Túnel ipsec de LAN a LAN entre un Cisco VPN 3000 Concentrator y un router con el ejemplo de configuración 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.

El AES es una nueva publicación del Estándar de procesamiento de la información federal (FIP) creada por el National Institute of Standards and Technology (NIST) que se utilizará como método de encripción. Este estándar especifica un algoritmo de encripción simétrica AES que substituya el Data Encryption Standard (DES) mientras que una aislamiento transforma para el IPSec y el Internet Key Exchange (IKE). El AES tiene tres diversas longitudes de clave, una clave del 128-bit (el valor por defecto), una clave del 192-bit, y una clave del 256-bit. La característica AES en Cisco IOS® agrega el soporte para la nueva norma de encripción AES, con el modo del Cipher Block Chaining (CBC), al IPSec.

Refiera al sitio del centro de recursos de seguridad informática NIST para más información sobre el AES.

Refiérase túnel ipsec de LAN a LAN entre el Cisco VPN 3000 Concentrator y el ejemplo de configuración del firewall PIX para más información sobre configuración del túnel de LAN a LAN

entre un concentrador VPN 3000 y el firewall PIX.

Refiera al túnel IPsec entre PIX 7.x y ejemplo de configuración concentrador VPN 3000 para más información cuando el PIX tiene versión de software 7.1.

prerrequisitos

Requisitos

Este documento requiere una comprensión básica del Protocolo IPSec. Refiera a una introducción a la encripción de IPSec para aprender más sobre el IPSec.

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- **Requerimientos del router** - La característica AES fue introducida en el Cisco IOS Software Release 12.2(13)T. Para habilitar el AES, su router debe soportar el IPSec y funcionar con una imagen del IOS con las claves largas del "k9" (el subsistema del "k9").**Nota:** El soporte del hardware para el AES está también disponible en 2691, 3725, y 3745 los módulos VPN de aceleración AES del Cisco 2600XM. Esta característica no tiene ninguna consecuencia en la configuración y el módulo de hardware se selecciona automáticamente si ambos están disponibles.
- **Requisitos del concentrador VPN** - El software support para la característica AES fue introducido en la versión 3.6. El soporte del hardware es proporcionado por el nuevo procesador aumentado, scalable del cifrado (SEP-E). Esta característica no tiene ninguna consecuencia en la configuración.**Nota:** En la versión 3.6.3 del Cisco VPN 3000 Concentrator, los túneles no negocian al AES debido al Id. de bug Cisco CSCdy88797 (clientes registrados solamente). Esto se ha resuelto de la versión 3.6.4.**Nota:** El Cisco VPN 3000 Concentrator utiliza el cualquier septiembre o septiembre - Módulos E, no ambos. No instale ambos en el mismo dispositivo. Si usted instala un módulo SEP-E en un concentrador VPN que contenga ya 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 el Cisco IOS Software Release 12.3(5)
- Concentrador Cisco VPN 3060 con el Software Release 4.0.3

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

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

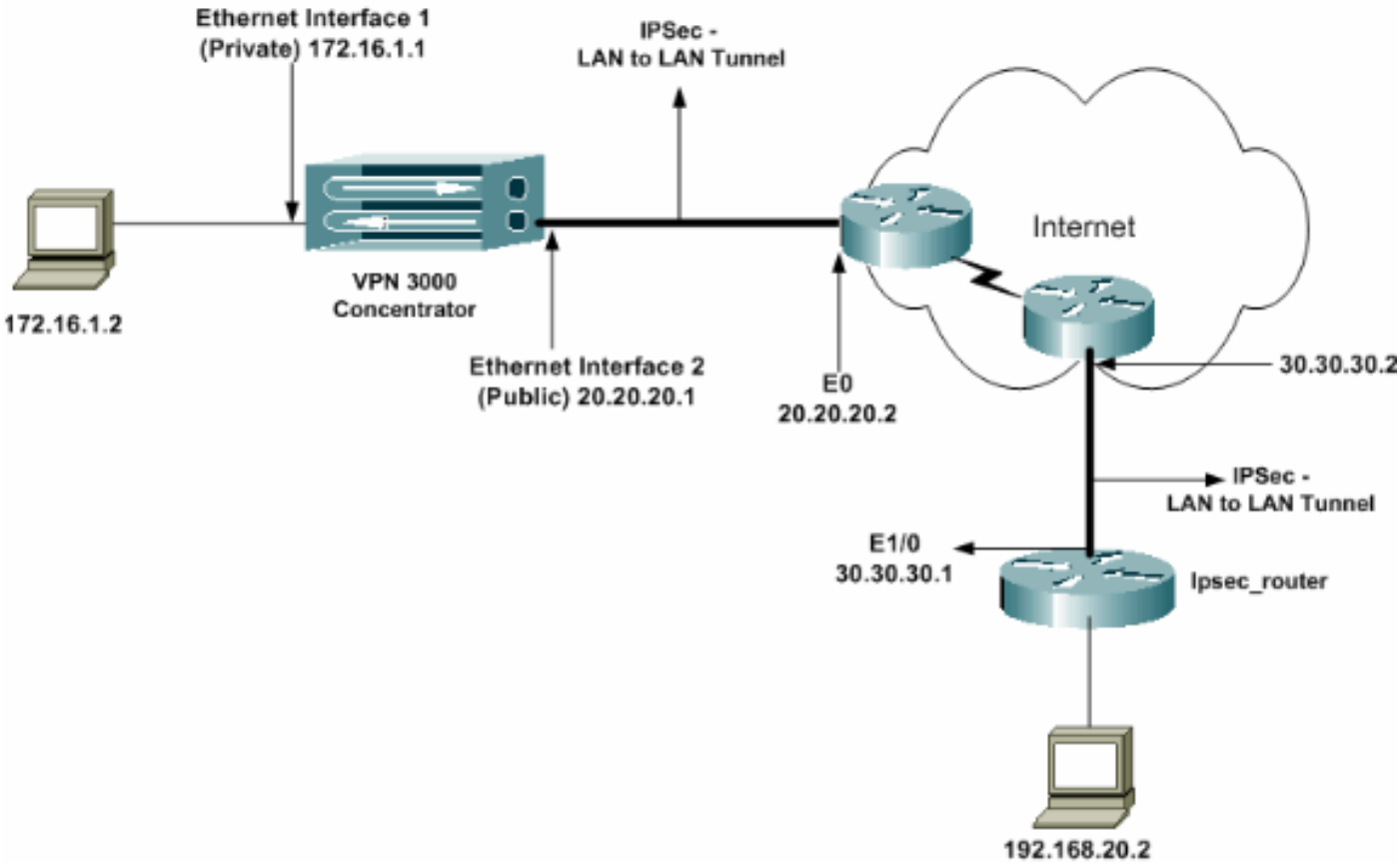
Configurar

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

Nota: Utilice la herramienta Command Lookup Tool (clientes registrados solamente) 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 del 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 ACL sea sin cambios, los significados son levemente diferentes para el ACL de criptografía. En el ACL de criptografía, el **permiso** especifica eso los paquetes que corresponden con debe ser cifrado, mientras que **niegue** especifica eso los paquetes que corresponden con no necesitan ser cifrados.

Configure el concentrador VPN

Los concentradores VPN no se preprograman con los IP Addresses en sus configuraciones de fábrica. Usted tiene que utilizar el puerto de la consola para configurar las configuraciones iniciales que son comando line interface(cli) con un menú. Refiera a configurar los concentradores VPN a través de la consola para la información sobre cómo configurar a través de la consola.

