Configurando un túnel IPsec - Cisco Secure PIX Firewall al Firewall del punto de verificación 4.1

Contenido

Introducción

Esta configuración de muestra demuestra cómo formar un túnel IPsec con las claves previamente compartidas para unirse a dos redes privadas. En nuestro ejemplo, las redes conectadas son la red privada 192.168.1.X dentro del firewall PIX de Cisco Secure (PIX) y la red privada 10.32.50.X dentro del punto de control. Se asume que el tráfico por dentro del PIX y del interior el Firewall del punto de verificación 4.1 a Internet (representado aquí por las redes 172.18.124.X) fluye antes de comenzar esta configuración.

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

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

- Versión 5.3.1 del software PIX
- Escudo de protección de punto de control 4.1

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.

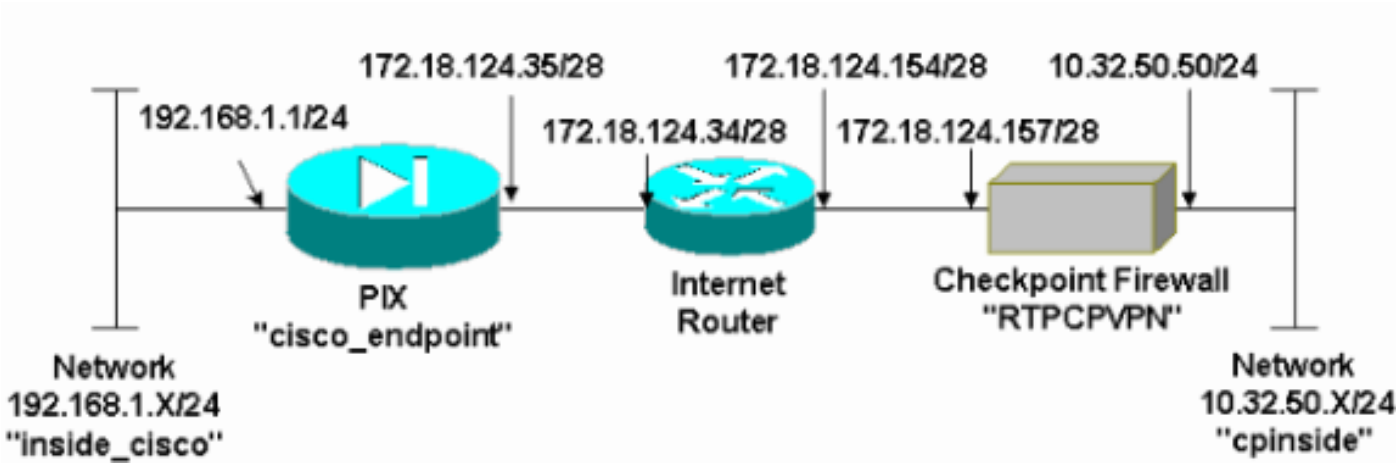
Configurar

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

Nota: Para obtener información adicional sobre los comandos que se utilizan en este documento, use la Command Lookup Tool (solo para clientes registrados).

Diagrama de la red

Este documento utiliza la configuración de red que se muestra en este diagrama:



Configuraciones

Este documento utiliza las configuraciones mostradas en esta sección.

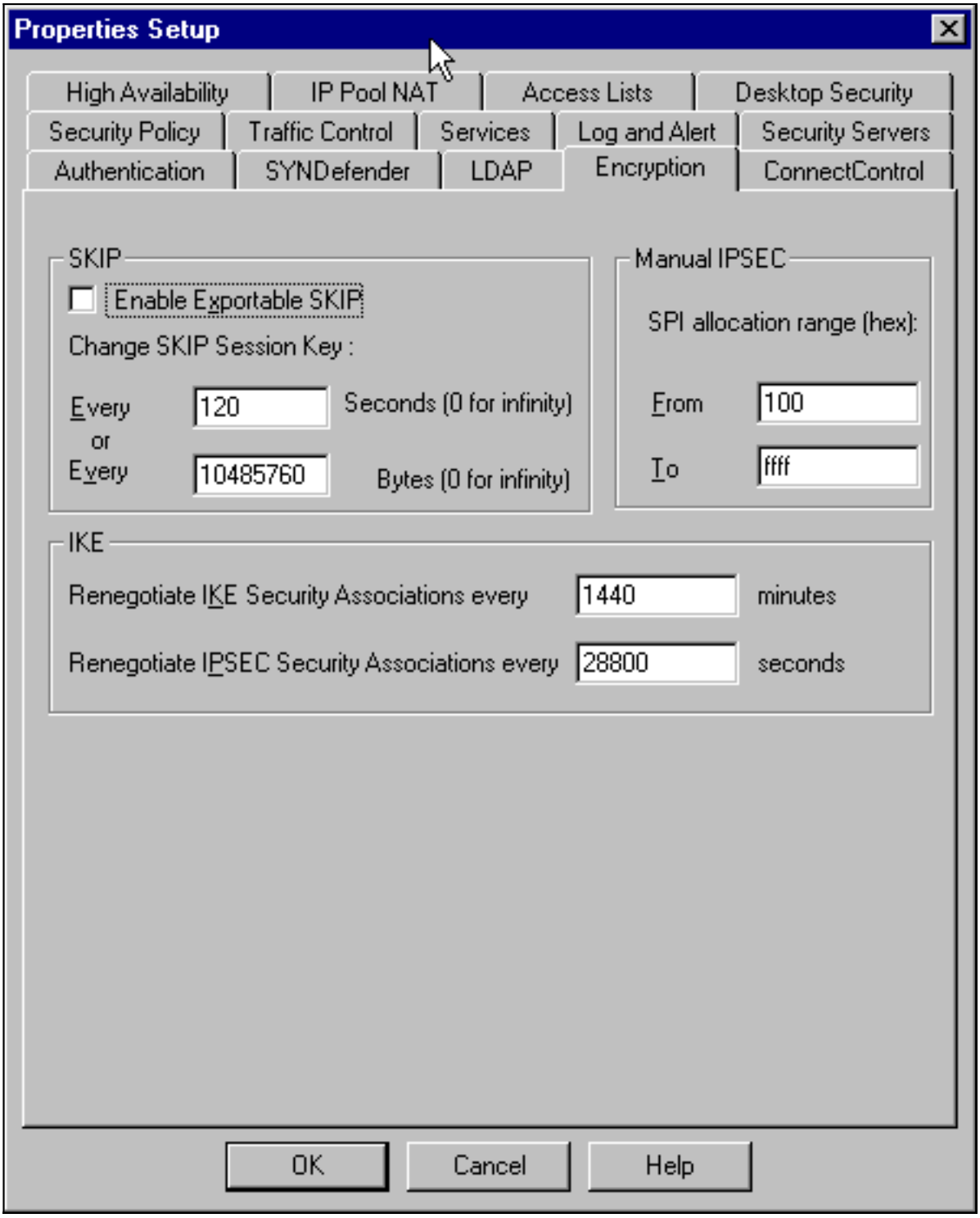
Configuración de PIX

```
PIX Version 5.3(1)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname cisco_endpoint
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 1720
fixup protocol rsh 514
```

