Ejemplo de Configuración de Túnel IPsec de LAN a LAN entre un Cisco VPN 3000 Concentrator y un Router con AES

Contenido

Introducción

Este documento muestra cómo configurar un túnel IPsec entre un Cisco VPN 3000 Concentrator y un router Cisco con Advance Encryption Standard (AES) como algoritmo de cifrado.

AES es una nueva publicación de la Norma Federal de Procesamiento de la Información (FIPS) creada por el Instituto Nacional de Normas y Tecnología (NIST) para ser utilizada como método de encriptación. Este estándar especifica un algoritmo de cifrado simétrico AES que reemplaza el estándar de cifrado de datos (DES) como transformación de la privacidad tanto para IPsec como para el intercambio de claves de Internet (IKE). AES tiene tres longitudes de clave diferentes, una clave de 128 bits (la predeterminada), una clave de 192 bits y una clave de 256 bits. La función AES de Cisco IOS® añade compatibilidad con el nuevo estándar de cifrado AES, con el modo de encadenamiento de bloques de cifrado (CBC), a IPsec.

Refiérase al sitio del Centro de Recursos de Seguridad Informática de NIST para obtener más información sobre AES.

Consulte Ejemplo de Configuración de IPsec de LAN a LAN entre el Concentrador VPN 3000 de Cisco y el Firewall PIX para obtener más información sobre la configuración de túnel de LAN a

LAN entre un concentrador VPN 3000 y un Firewall PIX.

Consulte Ejemplo de Configuración del Túnel IPSec entre PIX 7.x y VPN 3000 Concentrator para obtener más información cuando el PIX tiene la versión de software 7.1.

Prerequisites

Requirements

Este documento requiere una comprensión básica del protocolo IPSec Consulte Introducción al Cifrado IPSec para obtener más información sobre IPsec.

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- **Requisitos del router**: la función AES se introdujo en la versión 12.2(13)T del software del IOS de Cisco. Para habilitar AES, el router debe soportar IPsec y ejecutar una imagen IOS con claves largas "k9" (el subsistema "k9").**Nota:** El soporte de hardware para AES también está disponible en los módulos VPN de aceleración AES 2600XM, 2691, 3725 y 3745 de Cisco. Esta función no tiene implicaciones de configuración y el módulo de hardware se selecciona automáticamente si ambos están disponibles.
- **Requisitos del concentrador VPN** - El soporte de software para la función AES se introdujo en la versión 3.6. El nuevo procesador de cifrado mejorado y escalable (SEP-E) proporciona soporte de hardware. Esta función no tiene implicaciones para la configuración.**Nota:** En Cisco VPN 3000 Concentrator versión 3.6.3, los túneles no negocian con AES debido al ID de bug de Cisco CSCdy88797 (sólo para clientes registrados). Esto se ha resuelto desde la versión 3.6.4.**Nota:** El Cisco VPN 3000 Concentrator utiliza módulos SEP o SEP-E, no ambos. No instale ambos en el mismo dispositivo. Si instala un módulo SEP-E en un concentrador VPN que ya contiene un módulo SEP, el concentrador VPN inhabilita el módulo SEP y utiliza solamente el módulo SEP-E.

Componentes Utilizados

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

- Cisco 3600 Series Router con Cisco IOS Software Release 12.3(5)
- Concentrador VPN 3060 de Cisco con versión de software 4.0.3

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 Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Configurar

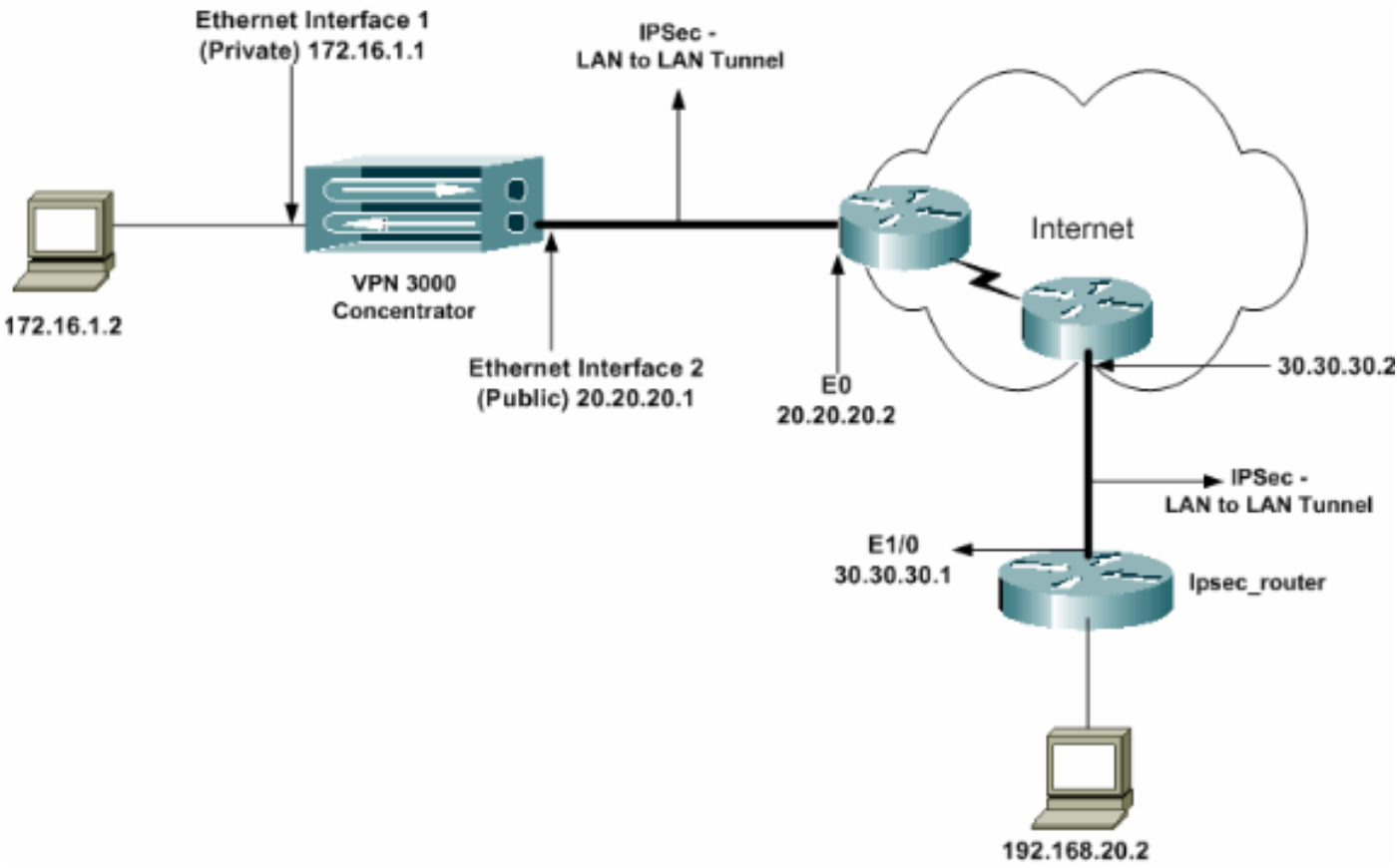
En esta sección encontrará la información para configurar las funciones descritas en este

documento.

Nota: Utilice la herramienta Command Lookup (sólo para clientes registrados) para obtener más información sobre los comandos utilizados en esta sección.

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Configuraciones

En este documento, se utilizan estas configuraciones:

- Router IPsec
- Concentrador VPN

Configuración de IPSec_Router

```
version 12.3
service timestamps debug uptime
service timestamps log datetime msec
no service password-encryption
!
hostname ipsec_router
!
memory-size iomem 10
no aaa new-model
ip subnet-zero
!
!--- Configuration for IKE policies. crypto isakmp
```

```
policy 1
!--- Enables the IKE policy configuration (config-
isakmp) command mode, !--- where you can specify the
parameters to be used during !--- an IKE negotiation.
encryption aes 256
!--- Specifies the encryption algorithm as AES with a
256 !--- bit key within an IKE policy. authentication
pre-share
group 2
crypto isakmp key cisco123 address 20.20.20.1
!--- Specifies the preshared key "cisco123" which !---
should be identical at both peers. !
!--- Configuration for IPsec policies. crypto ipsec
security-association lifetime seconds 28800
!--- Specifies the lifetime of the IPsec security
association (SA). ! crypto ipsec transform-set vpn esp-
aes 256 esp-md5-hmac
!--- Enables the crypto transform configuration mode,
where you can !--- specify the transform sets to be used
during an IPsec negotiation. ! crypto map vpn 10 ipsec-
isakmp
!--- Indicates that IKE is used to establish the IPsec
SA for protecting !--- the traffic specified by this
crypto map entry. set peer 20.20.20.1
!--- Sets the IP address of the remote end (VPN
Concentrator). set transform-set vpn
!--- Configures IPsec to use the transform-set "vpn"
defined earlier. ! !--- Specifies the traffic to be
encrypted. match address 110
!
interface Ethernet1/0
ip address 30.30.30.1 255.255.255.0
ip nat outside
half-duplex
crypto map vpn
!--- Configures the interface to use the crypto map
"vpn" for IPsec. !
interface FastEthernet2/0
ip address 192.168.20.1 255.255.255.0
ip nat inside
duplex auto
speed auto
!
ip nat pool mypool 30.30.30.3 30.30.30.3 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 30.30.30.2
!
access-list 110 permit ip 192.168.20.0 0.0.0.255
172.16.0.0 0.0.255.255
!--- This crypto ACL-permit identifies the matching
traffic !--- flows to be protected via encryption. !---
Specifies the traffic not to be encrypted. access-list
120 deny ip 192.168.20.0 0.0.0.255 172.16.0.0
0.0.255.255
!--- This crypto ACL-deny identifies the matching
traffic flows not to be encrypted. !
access-list 120 permit ip 192.168.20.0 0.0.0.255 any
!--- The access control list (ACL) used in the NAT
configuration exempts !--- the LAN-to-LAN traffic from
```

```
the NAT process, !--- but allows all traffic going to
the Internet to be translated. !
route-map nonat permit 10
!--- The traffic flows not encrypted from the !--- peer
network are allowed. match ip address 120
!
line con 0
line aux 0
line vty 0 4
login
!
end
```

Nota: Aunque la sintaxis de ACL no se modifica, los significados son ligeramente diferentes para las ACL crypto. En las ACL crypto, **permit** especifica que los paquetes coincidentes deben ser cifrados, mientras que **deny** especifica que los paquetes coincidentes no necesitan ser cifrados.

Configuración del concentrador VPN

Los concentradores VPN no están preprogramados con direcciones IP en sus configuraciones de fábrica. Debe utilizar el puerto de la consola para configurar las configuraciones iniciales que son una interfaz de línea de comandos (CLI) basada en menús. Consulte Configuración de Concentradores VPN a través de la Consola para obtener información sobre cómo configurar a través de la consola.

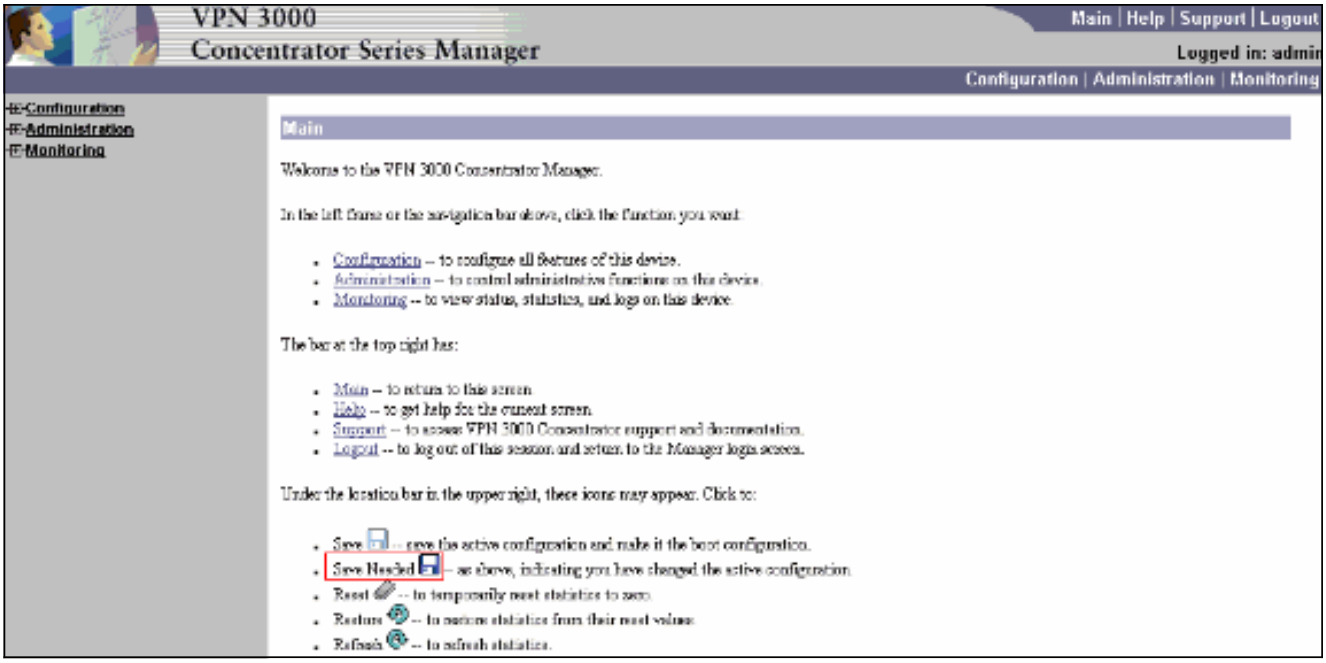
Después de configurar la dirección IP en la interfaz Ethernet 1 (privada), el resto se puede configurar mediante la CLI o a través de la interfaz del explorador. La interfaz del explorador admite HTTP y HTTP a través de Secure Socket Layer (SSL).

Estos parámetros se configuran a través de la consola:

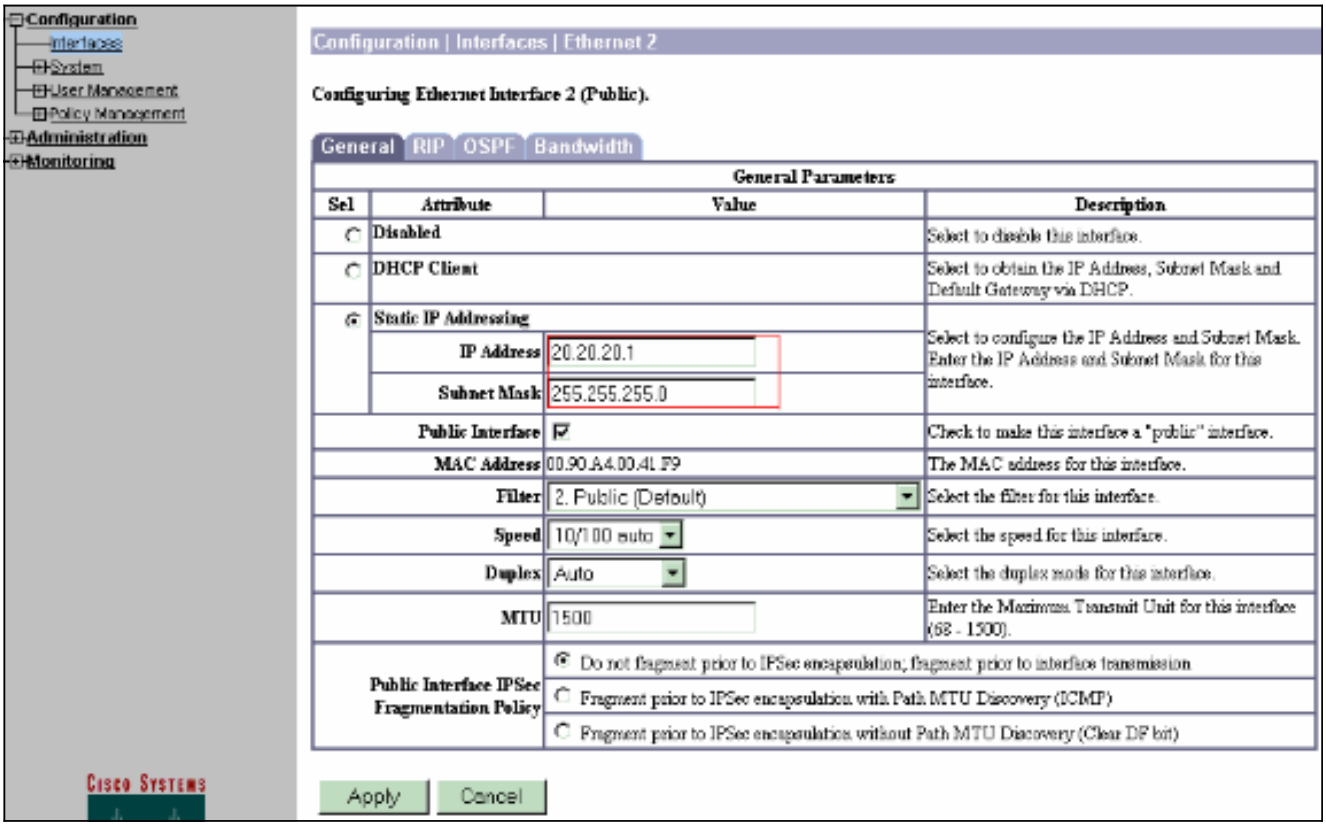
- **Hora/Fecha**: la hora y la fecha correctas son muy importantes. Ayudan a garantizar que las entradas de registro y de contabilidad sean exactas y que el sistema pueda crear un certificado de seguridad válido.
- **Interfaz Ethernet 1 (privada)**: dirección IP y máscara (de nuestra topología de red 172.16.1.1/24).

