Configuración del concentrador Cisco VPN 3000 en un router Cisco

Contenido

Introducción

Este ejemplo de configuración muestra cómo conectar una red privada detrás de un router que ejecuta el software Cisco IOS® a una red privada detrás del concentrador Cisco VPN 3000. Los dispositivos de las redes se reconocen entre sí por las direcciones privadas.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco 2611 Router con Cisco IOS Software Release 12.3.1(1)a**Nota:** Asegúrese de que los

routers Cisco serie 2600 estén instalados con una imagen de IPsec VPN IOS crypto que soporte la función VPN.
- Concentrador Cisco VPN 3000 con 4.0.1 B

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Convenciones

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

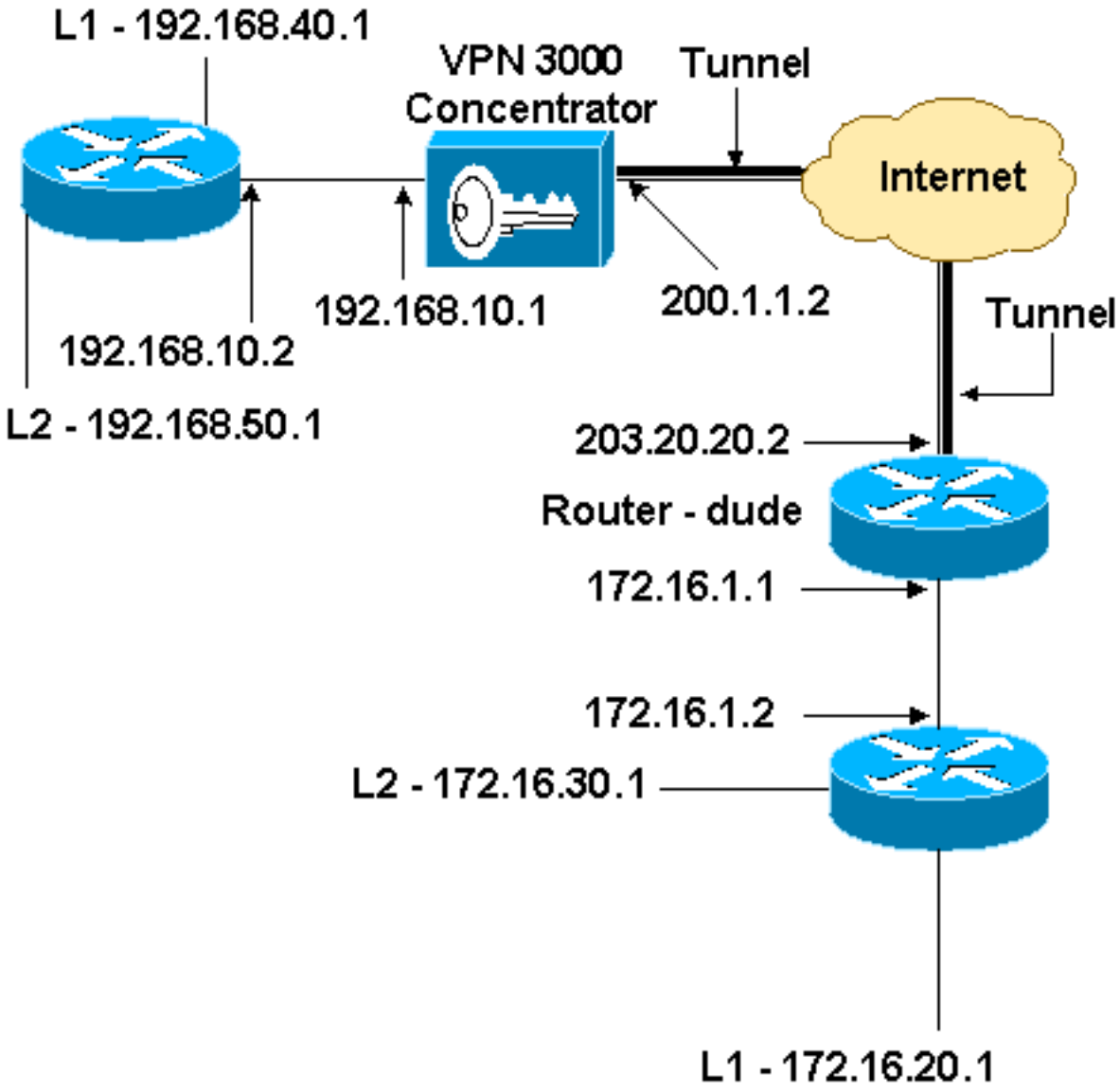
Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Nota: Use la Command Lookup Tool (sólo clientes registrados) para obtener más información sobre los comandos utilizados en este documento.

Diagrama de la red

Este documento utiliza esta configuración de red:



Configuraciones

Este documento usa esta configuración.

