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 de comunicación son la red privada 192.168.10.x dentro del Cisco Secure PIX Firewall y la red privada 10.32.x.x dentro del Firewall de la última generación del punto de verificación™ (NG).

prerrequisitos

Requisitos

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- Trafique por dentro del PIX y del interior que el punto de verificación™ NG a Internet (representado aquí por las redes 172.18.124.x) debe fluir antes de que usted comience esta configuración.
- Los usuarios deben ser familiares con el IPSec Negotiation. Este proceso se puede analizar en cinco pasos, incluyendo dos fases del Internet Key Exchange (IKE).Un túnel IPsec es iniciado por el tráfico interesante. El tráfico se considera interesante cuando viaja entre los peeres IPSec.En la fase 1 IKE, los peeres IPSec negocian la directiva establecida de la asociación de seguridad IKE (SA). Una vez que se autentican los pares, se crea un túnel seguro por medio de la Asociación de Seguridad en Internet y del Protocolo de administración de clave (ISAKMP).En la fase 2 IKE, los peeres IPSec utilizan el túnel seguro y autenticado para negociar IPSec SA transforman. La negociación de la política compartida determina cómo se establece el túnel IPsec.Se crea el túnel IPsec y los datos se transfieren entre los

peeres IPSec basados en los parámetros de IPSec configurados en el IPSec transforman los conjuntos.El túnel IPsec termina cuando se borra el SA de IPSec o cuando expira su curso de la vida.

Componentes Utilizados

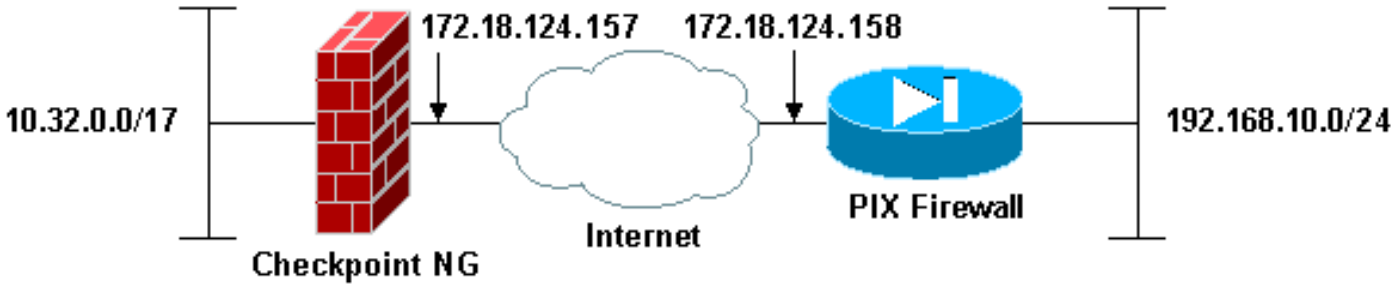
La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Versión de software PIX 6.2.1
- Firewall del punto de verificación™ NG

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.

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Convenciones

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

Configure el PIX

Esta sección le presenta con la información para configurar las características descritas en este documento.

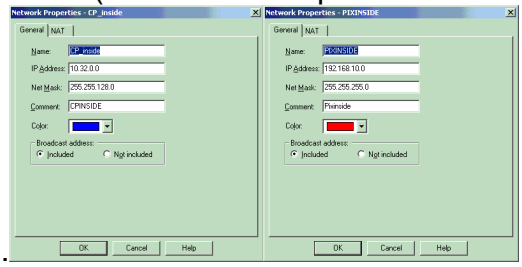
Configuración de PIX

```
PIX Version 6.2(1)nameif ethernet0 outside
security0nameif ethernet1 inside security100enable
password 8Ry2YjIyt7RRXU24 encryptedpasswd
2KFQnbNIdI.2KYOU encryptedhostname PIXRTPVPNdomain-name
cisco.comfixup protocol ftp 21fixup protocol http
80fixup protocol h323 h225 1720fixup protocol h323 ras
1718-1719fixup protocol ils 389fixup protocol rsh
514fixup protocol rtsp 554fixup protocol smtp 25fixup
protocol sqlnet 1521fixup protocol sip 5060fixup
protocol skinny 2000names!--- Interesting traffic to be
encrypted to the Checkpoint? NG.access-list 101 permit
ip 192.168.10.0 255.255.255.0 10.32.0.0 255.255.128.0!--
```

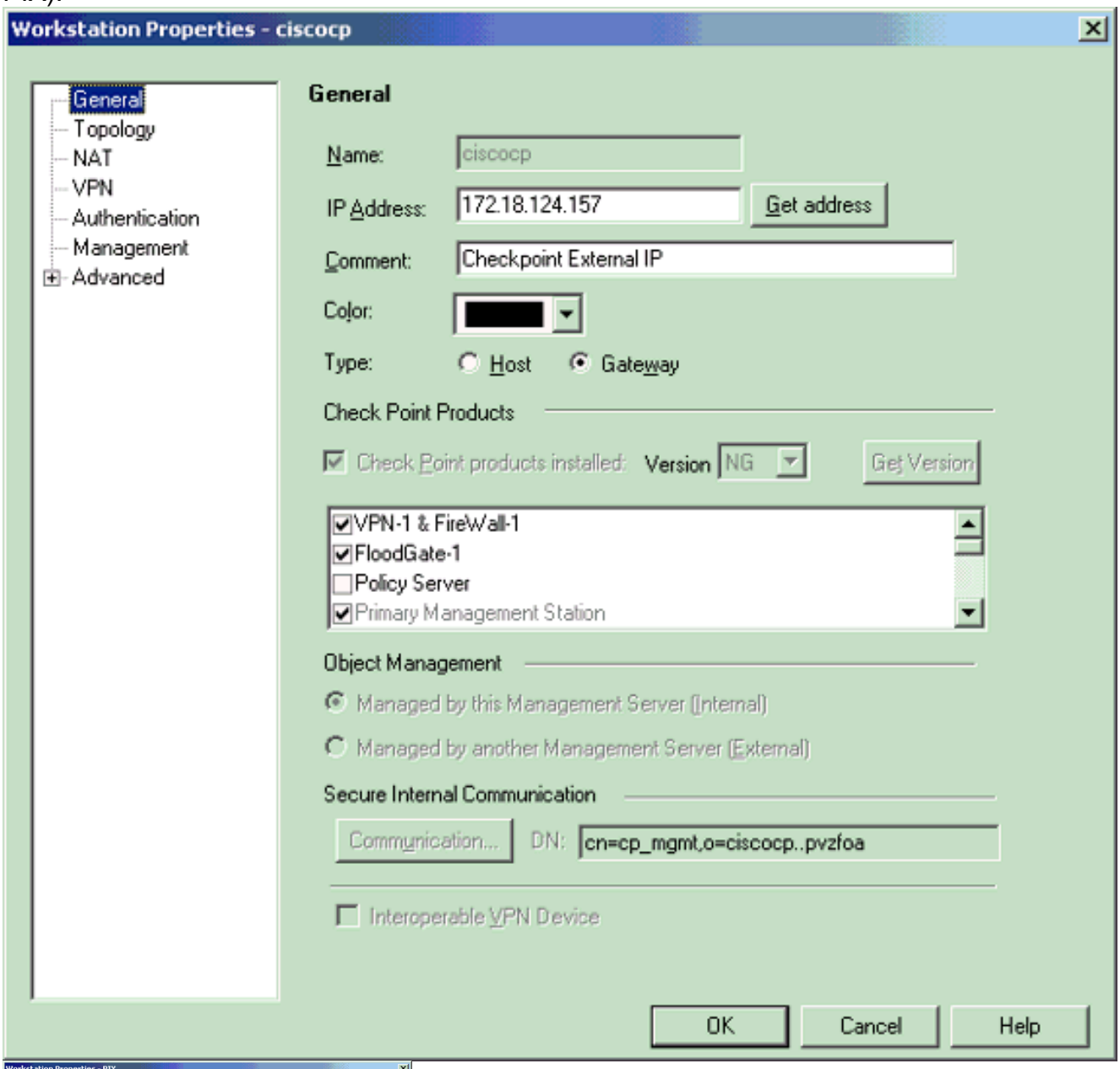
```
- Do not perform Network Address Translation (NAT) on
traffic to the Checkpoint? NG.access-list nonat permit
ip 192.168.10.0 255.255.255.0 10.32.0.0
255.255.128.0pager lines 24interface ethernet0
10basetinterface ethernet1 10fullmtu outside 1500mtu
inside 1500ip address outside 172.18.124.158
255.255.255.0ip address inside 192.168.10.1
255.255.255.0ip audit info action alarmip audit attack
action alarmpdm history enablearp timeout 14400global
(outside) 1 interface!--- Do not perform NAT on traffic
to the Checkpoint? NG.nat (inside) 0 access-list
nonatnat (inside) 1 0.0.0.0 0.0.0.0 0 0route outside
0.0.0.0 0.0.0.0 172.18.124.1 1timeout xlate
3:00:00timeout conn 1:00:00 half-closed 0:10:00 udp
0:02:00 rpc 0:10:00    h323 0:05:00 sip 0:30:00
sip_media 0:02:00timeout uauth 0:05:00 absoluteaaa-
server TACACS+ protocol tacacs+aaa-server RADIUS
protocol radiusaaa-server LOCAL protocol localno snmp-
server locationno snmp-server contactsnmp-server
community publicno snmp-server enable trapsfloodguard
enable!--- Permit all inbound IPsec authenticated cipher
sessions.sysopt connection permit-ipsecno sysopt route
dnat!--- Defines IPsec encryption and authentication
algorithms.crypto ipsec transform-set rtptac esp-3des
esp-md5-hmac!--- Defines crypto map.crypto map rtprules
10 ipsec-isakmpcrypto map rtprules 10 match address
101crypto map rtprules 10 set peer 172.18.124.157crypto
map rtprules 10 set transform-set rtptac!--- Apply
crypto map on the outside interface.crypto map rtprules
interface outsideisakmp enable outside!--- Defines pre-
shared secret used for IKE authentication.isakmp key
******** address 172.18.124.157 netmask
255.255.255.255!--- Defines ISAKMP policy.isakmp policy
1 authentication pre-shareisakmp policy 1 encryption
3desisakmp policy 1 hash md5isakmp policy 1 group
2isakmp policy 1 lifetime 86400telnet timeout 5ssh
timeout 5terminal width
80Cryptochecksum:089b038c8e0dbc38d8ce5ca72cf920a5: end
```

