Configuración de un Túnel IPsec - Cisco Router to Checkpoint Firewall 4.1

Contenido

Introducción

Este documento muestra cómo formar un túnel IPsec con claves previamente compartidas para unir dos redes privadas: la red privada 192.168.1.x dentro del router Cisco y la red privada 10.32.50.x dentro del Escudo de protección de punto de control.

Prerequisites

Requirements

Esta configuración de ejemplo supone que el tráfico desde dentro del router y dentro del punto de control a Internet (representado aquí por las redes 172.18.124.x) fluye antes de iniciar la configuración.

Componentes Utilizados

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

- Cisco 3600 router

- Software Cisco IOS® (C3640-JO3S56I-M), versión 12.1(5)T, SOFTWARE DE VERSIÓN (fc1)
- Firewall de punto de control 4.1

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.

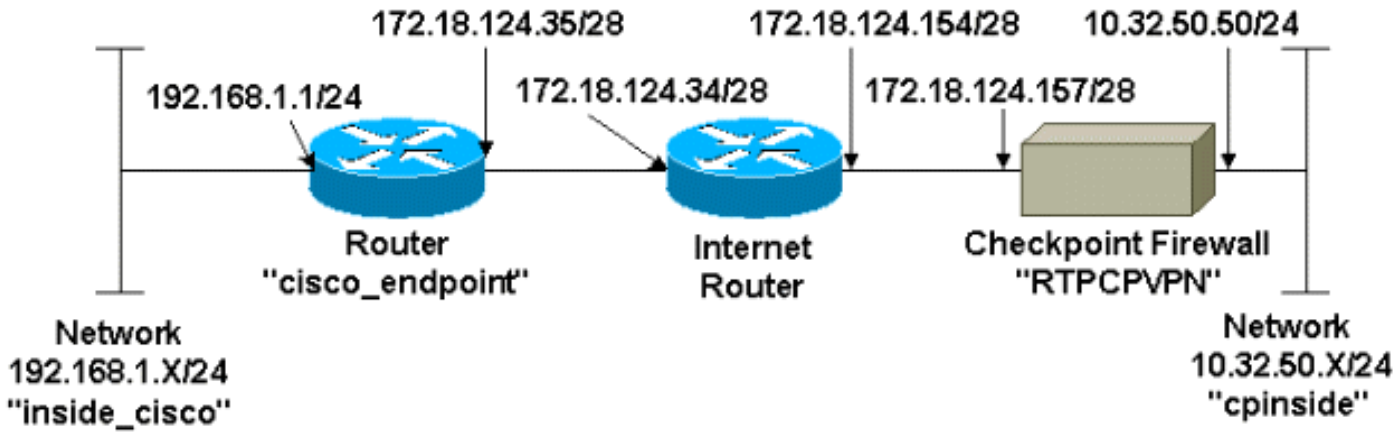
Configurar

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

En este documento, se utiliza esta configuración de red:



Configuraciones

Este documento usa estas configuraciones.

- Configuración del router
- Configuración del firewall del punto de control

Configuración del router

Configuración del router 3600 de Cisco

`Current configuration : 1608 bytes`
`!`
`version 12.1`

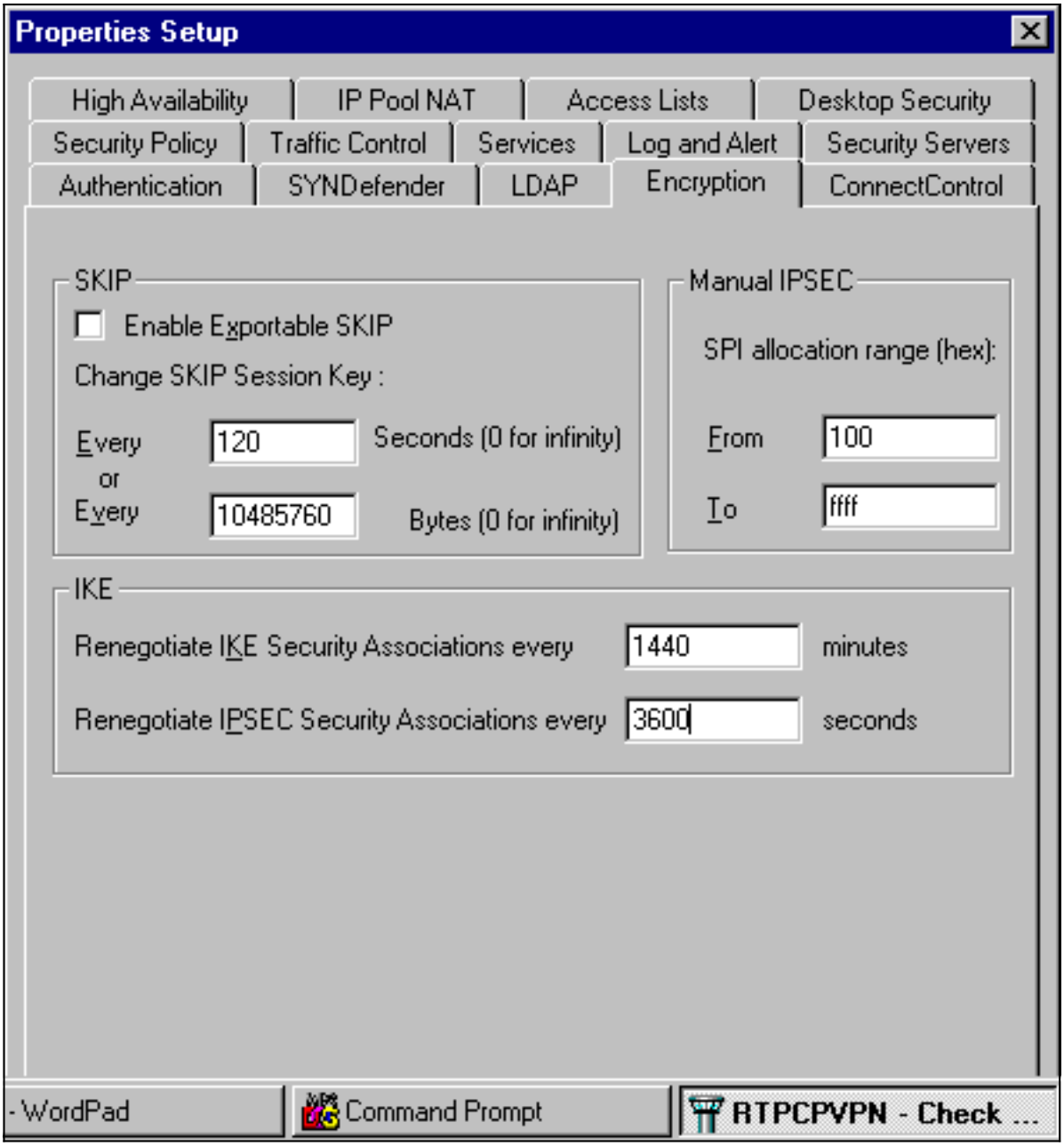
```
no service single-slot-reload-enable
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname cisco_endpoint
!
logging rate-limit console 10 except errors
!
ip subnet-zero
!
no ip finger
!
ip audit notify log
ip audit po max-events 100
!
!--- Internet Key Exchange (IKE) configuration crypto
isakmp policy 1
authentication pre-share
crypto isakmp key ciscorules address 172.18.124.157
!
!--- IPsec configuration crypto ipsec transform-set
rtpset esp-des esp-sha-hmac
!
crypto map rtp 1 ipsec-isakmp
set peer 172.18.124.157
set transform-set rtpset
match address 115
!
call rsvp-sync
cns event-service server
!
controller T1 1/0
!
controller T1 1/1
!
interface Ethernet0/0
ip address 172.18.124.35 255.255.255.240
ip nat outside
no ip mroute-cache
half-duplex
crypto map rtp
!
interface Ethernet0/1
ip address 192.168.1.1 255.255.255.0
ip nat inside
half-duplex
!
interface FastEthernet1/0
no ip address
shutdown
duplex auto
speed auto
!
ip kerberos source-interface any
ip nat pool INTERNET 172.18.124.36 172.18.124.36 netmask
255.255.255.240
ip nat inside source route-map nonat pool INTERNET
ip classless
ip route 0.0.0.0 0.0.0.0 172.18.124.34
no ip http server
!
access-list 101 deny ip 192.168.1.0 0.0.0.255 10.32.50.0
0.0.0.255
```

```
access-list 101 permit ip 192.168.1.0 0.0.0.255 any
access-list 115 permit ip 192.168.1.0 0.0.0.255
10.32.50.0 0.0.0.255
access-list 115 deny ip 192.168.1.0 0.0.0.255 any
route-map nonat permit 10
match ip address 101
!
dial-peer cor custom
!
line con 0
transport input none
line aux 0
line vty 0 4
login
!
end
```