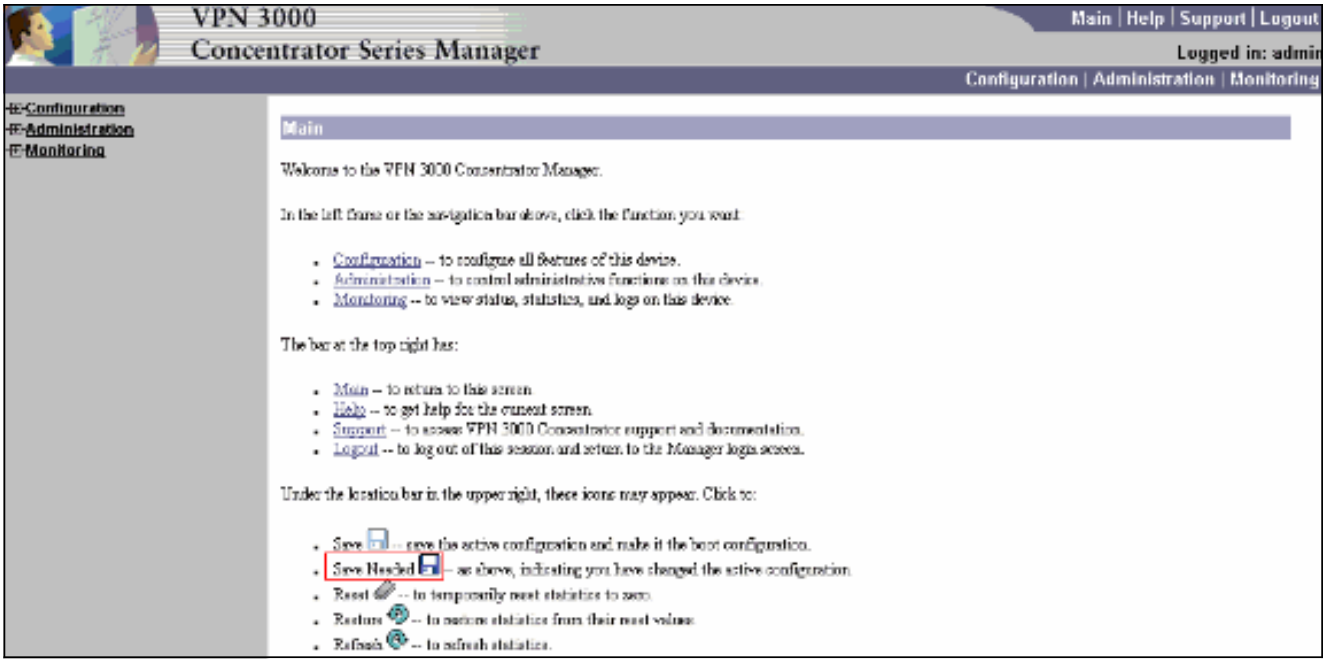
Después de que la dirección IP en la interfaz del Ethernet1 (soldado) se configure, el resto se puede configurar o con el CLI o vía la interfaz del buscador. La interfaz del buscador soporta el HTTP y el HTTP sobre el Secure Socket Layer (SSL).

Estos parámetros se configuran a través de la consola:

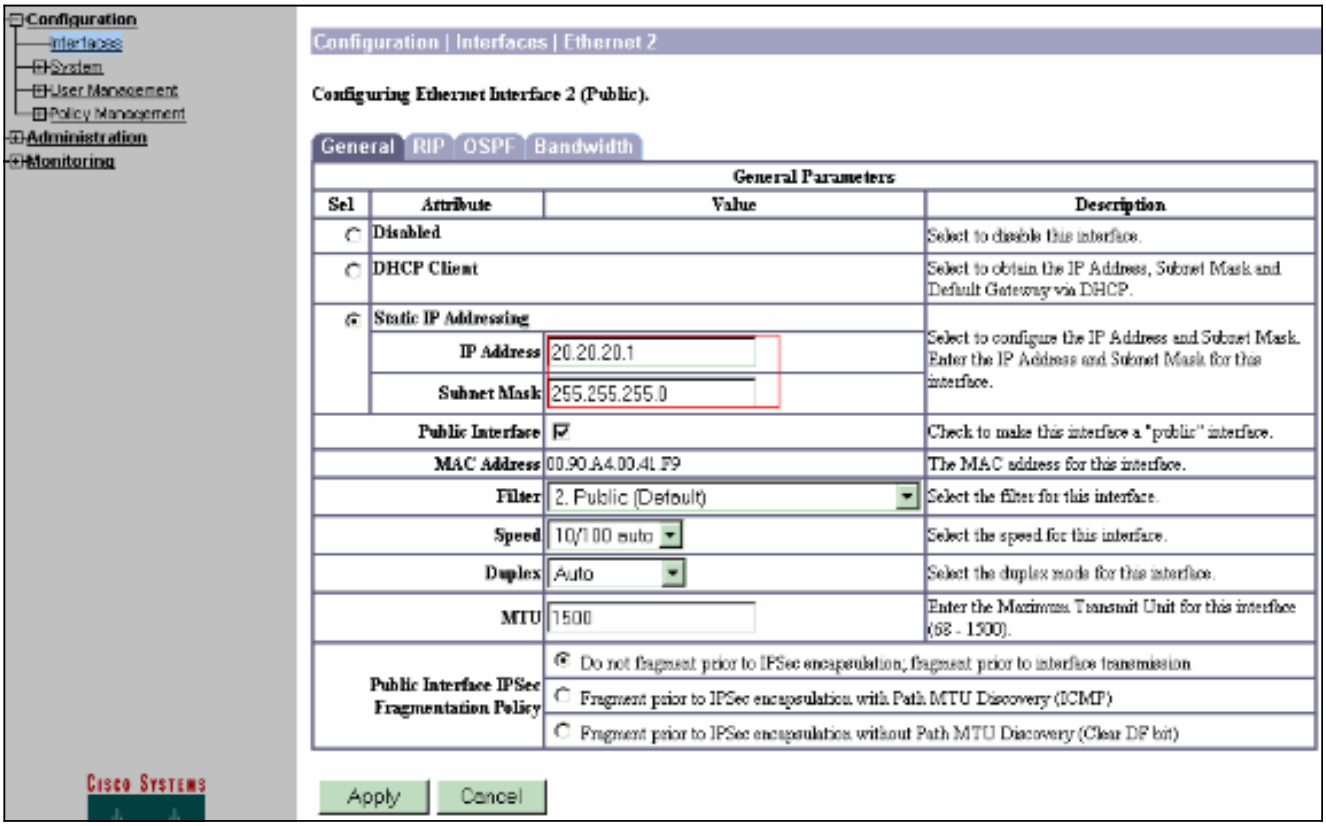
- **Hora/fecha** - La hora correcta y la fecha son muy importantes. Ayudan a asegurarse de que la registración y las entradas de contabilidad son exactas, y de que el sistema puede crear un Security Certificate válido.
- **Interfaz del Ethernet1 (soldado)** - La dirección IP y la máscara (de nuestra topología de red 172.16.1.1/24).

En este momento, el concentrador VPN es accesible a través de un buscador HTML de la red interna. Para la información sobre configurar el concentrador VPN en el modo CLI, refiera a la configuración rápida usando el CLI.

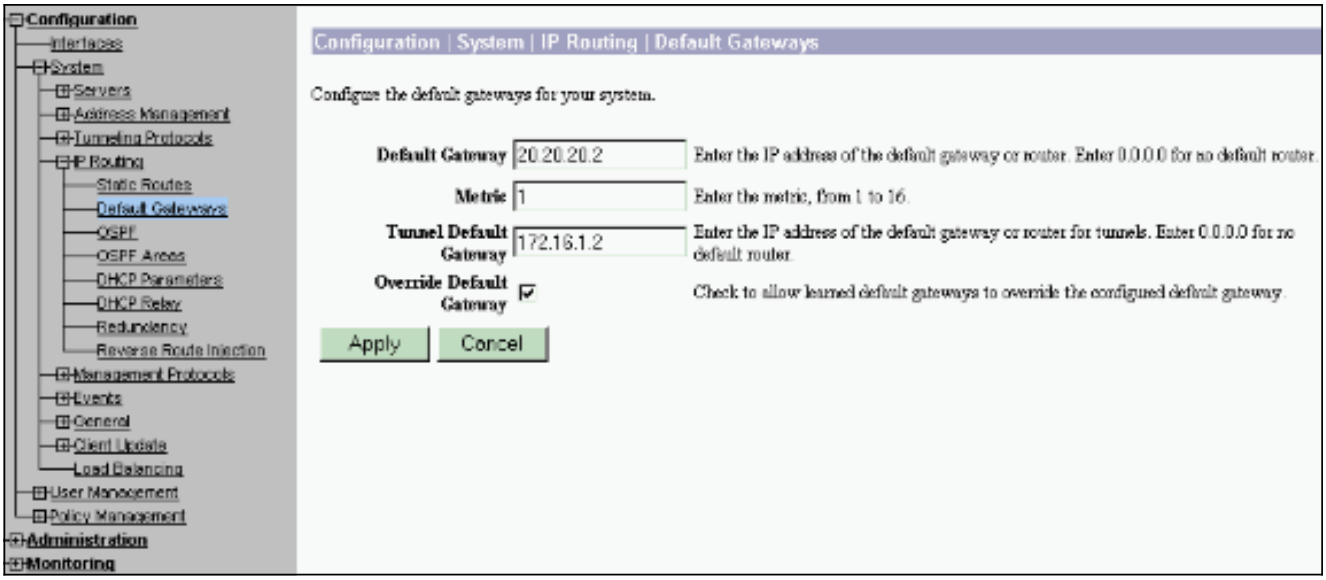
1. Teclee la dirección IP de la interfaz privada del buscador Web para habilitar la interfaz GUI.Haga clic en el icono **necesario salvaguardia** para salvar los cambios a la memoria. El nombre de usuario y contraseña del valor predeterminado de fábrica es el “admin” que es con diferenciación entre mayúsculas y minúsculas.