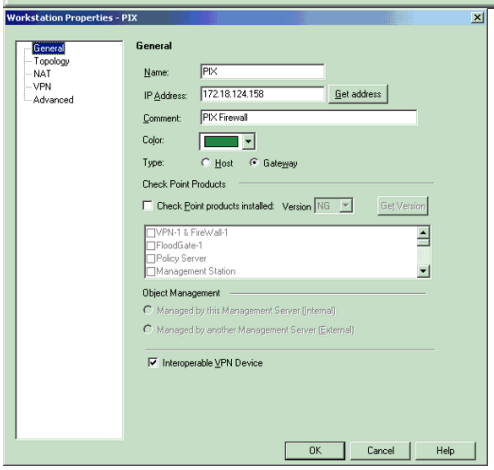
Configure NG de punto de control

Los objetos de red y las reglas se definen en el punto de verificación™ NG para componer la directiva que pertenece a la configuración VPN que se configurará. Esta directiva entonces está instalada usando el editor de políticas del punto de verificación™ NG para completar el lado del punto de verificación™ NG de la configuración.

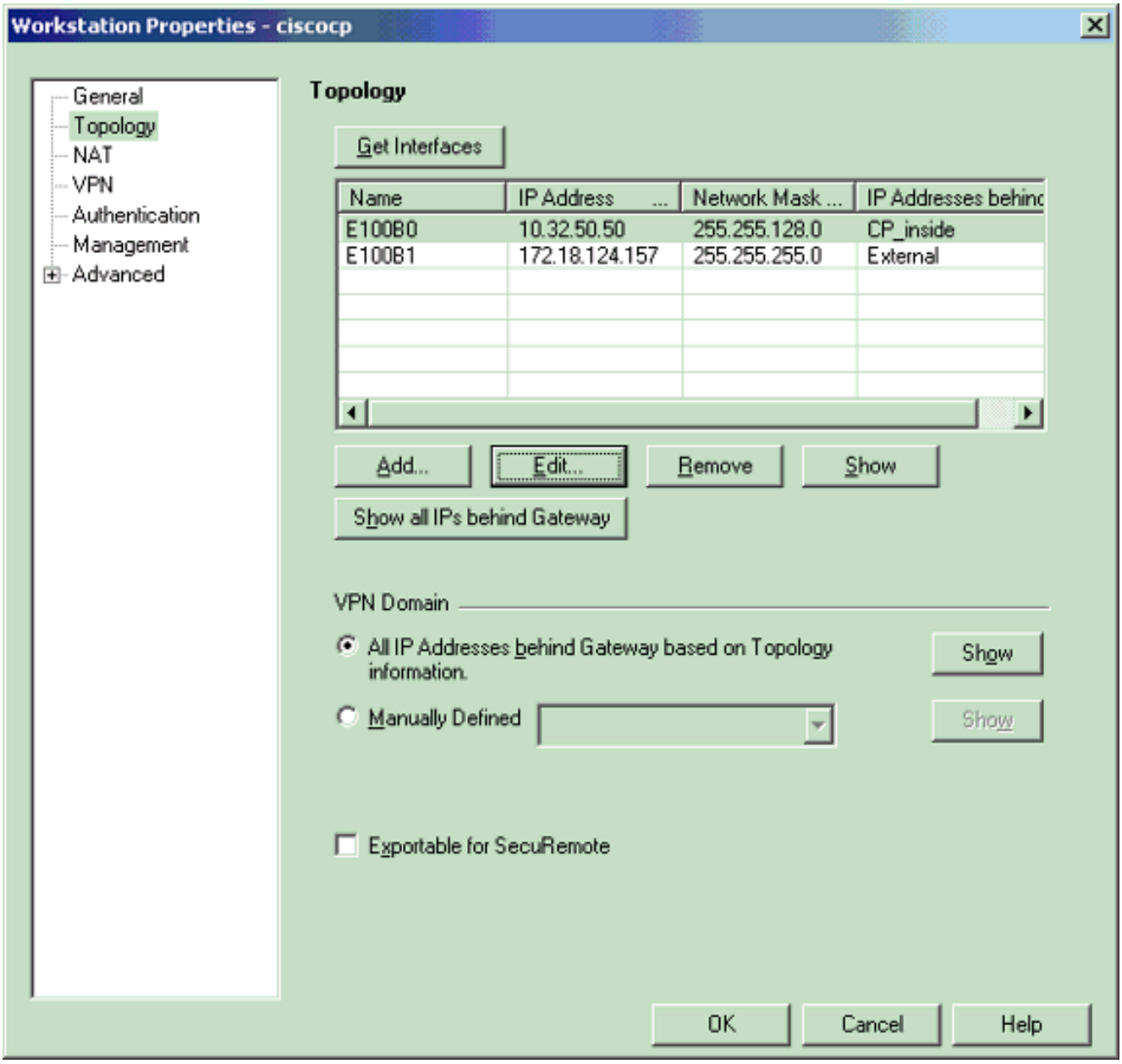
1. Cree los dos objetos de red para la red de punto de control y el firewall network PIX que cifran el tráfico interesante.Para hacer esto, seleccione **Manage > Network Objects**, después seleccione **New > Network**. Ingrese la información de red apropiada, después haga clic la **AUTORIZACIÓN**.Estos ejemplos muestran una configuración de los objetos de red llamados CP_Inside (red interna del punto de verificación™ NG) y PIXINSIDE (red interna del PIX). 

2. Cree los objetos de estación de trabajo para el punto de verificación™ NG y PIX. Para hacer esto, seleccione **Manage > Network Objects > New > Workstation**.Observe que usted puede utilizar el objeto de estación de trabajo del punto de verificación™ NG creado durante la configuración del punto de control inicial™ NG. Seleccione las opciones para fijar el puesto de trabajo como el gateway y dispositivo VPN interoperable, y después haga clic la **AUTORIZACIÓN**.Estos ejemplos muestran una configuración de los objetos llamados ciscocp (CheckpointTM NG) y PIX (firewall
PIX).