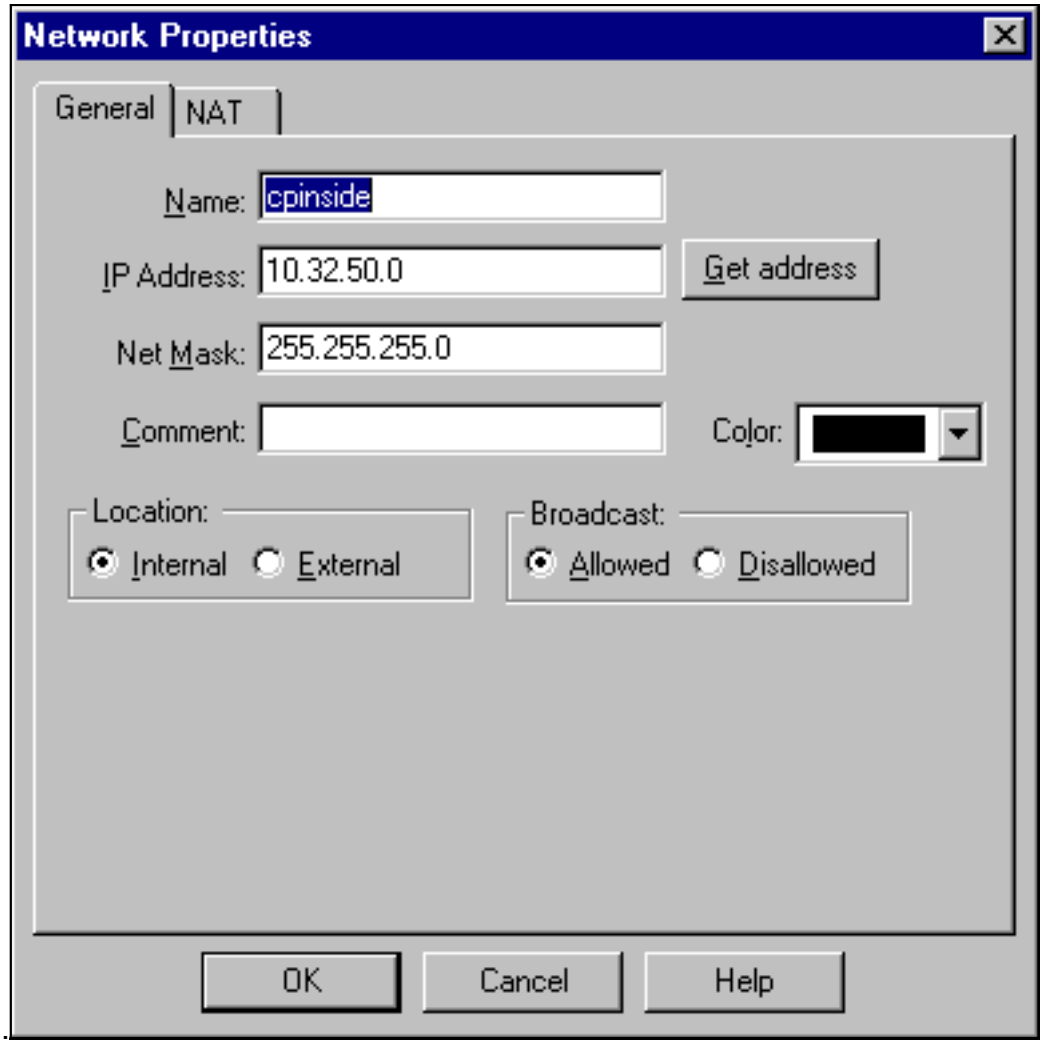
Configuración del firewall del punto de control

Complete estos pasos para configurar el firewall del punto de control.

1. Dado que las duraciones predeterminadas de IKE e IPsec difieren entre los proveedores, seleccione **Properties > Encryption** para establecer las duraciones del punto de comprobación de acuerdo con los valores predeterminados de Cisco.La duración IKE predeterminada de Cisco es de 86400 segundos (= 1440 minutos) y se puede modificar con estos comandos:**crypto isakmp policy #lifetime #**La duración configurable de Cisco IKE es de 60-86400 segundos. La duración predeterminada de IPSec de Cisco es de 3600 segundos y puede modificarse mediante el **comando crypto ipsec security-association lifetime seconds #**.La duración configurable de Cisco IPsec es de 120-86400 segundos.

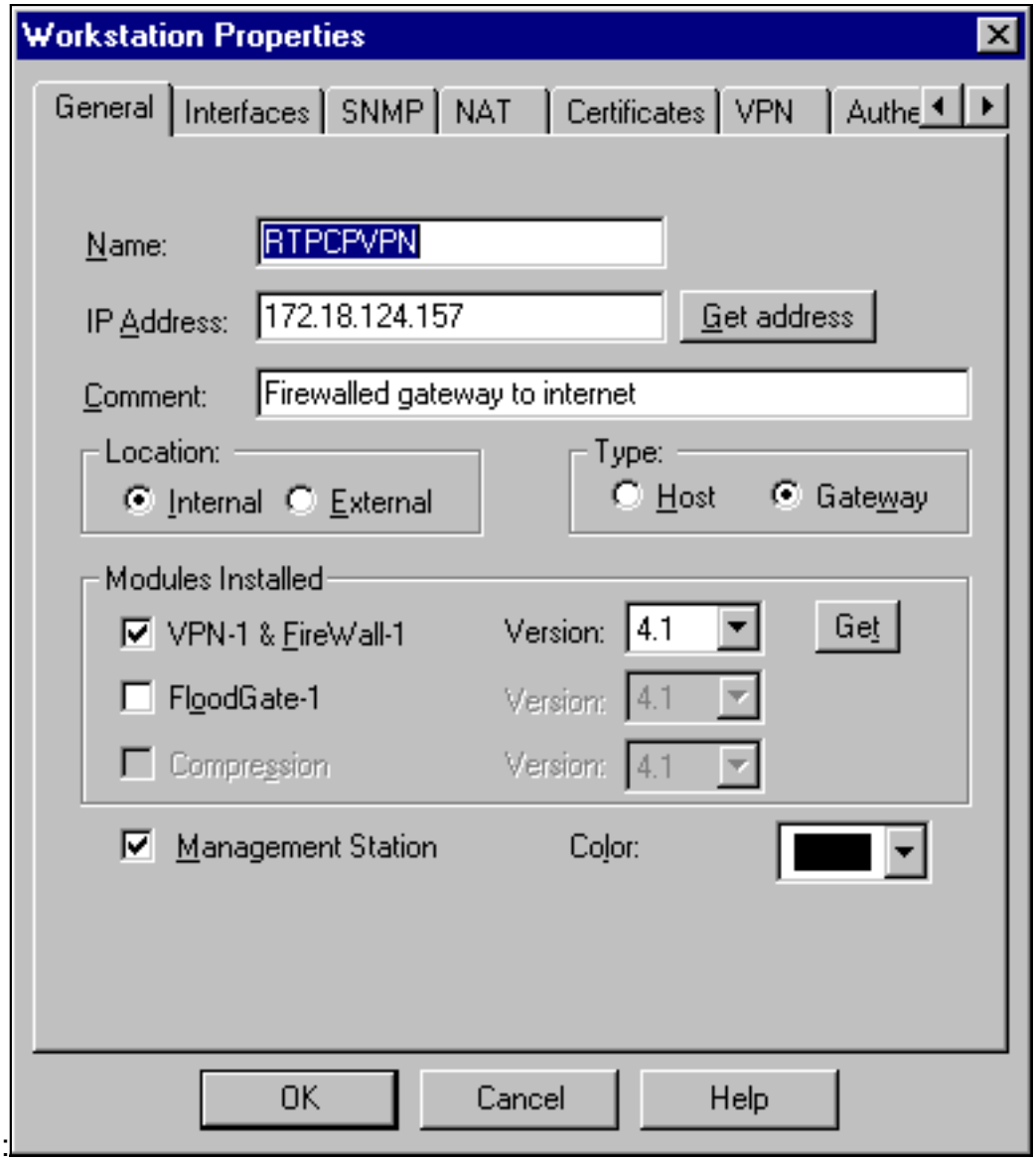


2. Seleccione **Manage > Network Objects > New (or Edit) > Network** para configurar el objeto para la red interna (llamada "cpinside") detrás del Checkpoint.Esto debe coincidir con la red de destino (segunda) en el **comando** Cisco **access-list 115 permit ip 192.168.1.0 0.0.0.255 10.32.50.0 0.0.255**.Seleccione **Interno** en