En este momento, el VPN Concentrator es accesible a través de un navegador HTML desde la red interna. Para obtener información sobre la configuración del concentrador VPN en modo CLI, refiérase a Configuración Rápida con CLI.

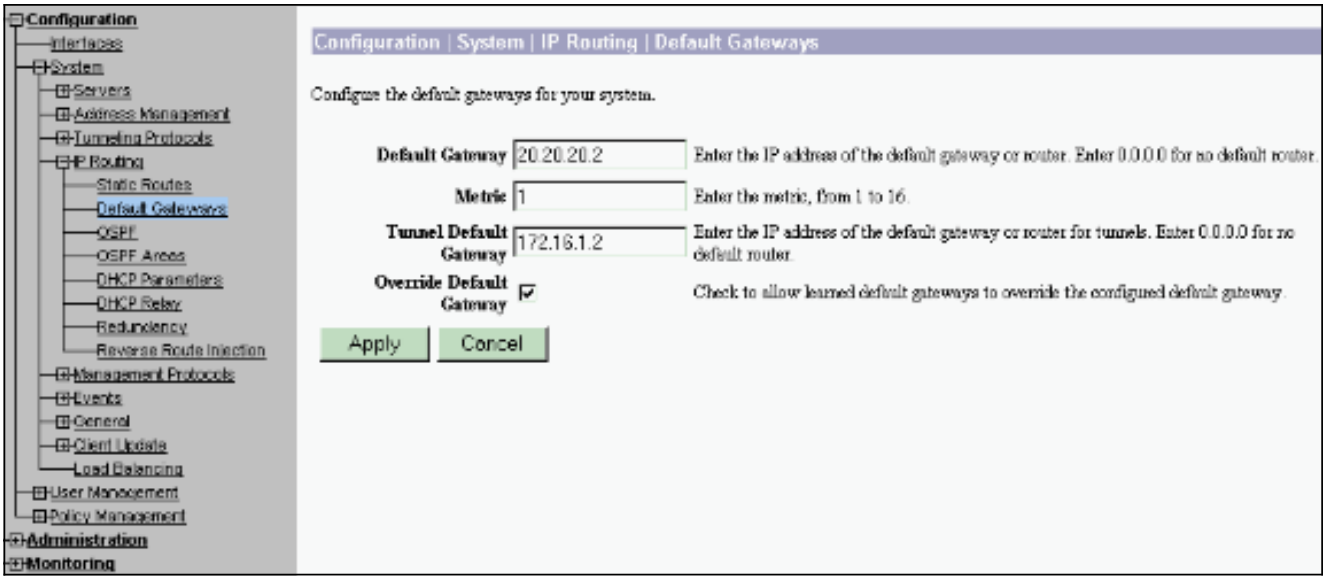
1. Escriba la dirección IP de la interfaz privada desde el navegador web para habilitar la interfaz GUI.Haga clic en el icono **guardar** los cambios necesarios para guardar la memoria. El nombre de usuario y la contraseña predeterminados de fábrica son "admin", que distingue entre mayúsculas y
minúsculas.



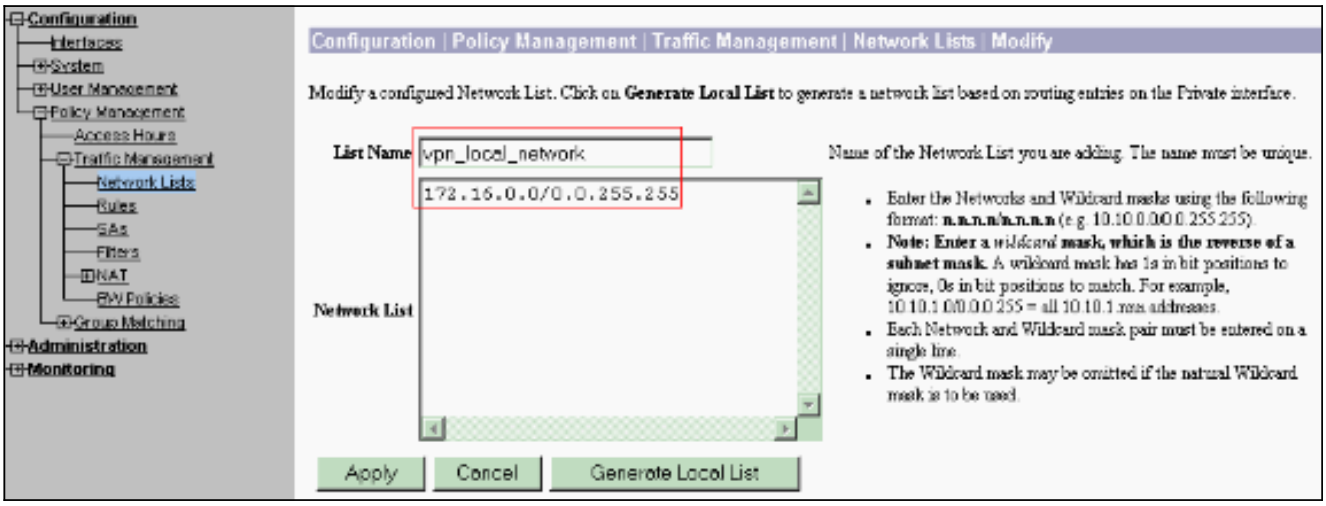
2. Después de activar la GUI, seleccione **Configuration > Interfaces > Ethernet 2 (Public)** para configurar la interfaz Ethernet
2.



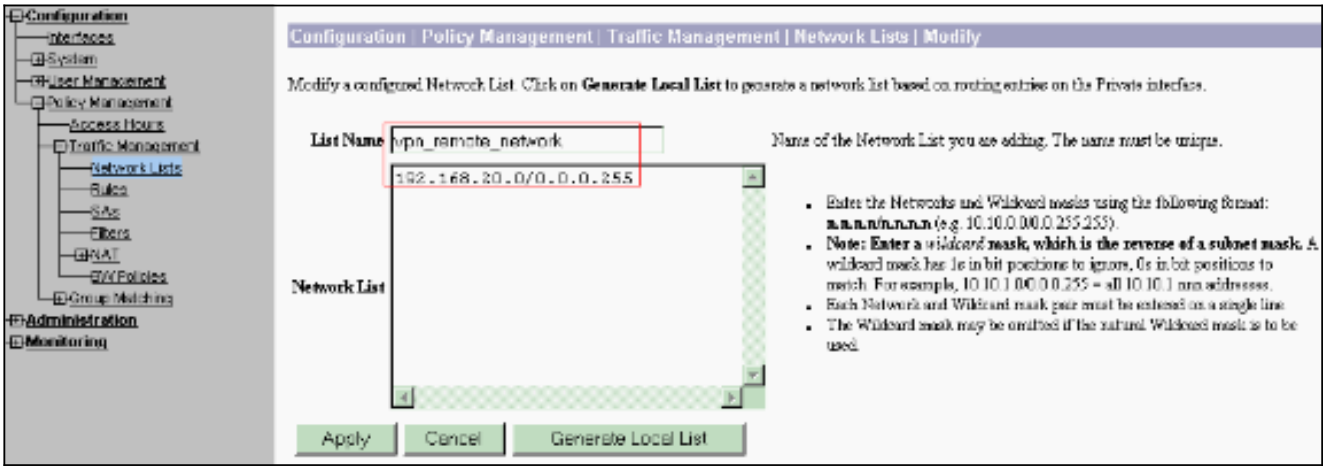
3. Seleccione **Configuration > System > IP Routing > Default Gateways** configure el gateway predeterminado (Internet) y el gateway predeterminado (interno) del túnel para IPsec para alcanzar las otras subredes en la red privada.En este escenario, sólo hay una subred disponible en la red
interna.