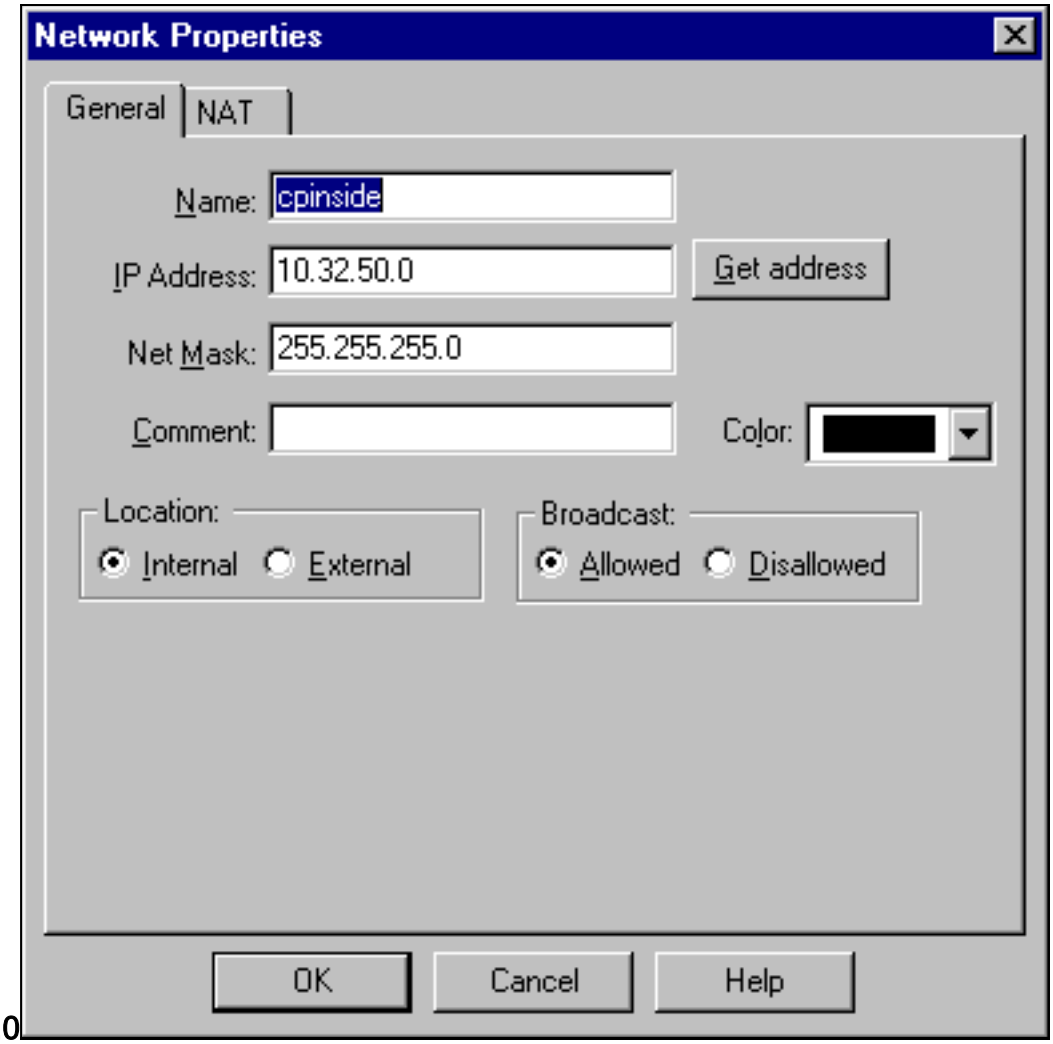
```
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
names
access-list 115 permit ip 192.168.1.0 255.255.255.0
10.32.50.0 255.255.255.0 access-list 115 deny ip
192.168.1.0 255.255.255.0 any pager lines 24 logging on
no logging timestamp no logging standby no logging
console logging monitor debugging no logging buffered
logging trap debugging no logging history logging
facility 20 logging queue 512 interface ethernet0 auto
interface ethernet1 auto mtu outside 1500 mtu inside
1500 ip address outside 172.18.124.35 255.255.255.240 ip
address inside 192.168.1.1 255.255.255.0 ip audit info
action alarm ip audit attack action alarm no failover
failover timeout 0:00:00 failover poll 15 failover ip
address outside 0.0.0.0 failover ip address inside
0.0.0.0 arp timeout 14400 global (outside) 1
172.18.124.36 nat (inside) 0 access-list 115 nat
(inside) 1 0.0.0.0 0.0.0.0 0 0 route outside 0.0.0.0
0.0.0.0 172.18.124.34 1 timeout xlate 3:00:00g SA
0x80bd6a10, conn_id = 0 timeout 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 0:02:00 timeout uauth 0:05:00 absolute aaa-
server TACACS+ protocol tacacs+ aaa-server RADIUS
protocol radius no snmp-server location no snmp-server
contact snmp-server community public no snmp-server
enable traps floodguard enable !--- IPSec configuration
sysopt connection permit-ipsec no sysopt route dnat
crypto ipsec transform-set myset esp-des esp-sha-hmac
crypto map rtpmap 10 ipsec-isakmp crypto map rtpmap 10
match address 115 crypto map rtpmap 10 set peer
172.18.124.157 crypto map rtpmap 10 set transform-set
myset crypto map rtpmap 10 set security-association
lifetime seconds 3600 kilobytes 4608000 crypto map
rtpmap interface outside !--- IKE configuration isakmp
enable outside isakmp key ******** address
172.18.124.157 netmask 255.255.255.240 isakmp identity
address isakmp policy 10 authentication pre-share isakmp
policy 10 encryption des isakmp policy 10 hash sha
isakmp policy 10 group 1 isakmp policy 10 lifetime 86400
telnet timeout 5 ssh timeout 5 terminal width 80
Cryptochecksum:dc43c44e4513d3633a3fc7b1c3802c79 : end
[OK]
```

Punto de control de Firewall

1. Dado que las duraciones predeterminadas de IKE y de IPSec difieren entre los proveedores, seleccione Properties (Propiedades) > Encryption (Codificación) para configurar la duración de los puntos de control y que éstos coincidan con los valores predeterminados de PIX.El tiempo de vida IKE predeterminado de PIX es 86400 segundos (minutos =1440), de modificable por este comando: **isakmp policy # lifetime 86400**El tiempo de vida de IKE PIX se puede configurar entre 60-86400 segundos.La vida útil de IPSec del valor predeterminado de PIX es 28800 segundos, de modificable por este comando: **crypto ipsec security-association lifetime seconds #**Usted puede configurar un curso de la vida del IPSec de PIX entre 120-86400
   segundos.