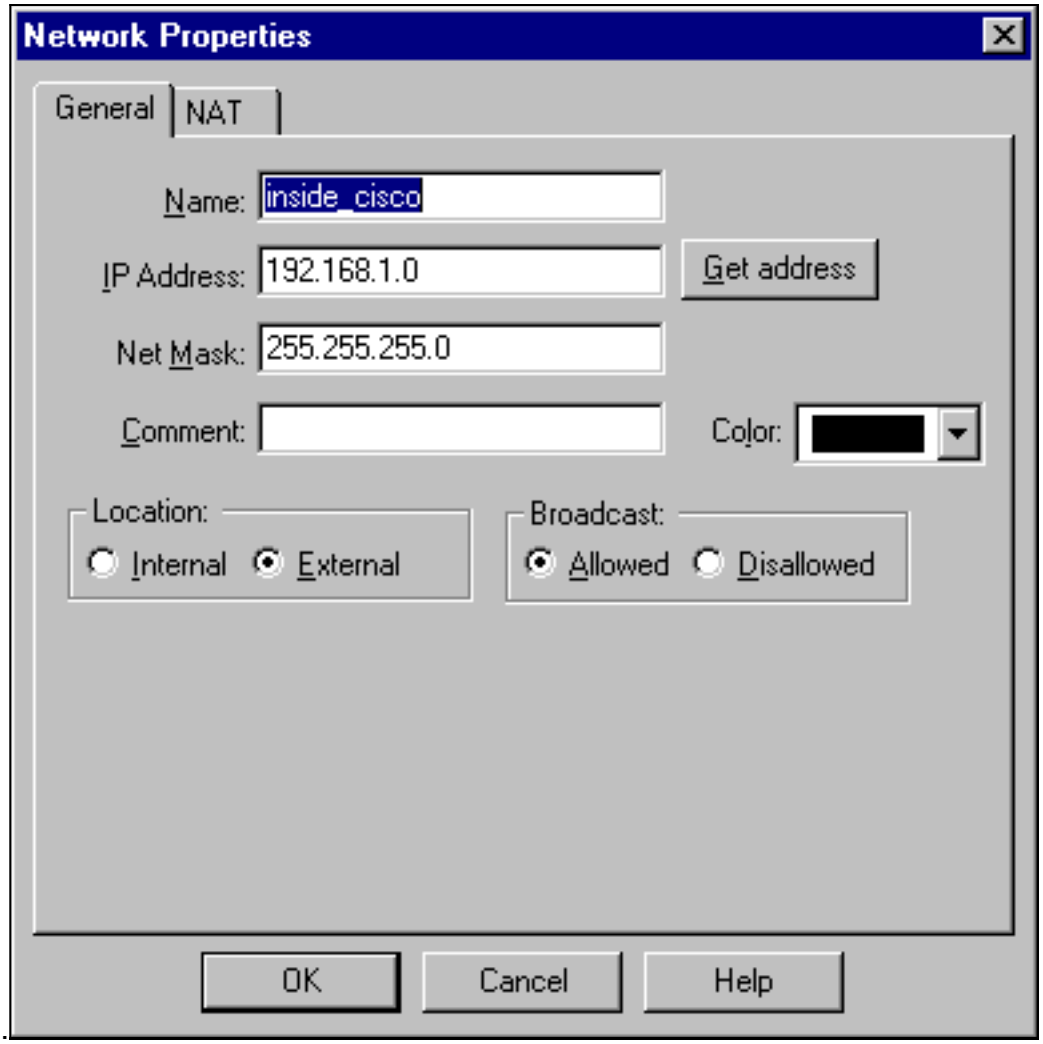
Ubicación.

3. Seleccione **Administrar > Objetos de red > Editar** para editar el objeto para el extremo de punto de control RTPCPVPN (gateway) al que apunta el router Cisco en el comando **set peer 172.18.124.157**.Seleccione **Interno** en Ubicación. En Type (Tipo), seleccione Gateway. En Modules Installed (Módulos instalados), seleccione la casilla de verificación **VPN-1 y FireWall-1**, y también active la **casilla de verificación Management**



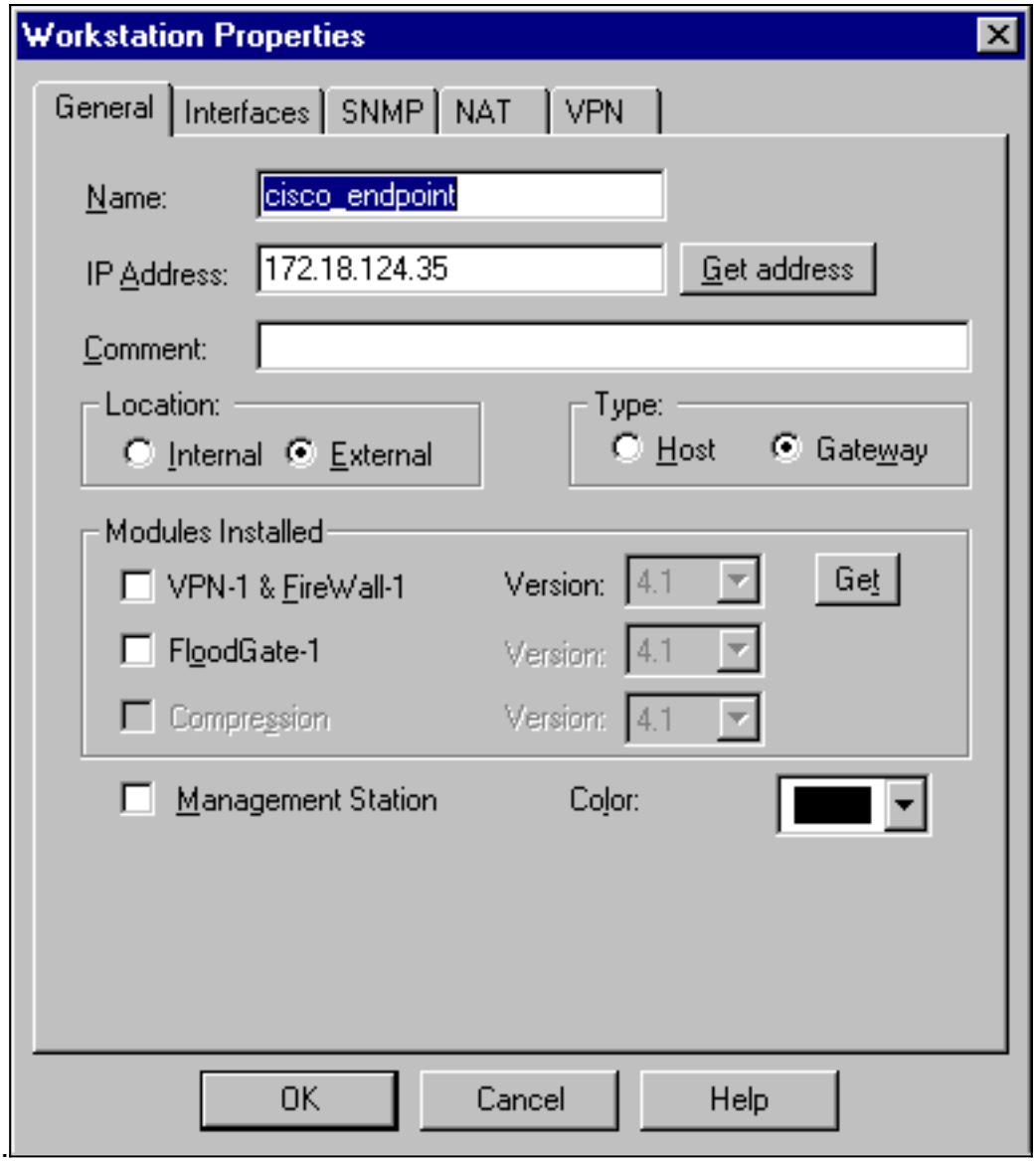
Station:

4. Seleccione **Manage > Network Objects > New > Network** para configurar el objeto para la red externa (llamada "inside_cisco") detrás del router de Cisco.Esto debe coincidir con la (primera) red de origen en el **comando** Cisco **access-list 115 permit ip 192.168.1.0 0.0.0.255 10.32.50.0 0.0.255**.Seleccione **External** en