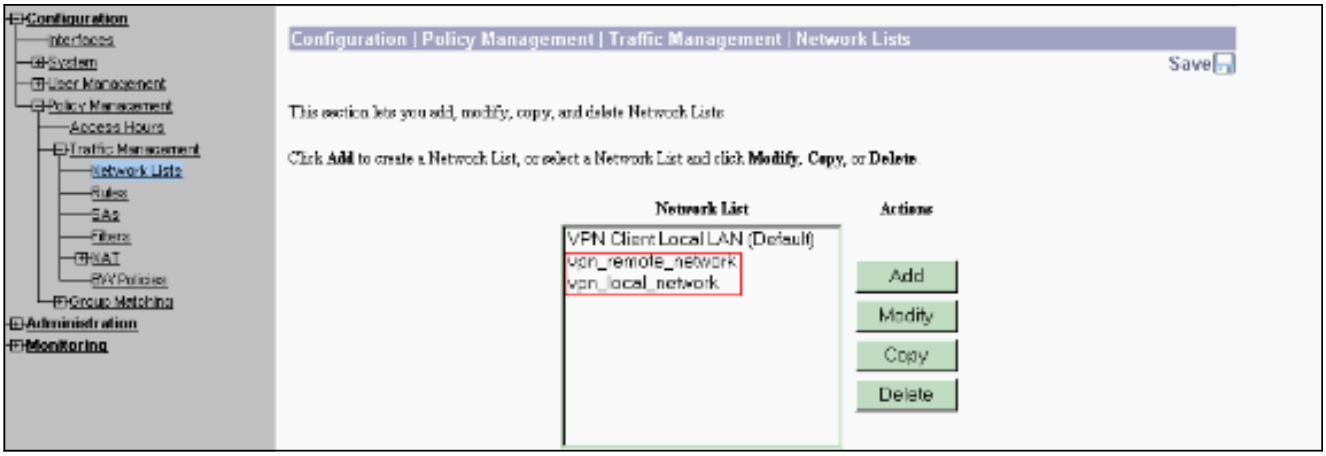
4. Seleccione Configuration > **Policy Management** > **Traffic Management** > Network Lists > Add para crear las listas de red que definen el tráfico que se cifrará.Las redes mencionadas en la lista son accesibles a la red remota. Las redes que se muestran en la siguiente lista son redes locales. También puede generar la lista de red local automáticamente a través de RIP al hacer clic en **Generar lista local**.



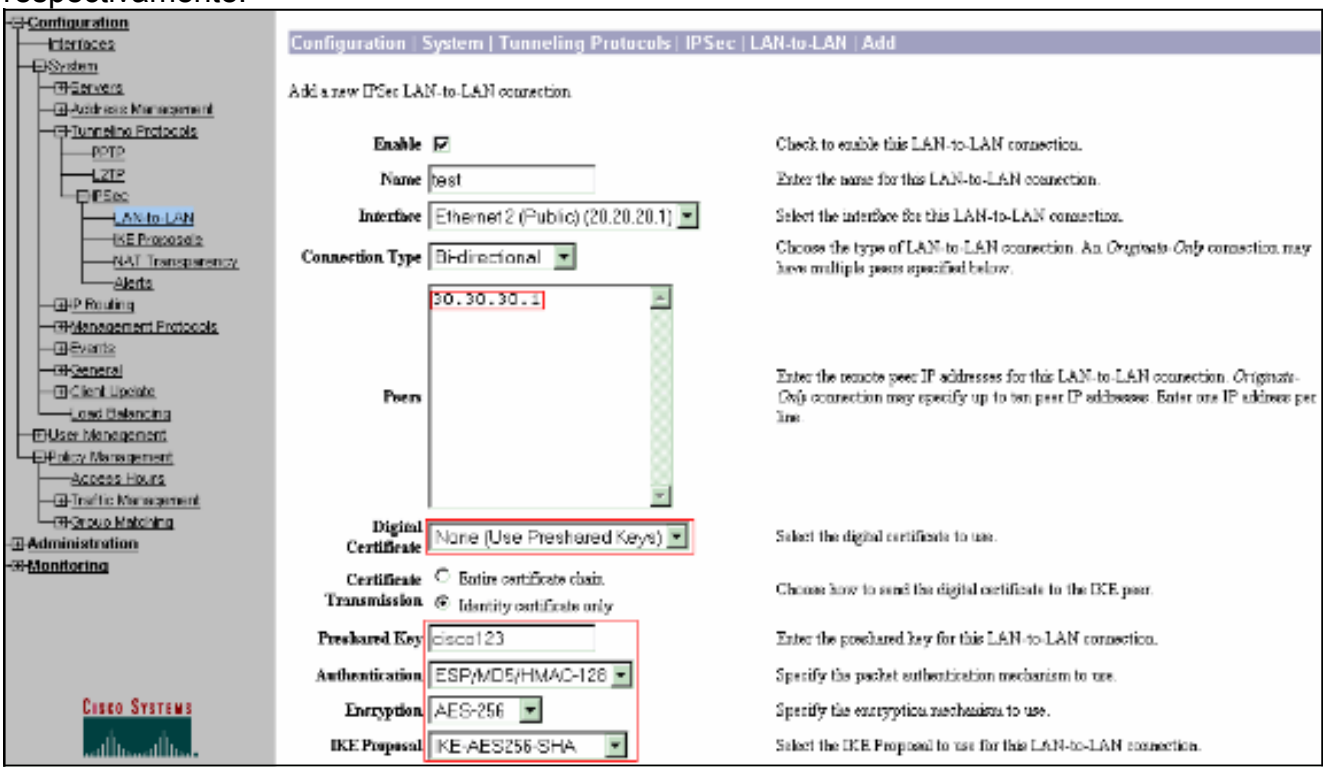
5. Las redes de esta lista son redes remotas y deben configurarse manualmente. Para hacer esto, ingrese la red/comodín para cada subred alcanzable.

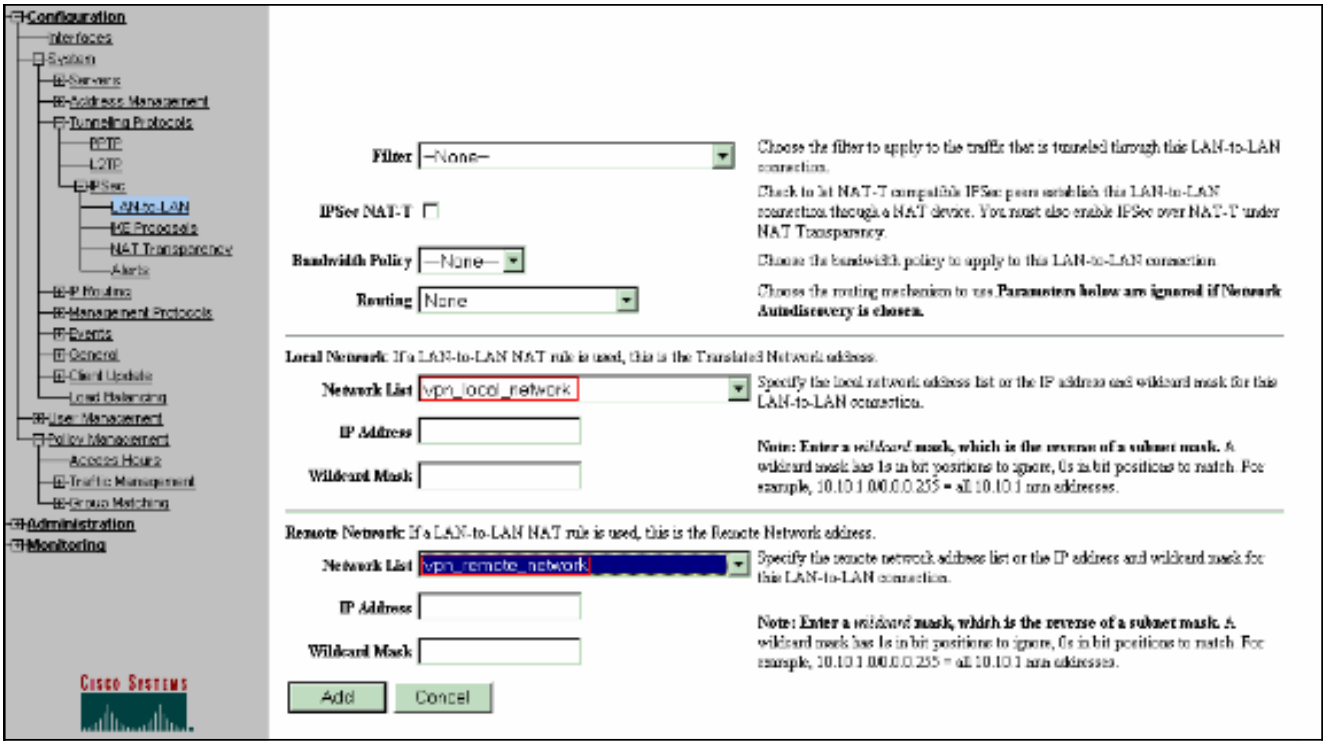


Una vez terminado, estas son las dos listas de red:

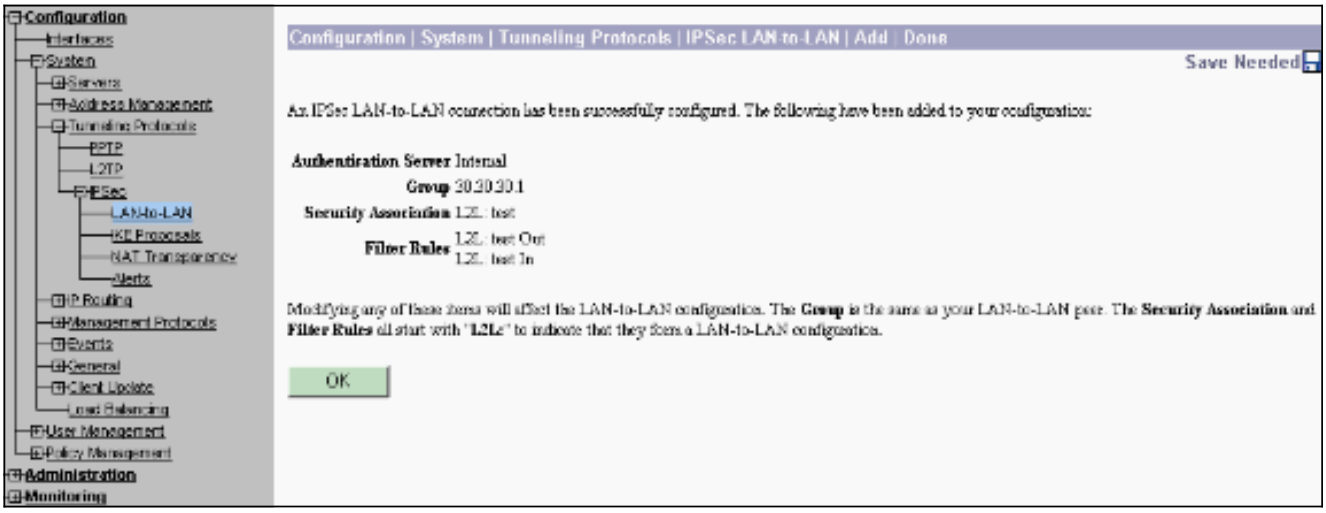


6. Seleccione Configuration > **System > Tunneling Protocols > IPSec LAN-to-LAN** > Add y defina el túnel de LAN a LAN.Esta ventana tiene tres secciones. La sección superior es para la información de red y las dos secciones inferiores son para las listas de red local y remota. En la sección Network Information (Información de red), seleccione el cifrado AES, el tipo de autenticación, la propuesta IKE y escriba la clave previamente compartida. En las secciones inferiores, señale las listas de red que ya ha creado, tanto las listas Local como Remota, respectivamente.



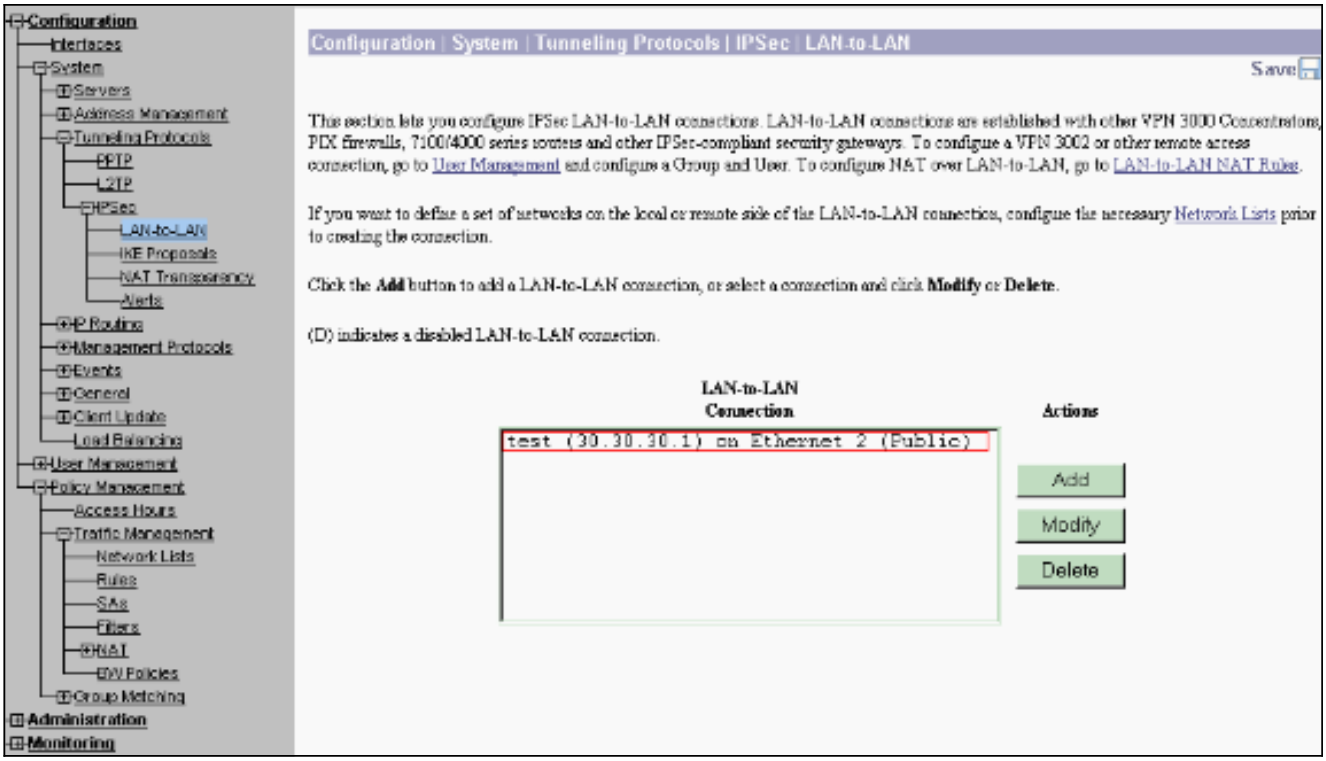


7. Después de hacer clic en **Agregar**, si la conexión es correcta, aparecerá la ventana IPSec LAN-to-LAN-Add-Done (IPSec LAN a LAN-Add-Done).Esta ventana presenta una sinopsis de la información de configuración del túnel. También configura automáticamente el nombre de grupo, el nombre SA y el nombre de filtro. Puede editar cualquier parámetro de esta tabla.



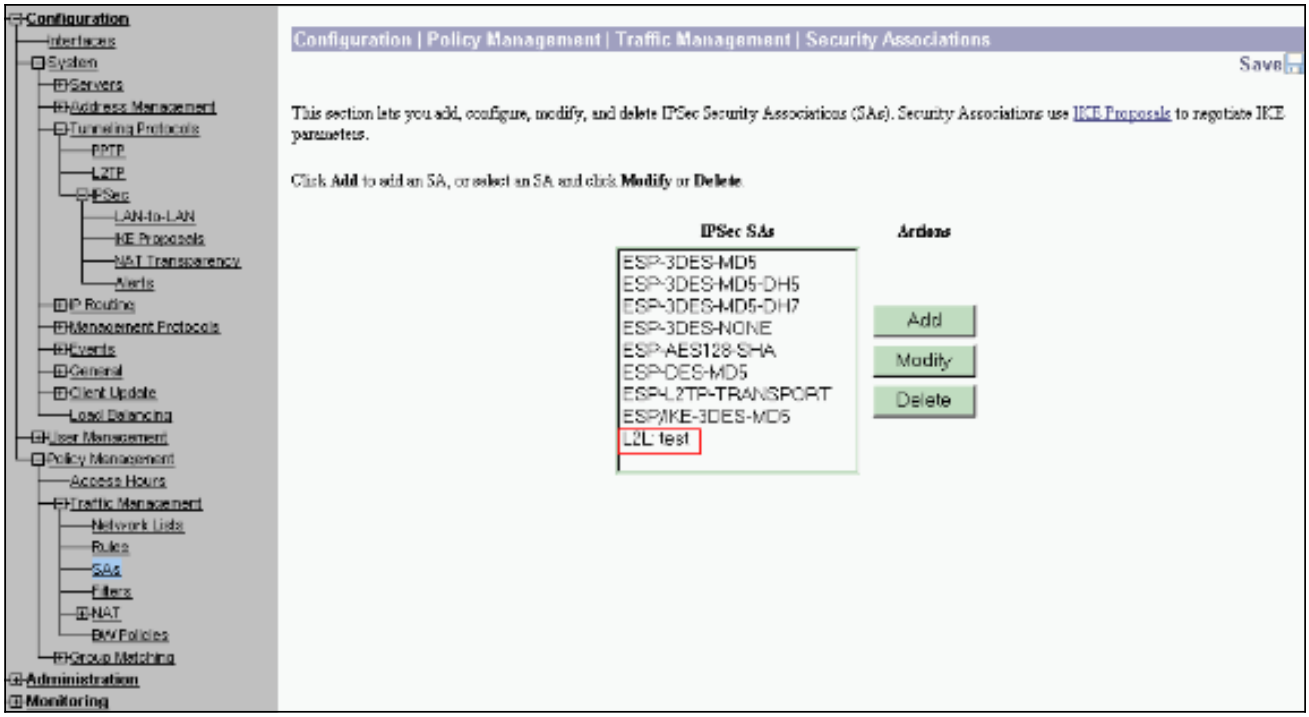
En este punto, el túnel de LAN a LAN IPSec se ha configurado y puede comenzar a funcionar. Si, por alguna razón, el túnel no funciona, puede verificar si hay configuraciones erróneas.