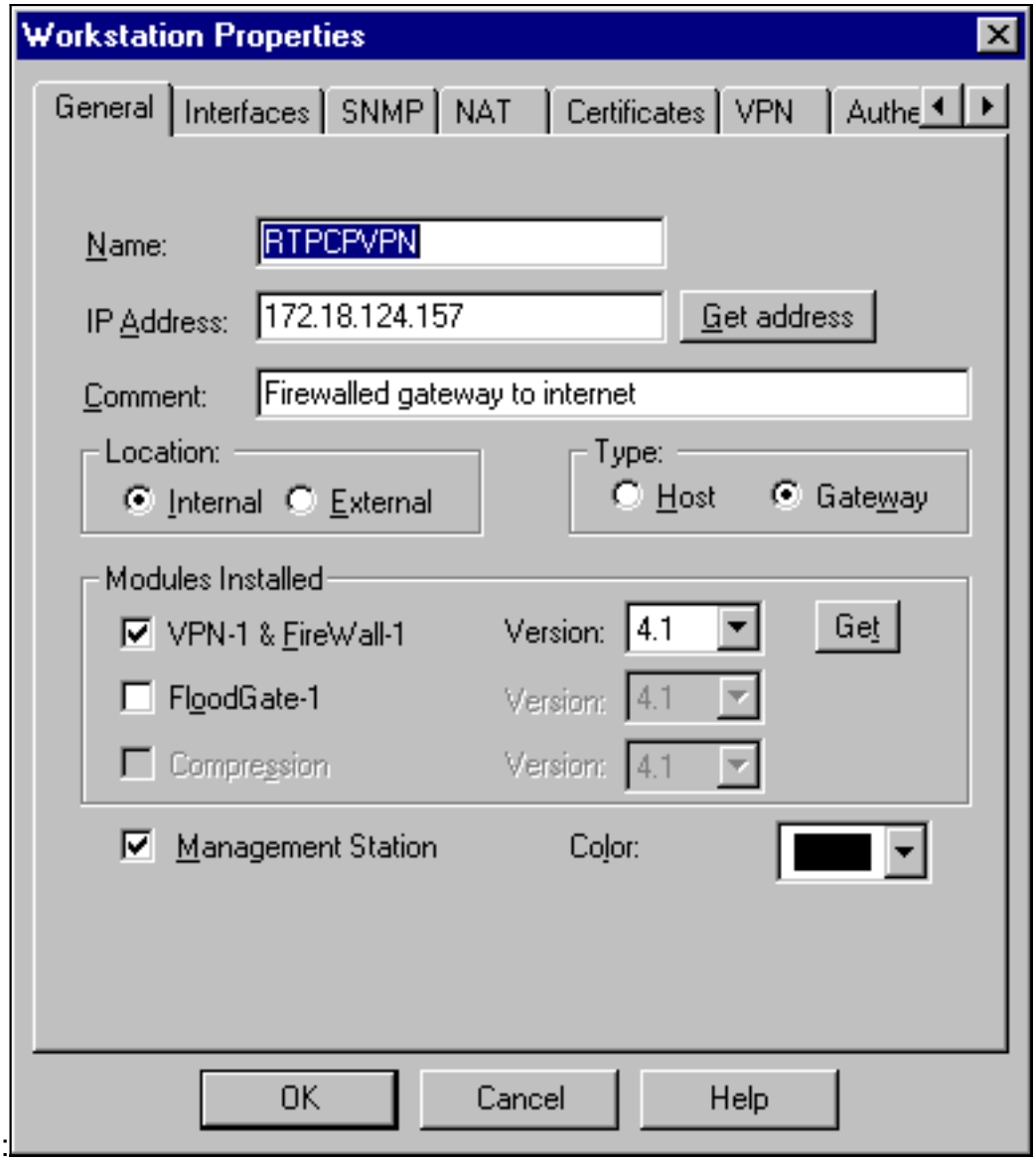


2. Seleccione Manage (Administración) > Network Objects (Objetos de red) > New (o Edit) Nuevo (o Editar) > Network (Red) para configurar el objeto para la red interna ("cpinside") detrás del punto de control.Esto debe estar de acuerdo con el (segunda) red de destino en este comando pix: **access-list 115 permit ip 192.168.1.0 255.255.255.0 10.32.50.0**



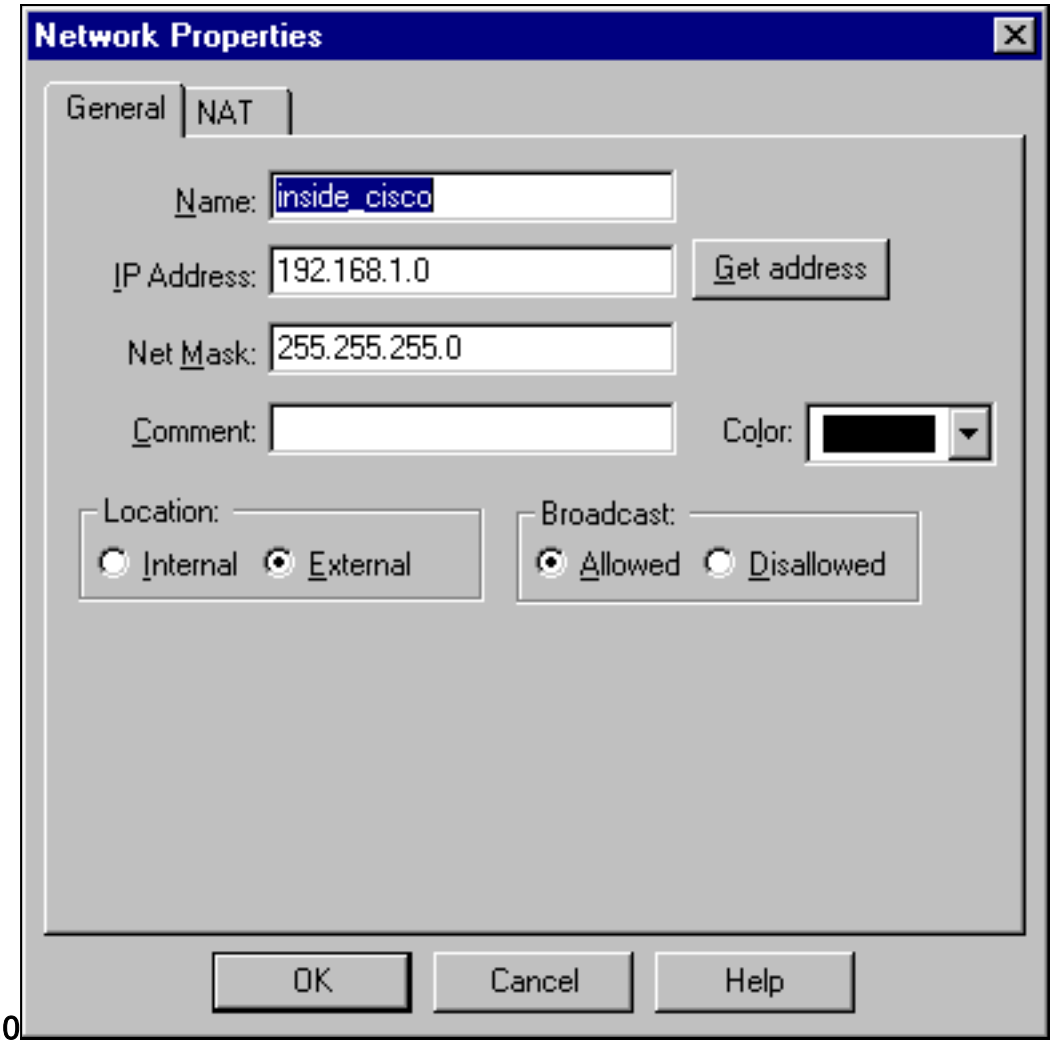
255.255.255.0

3. Seleccione **Manage > Network Objects > Edit** para editar el objeto para el punto final del gateway (punto de verificación “RTPCPVPN”) ese las puntas PIX en a este comando: **crypto map name # set peer ip_address**En Location (Ubicación), seleccione Internal (Interna). En Type (Tipo), seleccione Gateway. Bajo los módulos instalados, seleccione el checkbox el **VPN-1 y FireWall-1**, y también seleccione el checkbox de la **estación de**