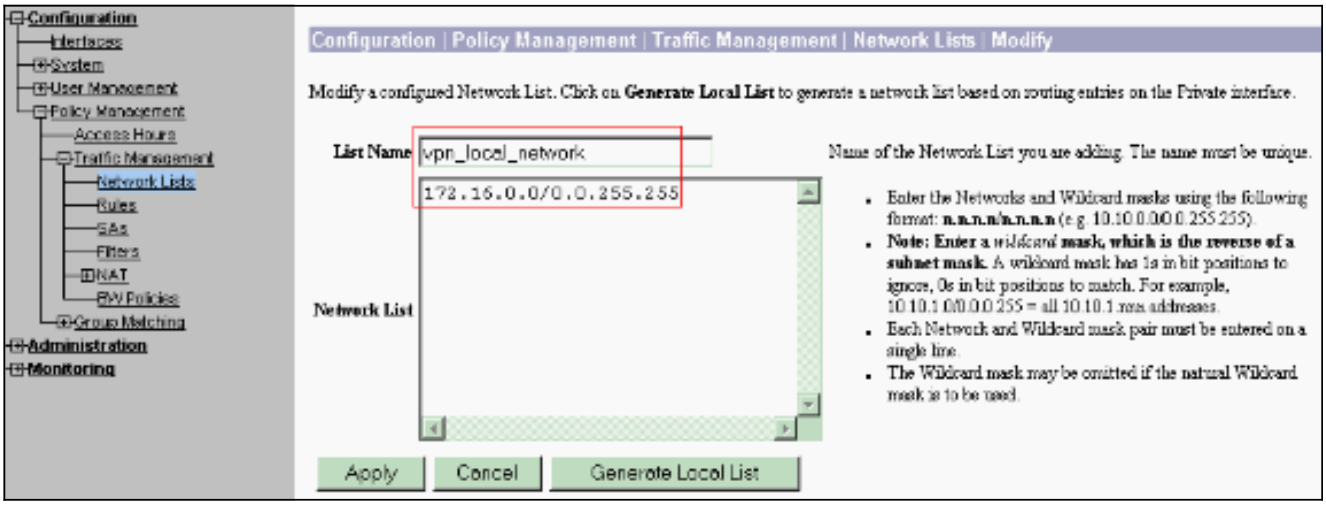
2. Después de que usted traiga para arriba el GUI, el **Configuration (Configuración) > Interfaces (Interfaces) > Ethernet** selecto **2 (público)** para configurar la interfaz de los Ethernetes 2.



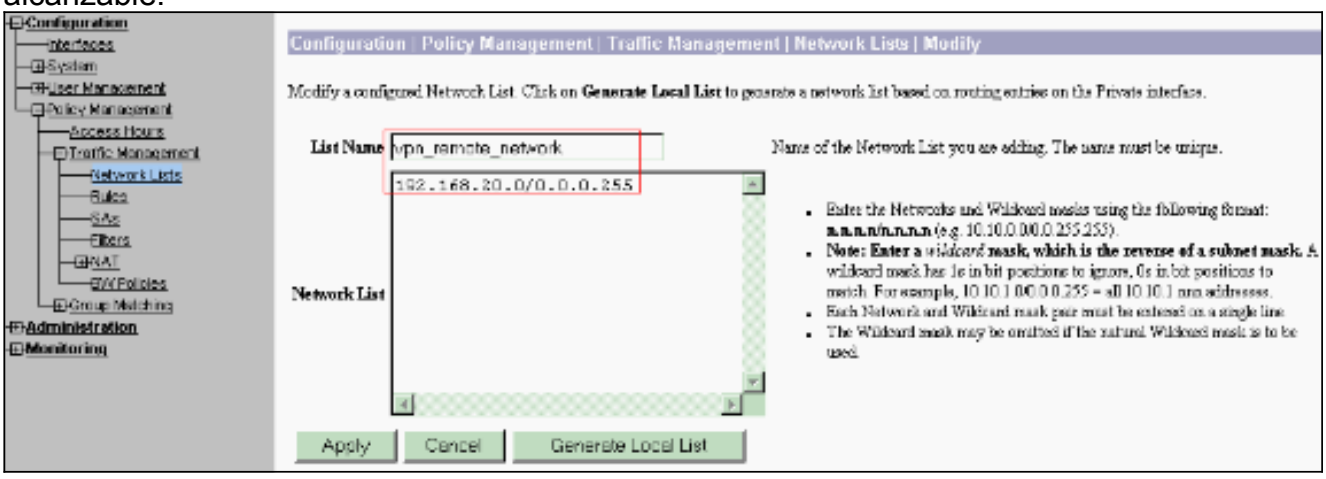
3. Seleccione **Configuration > System > Routing IP >** los **default gatewayes** configuran el gateway predeterminado (de Internet) y el gateway del valor por defecto del túnel (dentro) para que el IPSec alcance las otras subredes en la red privada.En este escenario, hay solamente una subred disponible en la red interna.



4. Seleccione el **Configuration (Configuración) > Policy Management (Administración de políticas) > Traffic Management (Administración de tráfico) > Network Lists (Lista de redes) >** 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 mostradas en la lista abajo son redes locales. Usted puede también generar la lista de red local automáticamente vía el RIP cuando usted tecleo **genera la lista local**.

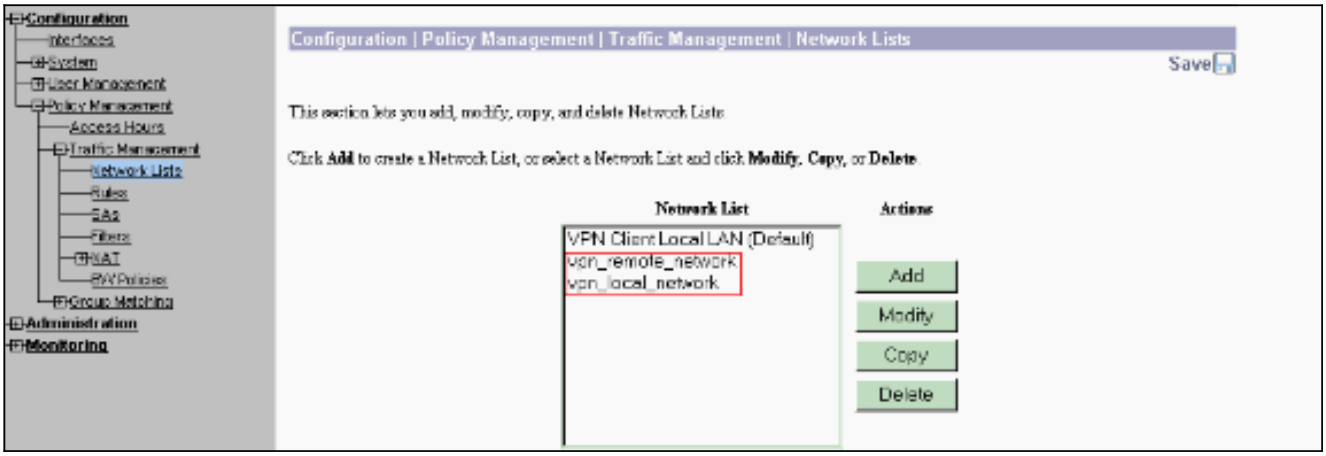


5. Las redes en esta lista son redes remotas y necesitan ser configuradas manualmente. Para hacer esto, ingrese la red/al comodín para cada subred alcanzable.