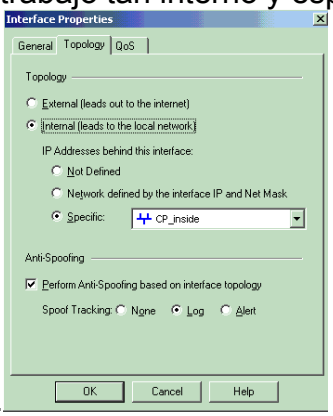




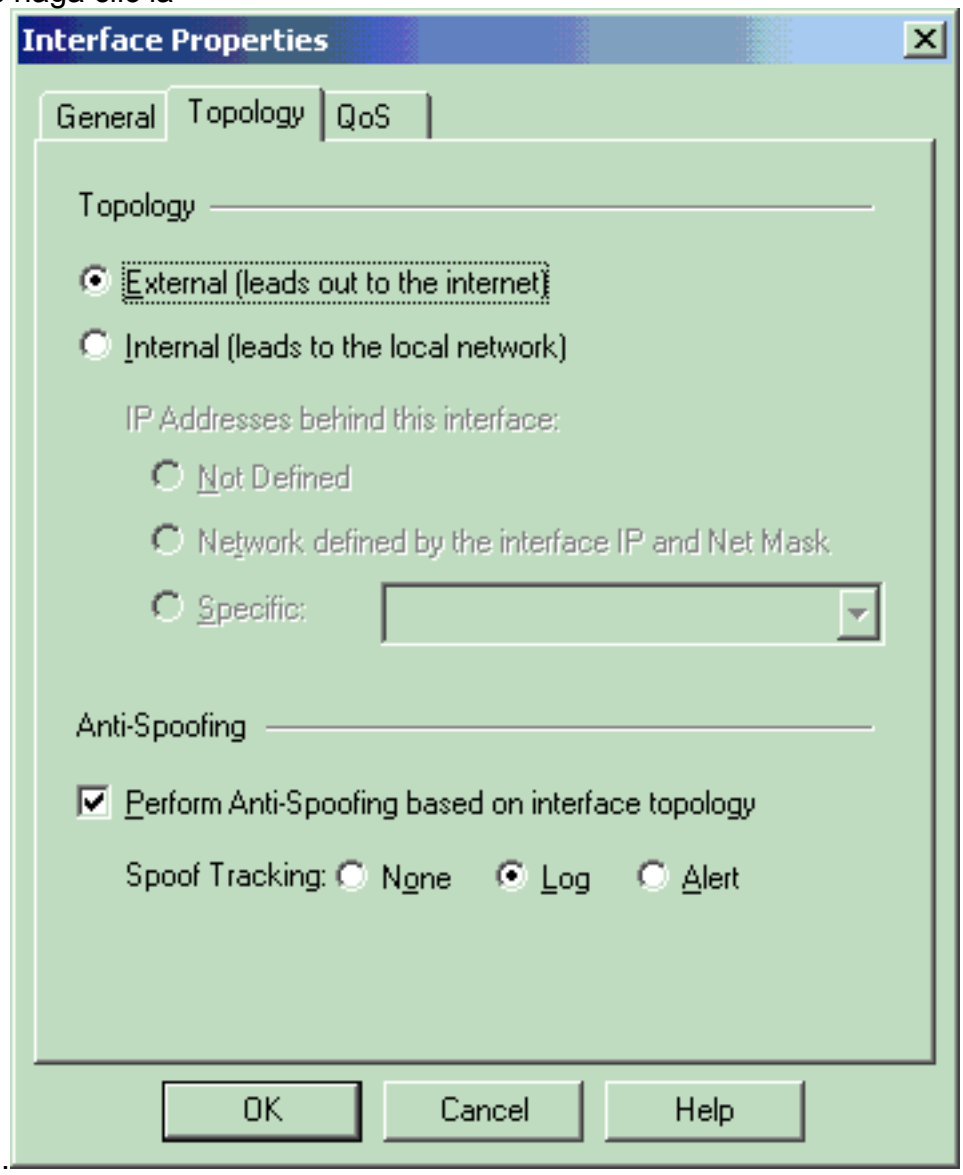
3. Seleccione **Manage > Network Objects > Edit** para abrir la ventana de Propiedades de la estación de trabajo para el puesto de trabajo del punto de verificación™ NG (ciscocp en este ejemplo).Seleccione la **topología de las** opciones en el lado izquierdo de la ventana, después seleccione la red para ser cifrado. El tecleo **edita** para fijar las propiedades de la interfaz.



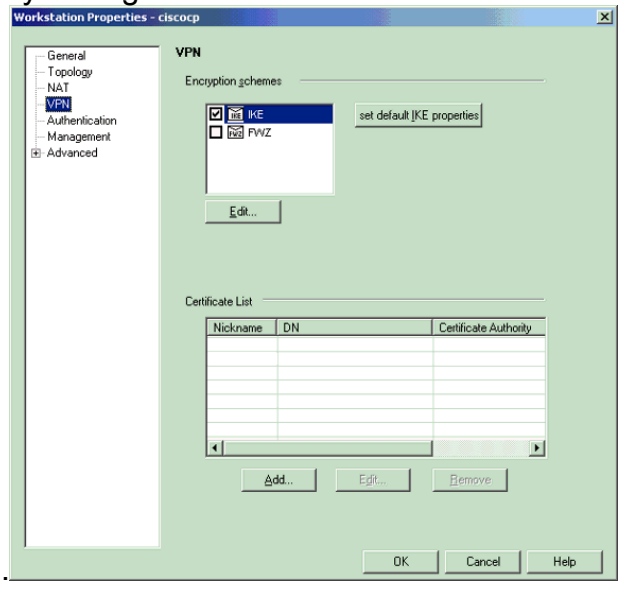
4. Seleccione la opción para señalar el puesto de trabajo como interno, después especifique la dirección IP apropiada. Haga clic en OK.En esta configuración, el CP_inside es la red interna del punto de verificación™ NG. Las selecciones de topología mostradas aquí señalan el puesto de trabajo tan interno y especifican el direccionamiento como el CP_inside.



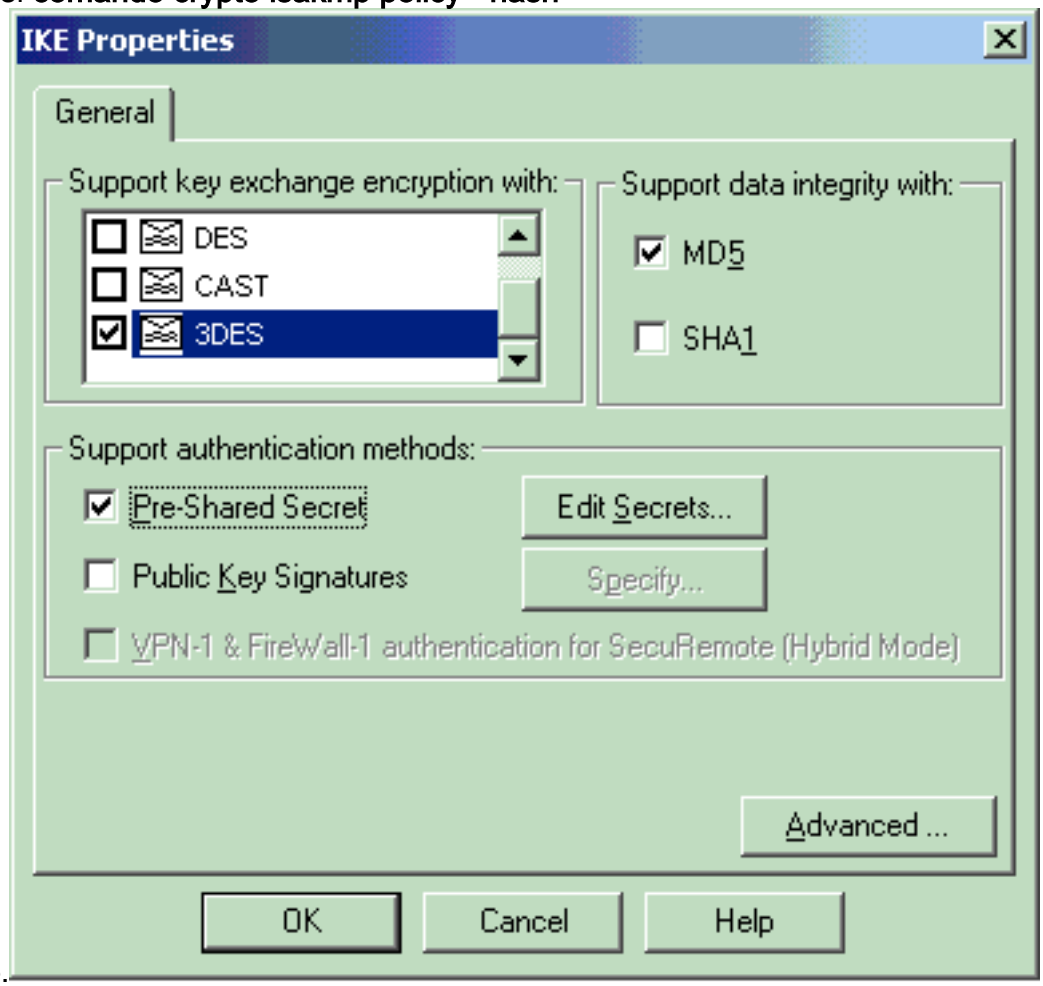
5. De la ventana de Propiedades de la estación de trabajo, seleccione la interfaz exterior en el punto de verificación™ NG que eso lleva hacia fuera a Internet, después haga clic **editan** para fijar las propiedades de la interfaz. Seleccione la opción para señalar la topología como externo, después haga clic la **AUTORIZACIÓN**.