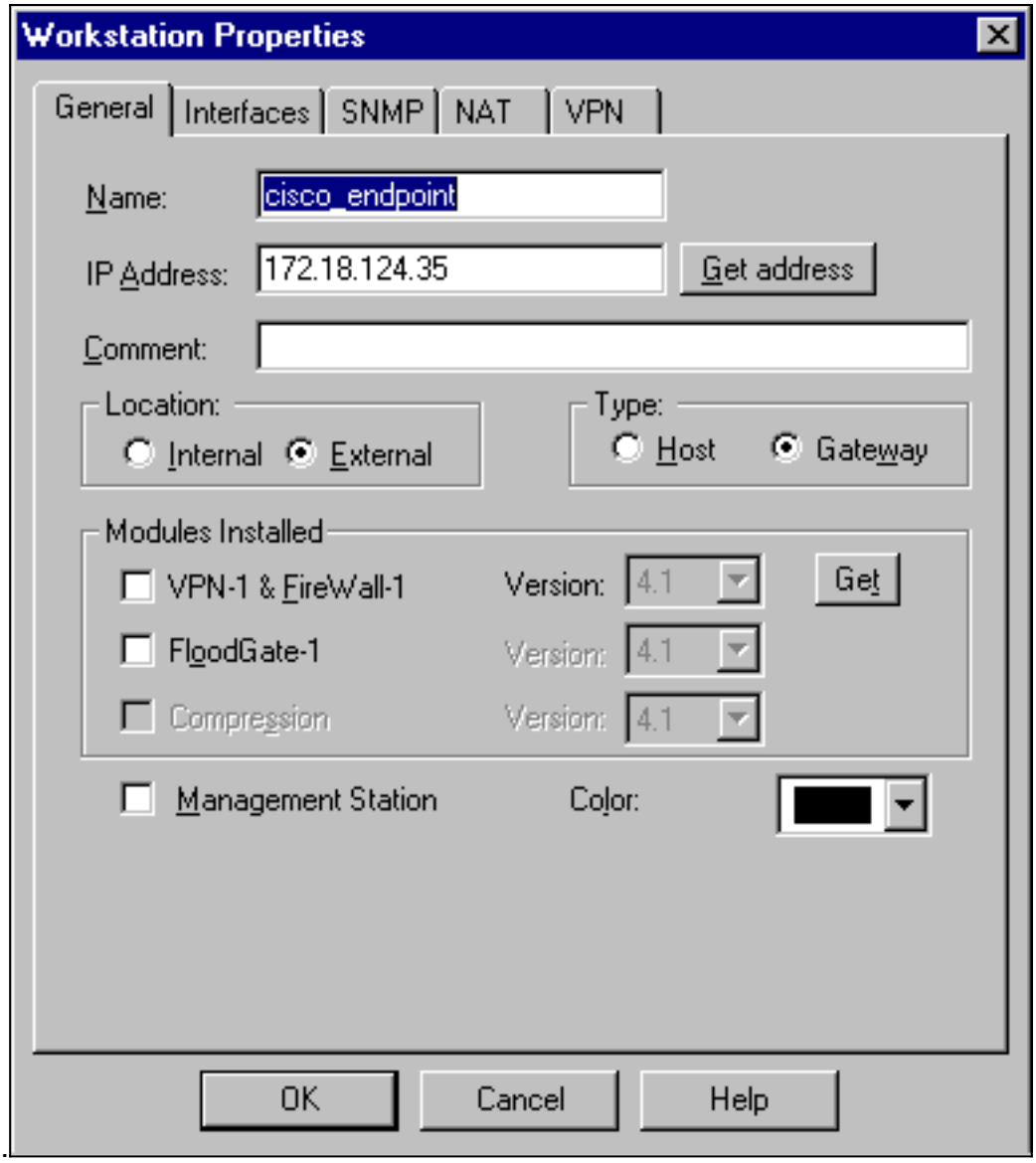
administración:

4. Seleccione **Manage > Network Objects > New > Network** para configurar el objeto para (“inside_cisco”) la red externa detrás del PIX.Esto debe estar de acuerdo con la primera) red de la fuente (en este comando pix: **access-list 115 permit ip 192.168.1.0 255.255.255.0 10.32.50.0**