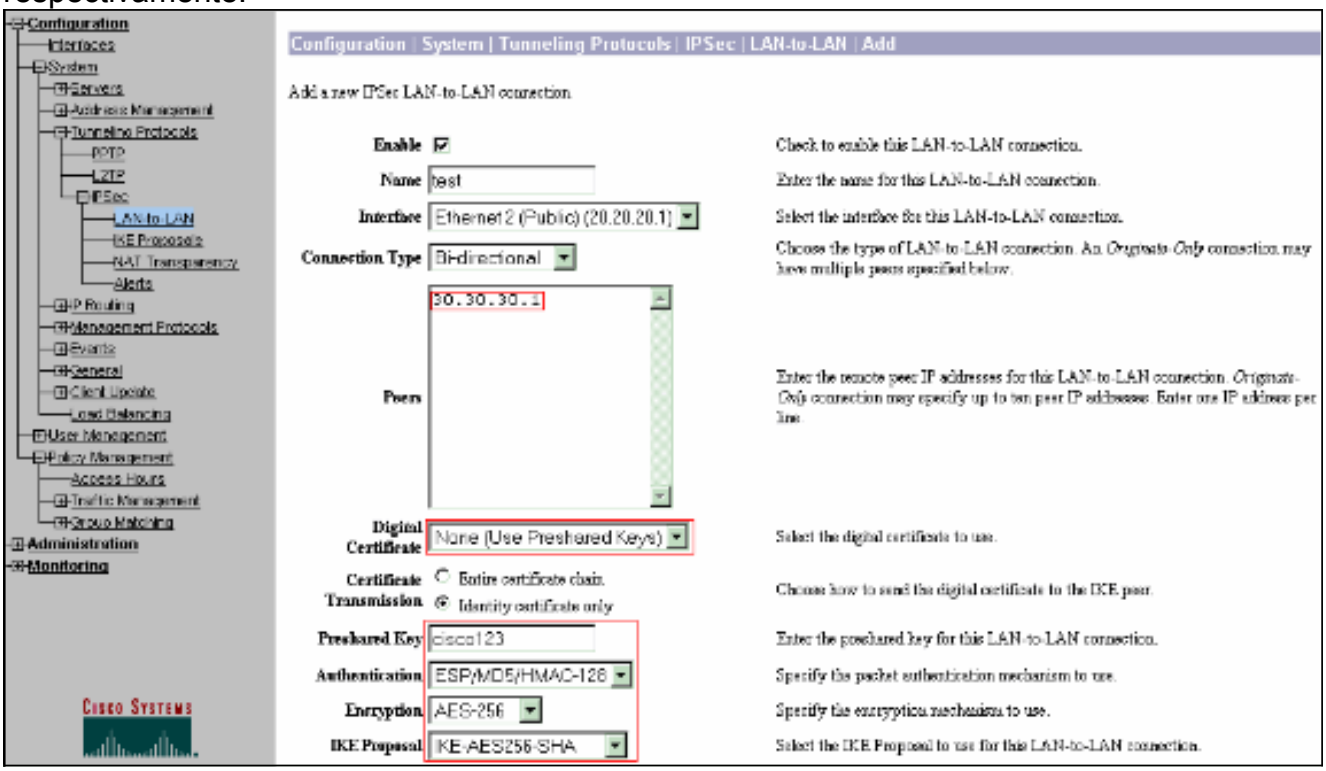


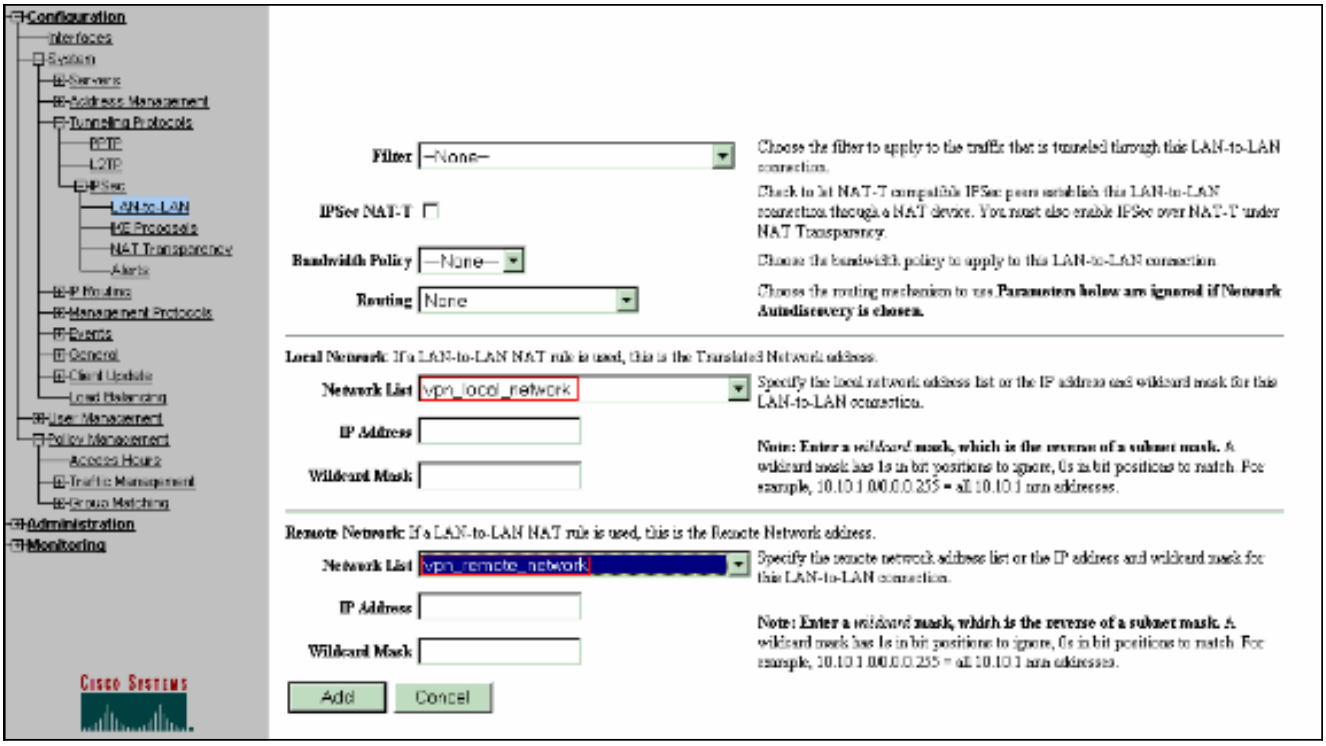
Una vez terminado, estas son las dos listas de

red:

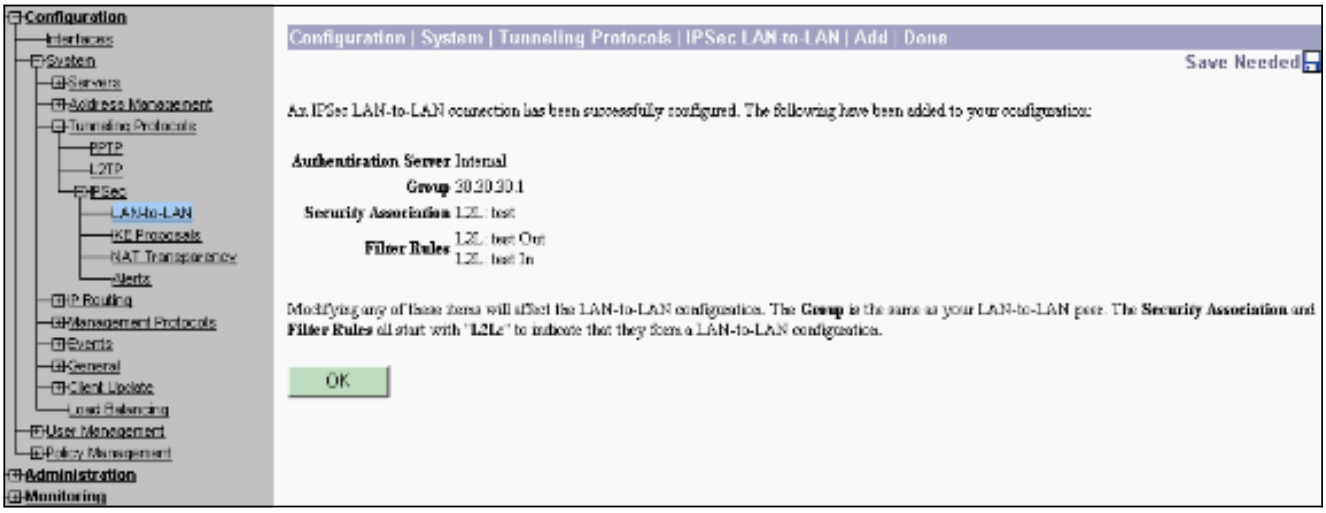


6. Seleccione el **Configuration (Configuración) > System (Sistema) > Tunneling Protocols (Protocolos de tunelización) > IPSec LAN-to-LAN (IPSec de LAN a LAN) > Add (Agregar)** y defina el túnel de LAN a LAN.Esta ventana tiene tres secciones. La sección superior está para la información de red y las dos secciones inferiores están para las listas de la red local y remota. En la sección de información de red, seleccione la encripción AES, tipo de autenticación, propuesta IKE, y teclee la clave previamente compartida. En las secciones inferiores, señale a las listas de red que usted creó ya, las listas locales y remotas respectivamente.