6. De la ventana de Propiedades de la estación de trabajo en el punto de verificación™ NG, el **VPN** selecto de las opciones en el lado izquierdo de la ventana, entonces selecciona los parámetros IKE para encripción y los algoritmos de autenticación. El tecleo **edita** para configurar las propiedades IKE.

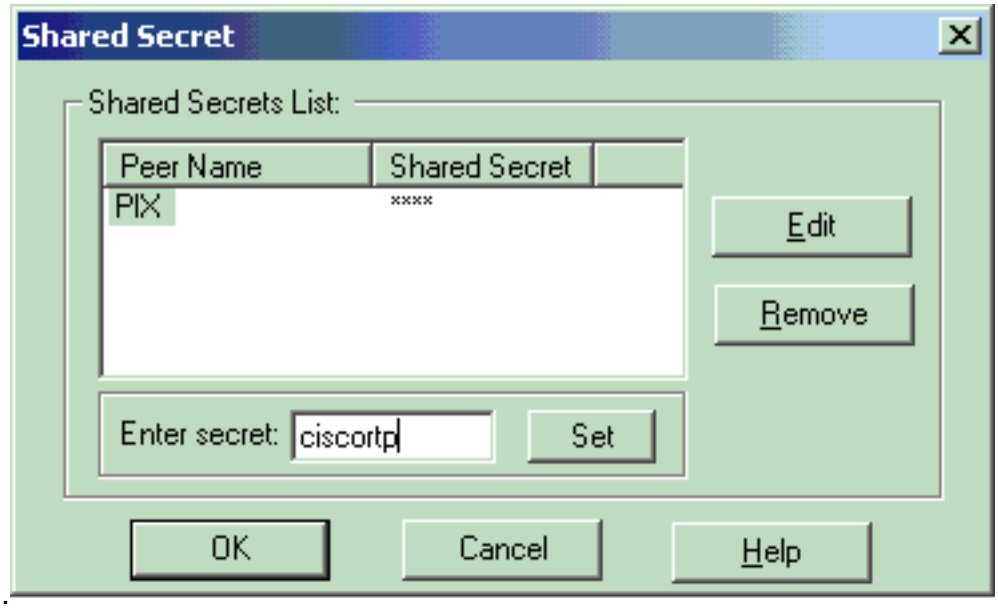


7. Configure las propiedades IKE:Seleccione la opción para el cifrado **3DES** de modo que las propiedades IKE sean compatibles con el **comando isakmp policy - encryption 3des**.Seleccione la opción para el **MD5** de modo que las propiedades IKE sean compatibles con el **comando crypto isakmp policy - hash**



md5.

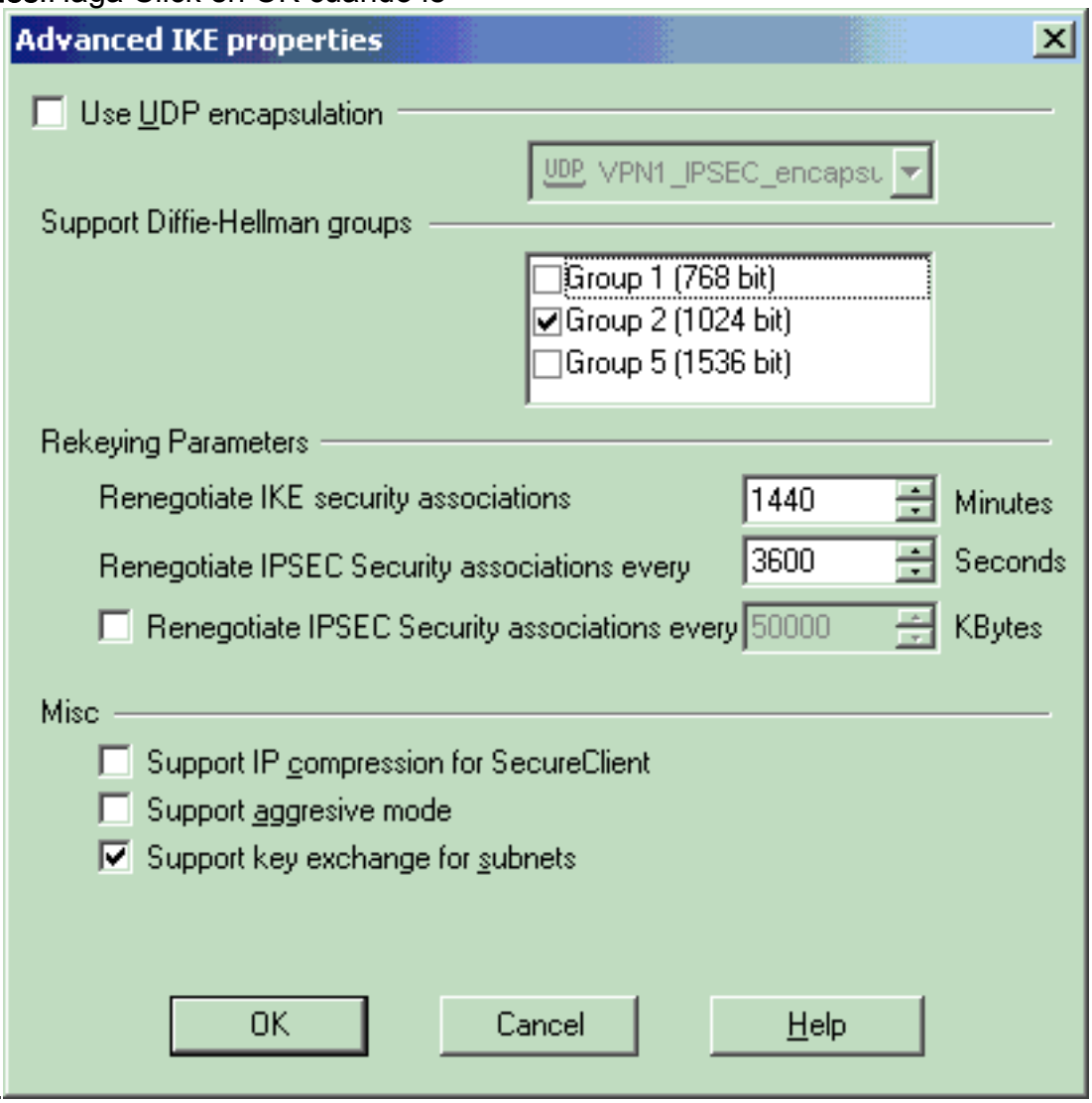
8. Seleccione la opción de autenticación para los **Secretos previamente compartidos**, después haga clic **editan los secretos** para fijar la clave previamente compartida como compatible con el *netmask del* **netmask de los address address de la** *clave de la* **clave del isakmp del** comando pix. El tecleo **edita** para ingresar su clave como se muestra aquí y para hacer clic el **conjunto,**



AUTORIZACIÓN.

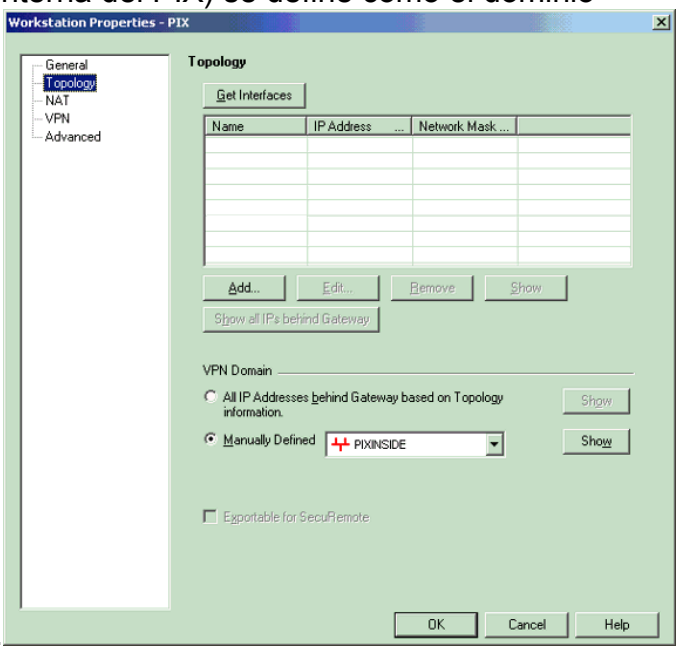
9. De la ventana de las propiedades IKE, haga clic **avanzado…** y cambie estas

configuraciones:No reelija como candidato la opción para **Support aggressive mode (Admitir modo agresivo)**.Seleccione la opción para el **intercambio de claves del soporte para las subredes**.Haga Click en OK cuando le