Configuración del router

```
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname dude
!
memory-size iomem 15
ip subnet-zero
!
ip audit notify log
ip audit po max-events 100
!!--- IKE policies. crypto isakmp policy 1
 encr 3des
 hash md5
 authentication pre-share
 group 2
crypto isakmp key cisco123 address 200.1.1.2
```

```
!!--- IPsec policies. crypto ipsec transform-set to_vpn
esp-3des esp-md5-hmac
!
crypto map to_vpn 10 ipsec-isakmp
 set peer 200.1.1.2
 set transform-set to_vpn
!--- Traffic to encrypt. match address 101
!
interface Ethernet0/0
 ip address 203.20.20.2 255.255.255.0
 ip nat outside
 half-duplex
 crypto map to_vpn
!
interface Ethernet0/1
 ip address 172.16.1.1 255.255.255.0
 ip nat inside
 half-duplex
!
ip nat pool mypool 203.20.20.3 203.20.20.3 netmask
255.255.255.0
ip nat inside source route-map nonat pool mypool
overload
ip http server
no ip http secure-server
ip classless
ip route 0.0.0.0 0.0.0.0 203.20.20.1
ip route 172.16.20.0 255.255.255.0 172.16.1.2
ip route 172.16.30.0 255.255.255.0 172.16.1.2
!!--- Traffic to encrypt. access-list 101 permit ip
172.16.1.0 0.0.0.255 192.168.10.0 0.0.0.255
access-list 101 permit ip 172.16.1.0 0.0.0.255
192.168.40.0 0.0.0.255
access-list 101 permit ip 172.16.1.0 0.0.0.255
192.168.50.0 0.0.0.255
access-list 101 permit ip 172.16.20.0 0.0.0.255
192.168.10.0 0.0.0.255
access-list 101 permit ip 172.16.20.0 0.0.0.255
192.168.40.0 0.0.0.255
access-list 101 permit ip 172.16.20.0 0.0.0.255
192.168.50.0 0.0.0.255
access-list 101 permit ip 172.16.30.0 0.0.0.255
192.168.10.0 0.0.0.255
access-list 101 permit ip 172.16.30.0 0.0.0.255
192.168.40.0 0.0.0.255
access-list 101 permit ip 172.16.30.0 0.0.0.255
192.168.50.0 0.0.0.255
!--- Traffic to except from the NAT process. access-list
110 deny   ip 172.16.1.0 0.0.0.255 192.168.10.0
0.0.0.255
access-list 110 deny   ip 172.16.1.0 0.0.0.255
192.168.40.0 0.0.0.255
access-list 110 deny   ip 172.16.1.0 0.0.0.255
192.168.50.0 0.0.0.255
access-list 110 deny   ip 172.16.20.0 0.0.0.255
192.168.10.0 0.0.0.255
access-list 110 deny   ip 172.16.20.0 0.0.0.255
192.168.40.0 0.0.0.255
access-list 110 deny   ip 172.16.20.0 0.0.0.255
192.168.50.0 0.0.0.255
access-list 110 deny   ip 172.16.30.0 0.0.0.255
192.168.10.0 0.0.0.255
access-list 110 deny   ip 172.16.30.0 0.0.0.255
192.168.40.0 0.0.0.255
```

```
access-list 110 deny   ip 172.16.30.0 0.0.0.255
192.168.50.0 0.0.0.255
access-list 110 permit ip 172.16.1.0 0.0.0.255 any
!
route-map nonat permit 10
 match ip address 110
!
line con 0
line aux 0
line vty 0 4
!
end
```

Configuración del concentrador VPN

En esta configuración de laboratorio, se accede primero al concentrador VPN a través del puerto de la consola y se agrega una configuración mínima para que se pueda realizar la configuración adicional a través de la interfaz gráfica de usuario (GUI).

Elija **Administration > System Reboot > Schedule reboot > Reboot with Factory/Default Configuration** para asegurarse de que no haya una configuración existente en el VPN Concentrator.

El concentrador VPN aparece en Configuración rápida y estos elementos se configuran después del reinicio:

- Fecha/hora
- Interfaces/Masks in Configuration > Interfaces (public=200.1.1.2/24, private=192.168.10.1/24)
- Gateway predeterminada en Configuration (Configuración) > System (Sistema) > ip routing (Ruteo de IP) > Default_Gateway (200.1.1.1) (Gateway predeterminada [200.1.1.1])

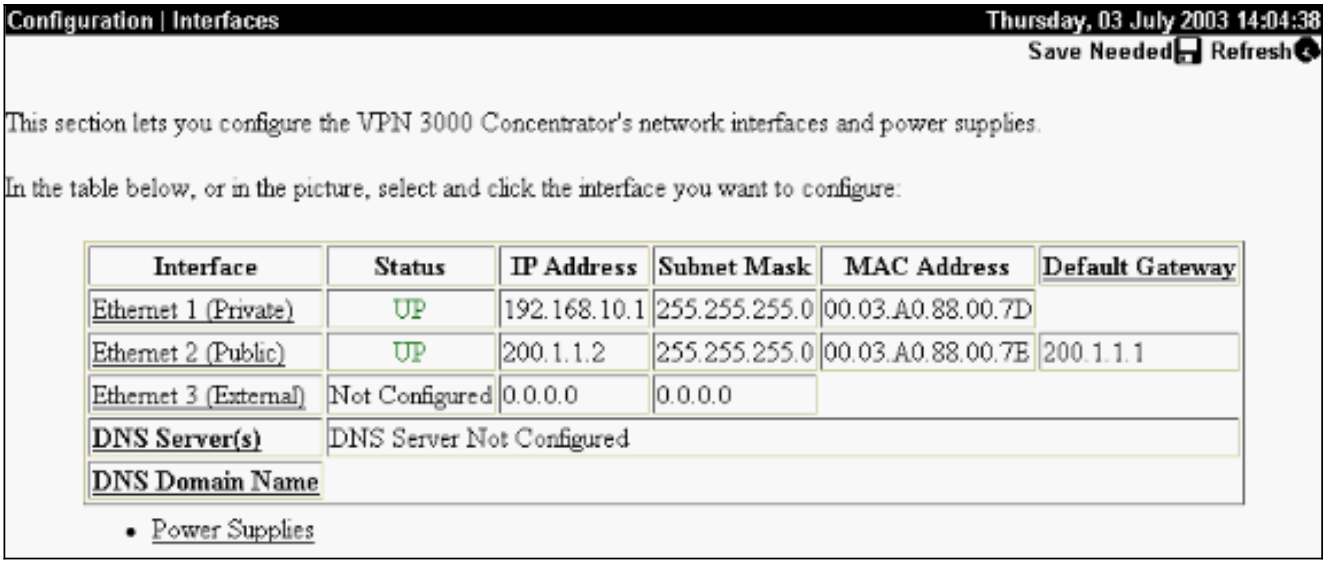
En este momento, el VPN Concentrator es accesible a través de HTML desde la red interna.