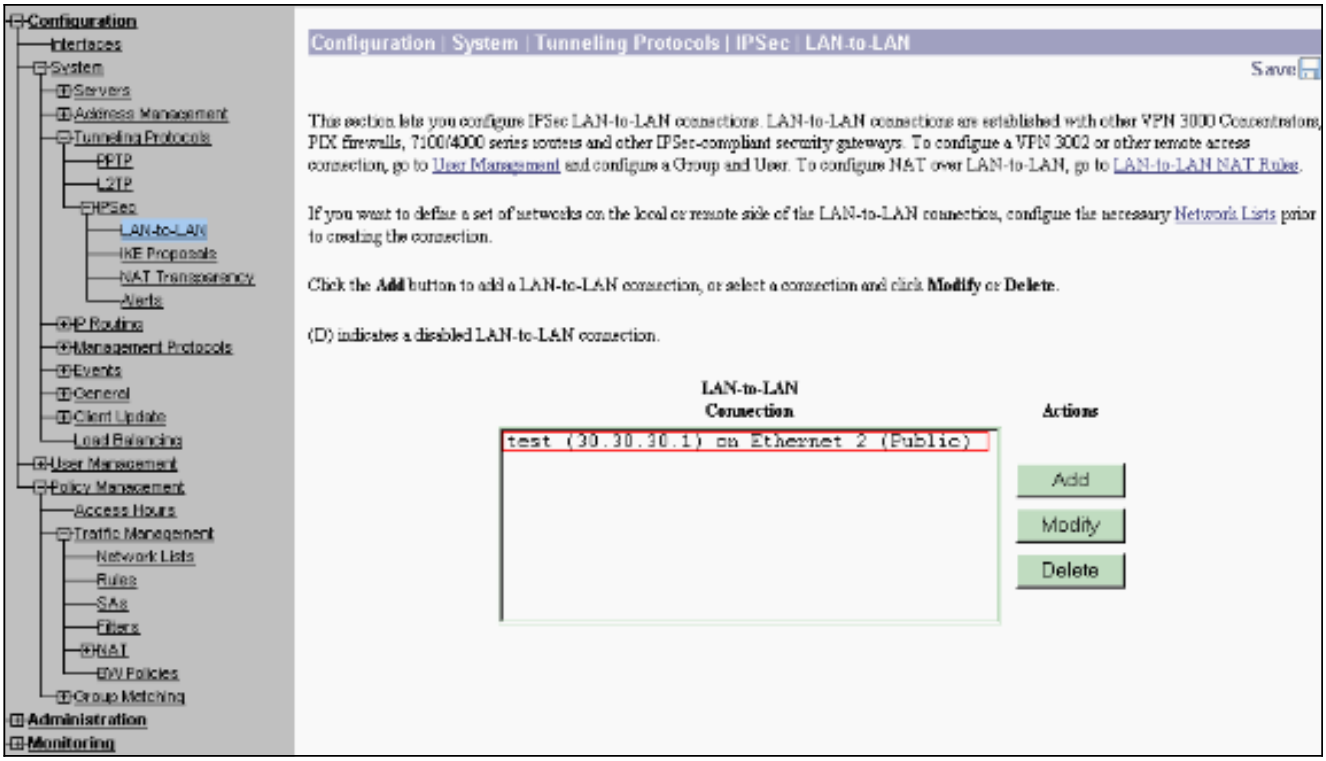


7. Después de que usted tecleo **agregue**, si su conexión está correcta, le presentan con la ventana LAN-a-LAN-agregar-hecha IPSec.Esta ventana presenta una sinopsis de la información de configuración del túnel. También configura automáticamente el nombre del grupo, el nombre SA, y el nombre del filtro. Usted puede editar cualquier parámetro en esta tabla.

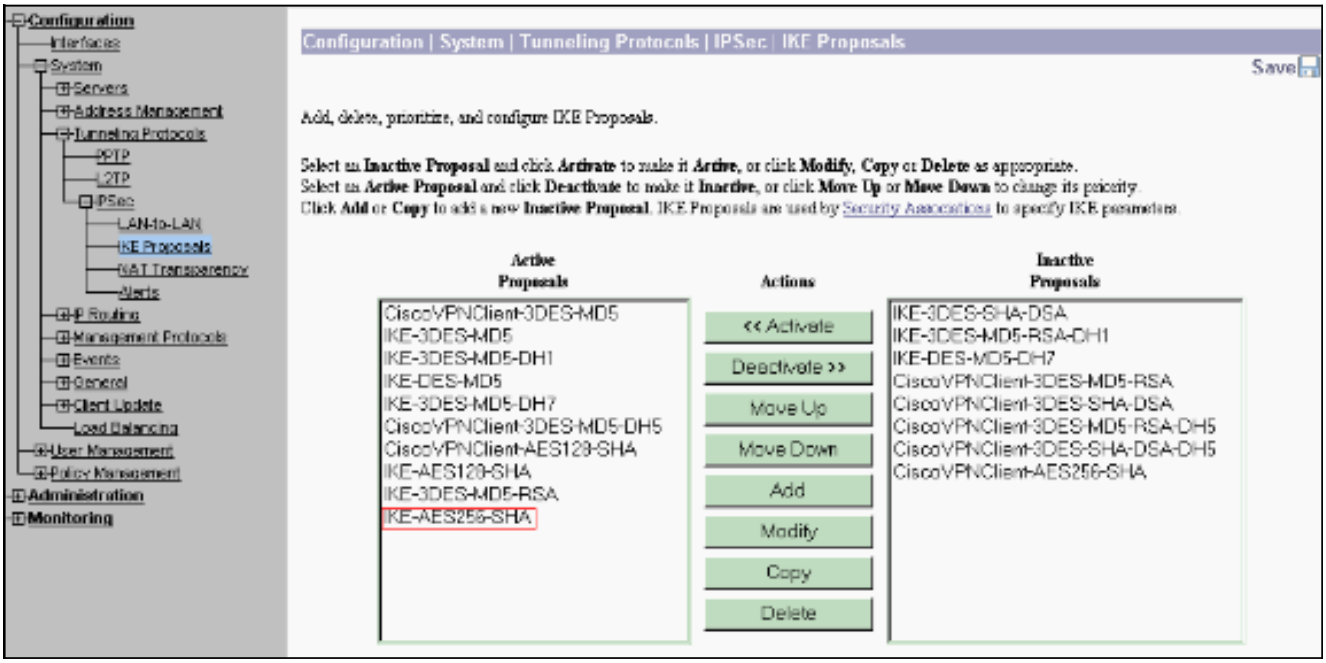


En este momento el túnel ipsec de LAN a LAN se ha configurado y usted puede comenzar a trabajar. Si, por alguna razón, el túnel no funciona, usted puede marcar para saber si hay misconfigurations.