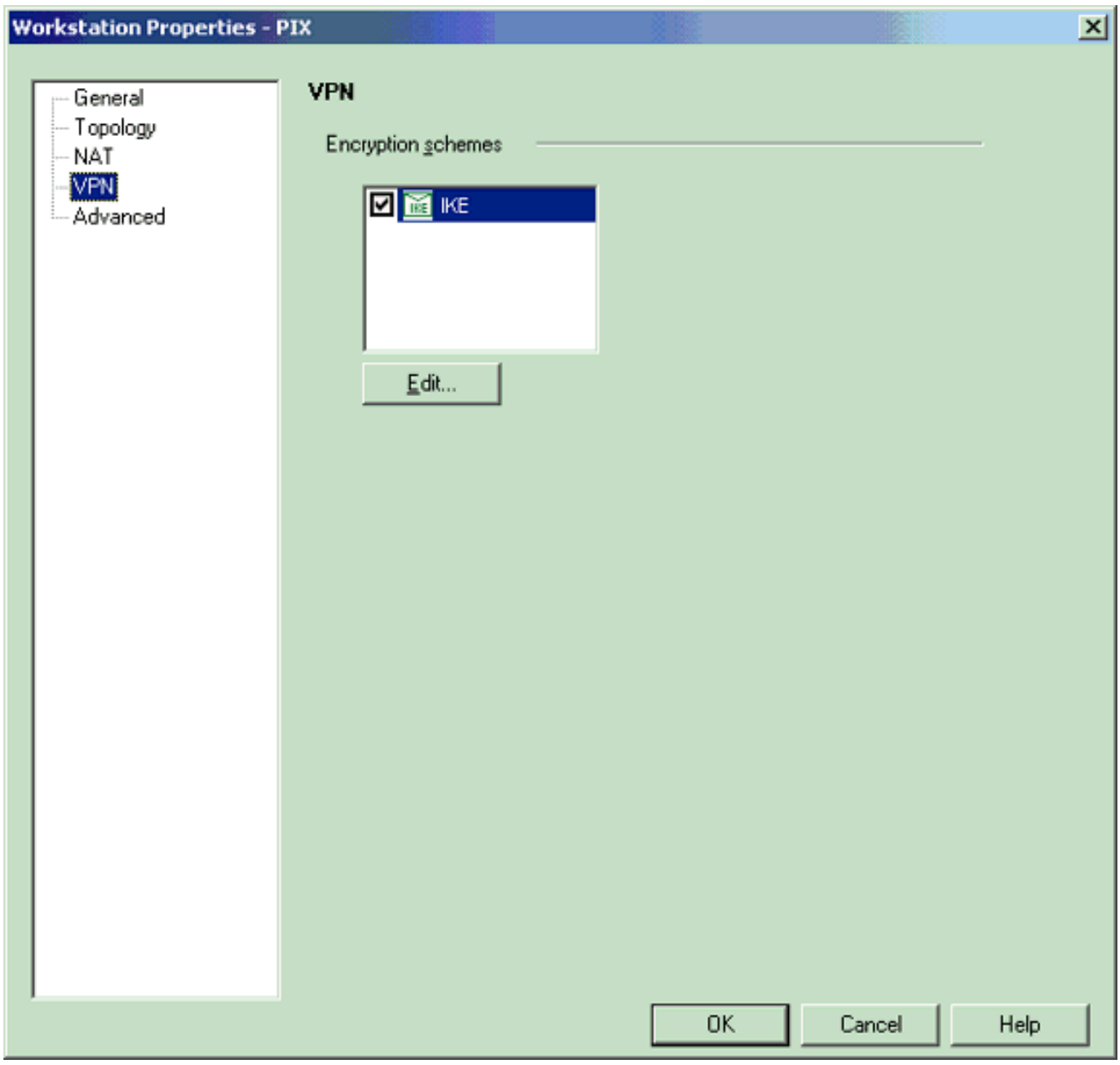
hacen.

10. Seleccione **Manage > Network Objects > Edit** para abrir la ventana de Propiedades de la estación de trabajo para el PIX. **Topología** selecta de las opciones en el lado izquierdo de la ventana para definir manualmente el dominio VPN.En esta configuración, el PIXINSIDE (red interna del PIX) se define como el dominio

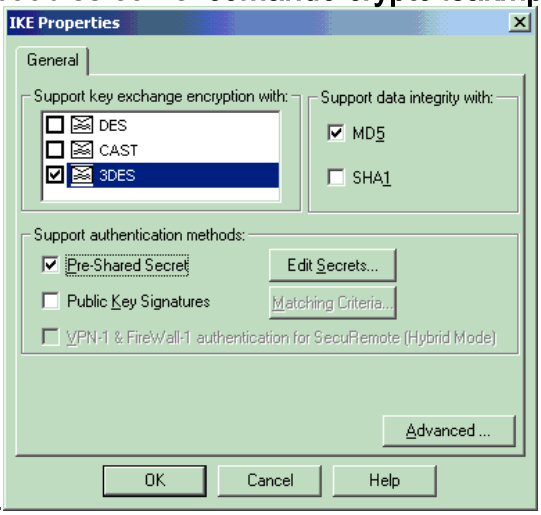


VPN.

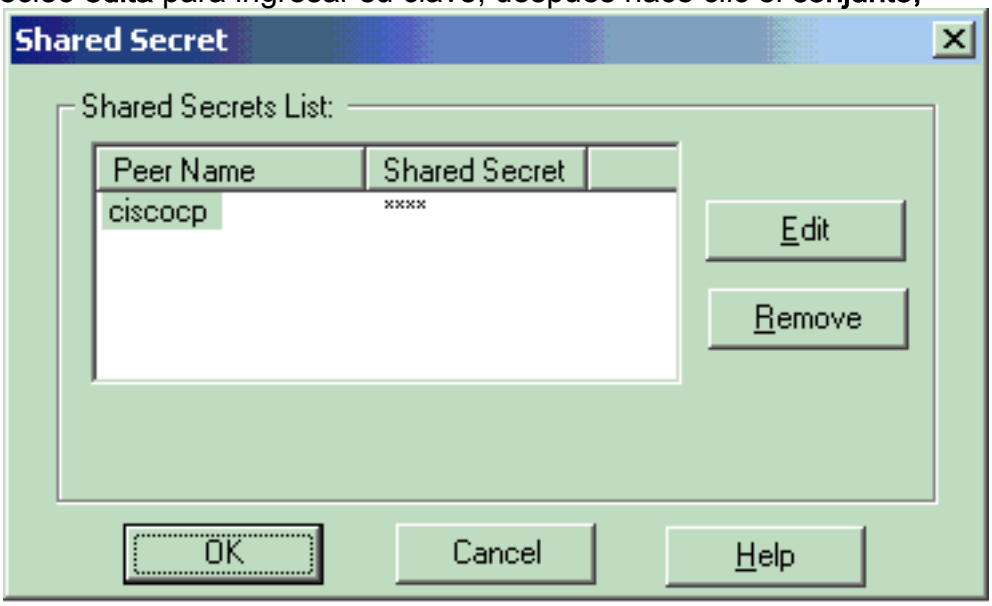
11. **El VPN** selecto de las opciones en el lado izquierdo de la ventana, entonces selecciona el IKE como el esquema de encripción. El tecleo **edita** para configurar las propiedades IKE.



12. Configure las propiedades IKE como se muestra aquí:Seleccione la opción para el cifrado **3DES** de modo que las propiedades IKE sean compatibles con el **comando isakmp policy - encryption 3des**.Seleccione la opción para el **MD5** de modo que las propiedades IKE sean compatibles con el **comando crypto isakmp policy - hash md5**.