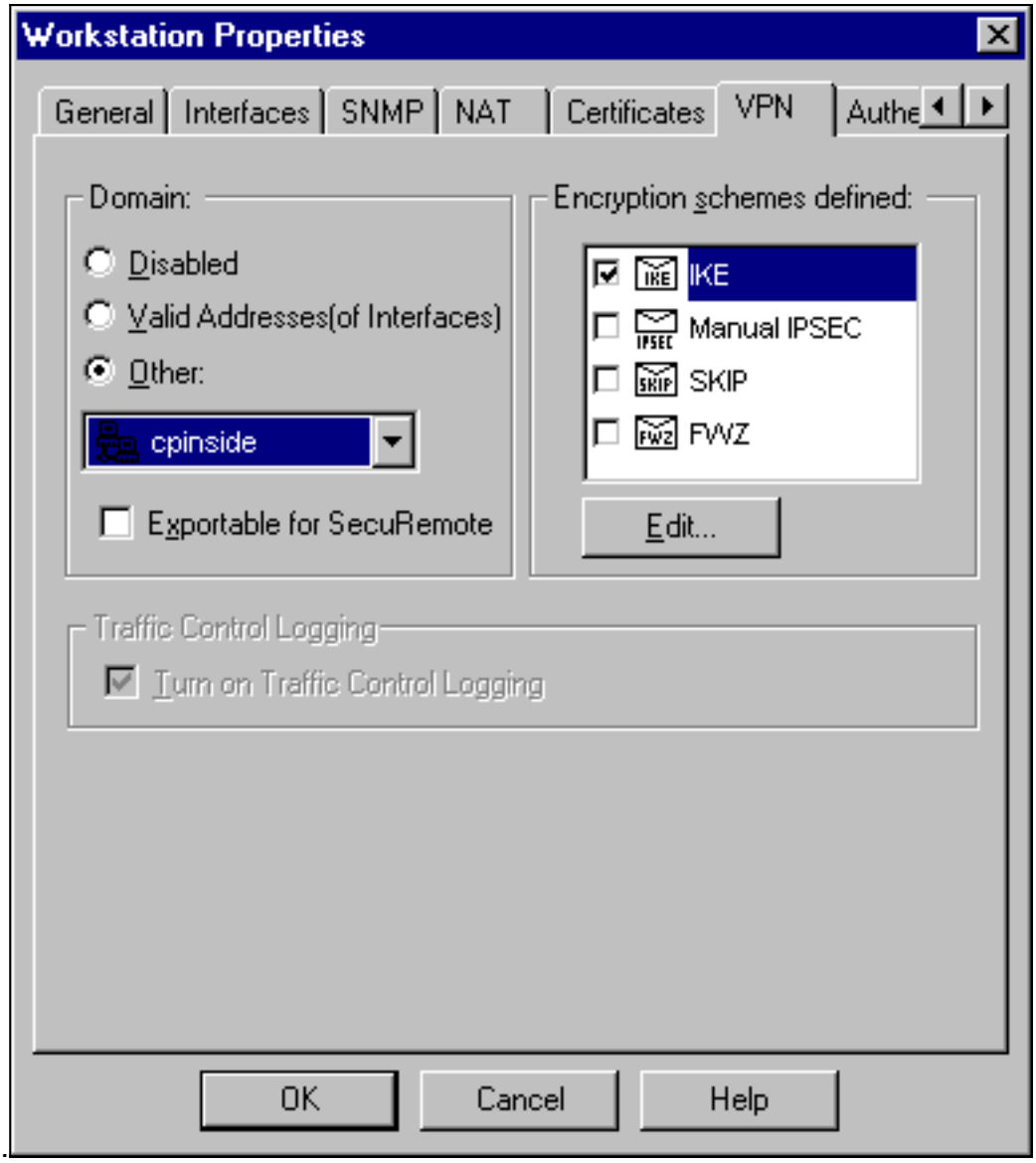
Location.

5. Seleccione **Administrar > Objetos de red > Nuevo > Estación de trabajo** para agregar un objeto para el gateway del router externo de Cisco (llamado "cisco_terminal"). Ésta es la interfaz de Cisco a la que se aplica el comando **crypto map** ***name.***Seleccione **External** en Location. En Type (Tipo), seleccione Gateway.**Nota:** No seleccione la casilla de verificación



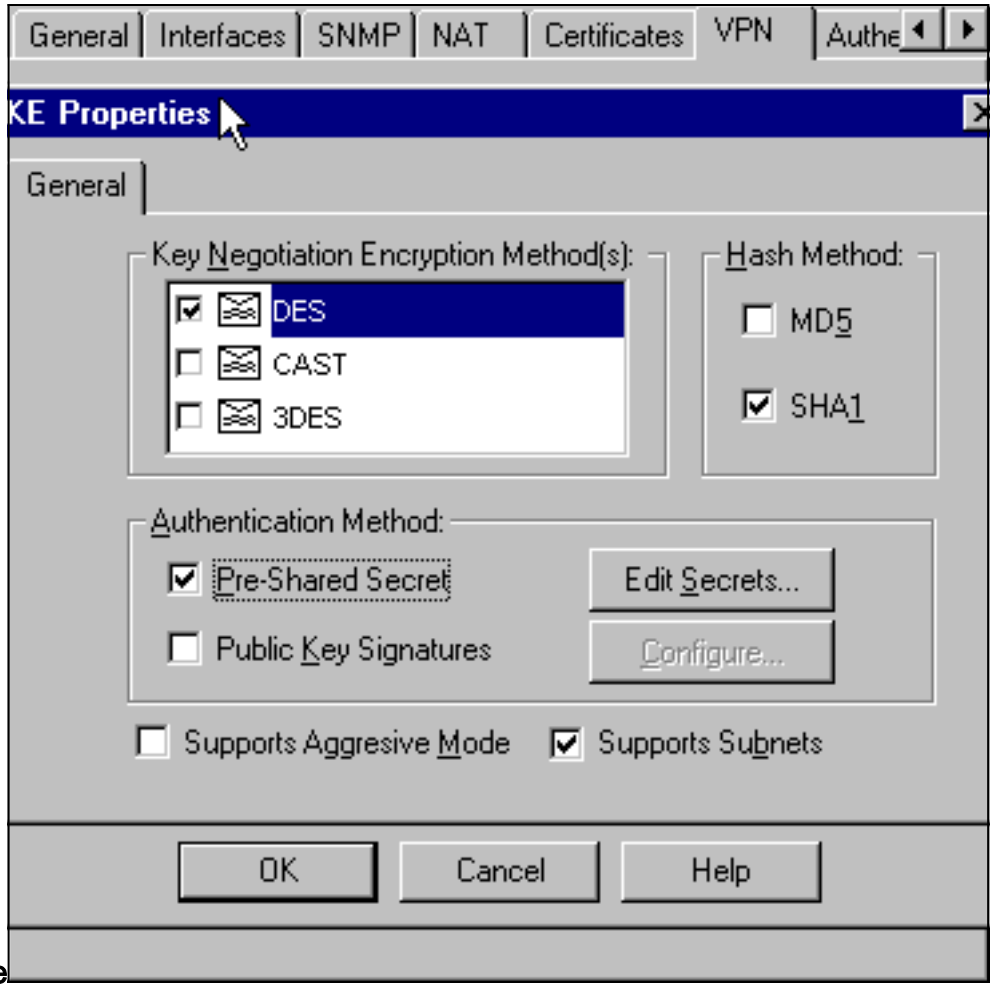
VPN-1/FireWall-1.

6. Seleccione Manage (Administración) > Network objects (Objetos de red) > Edit (Editar) para editar la ficha VPN del punto final del punto de control Gateway (denominado"RTPCPVPN"). En Domain (Dominio), seleccione Other (Otro) y luego, seleccione el interior de la red de Punto de control (denominado "cpinside") en la lista desplegable. Bajo los esquemas de encripción definidos, seleccione IKE y luego haga clic en Edit



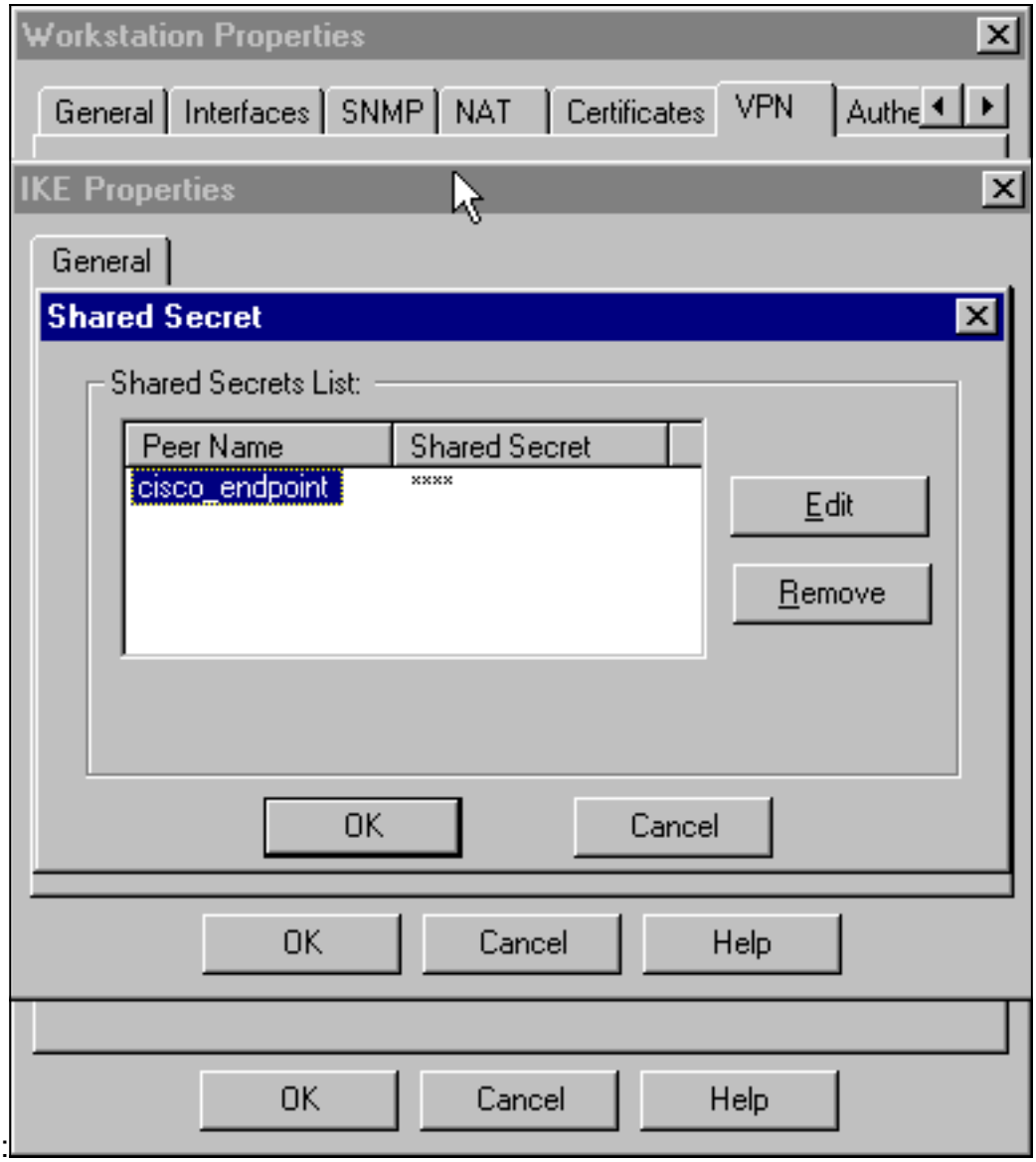
(Editar).