8. Puede ver o modificar los parámetros IPsec de LAN a LAN creados anteriormente cuando seleccione **Configuration > System > Tunneling Protocols > IPSec LAN a LAN**.Este gráfico muestra "prueba" como el nombre del túnel y la interfaz pública del extremo remoto es 30.30.30.1 según el
escenario.

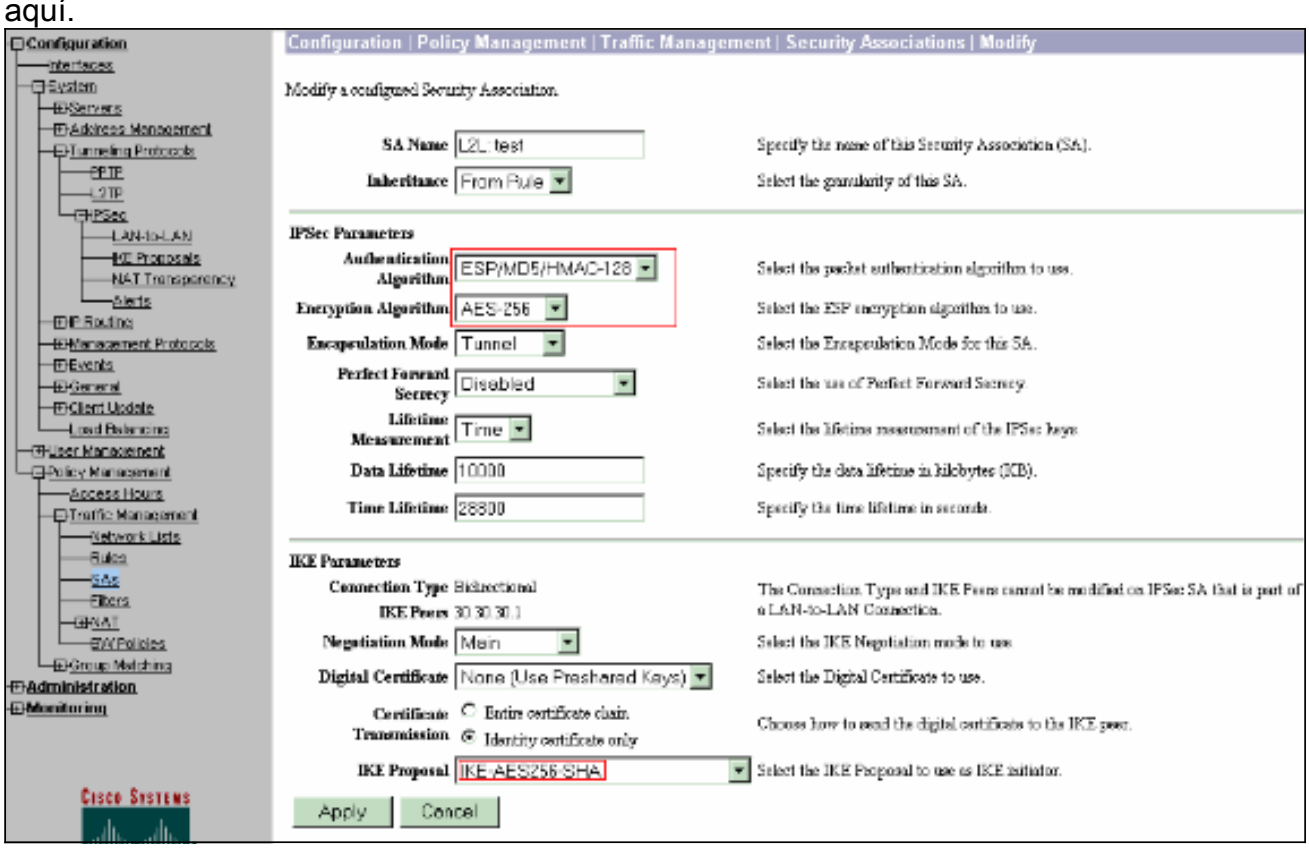


9. A veces, es posible que su túnel no aparezca si su propuesta IKE está en la lista Propuestas inactivas. Seleccione Configuration > **System > Tunneling Protocols > IPSec > IKE Proposale** para configurar la propuesta IKE activa.Si su propuesta IKE está en la lista "Propuestas inactivas", puede activarla cuando seleccione la propuesta IKE y haga clic en el botón **Activate**. En este gráfico, la propuesta seleccionada "IKE-AES256-SHA" se encuentra en la lista de propuestas activas.

10. Seleccione **Configuration > Policy Management > Traffic Management > Security Associations** para verificar si los parámetros SA son correctos.



11. Haga clic en el nombre SA (en este caso, **L2L: test**), y luego haga clic en **Modify** para verificar las SA.Si alguno de los parámetros no coincide con la configuración del par remoto, puede cambiarse
aquí.



Verificación

Verifique la configuración del router

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

La herramienta Output Interpreter (sólo para clientes registrados) permite utilizar algunos comandos “show” y ver un análisis del resultado de estos comandos.

- **show crypto isakmp sa — Muestra todas las asociaciones actuales de seguridad (SA) IKE de un par.** El estado QM_IDLE indica que la SA permanece autenticada con su peer y se puede utilizar para los intercambios de modo rápido subsiguientes. Está en estado de quietud.

```
ipsec_router#show crypto isakmp sa

 dst             src             state    conn-id   slot

 20.20.20.1      30.30.30.1      QM_IDLE         1      0
```

- **show crypto ipsec sa — Muestra la configuración actual utilizada por las SA actuales** Verifique la dirección IP par, las redes accesibles en los extremos remotos y locales y la transformación fijada que se utiliza. Hay dos ESP SA, uno en cada dirección. Dado que se utilizan conjuntos de transformación AH, está vacío.

```
ipsec_router#show crypto ipsec sa

interface: Ethernet1/0

       Crypto map tag: vpn, local addr. 30.30.30.1

       protected vrf:

        local ident (addr/mask/prot/port): (192.168.20.0/255.255.255.0/0/0)

       remote ident (addr/mask/prot/port): (172.16.0.0/255.255.0.0/0/0)

       current_peer: 20.20.20.1:500

         PERMIT, flags={origin_is_acl,}

        #pkts encaps: 145, #pkts encrypt: 145, #pkts digest 145

        #pkts decaps: 51, #pkts decrypt: 51, #pkts verify 51

        #pkts compressed: 0, #pkts decompressed: 0

        #pkts not compressed: 0, #pkts compr. failed: 0

        #pkts not decompressed: 0, #pkts decompress failed: 0

        #send errors 6, #recv errors 0

        local crypto endpt.: 30.30.30.1, remote crypto endpt.: 20.20.20.1

        path mtu 1500, media mtu 1500

        current outbound spi: 54FA9805

       inbound esp sas:

       spi: 0x4091292(67703442)

        transform: esp-256-aes esp-md5-hmac ,

        in use settings ={Tunnel, }

        slot: 0, conn id: 2000, flow_id: 1, crypto map: vpn

        sa timing: remaining key lifetime (k/sec): (4471883/28110)
```

```
 IV size: 16 bytes

 replay detection support: Y

inbound ah sas:

inbound pcp sas:

 outbound esp sas:

spi: 0x54FA9805(1425709061)

 transform: esp-256-aes esp-md5-hmac ,

 in use settings ={Tunnel, }

 slot: 0, conn id: 2001, flow_id: 2, crypto map: vpn

 sa timing: remaining key lifetime (k/sec): (4471883/28110)

 IV size: 16 bytes

 replay detection support: Y

outbound ah sas:

outbound pcp sas:
```