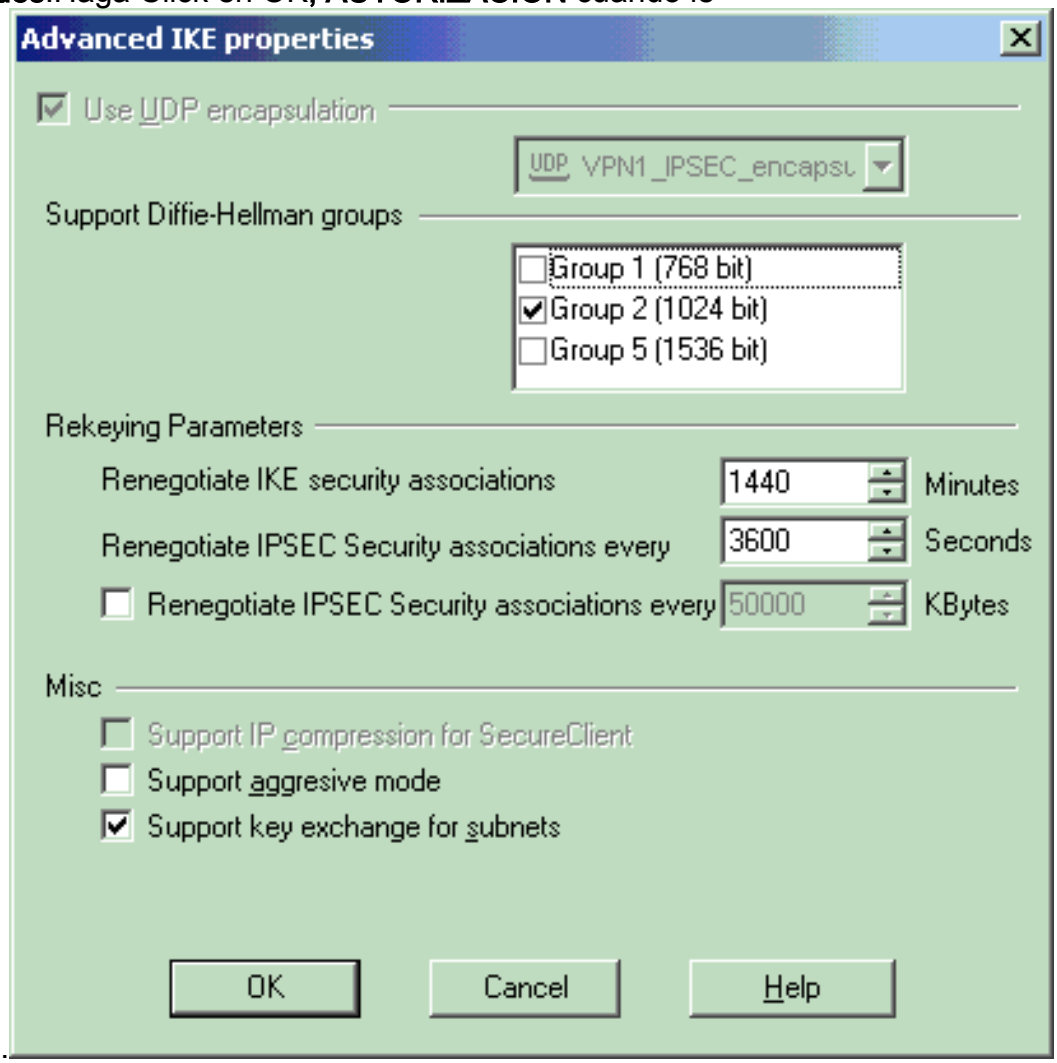


13. Seleccione la opción de autenticación para los **Secretos previamente compartidos**, después haga clic **editan los secretos** para fijar la clave previamente compartida como compatible con el *netmask del* **netmask de los address address de la** *clave de la* **clave del isakmp del** comando pix. El tecleo **edita** para ingresar su clave, después hace clic el **conjunto,**



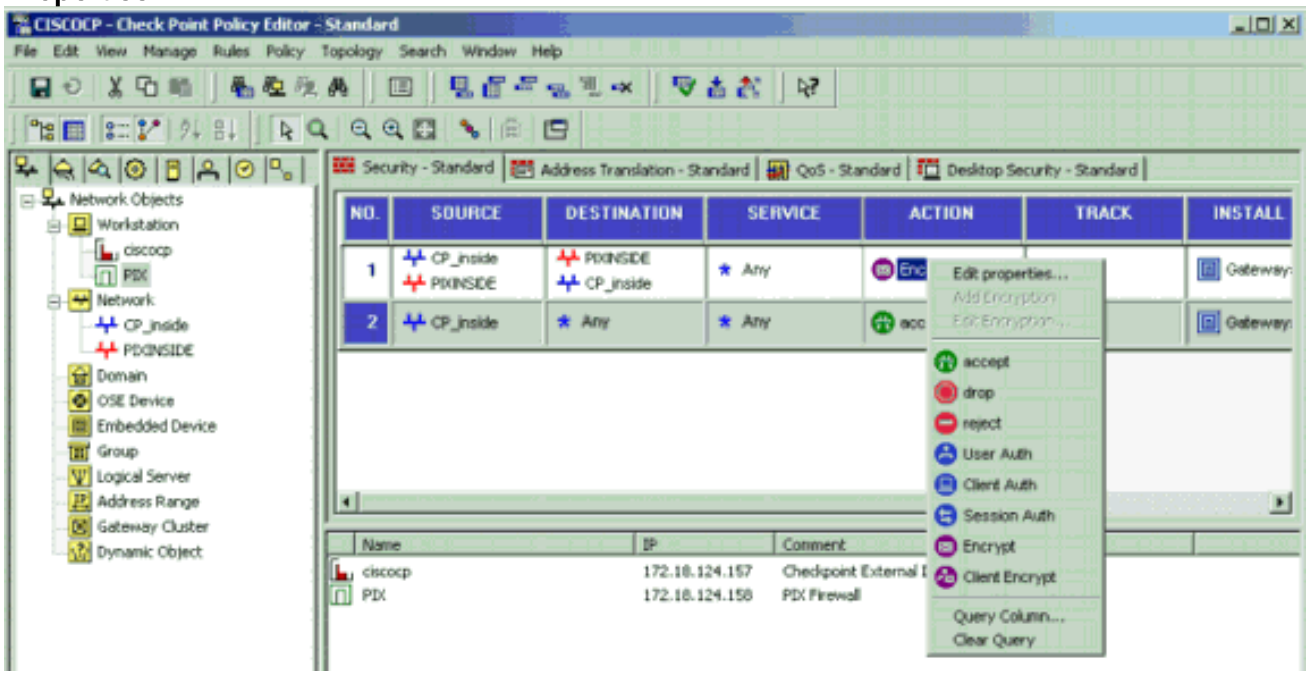
AUTORIZACIÓN.

14. De la ventana de las propiedades IKE, haga clic **avanzado…** y cambie estas configuraciones.Seleccione al grupo Diffie-Hellman apropiado para las propiedades IKE.No reelija como candidato la opción para **Support aggressive mode (Admitir modo agresivo)**.Seleccione la opción para el **intercambio de claves del soporte para las subredes**.Haga Click en OK**, AUTORIZACIÓN** cuando le

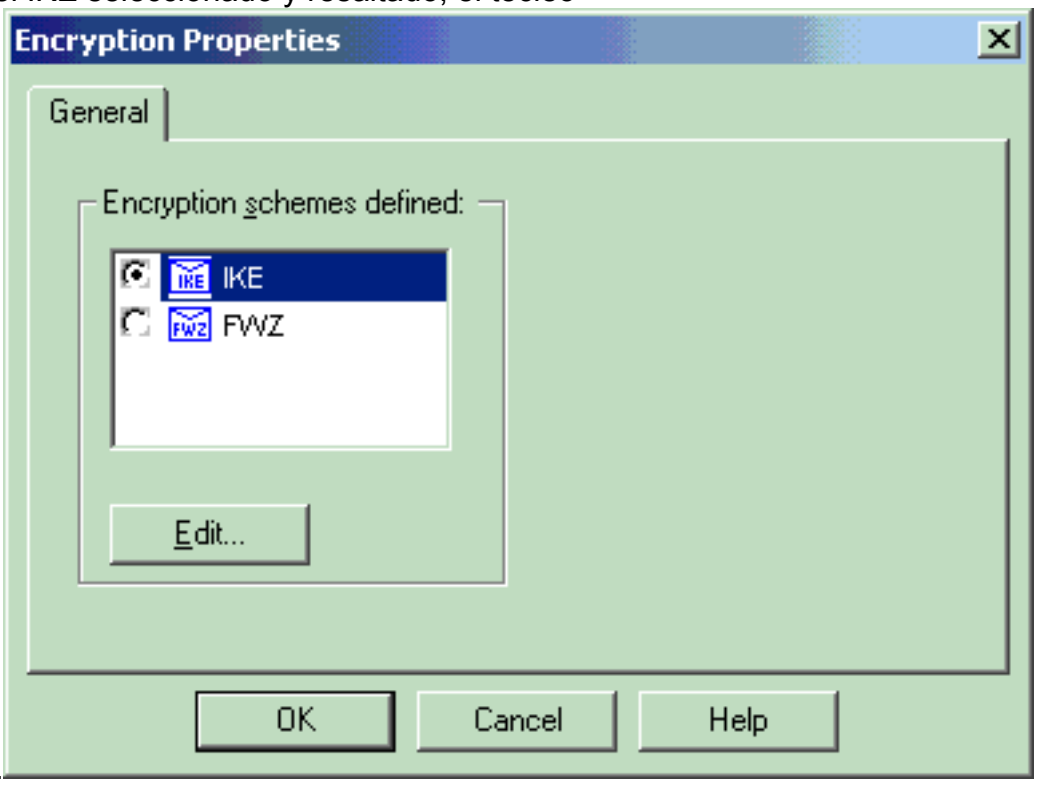


hacen.

