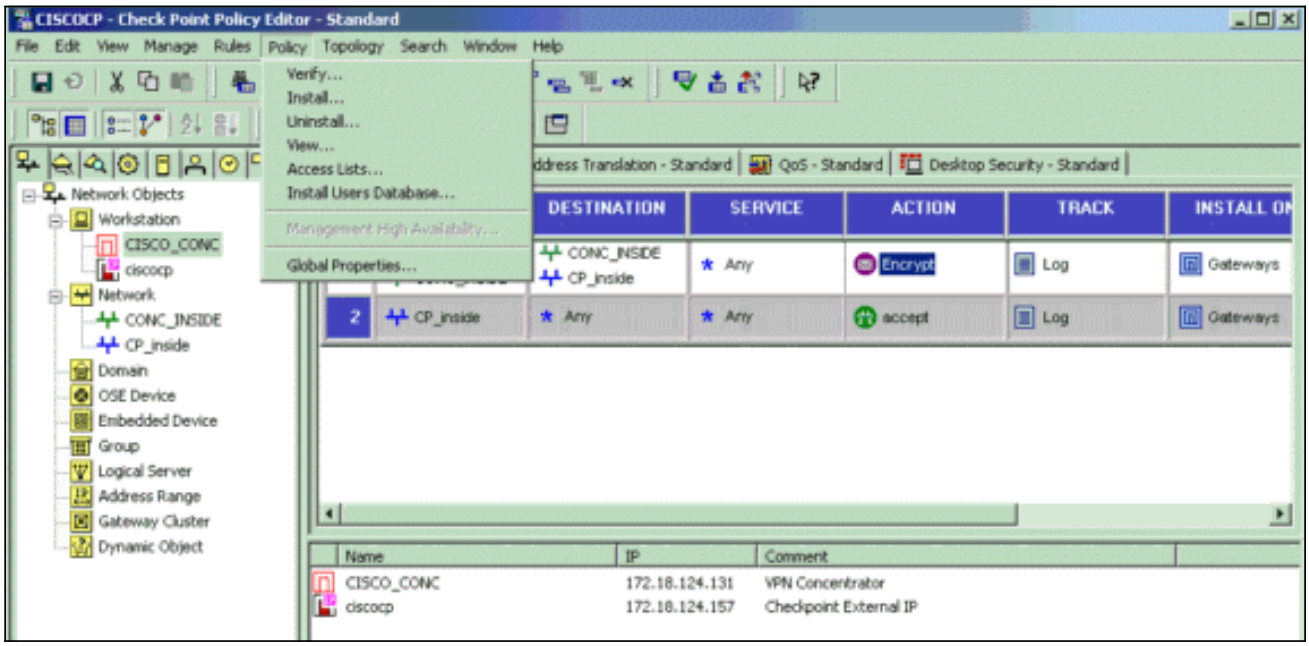


17. En la ventana IKE Properties , cambie las propiedades para coincidir con la transformación del concentrador VPN.Establezca la opción Transformar en **Cifrado + Integridad de datos (ESP)**.Establezca el algoritmo de cifrado en **3DES**.Establezca la integridad de los datos en **MD5**.Establezca la puerta de enlace de par permitida para que coincida con el concentrador VPN (CISCO_CONC).Cuando haya finalizado, haga clic en OK