7. Cambie las propiedades IKE para que el cifrado DES coincida con estos comandos:**crypto isakmp policy #encryption desNota:** El cifrado DES es el valor predeterminado, por lo que no está visible en la configuración de Cisco.
8. Cambie las propiedades IKE a Hashing SHA1 para coincidir con estos comandos:**crypto isakmp policy #hash shaNota:** El algoritmo hash SHA es el valor predeterminado, por lo que no está visible en la configuración de Cisco.Cambie esta configuración:Cancelar la selección del modo agresivoMarque **Compatible con subredes**.Verifique **Pre-Shared Secret** bajo Authentication Method. Esto coincide con estos comandos:**crypto isakmp policy #authentication pre-**



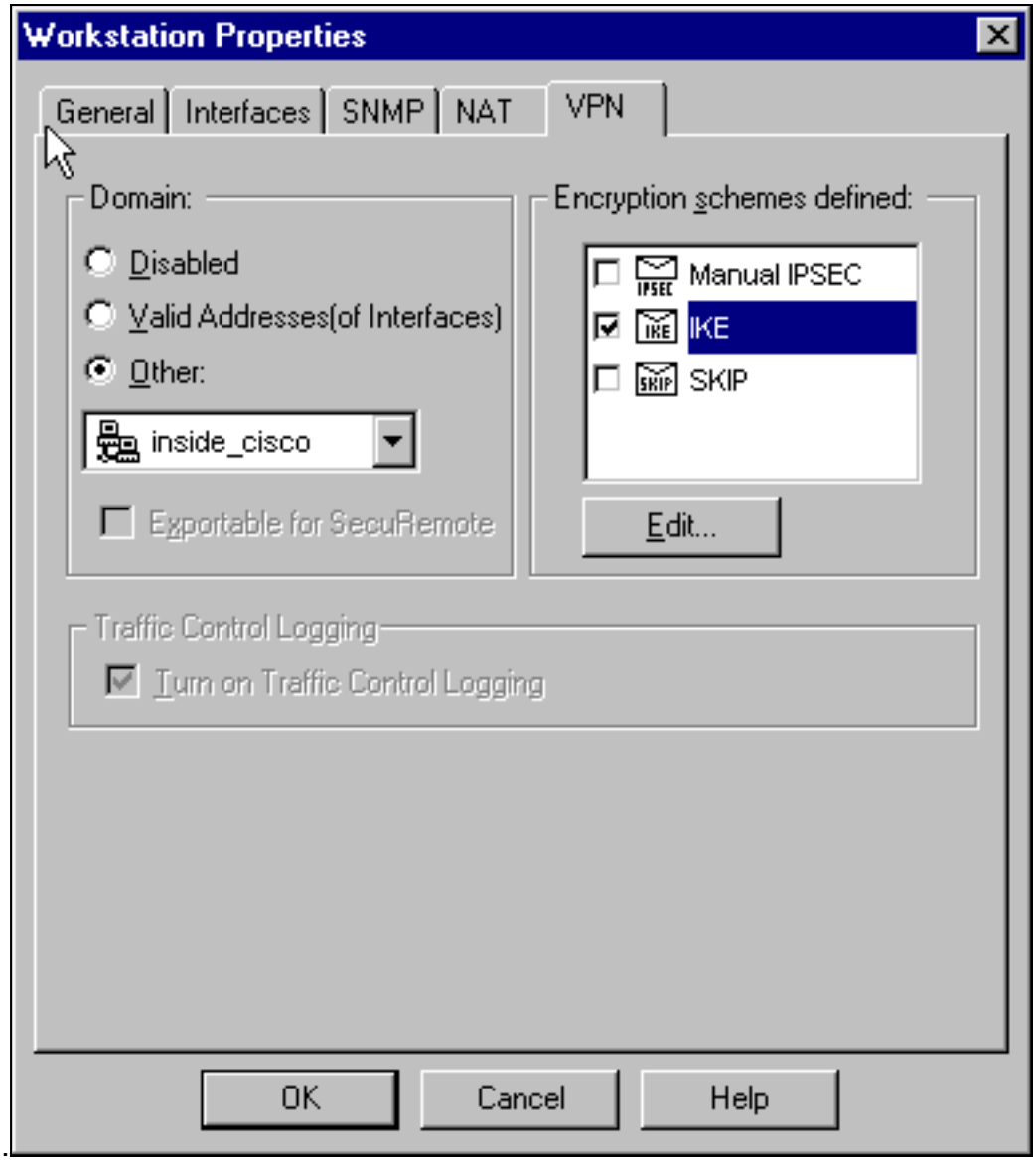
share

9. Haga clic en **Editar Secretos** para establecer la clave previamente compartida de acuerdo con el comando **crypto isakmp key *key***



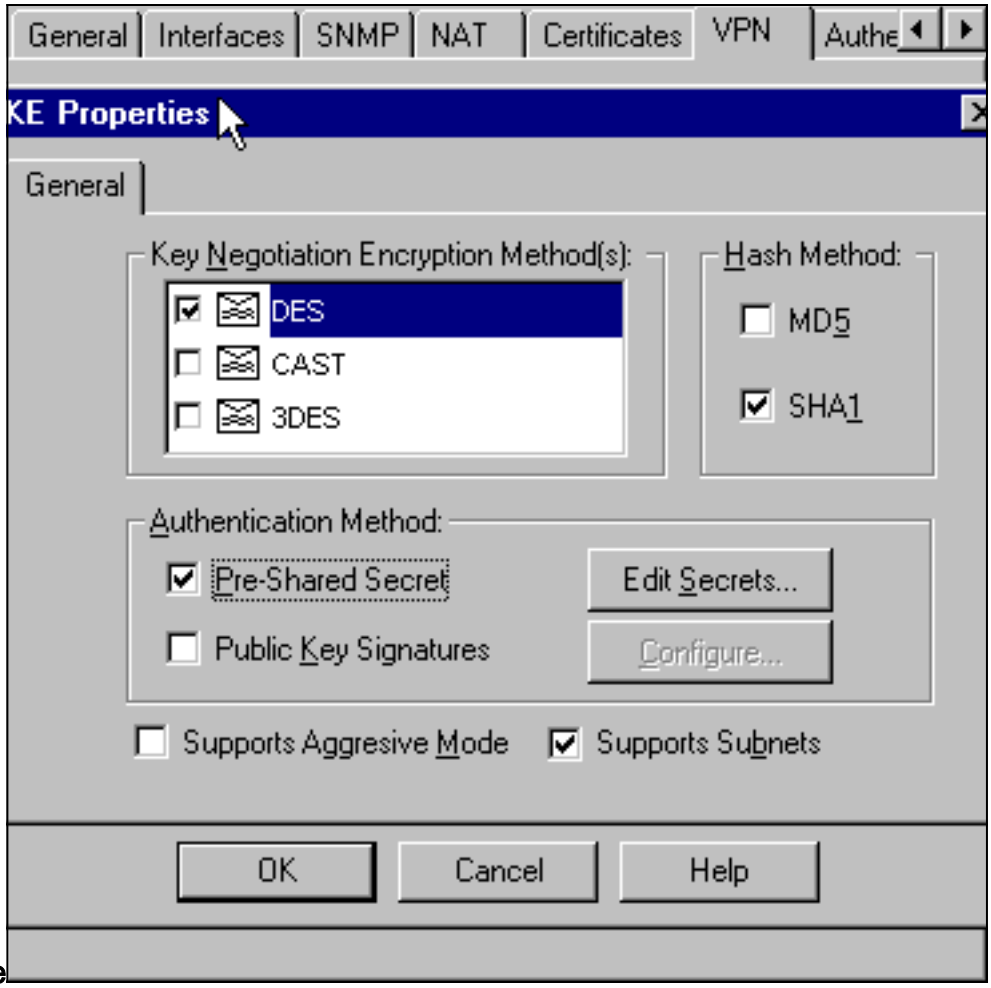
address:

10. Seleccione Manage (Administración) > Network Objects (Objetos de red) > Edit (Editar) para editar la ficha VPN de "cisco_endpoint". En Domain, seleccione Other y luego, seleccione el interior de la red de Cisco (denominado "inside_cisco"). Bajo los esquemas de encripción definidos, seleccione IKE y luego haga clic en Edit



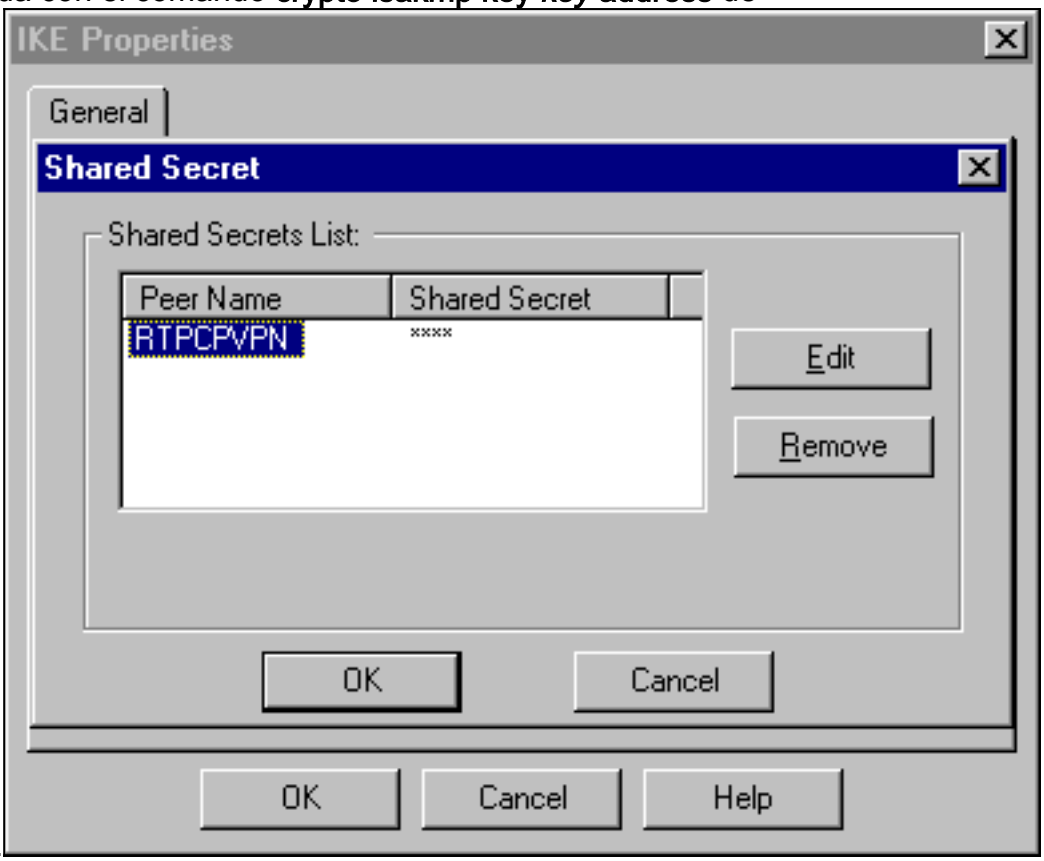
(Editar).

11. Cambie el encripción DES de las propiedades IKE para coincidir con estos comandos:**crypto isakmp policy #encryption desNota:** El cifrado DES es el valor predeterminado, por lo que no está visible en la configuración de Cisco.
12. Cambie las propiedades IKE a Hashing SHA1 para coincidir con estos comandos:**crypto isakmp policy #hash shaNota:** El algoritmo hash SHA es el valor predeterminado, por lo que no está visible en la configuración de Cisco.Cambie esta configuración:Cancelar la selección del modo agresivoMarque **Compatible con subredes**.Verifique **Pre-Shared Secret** bajo Authentication Method. Esto coincide con estos comandos:**crypto isakmp policy #authentication pre-**



share

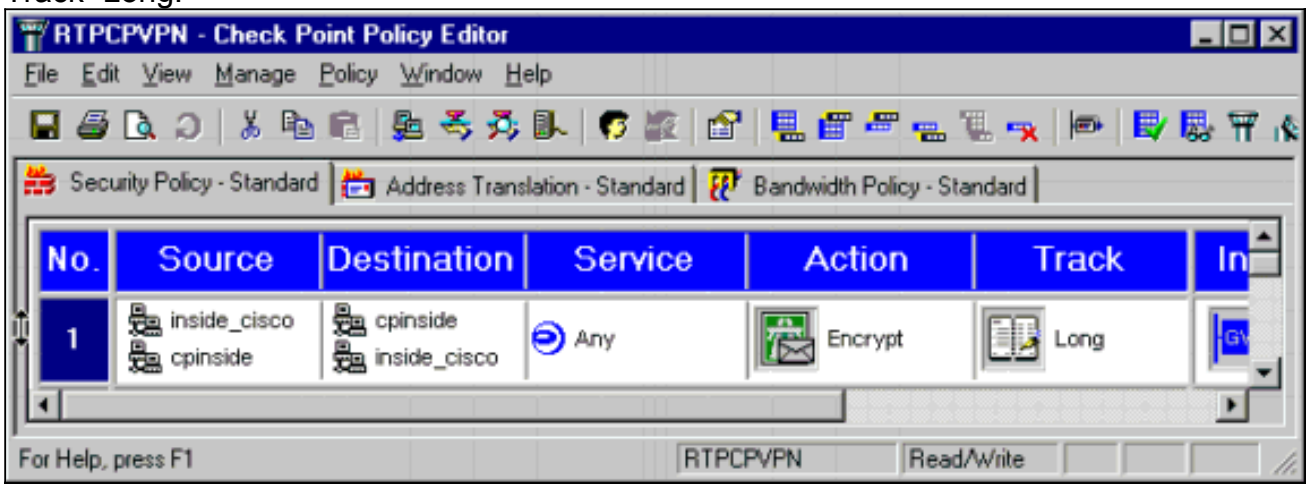
13. Haga clic en **Edit Secrets** para establecer la clave previamente compartida para que coincida con el comando **crypto isakmp key *key* address** de



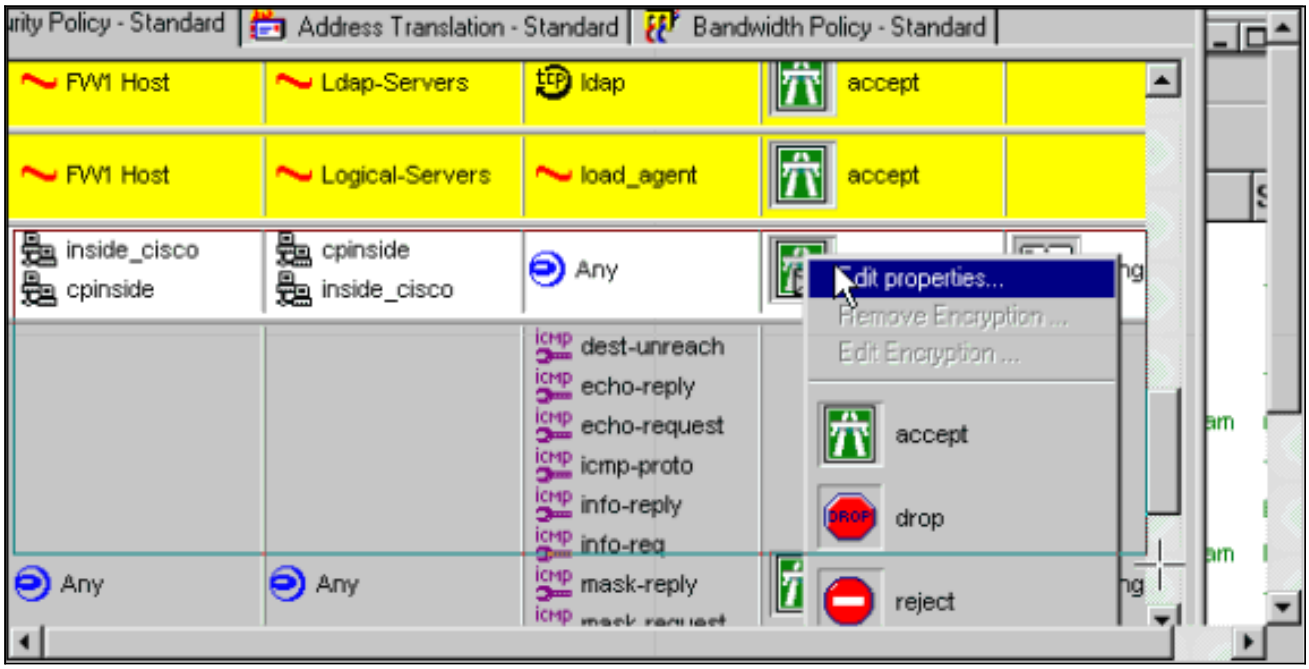
Cisco.