15. Seleccione el **Rules (Reglas) > Add Rules (Agregar reglas) > Top (Superiores)** para configurar las reglas de encripción para la directiva.En la ventana de editor de políticas, inserte una regla con una fuente del CP_inside (red interna del punto de verificación ™ NG) y de PIXINSIDE (red interna del PIX) en ambas las columnas de origen y destino. Los valores establecidos para el **servicio = ningunos**, **acción = cifran**, y **pista = registro**. Cuando usted ha agregado la sección de la acción del cifrar de la regla, haga clic con el botón derecho del ratón la **acción** y selecciónela **Edit Properties**.



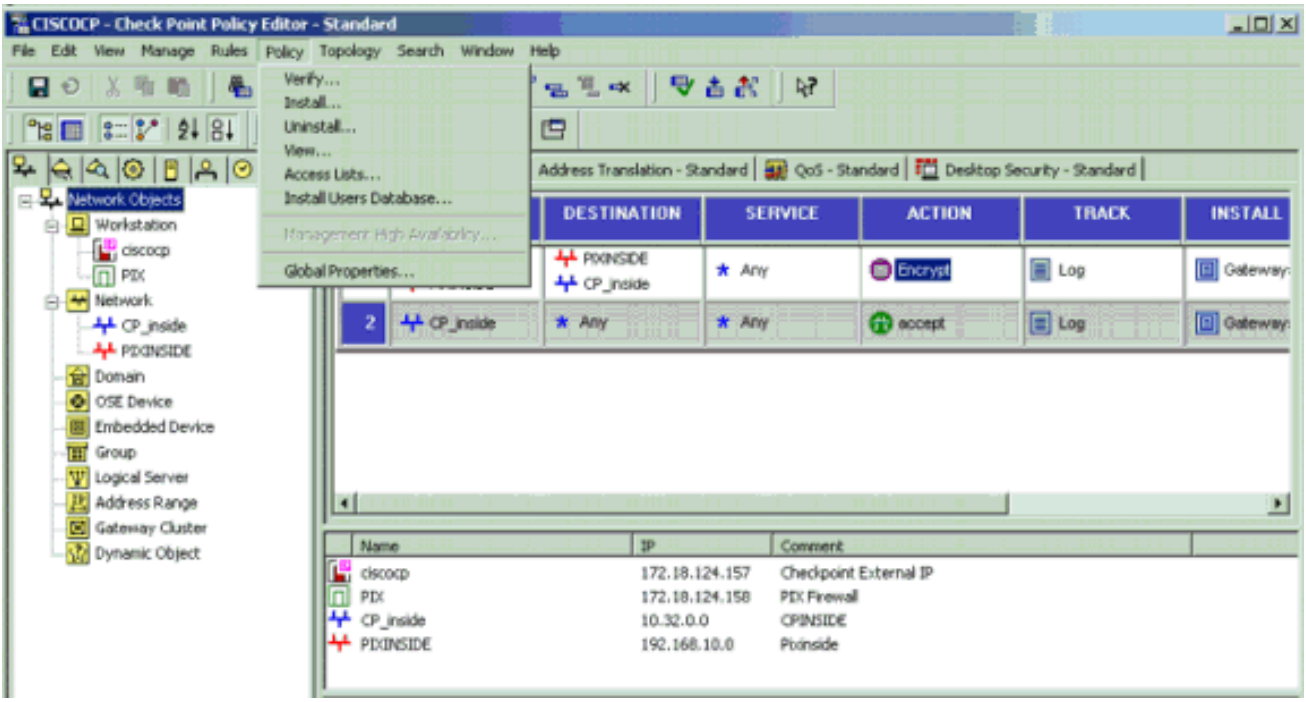
16. Con el IKE seleccionado y resaltado, el tecleo **edita**.



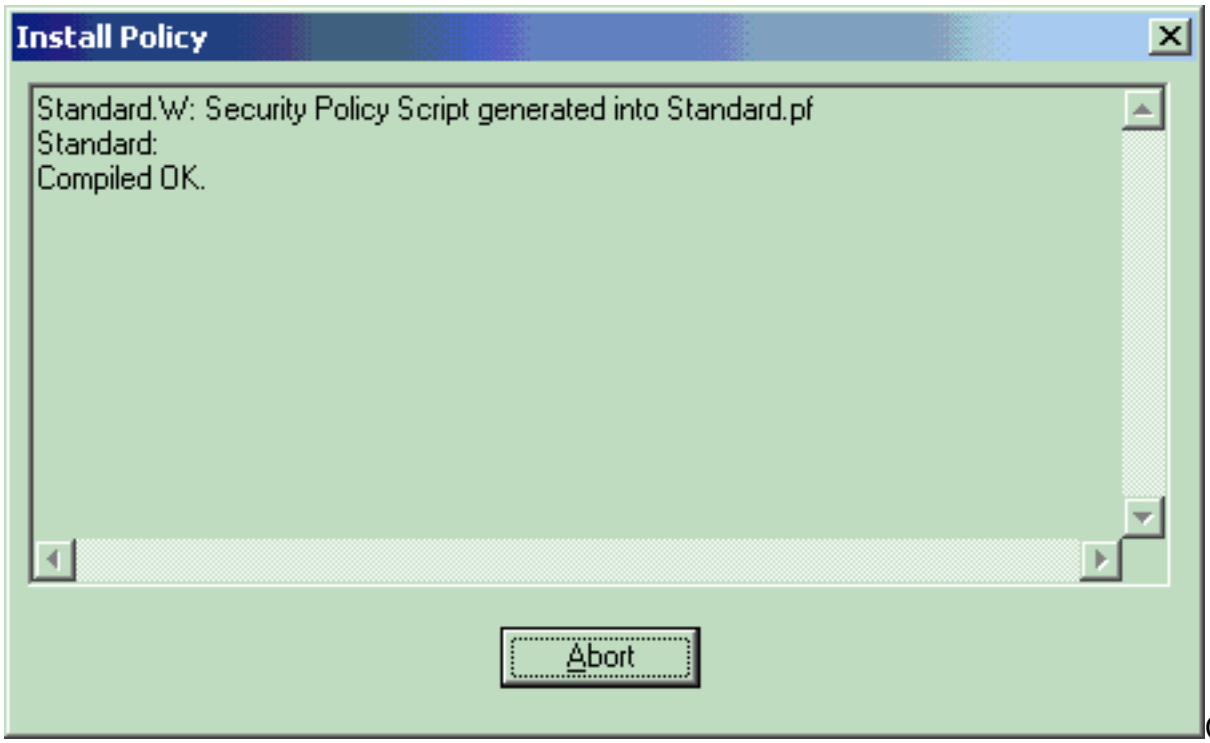
17. En la ventana de las propiedades IKE, cambie las propiedades para estar de acuerdo con el IPSec de PIX transforma en el **comando crypto ipsec transform-set rtptac esp-3des esp-md5-hmac**.Fije la opción de la transformación al **Encryption + Data Integrity (ESP)**, fije el algoritmo de encripción al **3DES**, fije la integridad de los datos al **MD5**, y fije el gateway de peer permitido para hacer juego el gateway PIX externo (llamado PIX aquí). Haga clic en

OK.

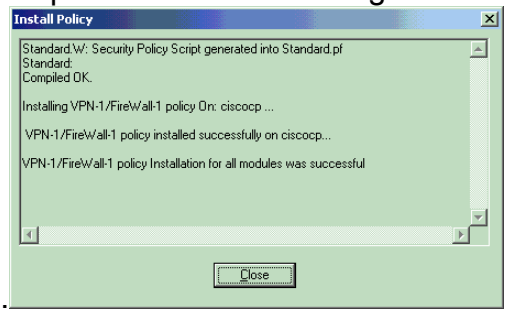
18. Después de que usted configure el punto de verificación™ NG, salve la directiva y la **directiva** selecta **> instala** para habilitarla.



La ventana de instalación visualiza las notas de progreso mientras que se compila la directiva.



Cuando la ventana de instalación indica que la instalación de regulación es completa. Tecleo **cerca del** final el procedimiento.