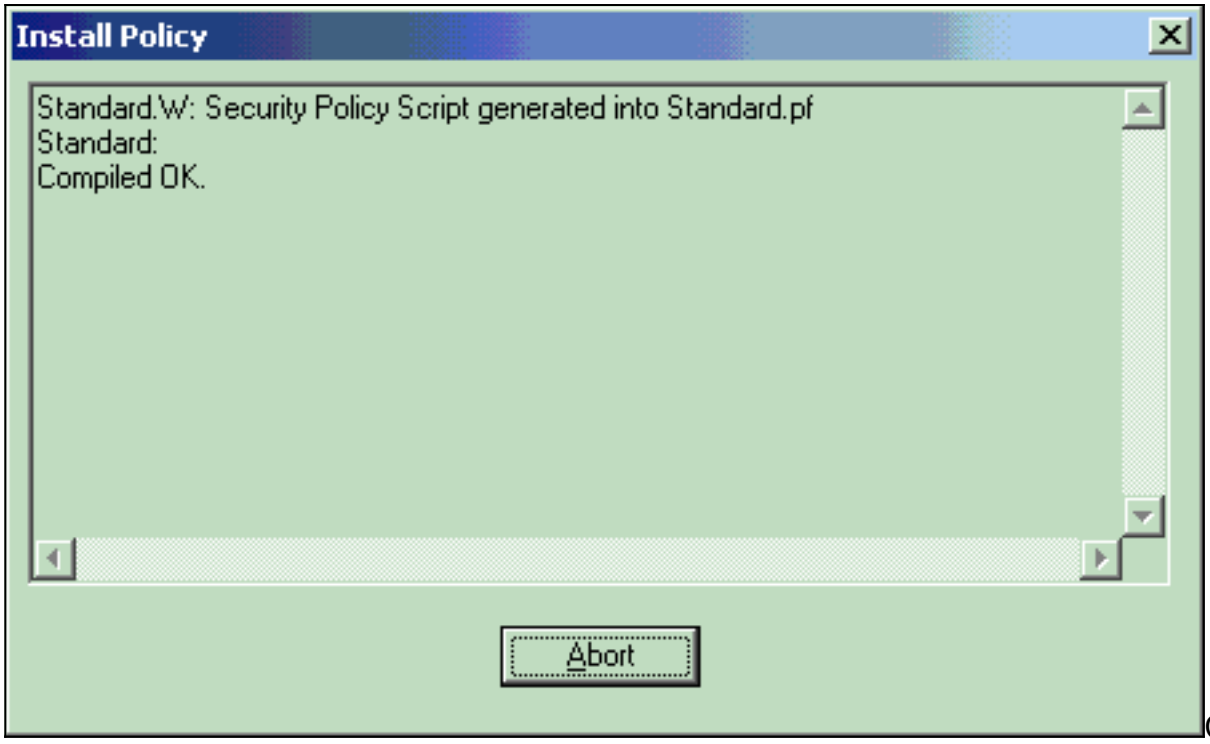


(Aceptar).

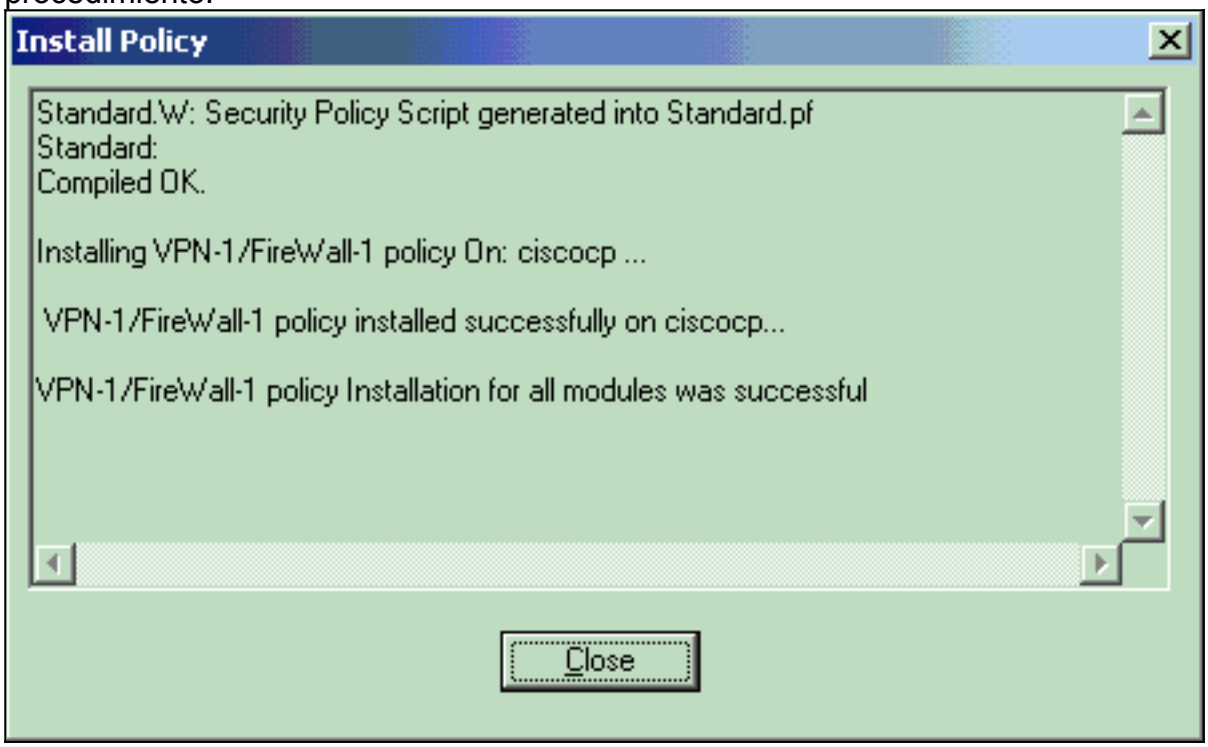
18. Después de configurar el punto de control NG, guarde la política y seleccione **Policy > Install** para habilitarla.