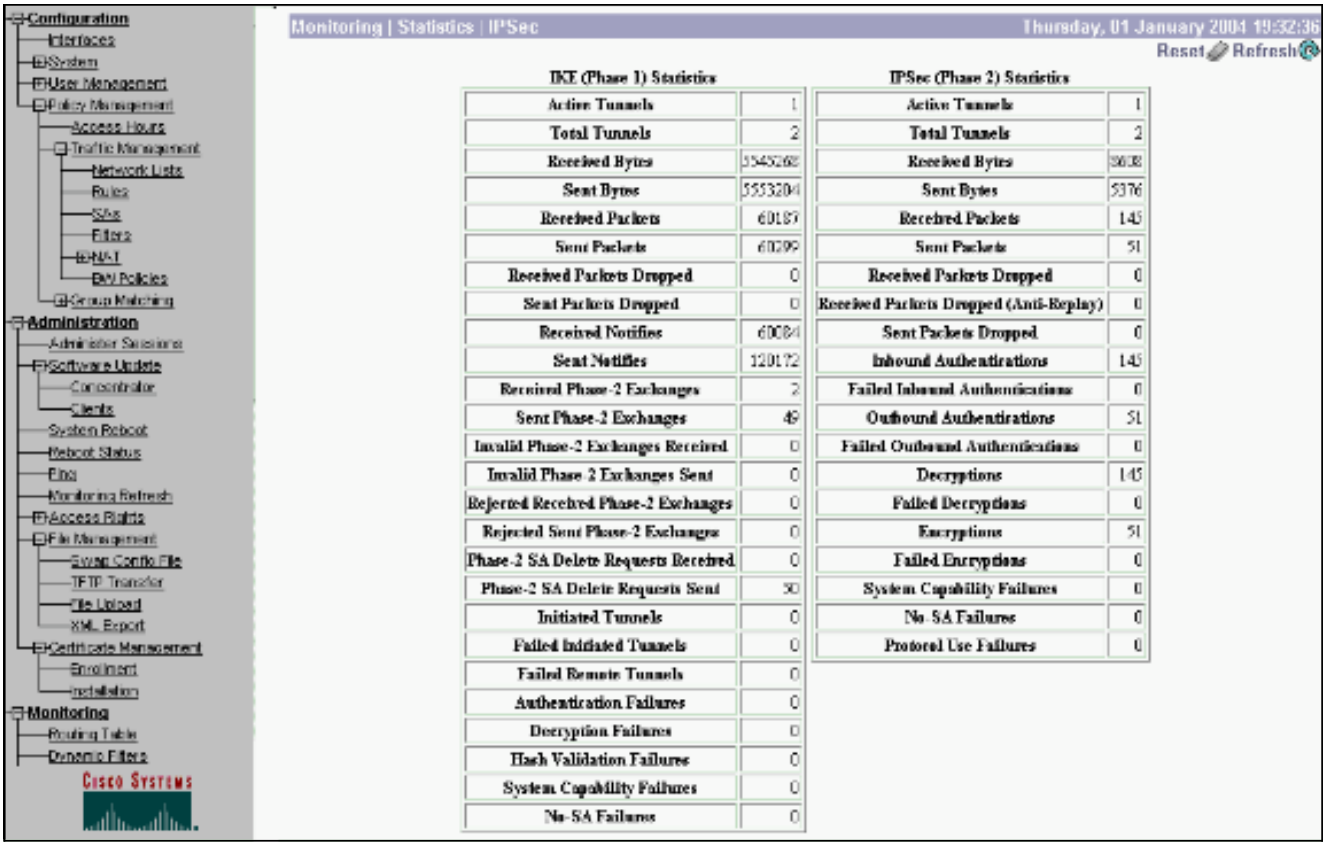
- **show crypto engine connections active**: muestra las conexiones de sesión cifradas activas actuales para todos los motores criptográficos. Cada ID de conexión es único. El número de paquetes cifrados y descifrados se muestra en las dos últimas columnas.

```
ipsec_router#show crypto engine connections active
   ID     Interface     IP-Address   State   Algorithm          Encrypt Decrypt

    1     Ethernet1/0   30.30.30.1   set     HMAC_SHA+AES_256_C       0       0

 2000     Ethernet1/0   30.30.30.1   set     HMAC_MD5+AES_256_C       0      19

 2001     Ethernet1/0   30.30.30.1   set     HMAC_MD5+AES_256_C      19       0
```

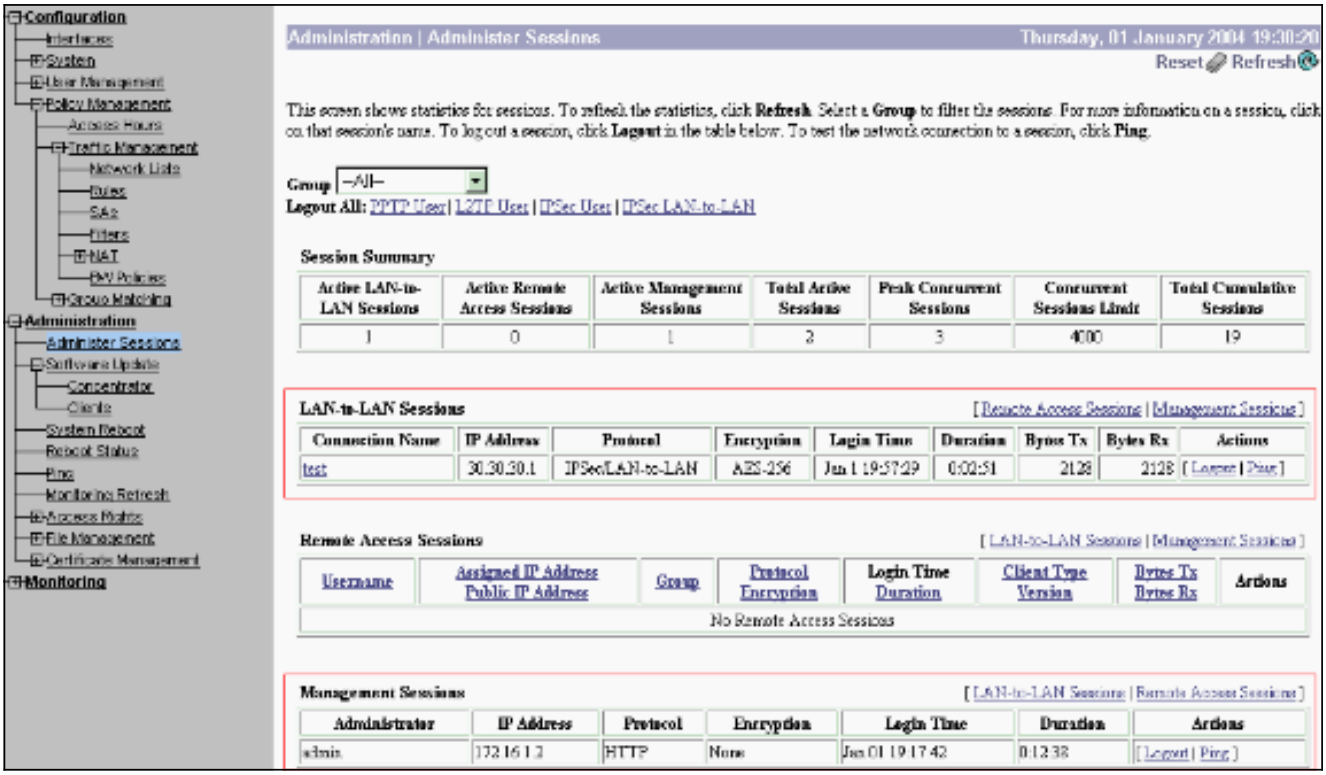
Verifique la configuración del concentrador VPN

Complete estos pasos para verificar la configuración del VPN Concentrator.

1. De manera similar a los comandos show crypto ipsec sa y **show crypto isakmp sa** en los routers, puede ver las estadísticas de IPsec e IKE cuando selecciona **Monitoring > Statistics >** IPSec en los concentradores
   VPN.



2. Al igual que el comando **show crypto engine connections active** en los routers, puede utilizar la ventana Administration-Sessions en el VPN Concentrator para ver los parámetros y estadísticas de todas las conexiones o túneles IPsec LAN a LAN activos.



Troubleshoot

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

Resolución de Problemas en el Router

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.

Nota: Consulte Información Importante sobre Comandos Debug antes de utilizar los comandos **debug**.