Nota: Debido a que el concentrador VPN se administra desde afuera, también debe seleccionar:

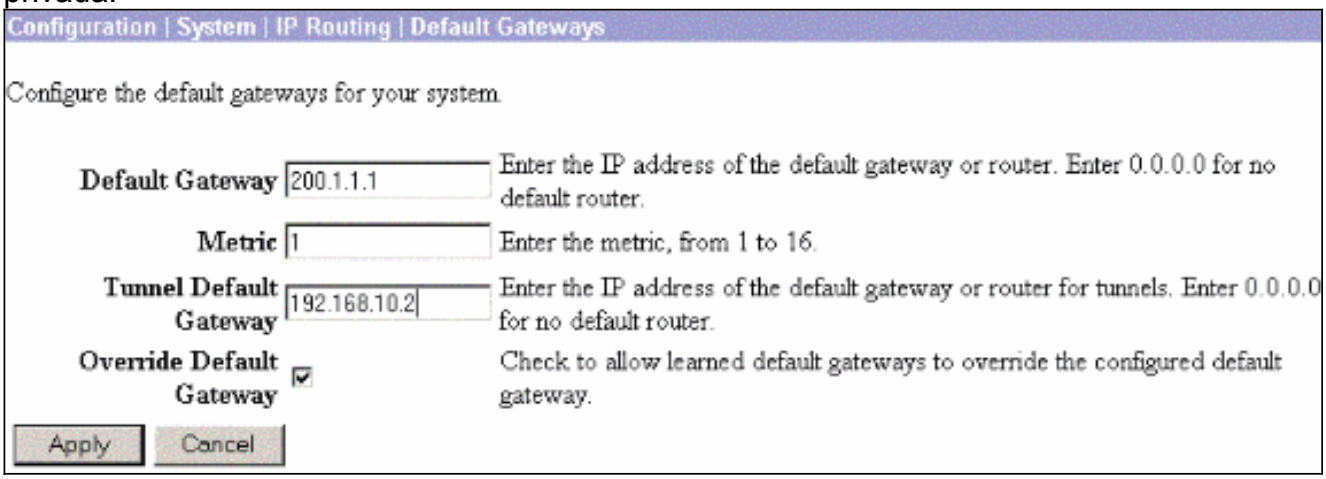
- **Configuration > Interfaces > 2-public > Select IP Filter > 1. Private (Default)**.
- **Administration > Access Rights > Access Control List > Add Manager Workstation para agregar la dirección IP del** administrador externo.

Esto no es necesario a menos que administre el VPN Concentrator desde *afuera*.

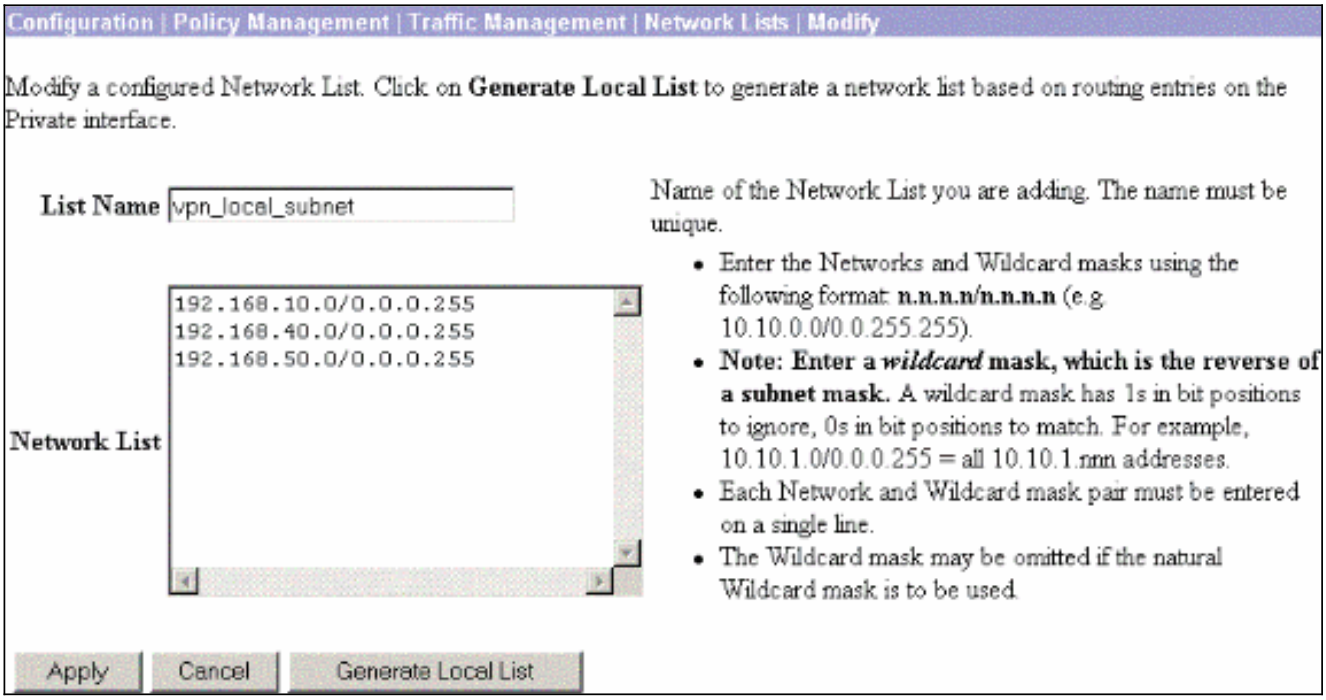
1. Elija **Configuration > Interfaces** para volver a verificar las interfaces después de activar la GUI.