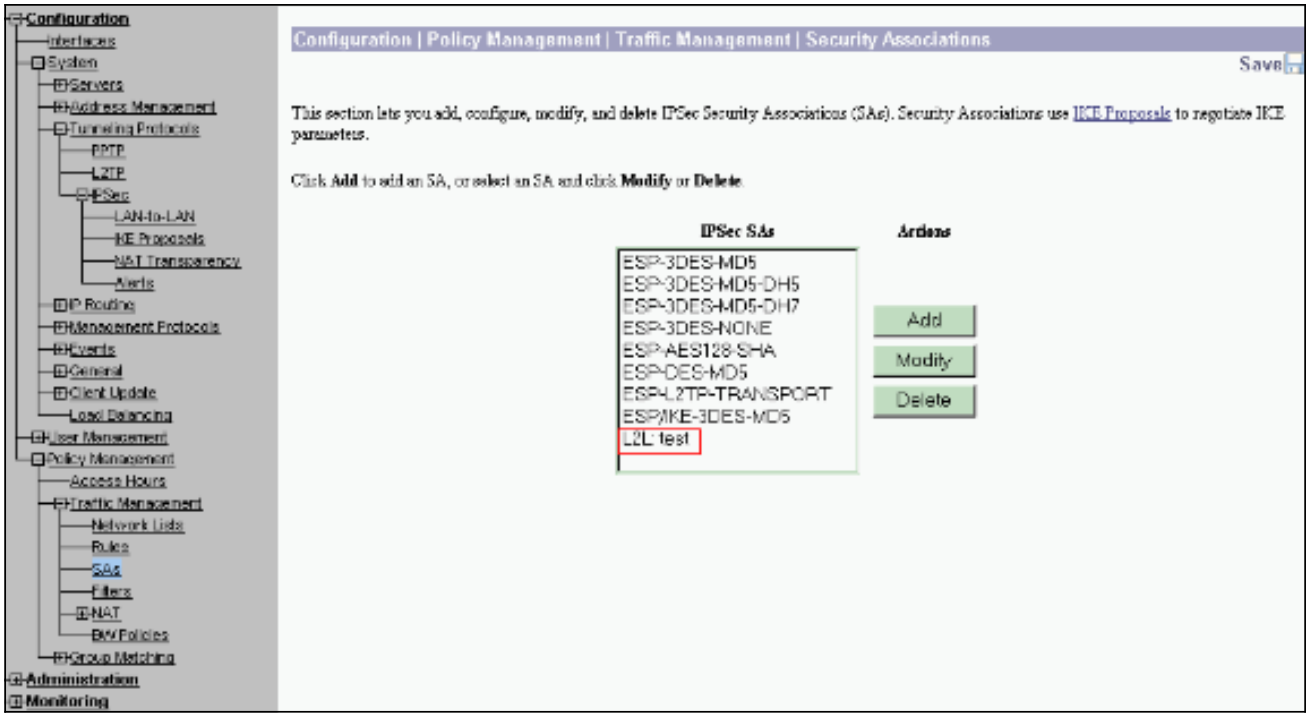
8. Usted puede ver o modificar los parámetros de IPSec previamente creados del LAN a LAN cuando usted selecciona el **Configuration (Configuración) > System (Sistema) > Tunneling Protocols (Protocolos de tunelización) > IPSec LAN-to-LAN (IPSec de LAN a LAN)**.Este gráfico muestra la “prueba” pues el nombre del túnel y de la interfaz pública del extremo remoto es 30.30.30.1 según el
escenario.



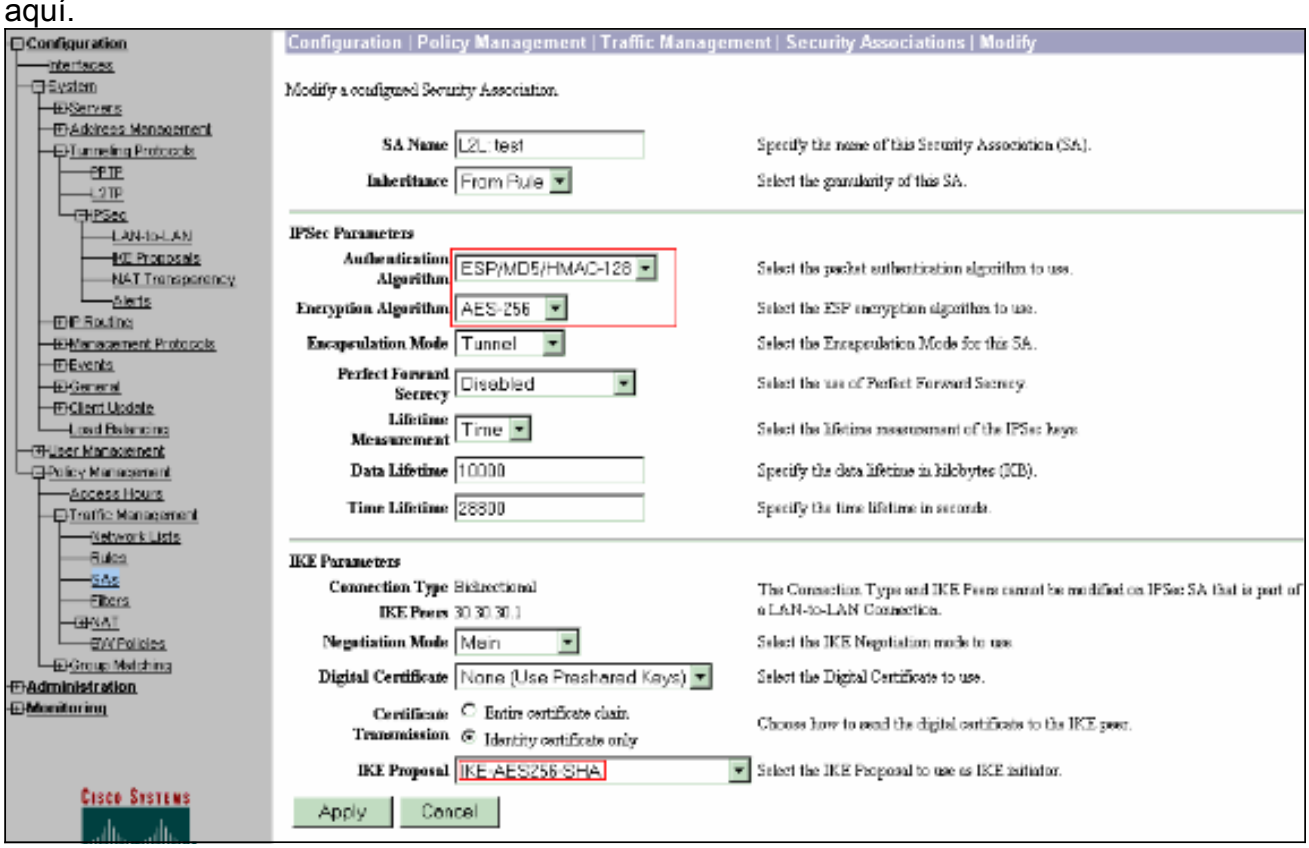
9. A veces, su túnel no pudo subir si su propuesta IKE está en la lista de las Propuestas inactivas. Seleccione el **Configuration (Configuración) > System (Sistema) > Tunneling Protocols (Protocolos de tunelización) > IPSec > IKE Proposals (Propuestas IKE)** para configurar la oferta del IKE activo.Si su propuesta IKE está en las “Propuestas inactivas” le enumeran pueden habilitarlo cuando usted selecciona la propuesta IKE y hace clic en el botón del **activar**. En este gráfico la oferta seleccionada el "IKE-AES256-SHA" está en la lista de las propuestas
activas.



10. Seleccione el **Configuration (Configuración) > Policy Management (Administración de políticas) > Management Traffic (Administración de tráfico) > Security Associations (Asociaciones de seguridad)** para verificar si los parámetros SA están correctos.



11. Haga clic el nombre SA (en este caso, **L2L: la prueba**), y entonces hace clic **se modifica** para verificar los SA.Si los parámetros uces de los no hacen juego con la configuración del peer remoto, puede ser cambiada
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 QM_IDLE del estado denota que los restos SA autenticados con su par y se puede utilizar para los intercambios subsiguientes del Quick Mode. Está en un estado quieto.

```
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. Puesto que AH transforme se utilizan los conjuntos, él están vacíos.