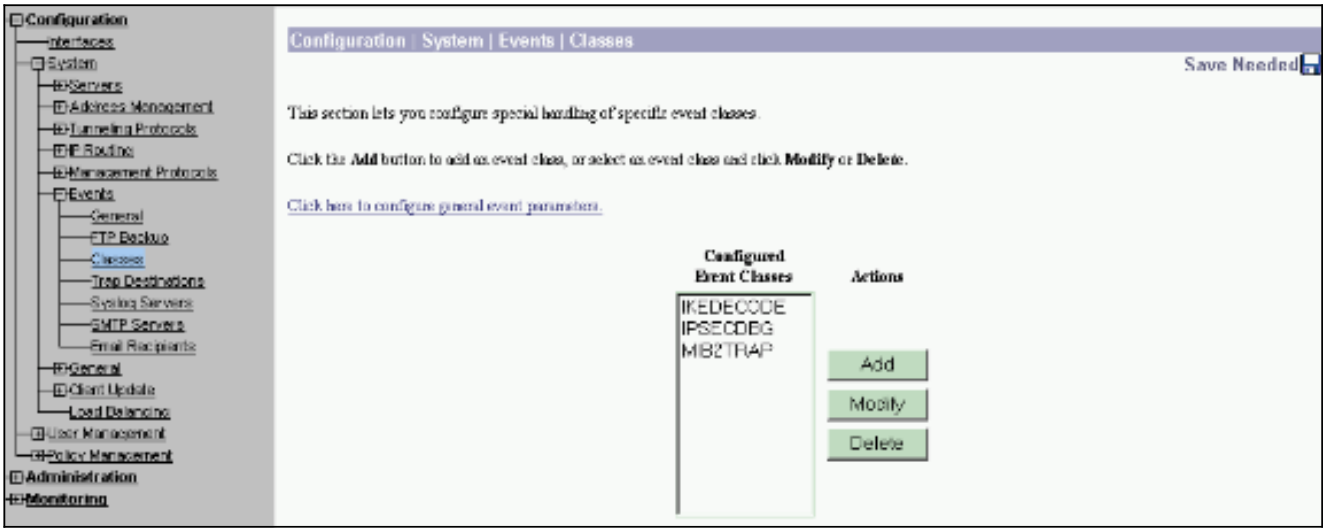
- **debug crypto engine**: muestra el tráfico cifrado. El motor criptográfico es el mecanismo real que realiza el cifrado y el descifrado. Un motor criptográfico puede ser un software o un acelerador de hardware.
- **debug crypto isakmp**: muestra las negociaciones ISAKMP (del inglés Internet Security Association and Key Management Protocol, Asociación de seguridad de Internet y protocolo de administración de claves) de la fase IKE 1.
- **debug crypto ipsec**: muestra las negociaciones IPSec de la fase IKE 2.

Refiérase a Resolución de Problemas de IPSec - Comprensión y Uso de Comandos **debug** para obtener información más detallada y salida de ejemplo.

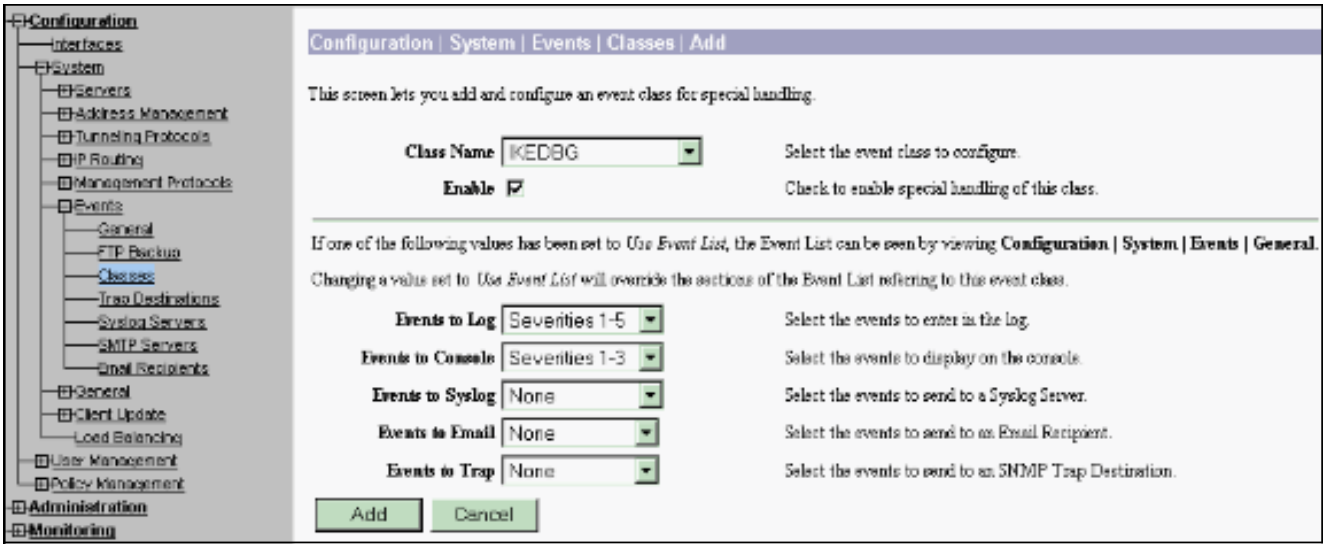
Solución de problemas del concentrador VPN

Al igual que los comandos **debug** en los routers Cisco, puede configurar las clases Event para ver todas las alarmas.

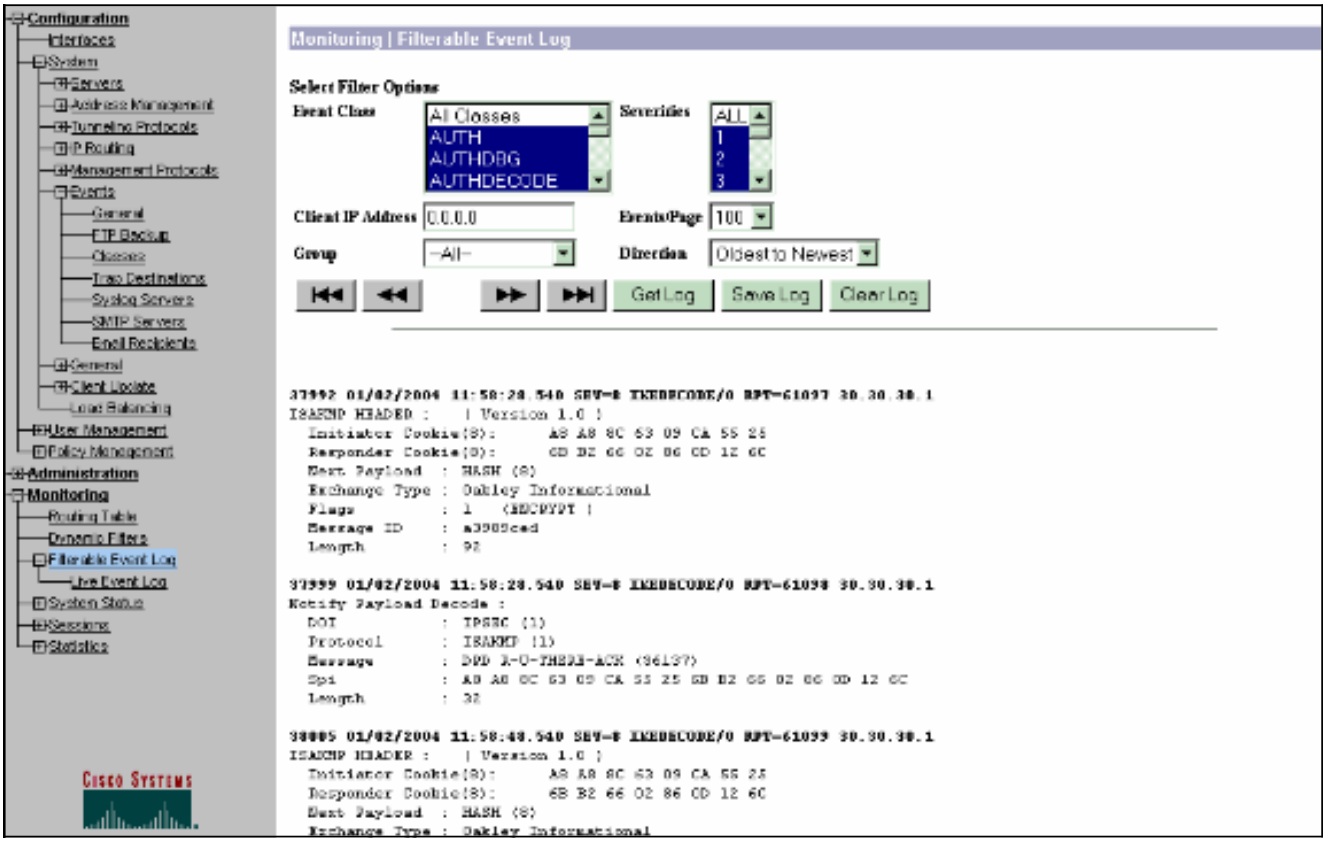
1. Seleccione Configuration > **System** > **Events** > **Classes** > Add para activar el registro de clases de evento.Estas clases están disponibles para IPSec:IKEIKEDBGIKEDECODEIPSECIPSECDBGIPSECDECODE



2. Al agregar, también puede seleccionar el nivel de gravedad para cada clase, en función del nivel de gravedad que se envía la alarma.Las alarmas pueden manejarse mediante uno de estos métodos:Por registroSe muestra en la consolaEnviado al servidor UNIX SyslogEnviado como correo electrónicoEnviado como trampa a un servidor SNMP



3. Seleccione **Monitoring** > **Filterable Event Log** para monitorear las alarmas activadas.



Información Relacionada

- Advanced Encryption Standard (AES)
- Módulo de cifrado VPN DES/3DES/AES
- Configuraciones de ejemplo de IPSec
- Página de soporte al cliente Serie Cisco VPN 3000
- Página de Soporte de IPSec Negotiation/IKE Protocols