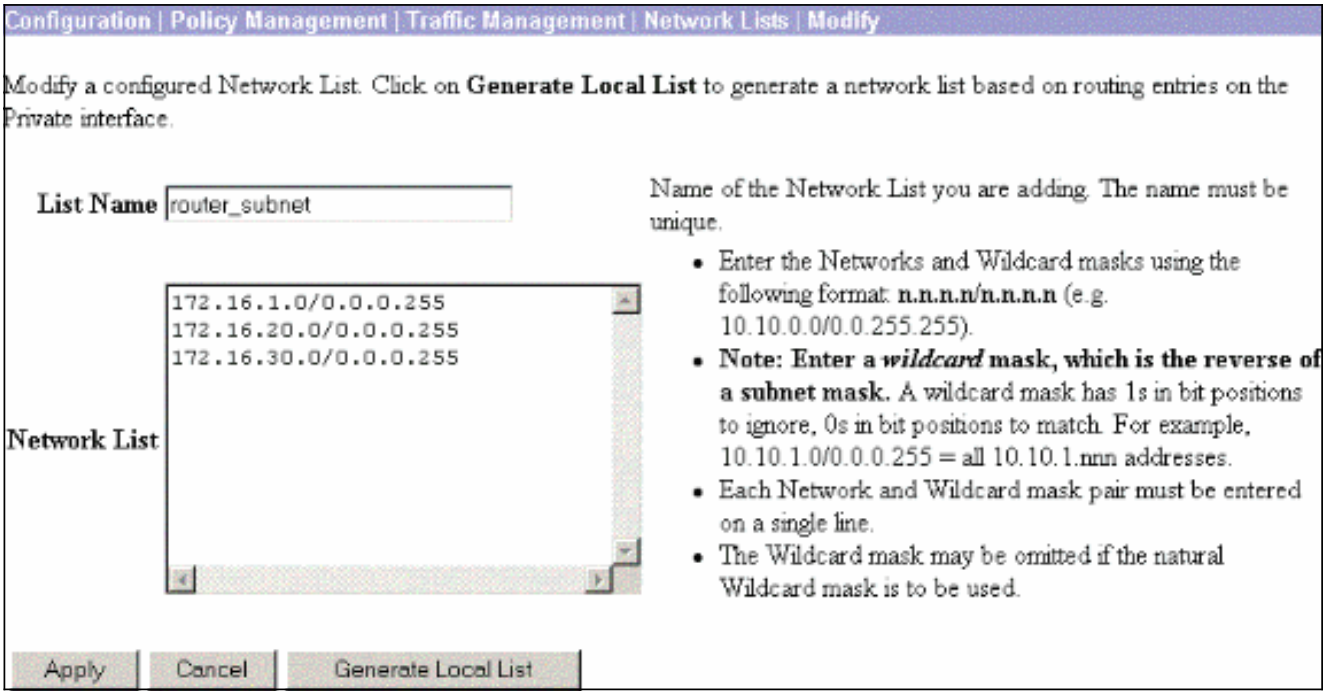
2. Elija Configuration > System > IP Routing > Default Gateways para configurar la gateway predeterminada(Internet) y la gateway predeterminada del túnel (interior) para IPsec para alcanzar las otras subredes en la red privada.



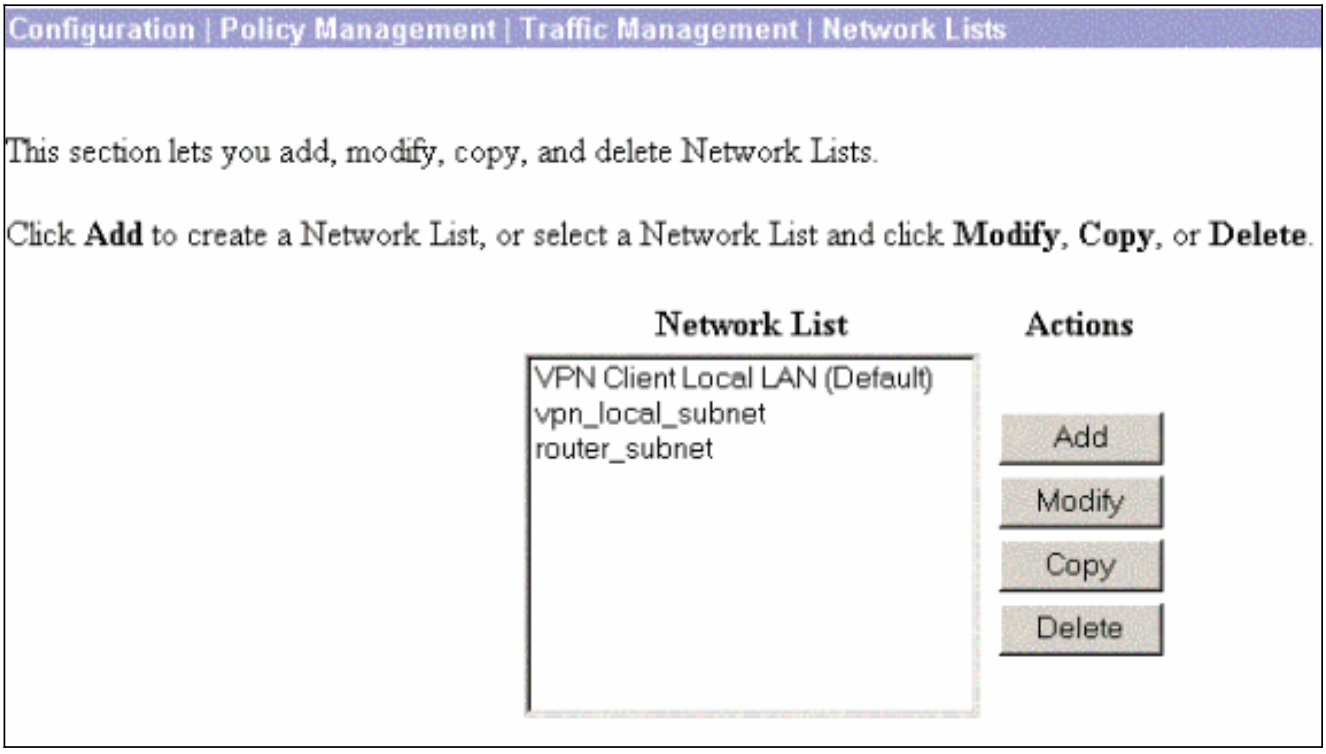
3. Elija **Configuration > Policy Management > Network Lists** para crear las listas de red que definen el tráfico que se cifrará.Estas son las redes locales:



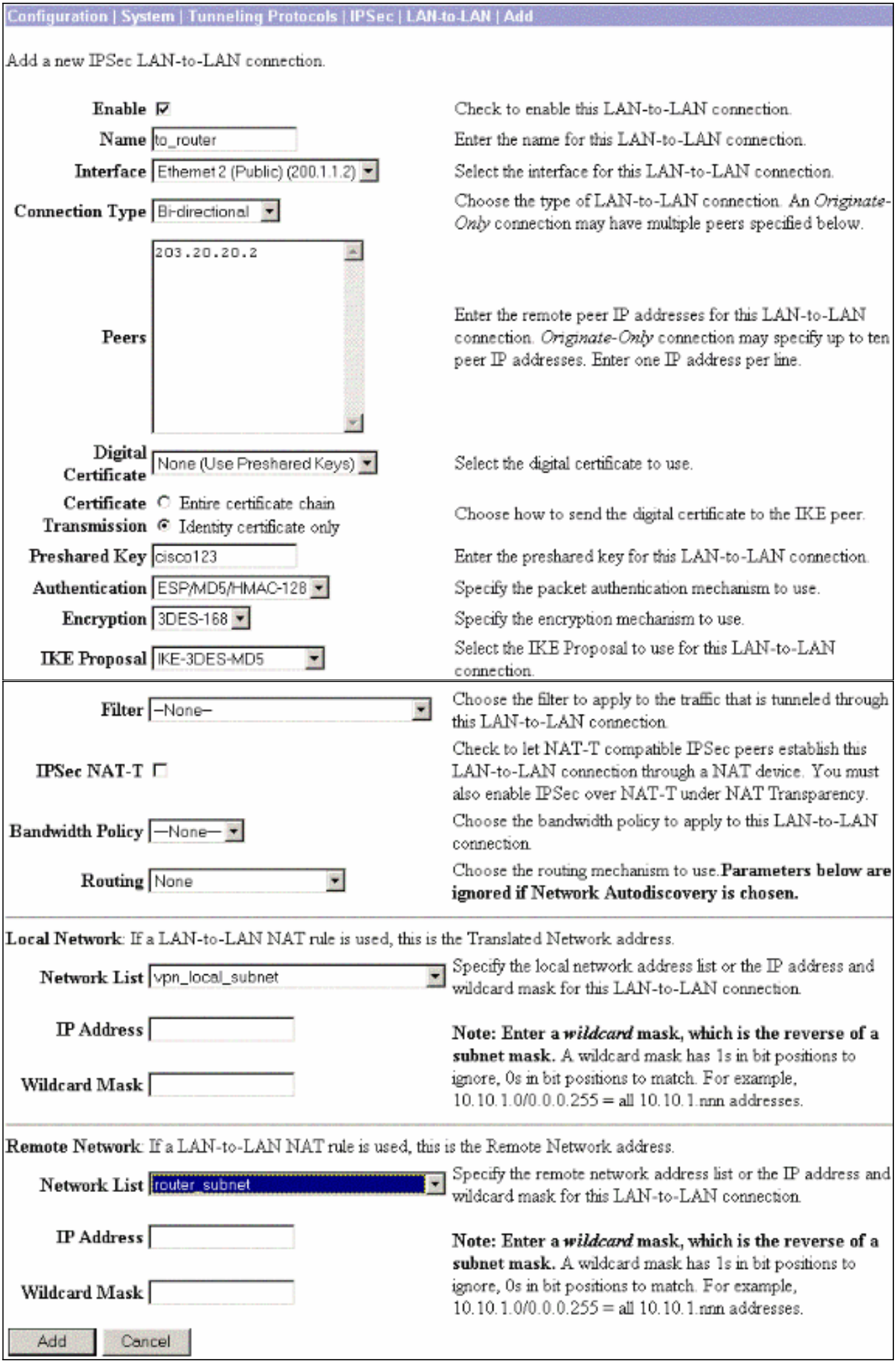
Estas son las redes
remotas:



4. Una vez terminado, estas son las dos listas de red:**Nota:** Si el túnel IPsec no se activa, verifique si el tráfico interesante coincide con ambos lados. El tráfico interesante se define por la lista de acceso en el router y los cuadros PIX. Se definen mediante listas de red en los concentradores
VPN.