La ventana de instalación muestra las notas de progreso a medida que se compila la política.



Cuando la ventana de instalación indique que la instalación de la política ha finalizado, haga clic en **Cerrar** para finalizar el procedimiento.

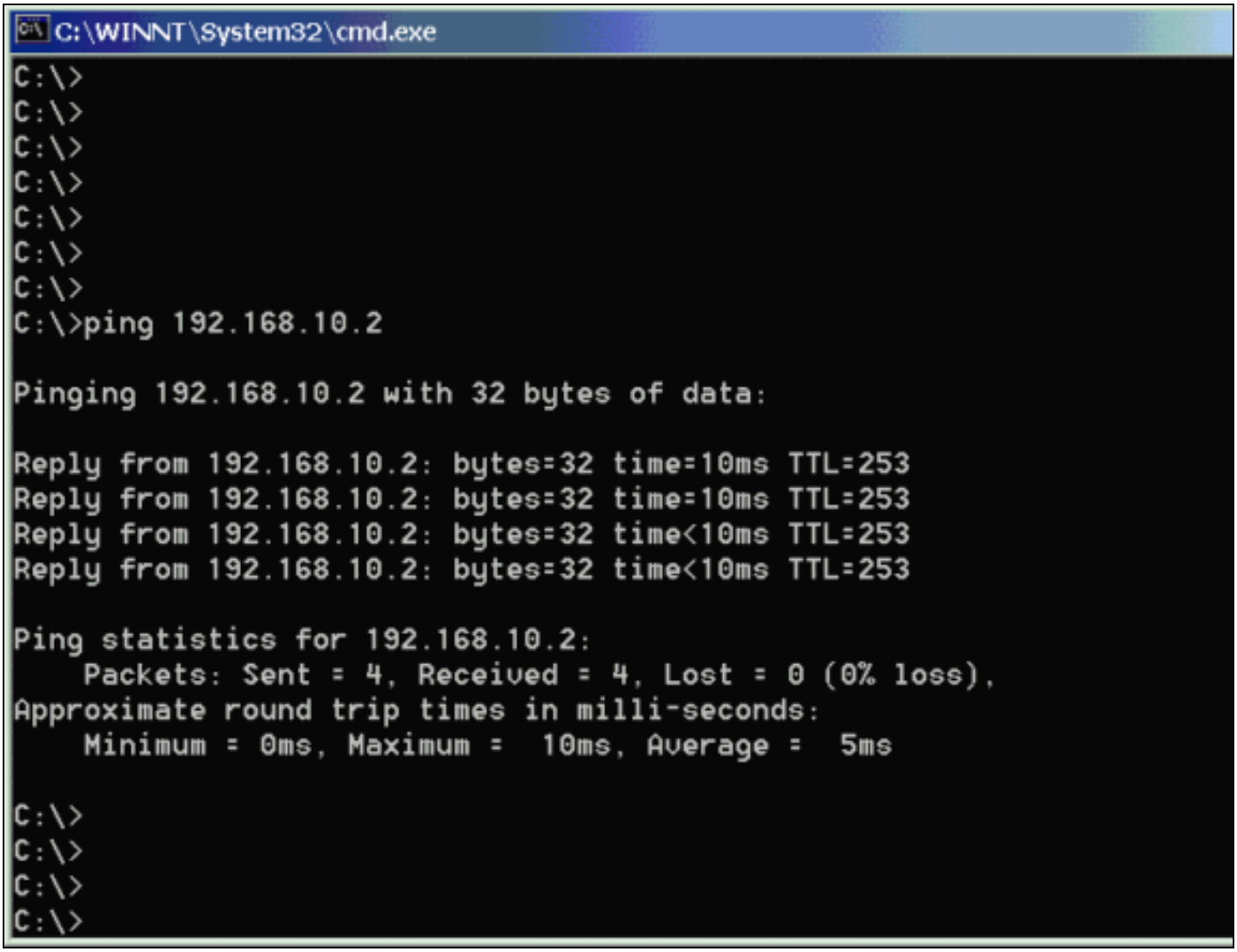


Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

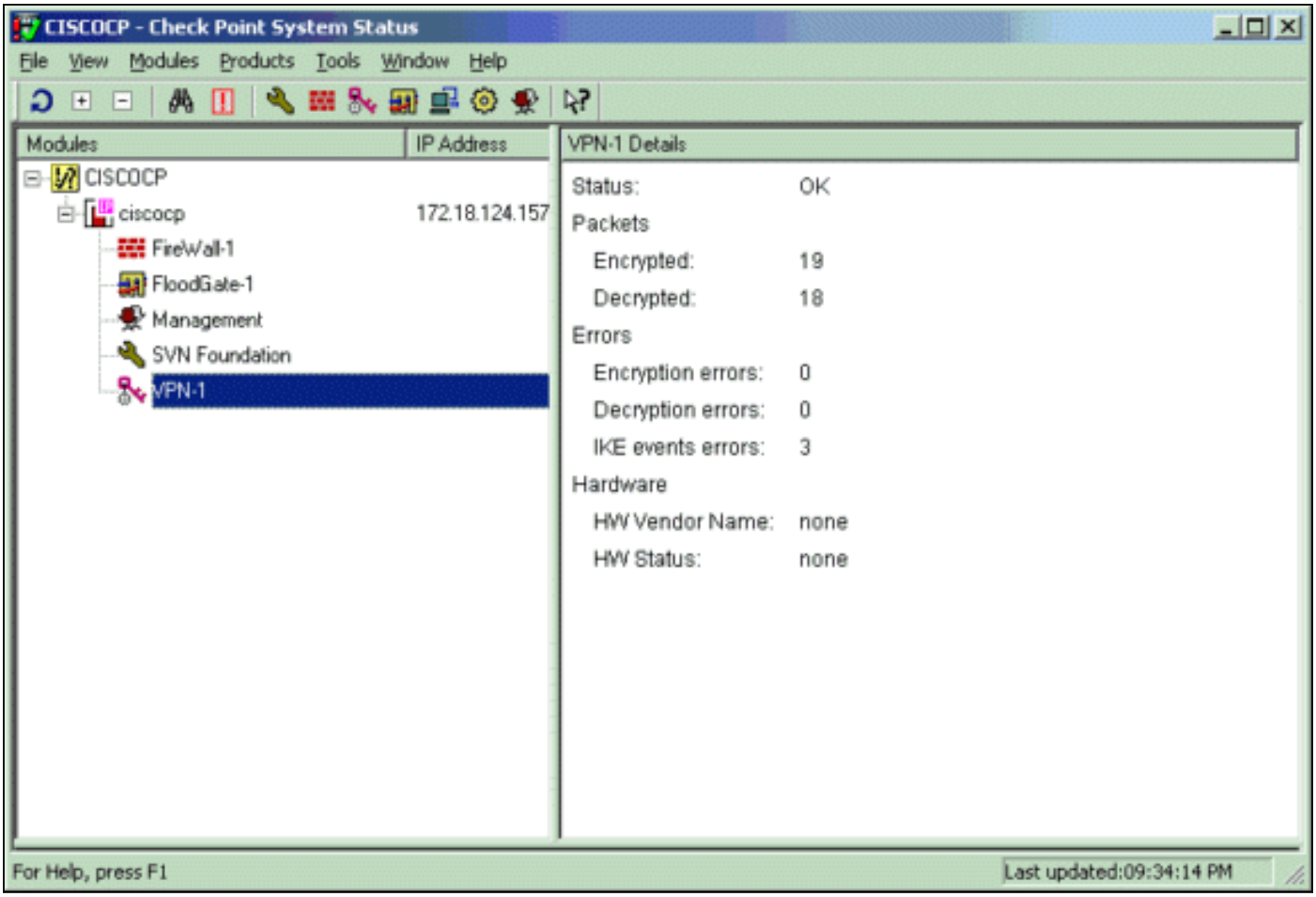
Verificar la comunicación de red

Para probar la comunicación entre las dos redes privadas, puede iniciar un ping desde una de las redes