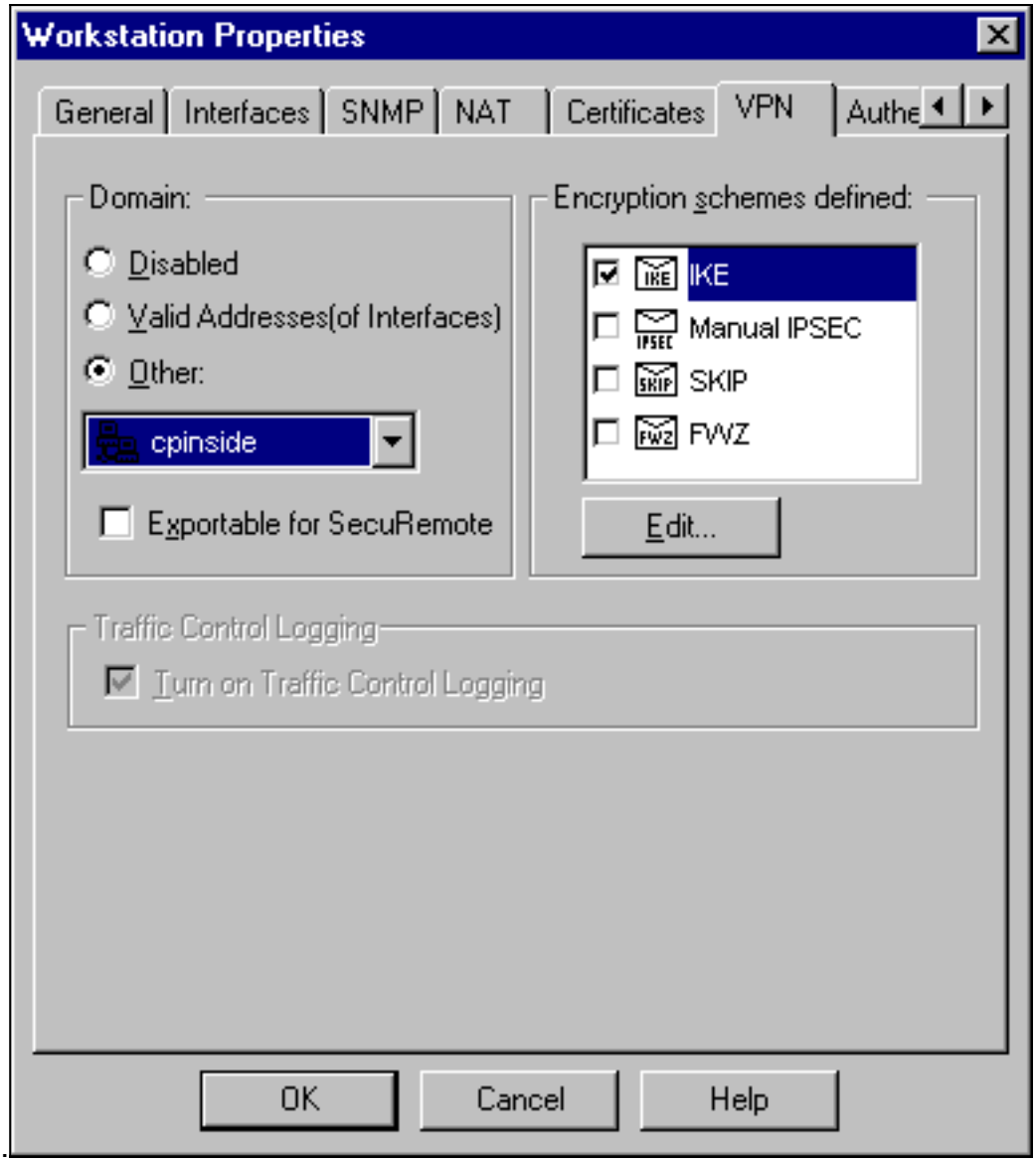
255.255.255.0

5. Seleccione Manage (Administrar) > Network objects (Objetos de la red) > New (Nuevo) > Workstation (Estación de trabajo) para agregar un objeto para el gateway PIX externa ("cisco_endpoint"). Ésta es la interfaz PIX a la cual este comando es aplicado: **interfaz del nombre de correspondencia de criptografía afuera**En Location (Ubicación), seleccione External (Externa). En Type (Tipo), seleccione Gateway.**Nota:** No seleccione el checkbox



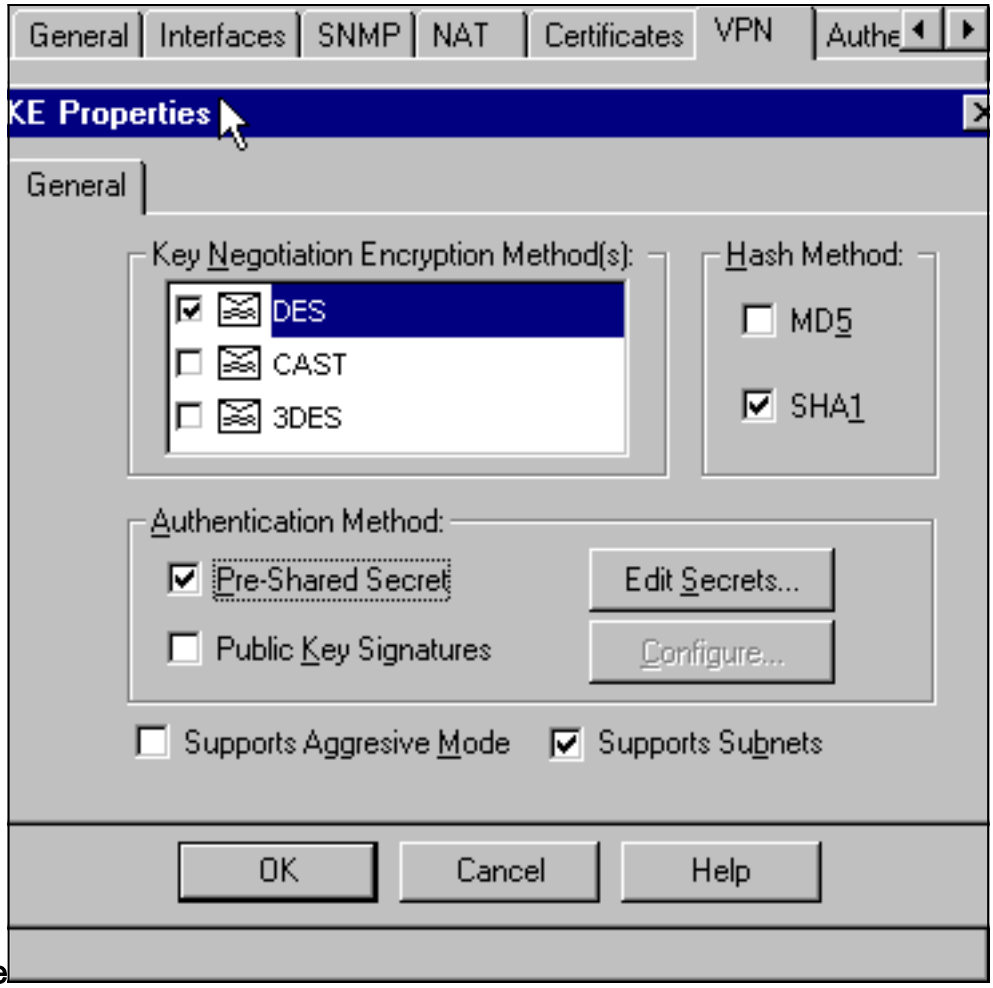
VPN-1/FireWall-1.

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



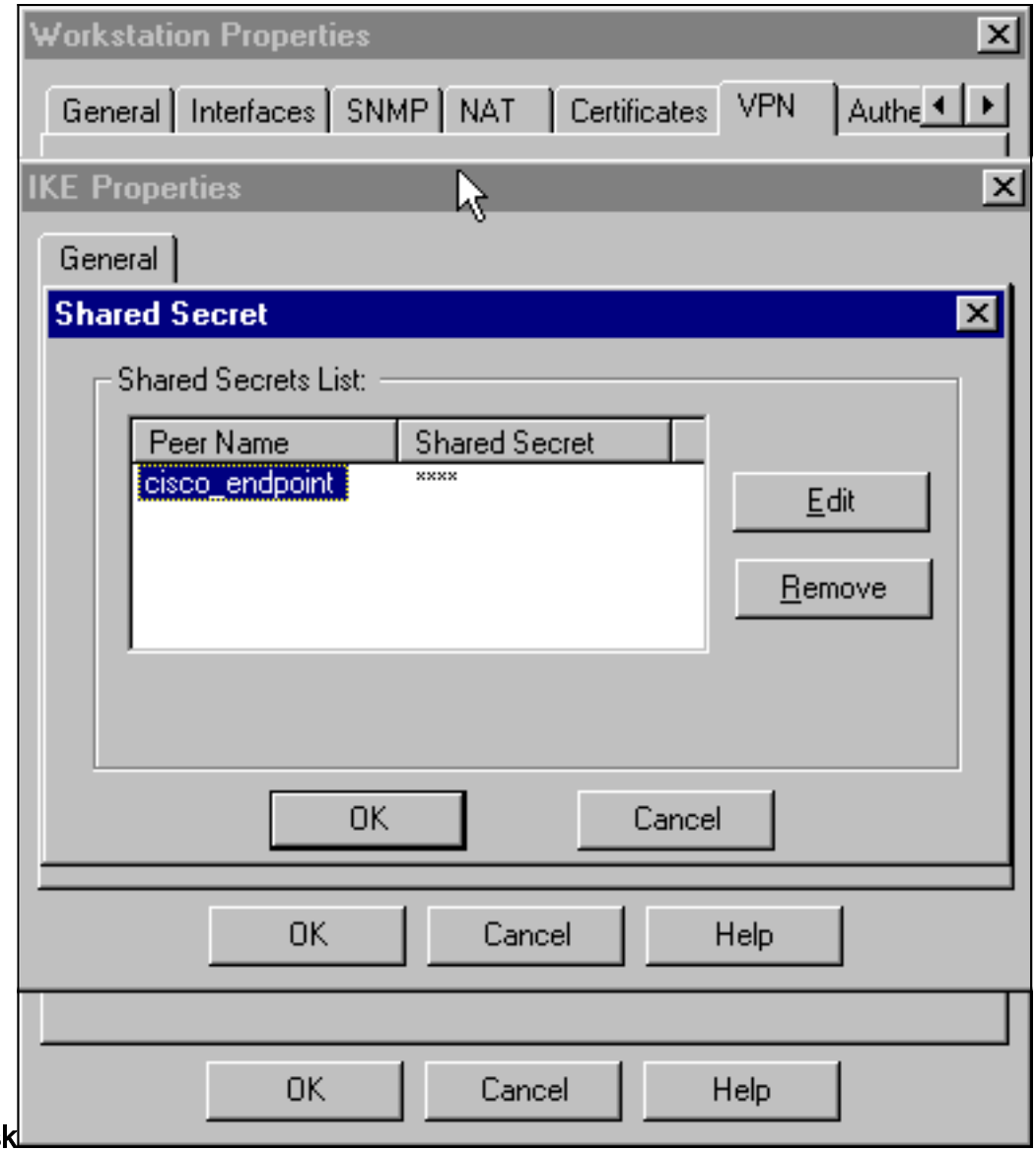
(Editar).