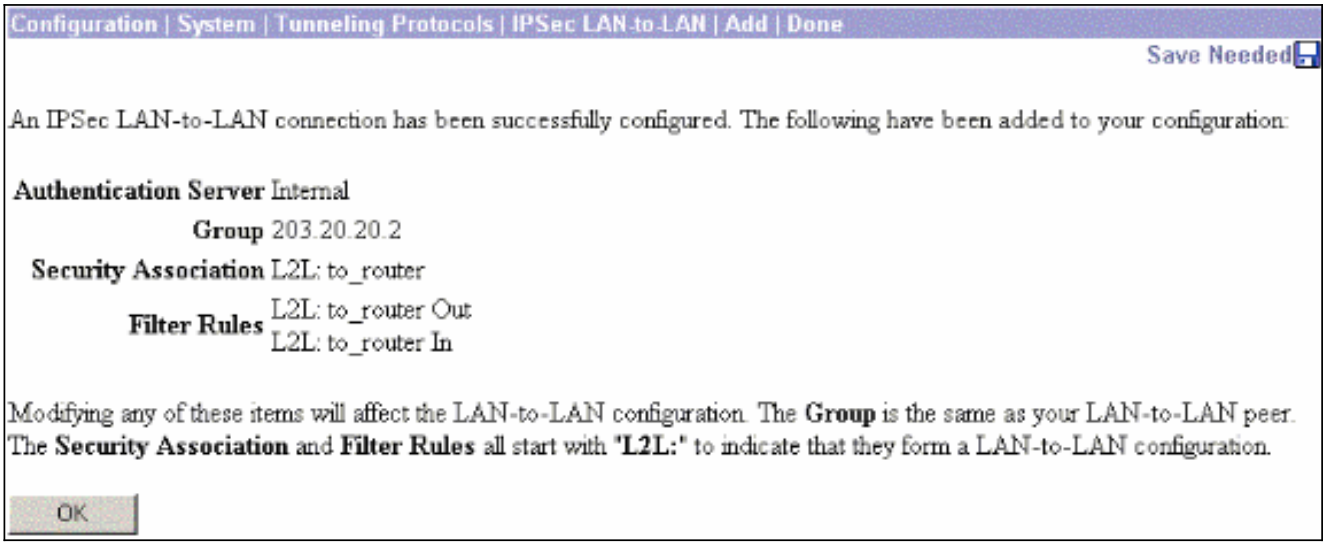


5. Elija **Configuration > System > Tunneling Protocols > IPSec LAN-to-LAN** y defina el túnel de LAN a
LAN.

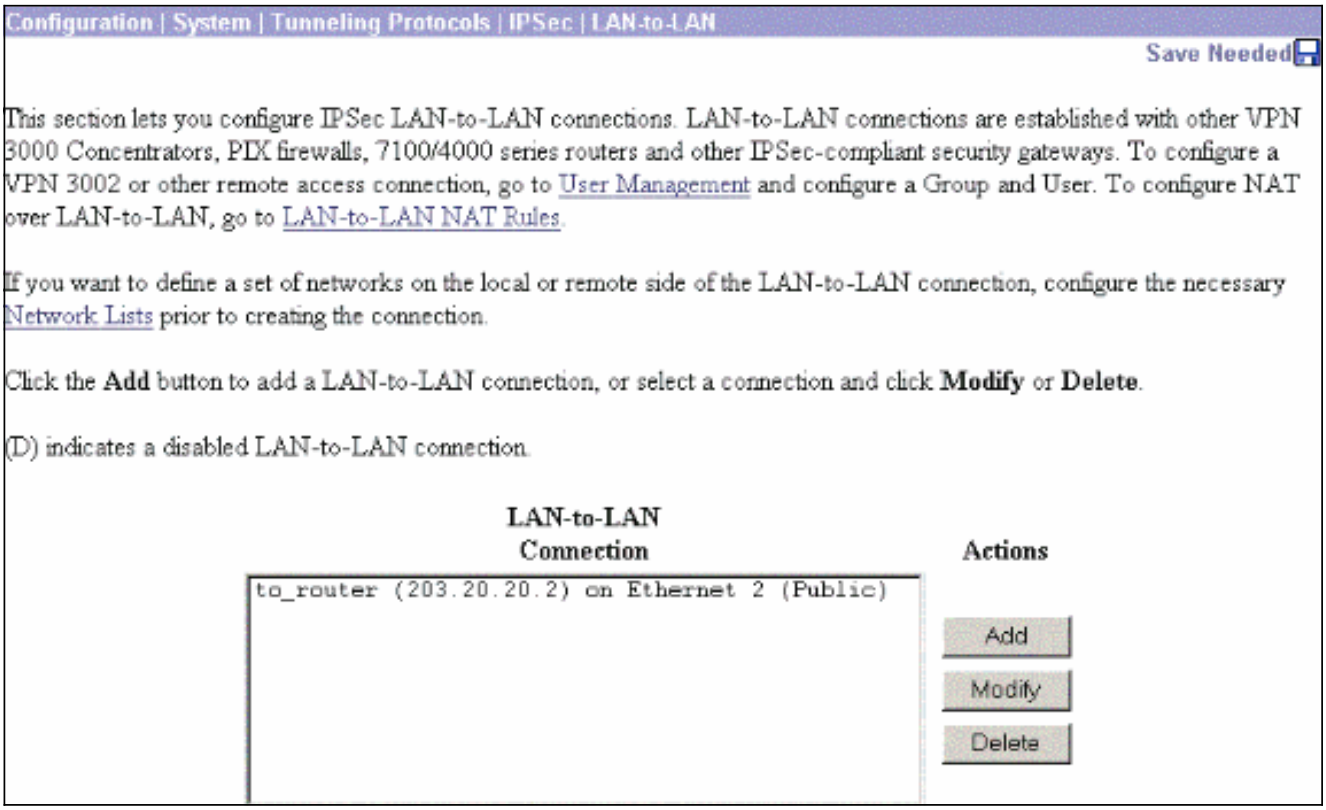


6. Después de hacer clic en **Aplicar**, esta ventana se muestra con la otra configuración que se

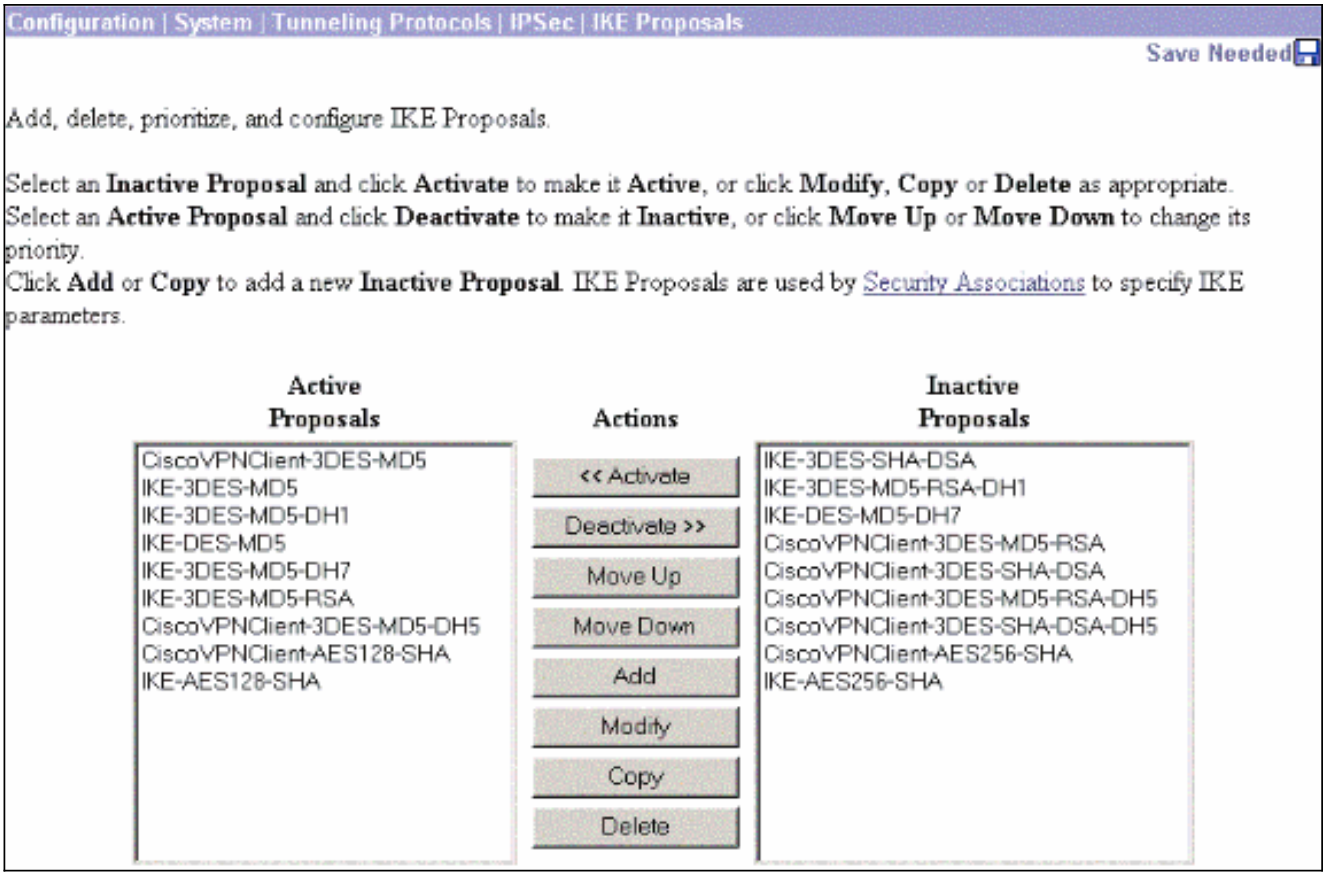
crea automáticamente como resultado de la configuración del túnel de LAN a LAN.