Verificación

Verificar la configuración de PIX

Use esta sección para confirmar que su configuración funciona correctamente.

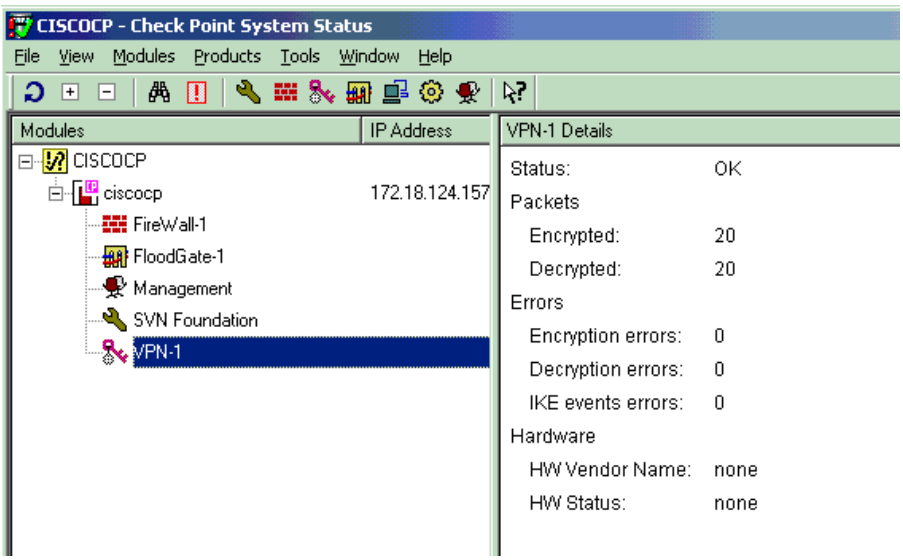
La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

Inicie un ping a partir de la una de las redes privadas a la otra red privada para probar la comunicación entre las dos redes privadas. En esta configuración, un ping fue enviado del lado PIX (192.168.10.2) a la red interna del punto de verificación™ NG (10.32.50.51).

- ¿**muestre isakmp crypto sa**? Visualiza todo el IKE actual SA en un par.**show crypto isakmp sa**Total : 1Embryonic : 0 dst src state pending created 172.18.124.157 172.18.124.158 **QM_IDLE** 0 1
- ¿**muestre IPSec crypto sa**? Visualiza las configuraciones usadas por los SA actuales.PIX501A#**show cry ipsec sa**interface: **outside** Crypto map tag: **rtprules**, local addr. 172.18.124.158 local ident (addr/mask/prot/port): (192.168.10.0/255.255.255.0/0/0) remote ident (addr/mask/prot/port): (10.32.0.0/255.255.128.0/0/0) current_peer: 172.18.124.157 PERMIT, flags={origin_is_acl,} **#pkts encaps: 19, #pkts encrypt: 19, #pkts digest 19 #pkts decaps: 19, #pkts decrypt: 19, #pkts verify 19** #pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0 #send errors 1, #recv errors 0 local crypto endpt.: **172.18.124.158**, remote crypto endpt.: 172.18.124.157 path mtu 1500, ipsec overhead 56, media mtu 1500 current outbound spi: 6b15a355 **inbound esp sas:** spi: 0xced238c7(3469883591) **transform: esp-3des esp-md5-hmac ,** in use settings ={**Tunnel**, } slot: 0, conn id: 3, **crypto map: rtprules** sa timing: remaining key lifetime (k/sec): (4607998/27019) IV size: 8 bytes replay detection support: Y inbound ah sas: inbound pcp sas: **outbound esp sas:** spi: 0x6b15a355(1796580181) **transform: esp-3des esp-md5-hmac ,** in use settings ={**Tunnel**, } slot: 0, conn id: 4, **crypto map: rtprules** sa timing: remaining key lifetime (k/sec): (4607998/27019) IV size: 8 bytes replay detection support: Y outbound ah sas: outbound pcp sas:

Estado del túnel de la visión encendido NG de punto de control

Vaya al editor de políticas y seleccione el **Window (Ventana) > Sytem Status (Estado del sistema)** para ver el estado del túnel.



Troubleshooting

Resuelva problemas la configuración PIX

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**.

Utilice estos comandos de habilitar los debugs en el firewall PIX.

- ¿**motor del debug crypto**? Mensajes del debug de las visualizaciones sobre los motores de criptografía, que realizan el cifrado y el desciframiento.
- ¿**isakmp del debug crypto**? Muestra mensajes sobre los eventos IKE.

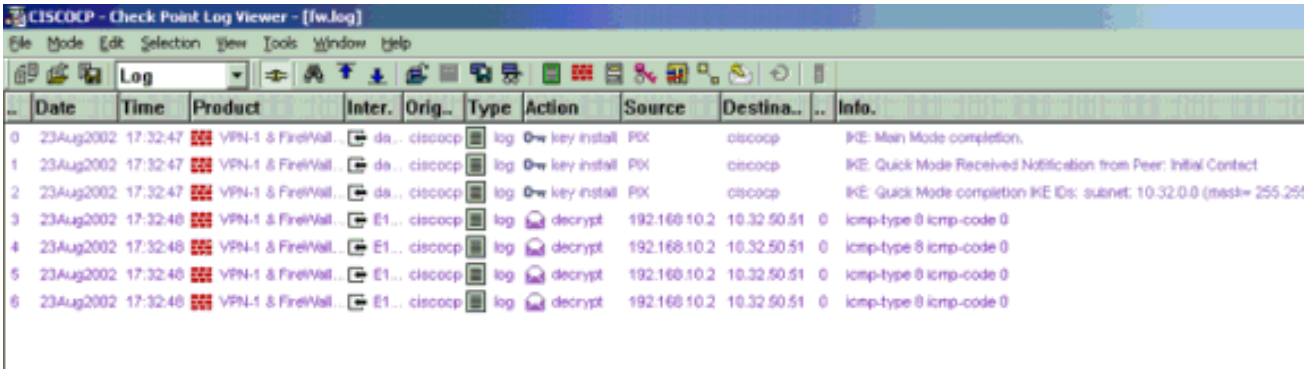
```
PIX501A#show cry ipsec sainterface: outside    Crypto map tag: rtprules, local addr.
172.18.124.158   local  ident (addr/mask/prot/port): (192.168.10.0/255.255.255.0/0/0)   remote
ident (addr/mask/prot/port): (10.32.0.0/255.255.128.0/0/0)   current_peer: 172.18.124.157
PERMIT, flags={origin_is_acl,}    #pkts encaps: 19, #pkts encrypt: 19, #pkts digest 19    #pkts
decaps: 19, #pkts decrypt: 19, #pkts verify 19    #pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0    #send errors 1,
#recv errors 0     local crypto endpt.: 172.18.124.158, remote crypto endpt.: 172.18.124.157
path mtu 1500, ipsec overhead 56, media mtu 1500     current outbound spi: 6b15a355     inbound
esp sas:      spi: 0xced238c7(3469883591)        transform: esp-3des esp-md5-hmac ,        in
use settings ={Tunnel, }        slot: 0, conn id: 3, crypto map: rtprules        sa timing:
remaining key lifetime (k/sec): (4607998/27019)        IV size: 8 bytes        replay detection
support: Y     inbound ah sas:     inbound pcp sas:     outbound esp sas:      spi:
0x6b15a355(1796580181)        transform: esp-3des esp-md5-hmac ,        in use settings
={Tunnel, }        slot: 0, conn id: 4, crypto map: rtprules        sa timing: remaining key
lifetime (k/sec): (4607998/27019)        IV size: 8 bytes        replay detection support: Y
outbound ah sas:     outbound pcp sas:
```

Resumen de la red

Cuando las redes internas adyacentes del múltiplo se configuran en el dominio del cifrado en el punto de verificación, el dispositivo pudo resumirlas automáticamente con respecto al tráfico interesante. Si el Access Control List crypto (ACL) en el PIX no se configura para hacer juego, el túnel es probable fallar. Por ejemplo, si las redes internas de 10.0.0.0 /24 y de 10.0.1.0 /24 se configuran para ser incluidas en el túnel, pueden ser resumidas a 10.0.0.0 /23.

Registros de la visión NG de punto de control

Seleccione el **Window (Ventana) > Log Viewer (Visor de registro)** para ver los registros.



Información Relacionada

- Cisco PIX Firewall Software
- Referencias de Comandos de Cisco Secure PIX Firewall
- Avisos de campos de productos de seguridad (incluido PIX)
- Solicitudes de Comentarios (RFC)
- Soporte Técnico y Documentación - Cisco Systems