7. Cambie las propiedades IKE para la encripción de DES para estar de acuerdo con este comando:**isakmp policy # encryption des**
8. Cambie las propiedades IKE al picado SHA1 para estar de acuerdo con este comando:**isakmp policy # hash sha**Cambie estas configuraciones:Cancelar la selección del modo agresivoSeleccione el checkbox de las **subredes de los soportes**.Bajo método de autentificación, seleccione el checkbox del **Secreto previamente compartido**. Esto está de acuerdo con este comando:**isakmp policy # authentication pre-**



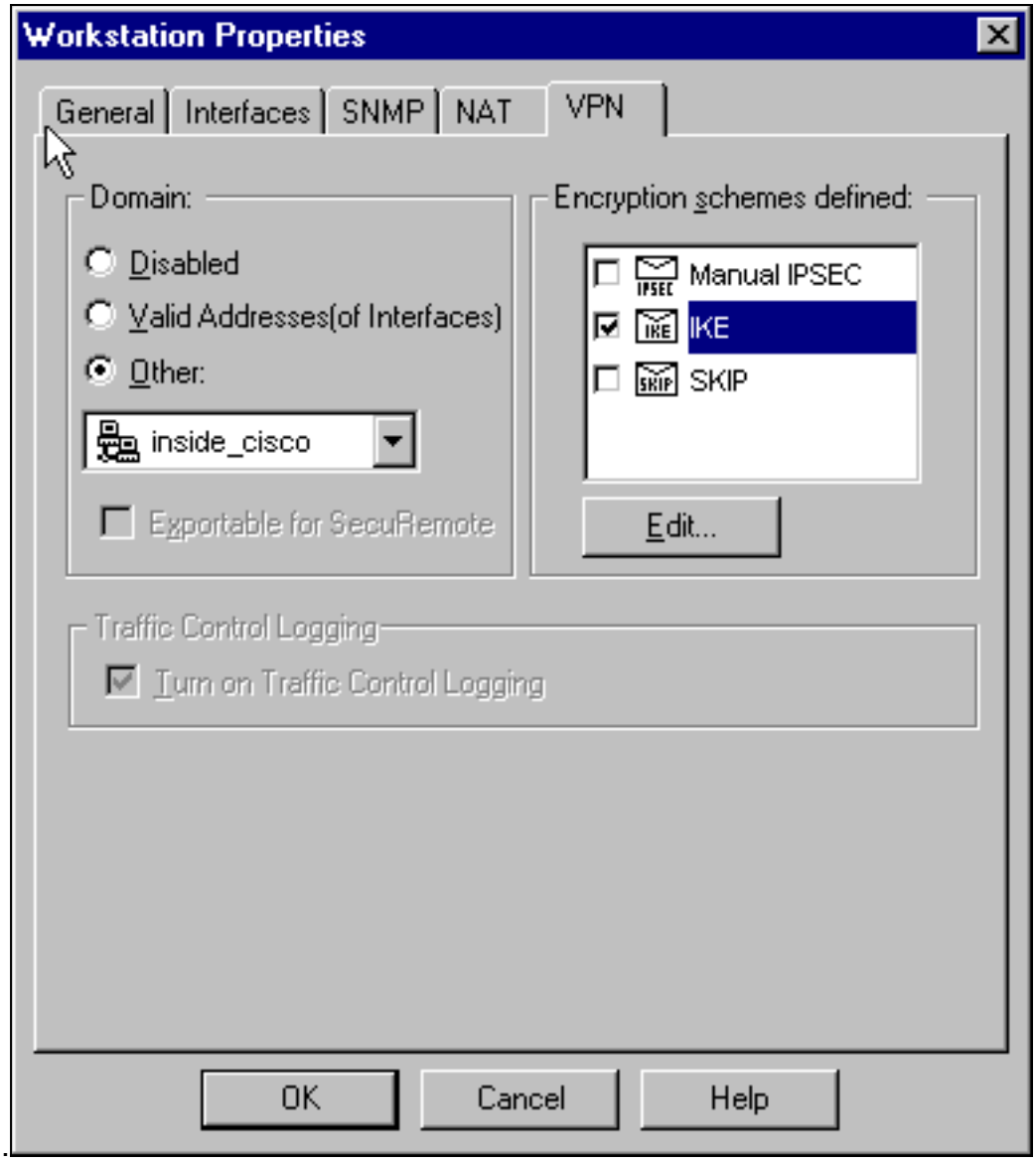
share

9. El tecleo **edita los secretos** para fijar la clave previamente compartida para estar de acuerdo con el comando pix:**isakmp key key address address netmask**