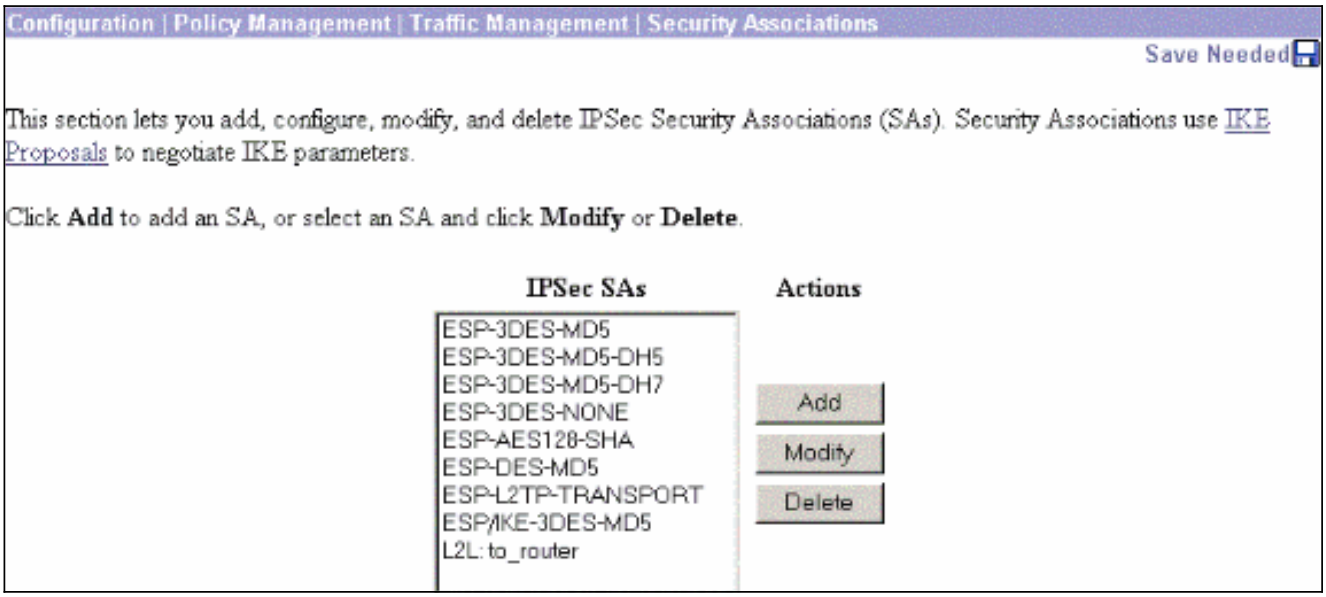
Los parámetros IPsec de LAN a LAN creados anteriormente se pueden ver o modificar en **Configuración > Sistema > Tunelización de los Protocolos > IPSec LAN a LAN**.



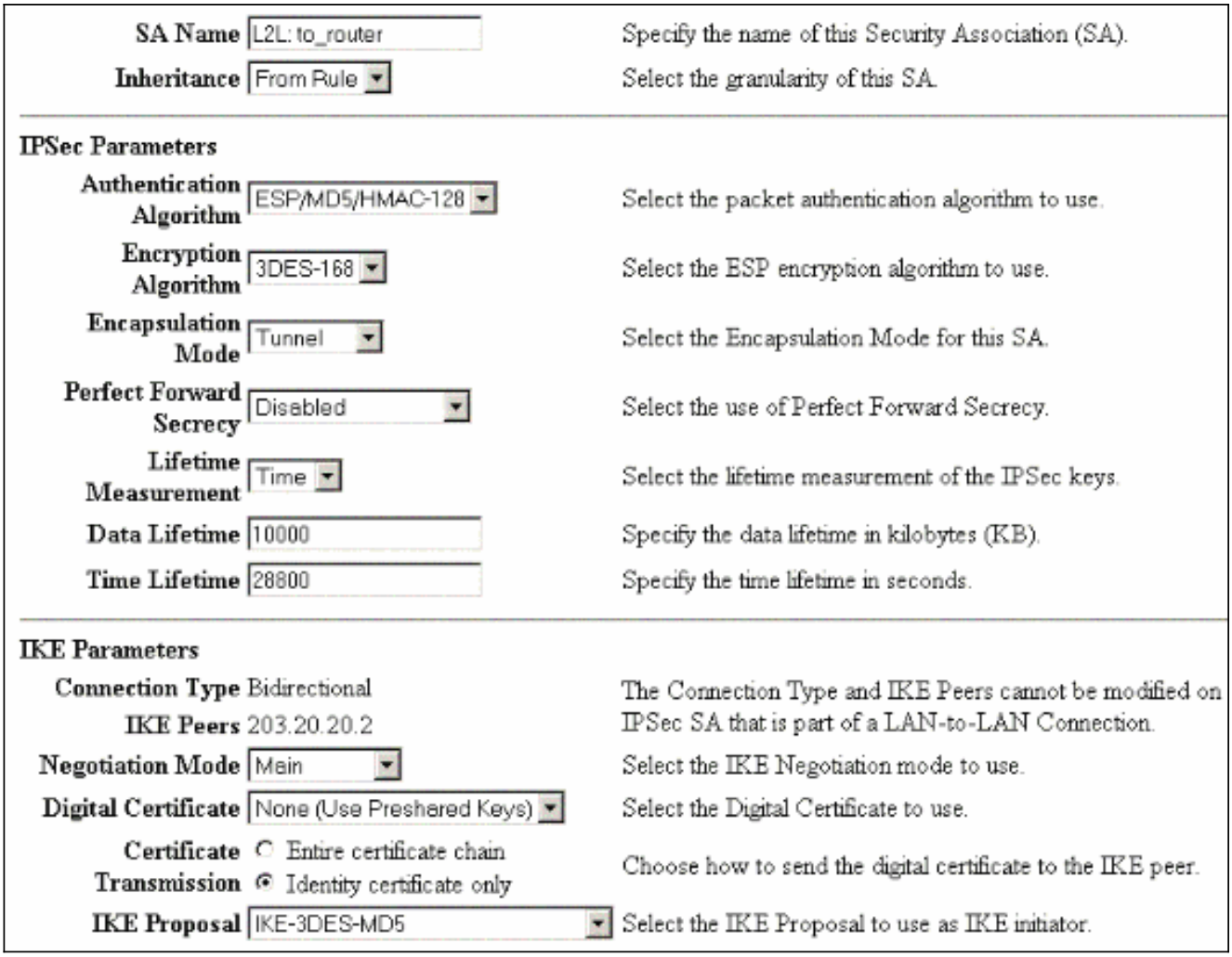
7. Elija Configuration > **System > Tunneling Protocols** > IPSec > IKE Proposale para confirmar la propuesta IKE activa.