```
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:
```

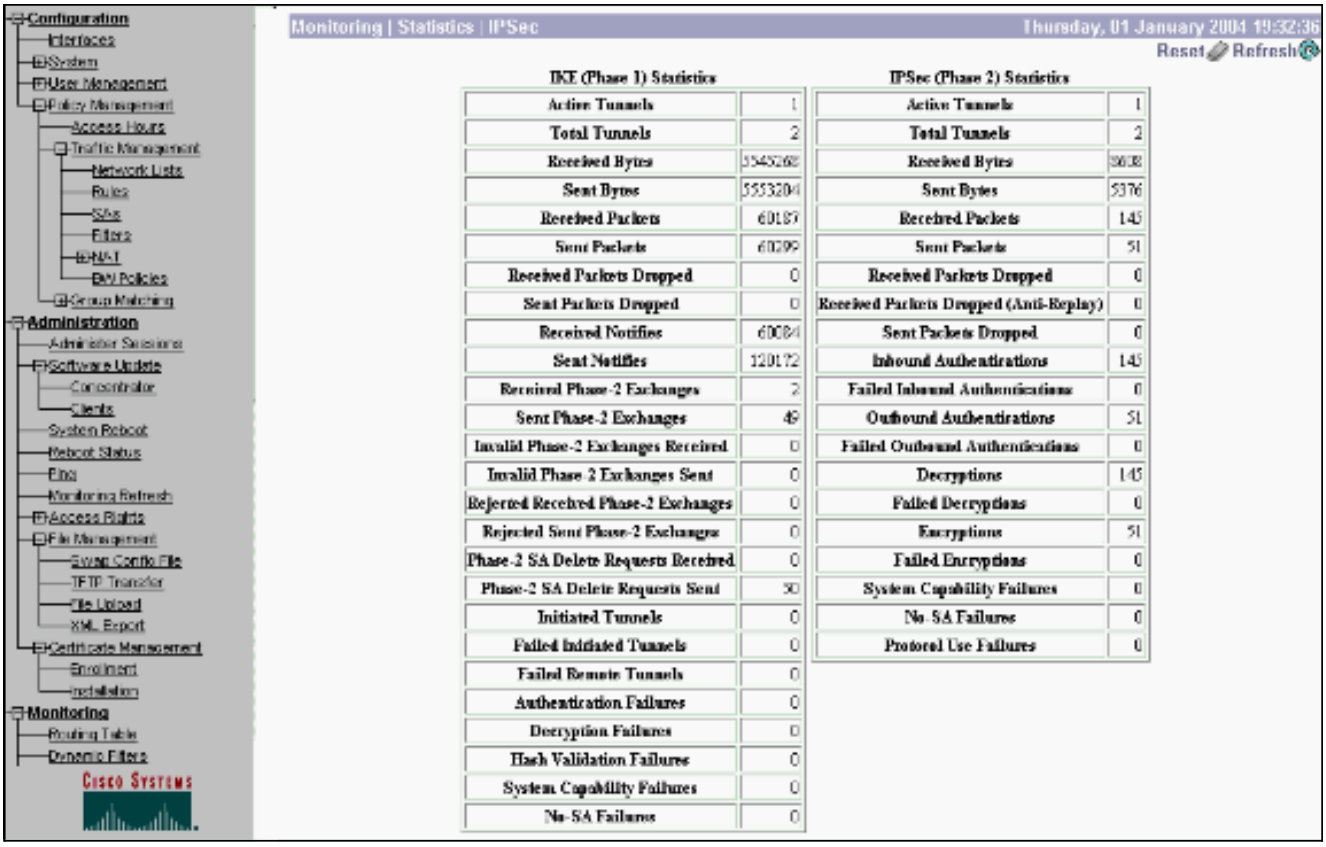
- **active del show crypto engine connections** — Visualiza las conexiones de sesión encriptada activas actuales para todos los motores de criptografía. Cada ID de conexión es único. El número de paquetes se cifren y se desencripten que se visualiza en las dos columnas más recientes.