14. En la ventana del editor de políticas, ingrese una ventana tanto con el origen como con el destino, como en "inside_cisco" y "cpinside" (bidireccional). Set Service=Any, Action=Encrypt, y

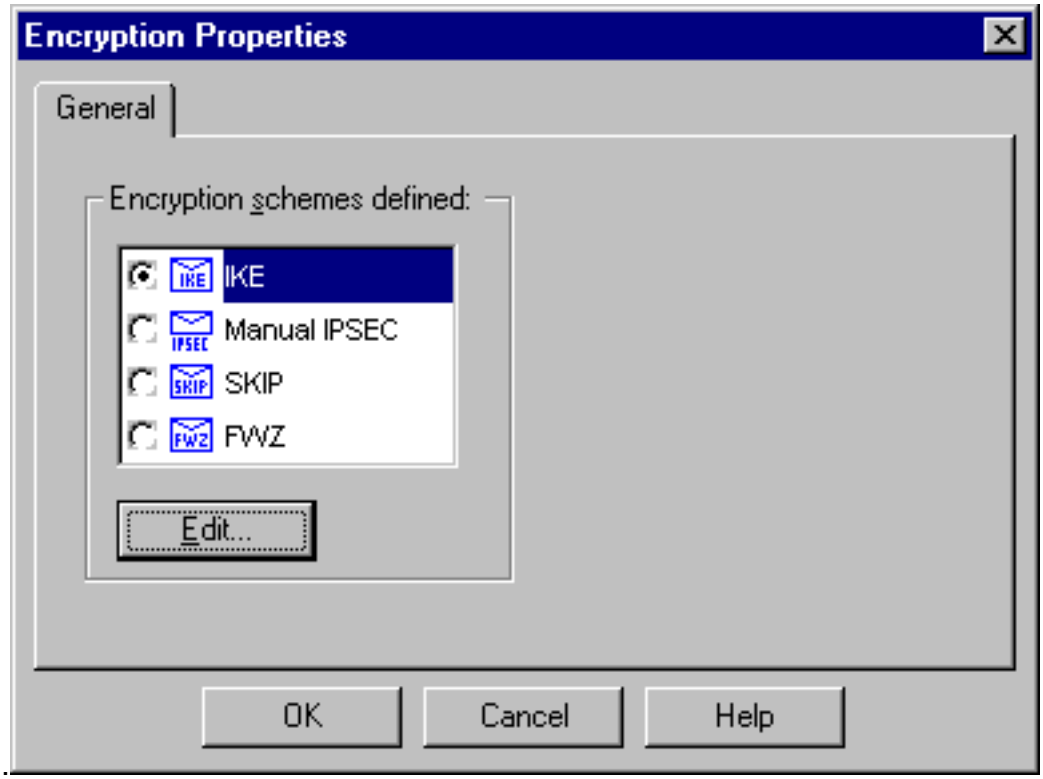
Track=Long.

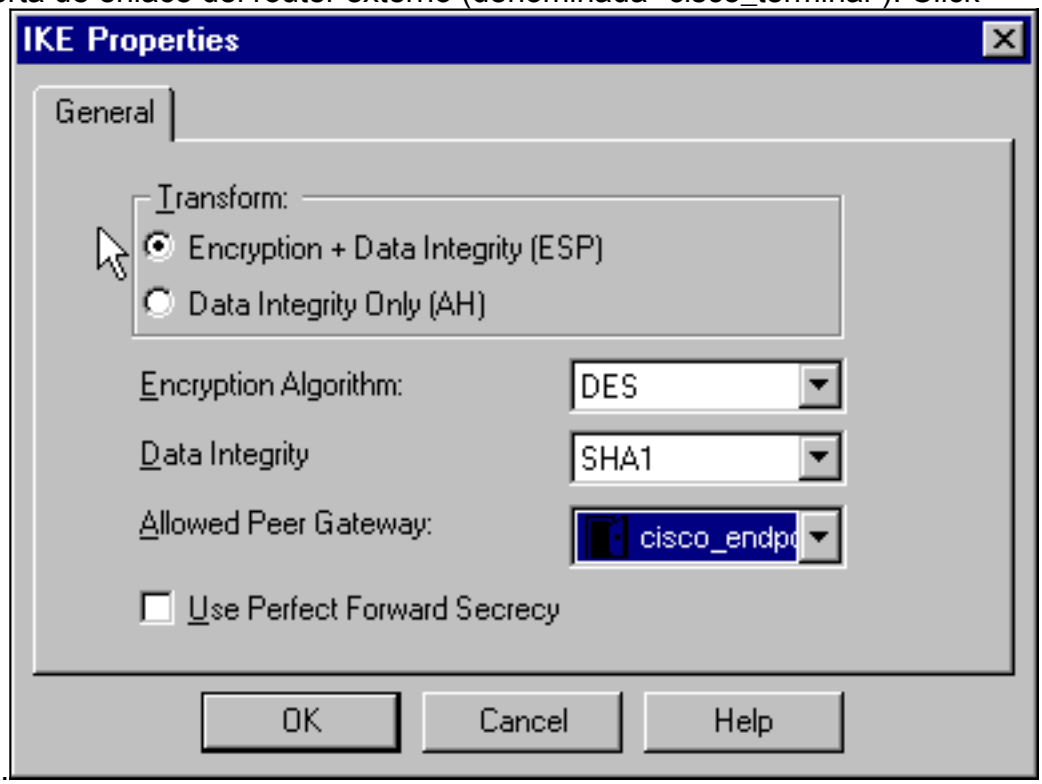


15. Haga clic en el icono verde **Cifrar** y seleccione **Editar propiedades** para configurar las políticas de cifrado bajo el encabezado Acción.



16. Seleccione IKE y luego haga clic en Edit

(Editar). 

17. En la ventana Propiedades IKE, cambie estas propiedades para coincidir con las transformaciones de Cisco IPsec en el comando **crypto ipsec transform-set rtchipset esp-des esp-sha-hmac**:En Transform (Transformar), seleccione Encryption (Encriptación) + Data Integrity (ESP) (Integridad de datos (ESP)). El algoritmo de cifrado debe ser **DES**, la integridad de los datos debe ser **SHA1** y la puerta de enlace de par permitida debe ser la puerta de enlace del router externo (denominada "cisco_terminal"). Click OK. 

18. Después de configurar el punto de control, seleccione **Policy > Install** en el menú Checkpoint para que los cambios surtan efecto.

Verificación

En esta sección encontrará información que puede utilizar para confirmar que su configuración esté funcionando 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 isakmp sa**: vea todas las asociaciones de seguridad (SA) IKE actuales en un par.
- **show crypto ipsec sa**: vea la configuración utilizada por las SA actuales.

Troubleshoot

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

Comandos para resolución de problemas

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

- **debug crypto engine**: muestra los mensajes de depuración sobre los motores criptográficos, que realizan el cifrado y el descifrado.
- **debug crypto isakmp — Muestra mensajes acerca de eventos IKE.**
- **debug crypto ipsec — Muestra eventos de IPSec.**
- **clear crypto isakmp**: borra todas las conexiones IKE activas.
- **clear crypto sa**: borra todas las SA IPsec.

Resumen de la red

Cuando se configuran varias redes internas adyacentes en el dominio de cifrado en el punto de control, el dispositivo podría resumirlas automáticamente con respecto al tráfico interesante. Si el router 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, podrían resumirse en 10.0.0.0 /23.

Punto de control

Dado que el seguimiento se configuró en Long (Prolongado) en la ventana del editor de políticas, el tráfico rechazado deberá aparecer en rojo en el visor de registros. Se puede obtener una depuración más detallada con:

```
C:\WINNT\FW1\4.1\fwstop
C:\WINNT\FW1\4.1\fw d -d
```

y en otra ventana.

```
C:\WINNT\FW1\4.1\fwstart
```

Nota: Se trata de una instalación de Microsoft Windows NT.