8. Elija **Configuration > Policy Management > Traffic Management > Security Associations** para ver la lista de Security Associations.



9. Haga clic en el nombre de la asociación de seguridad y, a continuación, haga clic en **Modificar** para verificar las asociaciones de seguridad.



Verificación

Esta sección enumera los comandos **show** utilizados en esta configuración.

En el router

En esta sección encontrará información que puede utilizar para comprobar que su configuración funcione correctamente.

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

- **show crypto ipsec sa**: muestra la configuración utilizada por las asociaciones de seguridad actuales.
- **show crypto isakmp sa**: muestra todas las asociaciones de seguridad de intercambio de claves de Internet actuales en un par.
- **show crypto engine connection active**: muestra las conexiones de sesión cifradas activas actuales para todos los motores criptográficos.

Puede utilizar la Herramienta de Búsqueda de Comandos de IOS (sólo clientes registrados) para ver más información sobre comandos específicos.

En el concentrador VPN

Elija Configuration > **System** > **Events** > **Classes** > Modify para activar el registro. Estas opciones están disponibles:

- IKE
- IKEDBG
- IKEDECODE
- IPSEC
- IPSECDBG
- IPSECDECODE

Gravedad de registro = 1-13

Gravedad en la consola = 1-3

Seleccione **Monitoring** > **Event Log** para recuperar el registro de eventos.

Troubleshoot

En el router

Consulte Información Importante sobre Comandos Debug antes de intentar cualquier comando debug.

- **debug crypto engine**: muestra el tráfico cifrado.
- **debug crypto ipsec — Muestra los IPSec Negotiations de la Fase 2.**
- **debug crypto isakmp — Muestra las negociaciones ISAKMP para la fase 1.**

Problema - No se puede iniciar el túnel

Mensaje de error

```
20932 10/26/2007 14:37:45.430 SEV=3 AUTH/5 RPT=1863 10.19.187.229
Authentication rejected: Reason = Simultaneous logins exceeded for user
handle = 623, server = (none), user = 10.19.187.229, domain = <not
specified>
```

Solución

Complete esta acción para configurar el número deseado de inicios de sesión simultáneos o establezca los inicios de sesión simultáneos en 5 para esta SA:

Vaya a **Configuration > User Management > Groups > Modify 10.19.187.229 > General > Simultaneouts Logins** y cambie el número de logins a 5.

PFS

En las negociaciones de IPSec, Perfect Forward Secrecy (PFS) garantiza que cada clave criptográfica nueva no esté relacionada a cualquier clave anterior. Habilite o inhabilite PFS en ambos peers de túnel. De lo contrario, el túnel IPsec de LAN a LAN (L2L) no se establece en los routers.

Para especificar que IPsec debe solicitar PFS cuando se solicitan nuevas Asociaciones de Seguridad para esta entrada de mapa crypto, o que IPsec requiere PFS cuando recibe solicitudes de nuevas Asociaciones de Seguridad, utilice el comando **set pfs** en el modo de configuración de mapa crypto. Para especificar que IPsec no debe solicitar PFS, utilice la forma **no** de este comando.

```
set pfs [group1 | group2]
no set pfs
```

Para el comando set pfs:

- *group1* : especifica que IPsec debe utilizar el grupo de módulos primos Diffie-Hellman de 768 bits cuando se realiza el nuevo intercambio Diffie-Hellman.
- *group2* : especifica que IPsec debe utilizar el grupo de módulos primos Diffie-Hellman de 1024 bits cuando se realiza el nuevo intercambio Diffie-Hellman.

De forma predeterminada, PFS no se solicita. Si no se especifica ningún grupo con este comando, como valor predeterminado se utiliza group1.

Ejemplo:

```
Router(config)#crypto map map 10 ipsec-isakmp
Router(config-crypto-map)#set pfs group2
```

Consulte Referencia de Comandos de Seguridad de Cisco IOS para obtener más información sobre el comando **set pfs**.

Información Relacionada

- Soluciones a los Problemas más frecuentes de IPSec VPN L2L y de Acceso Remoto
- Cisco VPN 3000 Series Concentrators
- Cisco VPN 3002 Hardware Clients
- Negociación IPSec/Protocolos IKE
- Soporte Técnico y Documentación - Cisco Systems