```
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
```

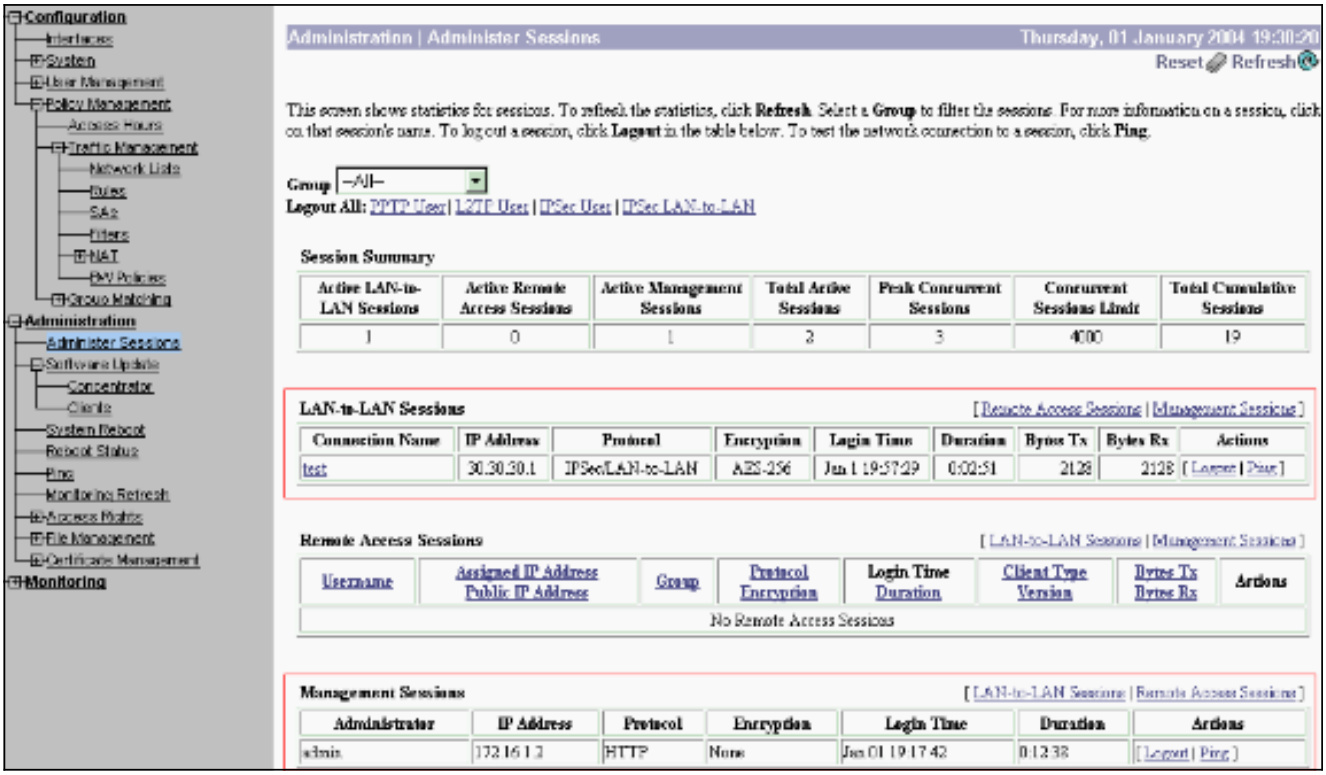
Verifique la configuración del concentrador VPN

Complete estos pasos para verificar la configuración del concentrador VPN.

1. Similar a los **comandos show crypto ipsec sa y show crypto isakmp sa** en el Routers, usted puede ver el IPSec y las estadísticas de IKE cuando usted selecciona el **Monitoring (Monitoreo) > Statistics (Estadísticas) > IPSec** en los concentradores VPN.



2. Similar al **comando show crypto engine connections active** en el Routers, usted puede utilizar la ventana de las Administración-sesiones en el concentrador VPN para ver los parámetros y las estadísticas para todas las conexiones de LAN a LAN o túneles del IPSec activo.



Troubleshooting

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 de Debug antes de usar un **comando debug**.

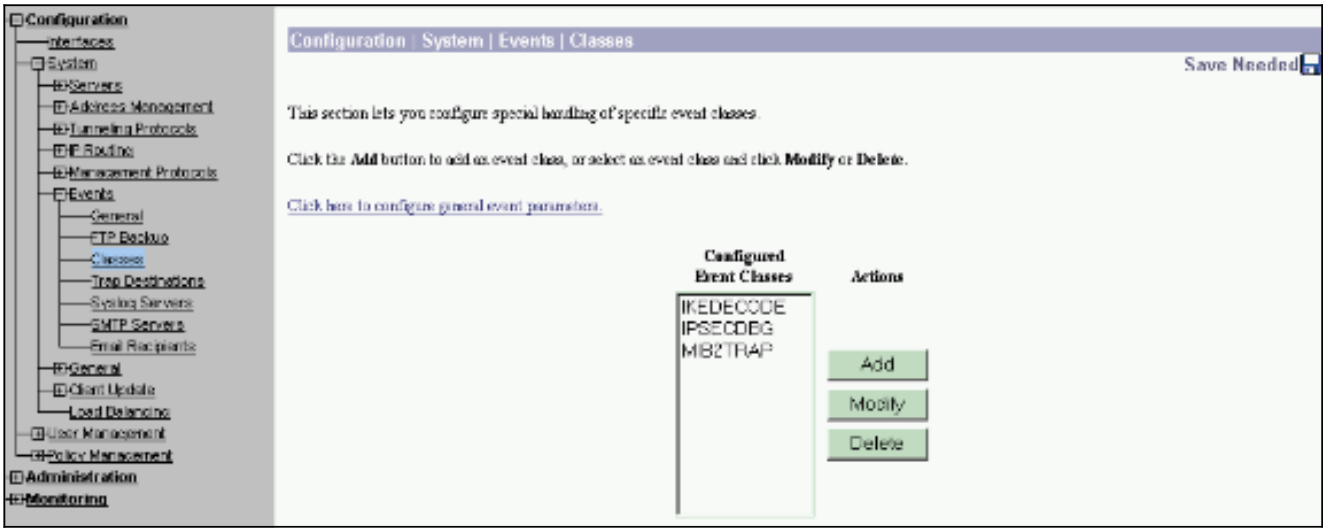
- debug crypto engine - Muestra el tráfico cifrado. El motor de criptografía es el mecanismo real que realiza el cifrado y el desciframiento. Un motor de criptografía puede ser un software o un acelerador por hardware.
- **isakmp del debug crypto** — Visualiza las negociaciones del Internet Security Association and Key Management Protocol (ISAKMP) de la fase 1. IKE.
- **IPSec del debug crypto** — Visualiza los IPSec Negotiations de la fase 2. IKE.

Refiera al Troubleshooting de IPSec - Entendiendo y con los comandos debug para más información detallada y salida de muestra.

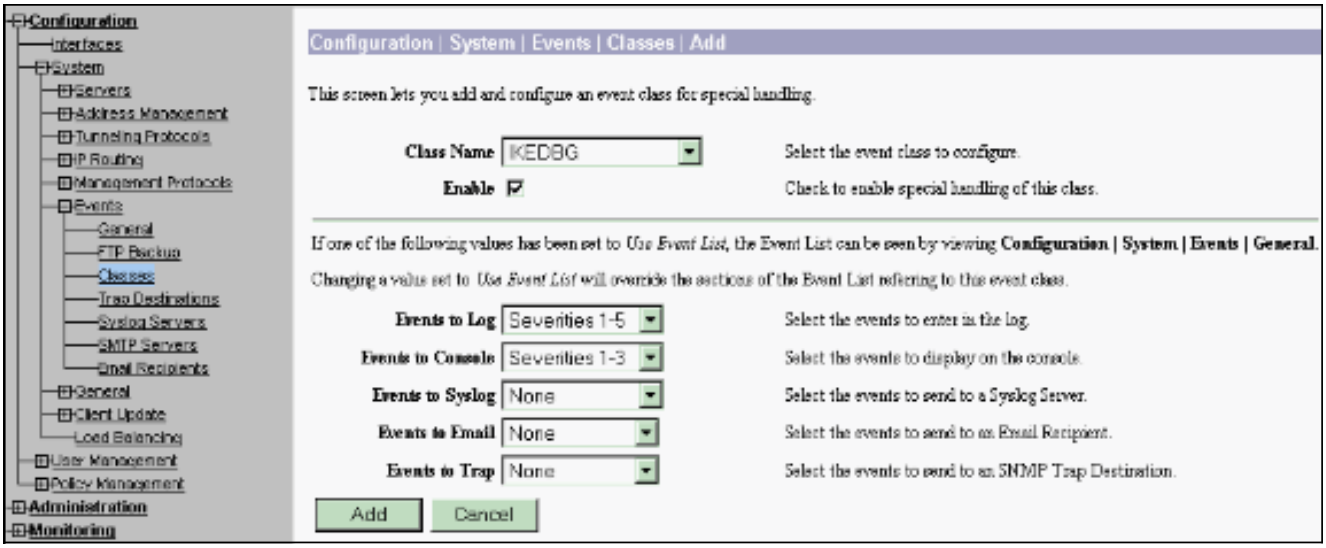
Resuelva problemas el concentrador VPN

Similar a los **comandos debug** en los routeres Cisco, usted puede configurar las clases de evento para ver todas las alarmas.

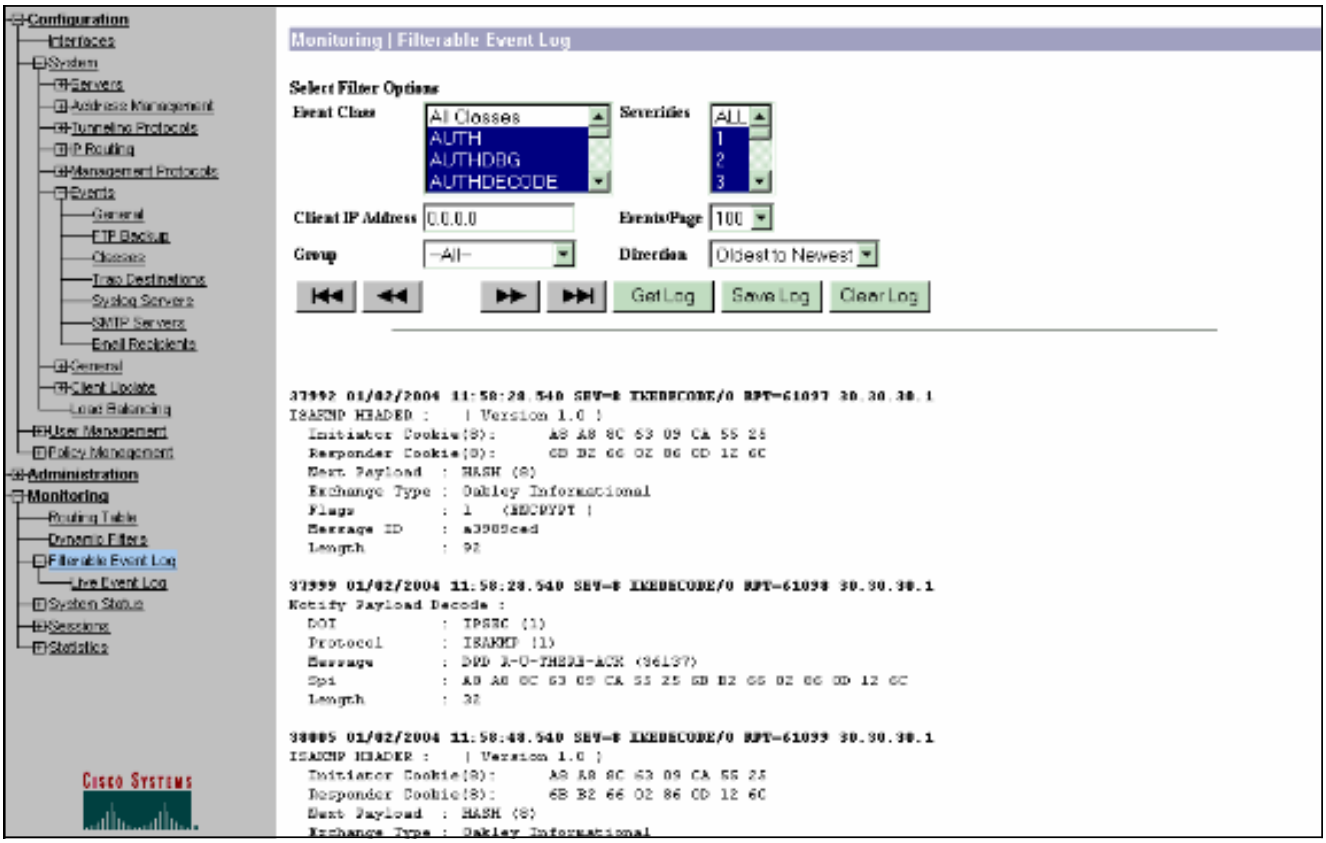
1. Seleccione el **Configuration (Configuración) > System (Sistema) > Event (Eventos) > Classes (Clases) > Add (Agregar)** para dar vuelta encendido a la registración de las clases de evento.Estas clases están disponibles para el IPSec:IKEIKEDBGIKEDECODEIPSECIPSECDBGIPSECDECODE



2. Mientras que agrega, usted puede también seleccionar el nivel de gravedad para cada clase, sobre la base del nivel de gravedad que la alarma está enviada.Las alarmas se pueden manejar por uno de estos métodos:Por el registroVisualizado en la consolaEnviado al servidor Syslog UNIXEnviado como correo electrónicoEnviado como desvío a un servidor del Simple Network Management Protocol
(SNMP)



3. Seleccione el **Monitoring (Monitoreo) > Filterable Event Log (Registro de eventos filtrables)** para monitorear las alarmas habilitadas.



Información Relacionada

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