Ejecute estos comandos para borrar las SA en el punto de control:

```
fw tab -t IKE_SA_table -x
fw tab -t ISAKMP_ESP_table -x
fw tab -t inbound_SPI -x
fw tab -t ISAKMP_AH_table -x
```

Responda **sí** al mensaje

Ejemplo de resultado del comando debug

```
Configuration register is 0x2102

cisco_endpoint#debug crypto isakmp
Crypto ISAKMP debugging is on
cisco_endpoint#debug crypto isakmp
Crypto IPSEC debugging is on
cisco_endpoint#debug crypto engine
Crypto Engine debugging is on
cisco_endpoint#
20:54:06: IPSEC(sa_request): ,
  (key eng. msg.) src= 172.18.124.35, dest= 172.18.124.157,
    src_proxy= 192.168.1.0/255.255.255.0/0/0 (type=4),
    dest_proxy= 10.32.50.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-des esp-sha-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0xA29984CA(2727969994), conn_id= 0, keysize= 0, flags= 0x4004
20:54:06: ISAKMP: received ke message (1/1)
20:54:06: ISAKMP: local port 500, remote port 500
20:54:06: ISAKMP (0:1): beginning Main Mode exchange
20:54:06: ISAKMP (0:1): sending packet to 172.18.124.157 (I) MM_NO_STATE
20:54:06: ISAKMP (0:1): received packet from 172.18.124.157 (I) MM_NO_STATE
20:54:06: ISAKMP (0:1): processing SA payload. message ID = 0
20:54:06: ISAKMP (0:1): found peer pre-shared key matching 172.18.124.157
20:54:06: ISAKMP (0:1): Checking ISAKMP transform 1 against priority 1 policy
20:54:06: ISAKMP:      encryption DES-CBC
20:54:06: ISAKMP:      hash SHA
20:54:06: ISAKMP:      default group 1
20:54:06: ISAKMP:      auth pre-share
20:54:06: ISAKMP (0:1): atts are acceptable. Next payload is 0
20:54:06: CryptoEngine0: generate alg parameter
20:54:06: CRYPTO_ENGINE: Dh phase 1 status: 0
20:54:06: CRYPTO_ENGINE: Dh phase 1 status: 0
20:54:06: ISAKMP (0:1): SA is doing pre-shared key authentication
   using id type ID_IPV4_ADDR
20:54:06: ISAKMP (0:1): sending packet to 172.18.124.157 (I) MM_SA_SETUP
20:54:06: ISAKMP (0:1): received packet from 172.18.124.157 (I) MM_SA_SETUP
20:54:06: ISAKMP (0:1): processing KE payload. message ID = 0
20:54:06: CryptoEngine0: generate alg parameter
20:54:06: ISAKMP (0:1): processing NONCE payload. message ID = 0
20:54:06: ISAKMP (0:1): found peer pre-shared key matching 172.18.124.157
20:54:06: CryptoEngine0: create ISAKMP SKEYID for conn id 1
20:54:06: ISAKMP (0:1): SKEYID state generated
20:54:06: ISAKMP (1): ID payload
        next-payload : 8
        type         : 1
        protocol     : 17
        port         : 500
        length       : 8
20:54:06: ISAKMP (1): Total payload length: 12
20:54:06: CryptoEngine0: generate hmac context for conn id 1
20:54:06: ISAKMP (0:1): sending packet to 172.18.124.157 (I) MM_KEY_EXCH
20:54:06: ISAKMP (0:1): received packet from 172.18.124.157 (I) MM_KEY_EXCH
```

```
20:54:06: ISAKMP (0:1): processing ID payload. message ID = 0
20:54:06: ISAKMP (0:1): processing HASH payload. message ID = 0
20:54:06: CryptoEngine0: generate hmac context for conn id 1
20:54:06: ISAKMP (0:1): SA has been authenticated with 172.18.124.157
20:54:06: ISAKMP (0:1): beginning Quick Mode exchange, M-ID of 1855173267
20:54:06: CryptoEngine0: generate hmac context for conn id 1
20:54:06: ISAKMP (0:1): sending packet to 172.18.124.157 (I) QM_IDLE
20:54:06: CryptoEngine0: clear dh number for conn id 1
20:54:06: ISAKMP (0:1): received packet from 172.18.124.157 (I) QM_IDLE
20:54:06: CryptoEngine0: generate hmac context for conn id 1
20:54:06: ISAKMP (0:1): processing HASH payload. message ID = 1855173267
20:54:06: ISAKMP (0:1): processing SA payload. message ID = 1855173267
20:54:06: ISAKMP (0:1): Checking IPSec proposal 1
20:54:06: ISAKMP: transform 1, ESP_DES
20:54:06: ISAKMP:   attributes in transform:
20:54:06: ISAKMP:      encaps is 1
20:54:06: ISAKMP:      SA life type in seconds
20:54:06: ISAKMP:      SA life duration (basic) of 3600
20:54:06: ISAKMP:      SA life type in kilobytes
20:54:06: ISAKMP:      SA life duration (VPI) of  0x0 0x46 0x50 0x0
20:54:06: ISAKMP:      authenticator is HMAC-SHA
20:54:06: validate proposal 0
20:54:06: ISAKMP (0:1): atts are acceptable.
20:54:06: IPSEC(validate_proposal_request): proposal part #1,
  (key eng. msg.) dest= 172.18.124.157, src= 172.18.124.35,
    dest_proxy= 10.32.50.0/255.255.255.0/0/0 (type=4),
    src_proxy= 192.168.1.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-des esp-sha-hmac ,
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
20:54:06: validate proposal request 0
20:54:06: ISAKMP (0:1): processing NONCE payload. message ID = 1855173267
20:54:06: ISAKMP (0:1): processing ID payload. message ID = 1855173267
20:54:06: ISAKMP (0:1): processing ID payload. message ID = 1855173267
20:54:06: CryptoEngine0: generate hmac context for conn id 1
20:54:06: ipsec allocate flow 0
20:54:06: ipsec allocate flow 0
20:54:06: ISAKMP (0:1): Creating IPSec SAs
20:54:06:         inbound SA from 172.18.124.157 to 172.18.124.35
        (proxy 10.32.50.0 to 192.168.1.0)
20:54:06:         has spi 0xA29984CA and conn_id 2000 and flags 4
20:54:06:         lifetime of 3600 seconds
20:54:06:         lifetime of 4608000 kilobytes
20:54:06:         outbound SA from 172.18.124.35   to 172.18.124.157
   (proxy 192.168.1.0 to 10.32.50.0)
20:54:06:         has spi 404516441 and conn_id 2001 and flags 4
20:54:06:         lifetime of 3600 seconds
20:54:06:         lifetime of 4608000 kilobytes
20:54:06: ISAKMP (0:1): sending packet to 172.18.124.157 (I) QM_IDLE
20:54:06: ISAKMP (0:1): deleting node 1855173267 error FALSE reason ""
20:54:06: IPSEC(key_engine): got a queue event...
20:54:06: IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 172.18.124.35, src= 172.18.124.157,
    dest_proxy= 192.168.1.0/255.255.255.0/0/0 (type=4),
    src_proxy= 10.32.50.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-des esp-sha-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0xA29984CA(2727969994), conn_id= 2000, keysize= 0, flags= 0x4
20:54:06: IPSEC(initialize_sas): ,
  (key eng. msg.) src= 172.18.124.35, dest= 172.18.124.157,
    src_proxy= 192.168.1.0/255.255.255.0/0/0 (type=4),
    dest_proxy= 10.32.50.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-des esp-sha-hmac ,
    lifedur= 3600s and 4608000kb,
```

```
    spi= 0x181C6E59(404516441), conn_id= 2001, keysize= 0, flags= 0x4
20:54:06: IPSEC(create_sa): sa created,
  (sa) sa_dest= 172.18.124.35, sa_prot= 50,
    sa_spi= 0xA29984CA(2727969994),
    sa_trans= esp-des esp-sha-hmac , sa_conn_id= 2000
20:54:06: IPSEC(create_sa): sa created,
  (sa) sa_dest= 172.18.124.157, sa_prot= 50,
    sa_spi= 0x181C6E59(404516441),
    sa_trans= esp-des esp-sha-hmac , sa_conn_id= 2001
cisco_endpoint#sho cry ips sa

interface: Ethernet0/0
    Crypto map tag: rtp, local addr. 172.18.124.35

   local  ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (10.32.50.0/255.255.255.0/0/0)
   current_peer: 172.18.124.157
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 14, #pkts encrypt: 14, #pkts digest 14
    #pkts decaps: 14, #pkts decrypt: 14, #pkts verify 14
    #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.: 172.18.124.35, remote crypto endpt.: 172.18.124.157
     path mtu 1500, media mtu 1500
     current outbound spi: 181C6E59

     inbound esp sas:
      spi: 0xA29984CA(2727969994)
        transform: esp-des esp-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2000, flow_id: 1, crypto map: rtp
 --More--                 sa timing: remaining key lifetime (k/sec):
    (4607998/3447)
        IV size: 8 bytes
        replay detection support: Y

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x181C6E59(404516441)
        transform: esp-des esp-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2001, flow_id: 2, crypto map: rtp
        sa timing: remaining key lifetime (k/sec): (4607997/3447)
        IV size: 8 bytes
        replay detection support: Y

     outbound ah sas:

     outbound pcp sas:


cisco_endpoint#show crypto isakmp sa
    dst           src          state        conn-id   slot
172.18.124.157 172.18.124.35  QM_IDLE           1       0

cisco_endpoint#exit
```

Información Relacionada

- Negociación IPSec/Protocolos IKE
- Configuración de seguridad de red IPSec
- Configuración del protocolo de seguridad de intercambio de claves de Internet
- Soporte Técnico y Documentación - Cisco Systems