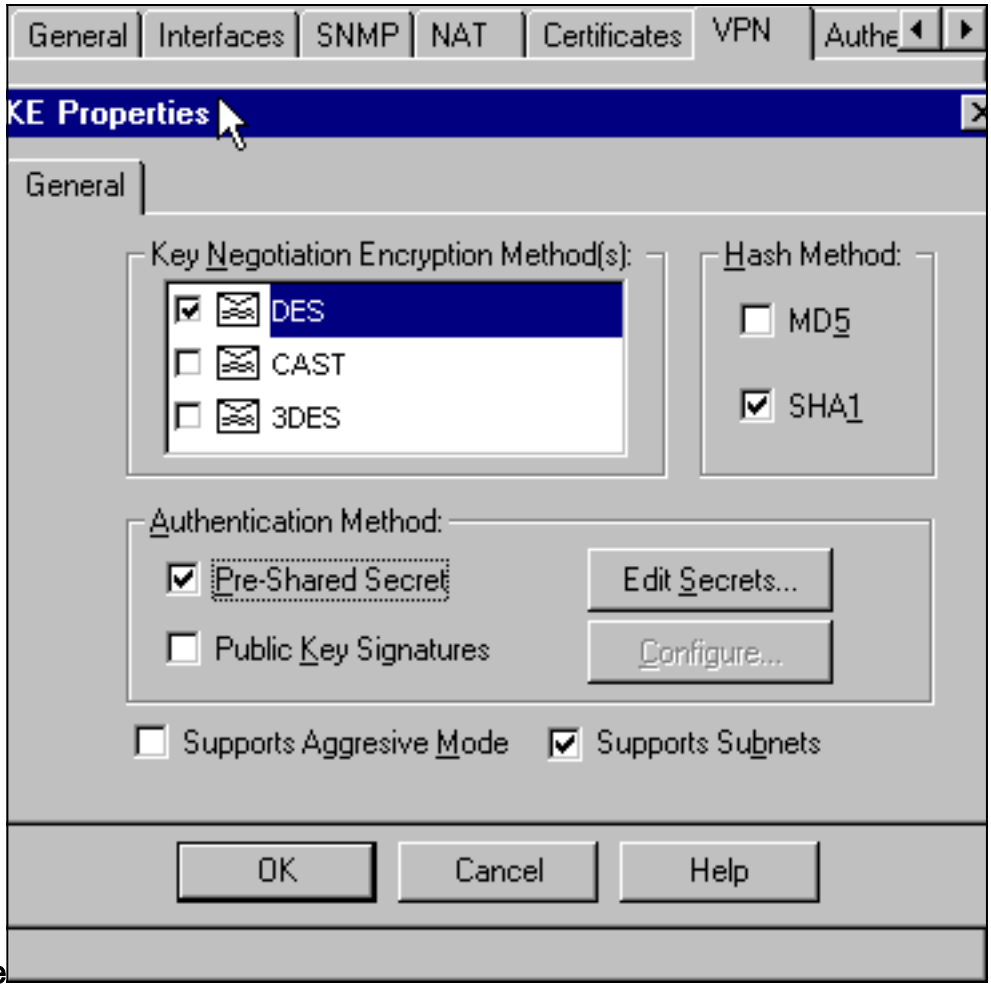
netmask

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



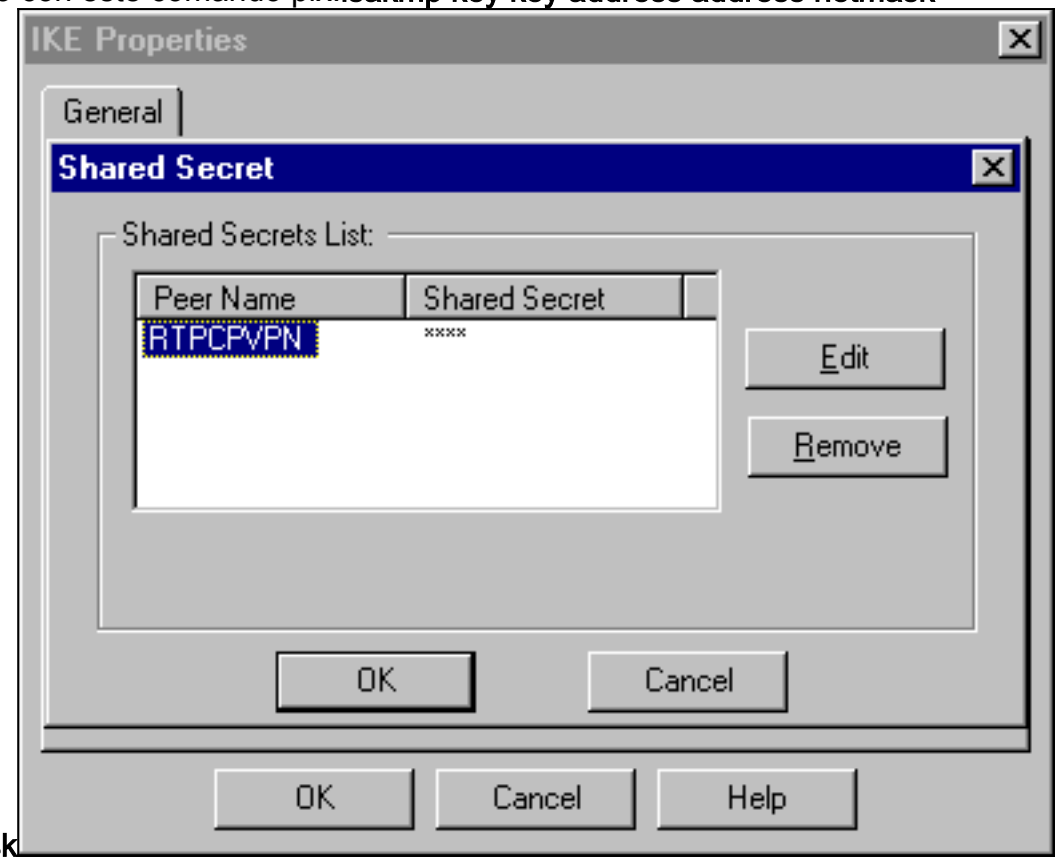
(Editar).

11. Cambie la encripción de DES de las propiedades IKE para estar de acuerdo con este comando:**isakmp policy # encryption des**
12. Cambie las propiedades IKE al picado SHA1 para estar de acuerdo con este comando:**crypto isakmp policy # hash sha**Cambie estas configuraciones:Cancelar la selección del modo agresivoSeleccione el checkbox de las **subredes de los soportes**.Bajo método de autentificación, seleccione el checkbox del **Secreto previamente compartido**. Esta acción está de acuerdo con este comando:**isakmp policy # authentication pre-**



share

13. El tecleo **edita los secretos** para fijar la clave previamente compartida para estar de acuerdo con este comando pix:**isakmp key key address address netmask**