privadas a la otra red privada. En esta configuración, se envió un ping desde el lado NG del punto de control (10.32.50.51) a la red del concentrador VPN (192.168.10.2).



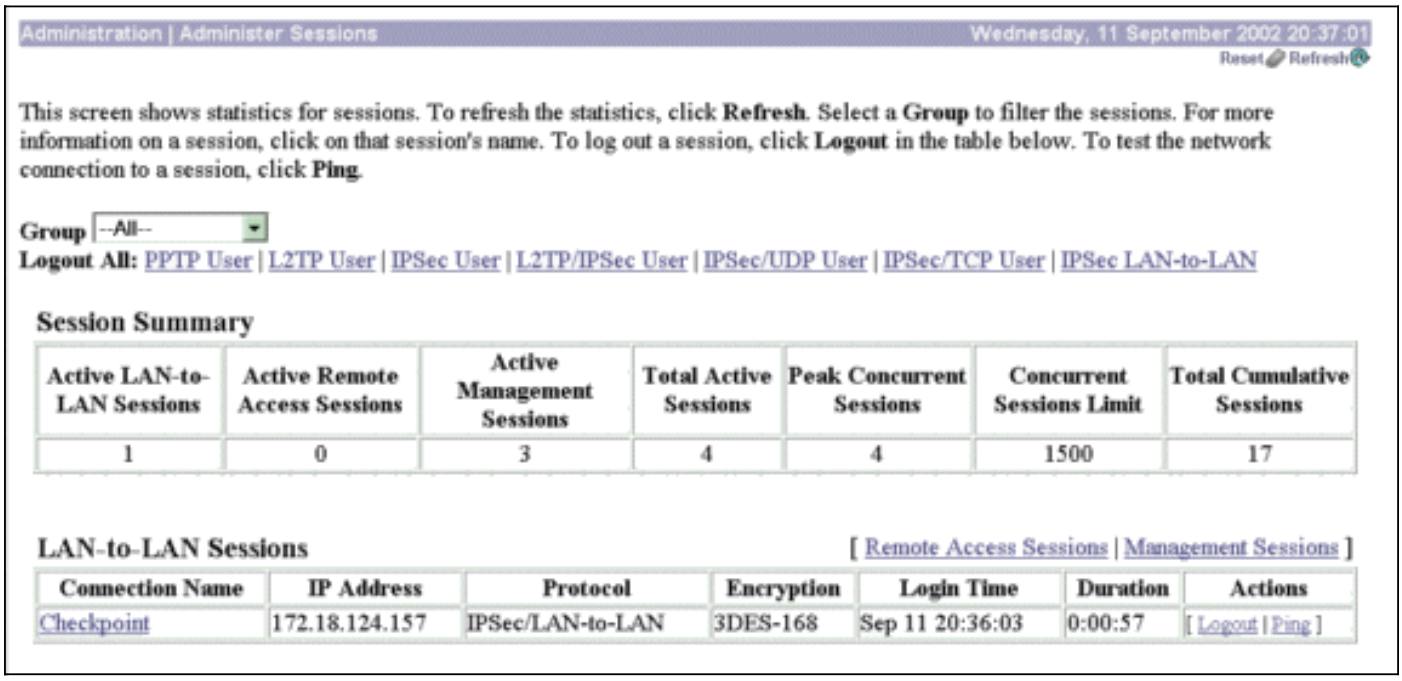
Ver el estado del túnel en el punto de control NG

Para ver el estado del túnel, vaya al Editor de directivas y seleccione **Ventana > Estado del sistema**.

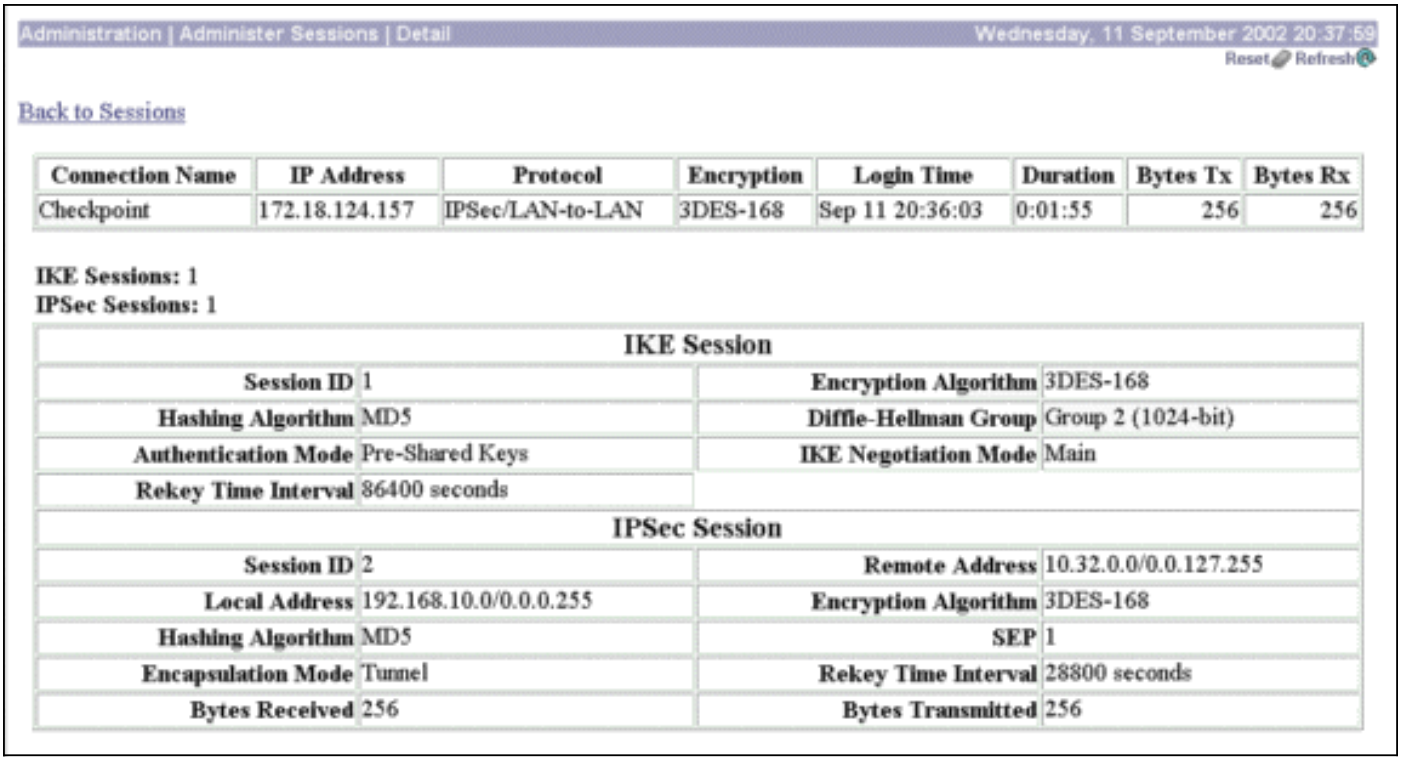


Ver el estado del túnel en el concentrador VPN

Para verificar el estado del túnel en el VPN Concentrator, vaya a **Administración > Administrar sesiones**.



En Sesiones de LAN a LAN, seleccione el nombre de conexión para el punto de control para ver los detalles de las SA creadas y el número de paquetes transmitidos/recibidos.



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

Troubleshoot

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

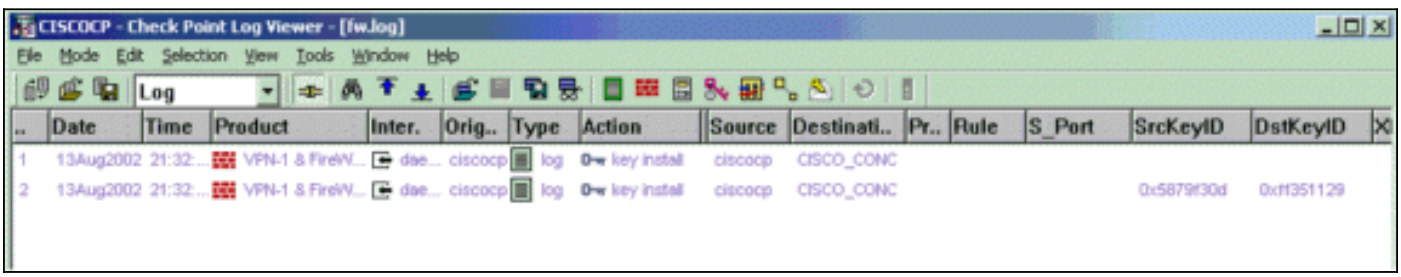
Nota: El tráfico no debe ser PATed a través del túnel IPSec usando la dirección IP pública del concentrador VPN (interfaz externa). De lo contrario, el túnel falla. Por lo tanto, la dirección IP utilizada para PATing debe ser una dirección distinta a la configurada en la interfaz externa.

Resumen de la red

Cuando se configuran varias redes adyacentes dentro del dominio de cifrado en el punto de control, el dispositivo puede resumir automáticamente las redes con respecto al tráfico interesante. Si el concentrador VPN no está configurado para coincidir, es probable que el túnel falle. Por ejemplo, si las redes internas de 10.0.0.0 /24 y 10.0.1.0 /24 están configuradas para ser incluidas en el túnel, estas redes se pueden resumir en 10.0.0.0 /23.

Depuración del punto de control NG

Para ver los registros, seleccione **Window > Log Viewer**.



Depuración del concentrador de VPN

Para habilitar los debugs en el VPN Concentrator, vaya a **Configuration > System > Events > Classes**. Habilite AUTH, AUTHDBG, IKE, IKEDBG, IPSEC e IPSECDBG para que la gravedad se registre como 1 - 13. Para ver las depuraciones, seleccione **Monitoring > Filterable Event Log**.

```
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)
```

Información Relacionada

- Página de soporte del concentrador de la serie Cisco VPN 3000
- Página de soporte al cliente Serie Cisco VPN 3000
- Página de soporte de IPSec
- Soporte Técnico - Cisco Systems