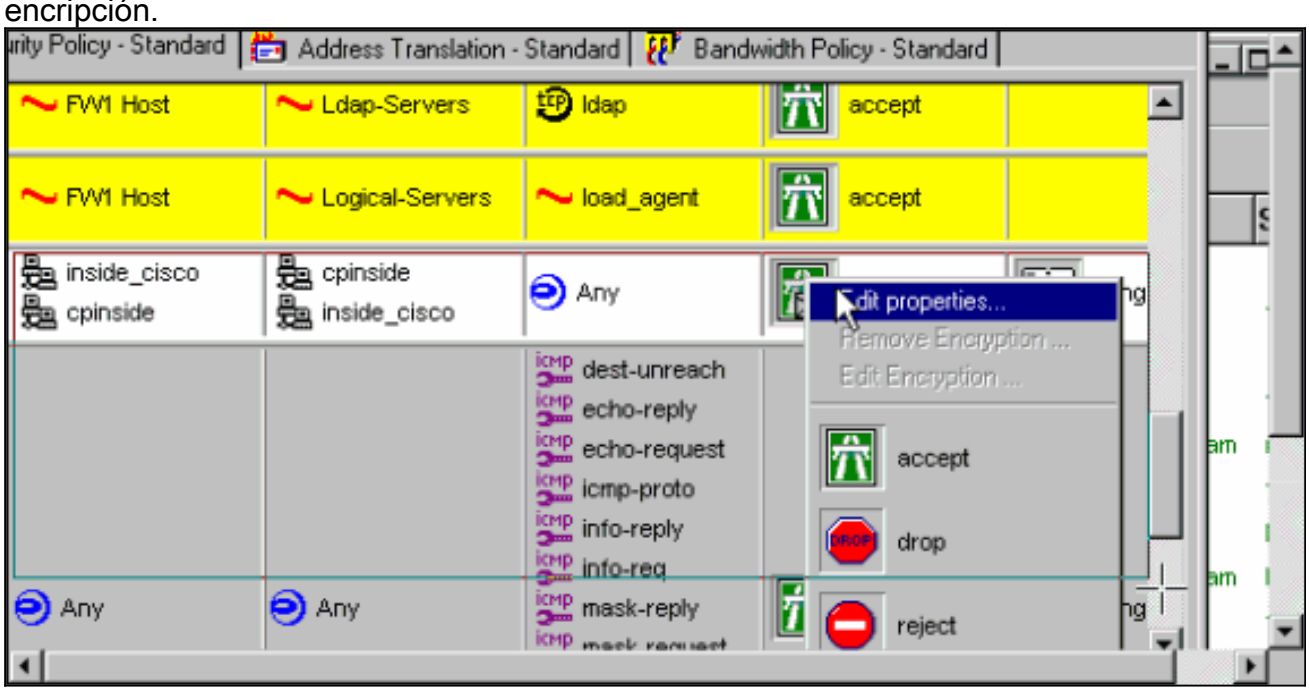


netmask

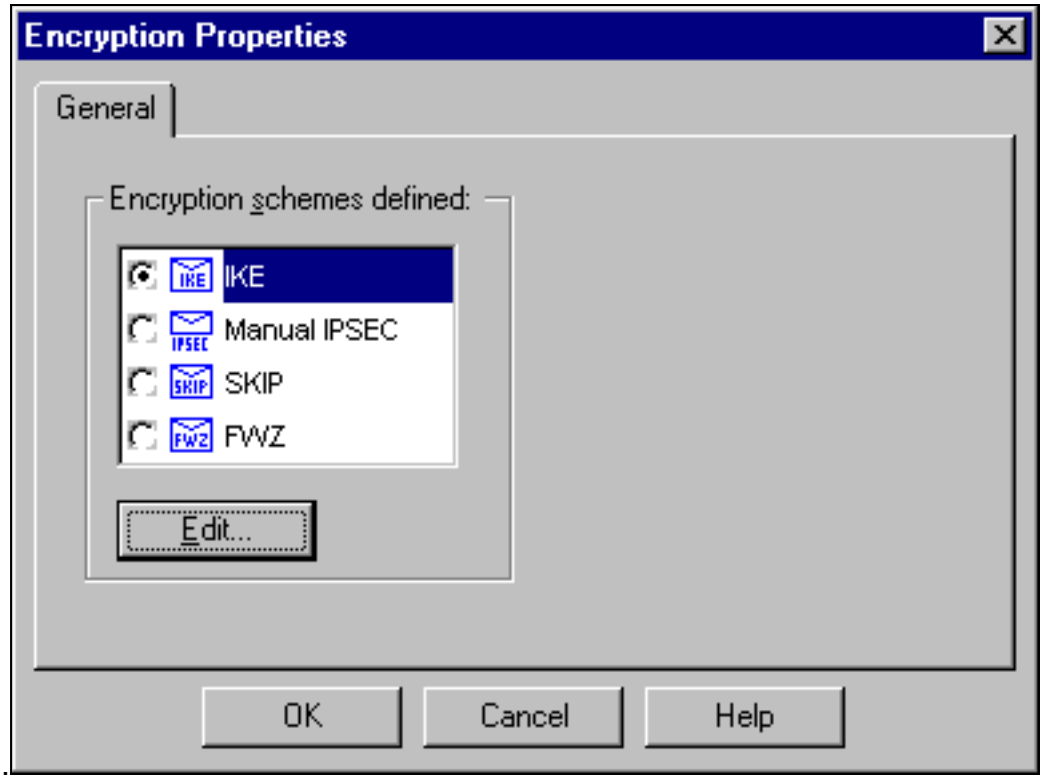
14. En la ventana del editor de políticas, ingrese una ventana tanto con el origen como con el destino, como en "inside_cisco" y "cpinside" (bidireccional). Set Service=Any, Action=Encrypt, y

Track=Long.

15. Bajo título de la acción, haga clic el verde **cifran el** icono y lo seleccionan **Edit Properties** para configurar las políticas de encripción.

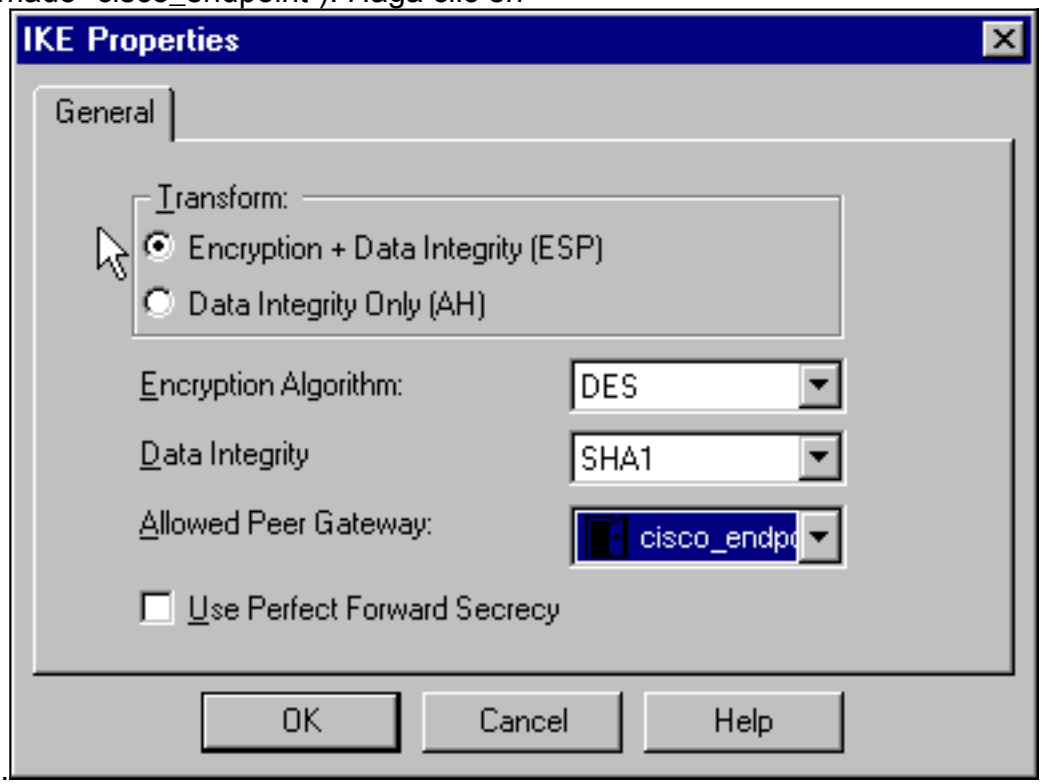


16. Seleccione IKE y luego haga clic en Edit



(Editar).

17. En las propiedades IKE defienda, cambie estas propiedades para estar de acuerdo con el IPSec de PIX transforma en este comando:**crypto ipsec transform-set myset esp-des esp-sha-hmac**En Transform (Transformar), seleccione Encryption (Encriptación) + Data Integrity (ESP) (Integridad de datos (ESP)). El algoritmo de encripción debe ser **DES**, integridad de los datos debe ser **SHA1**, y el gateway de peer permitido debe ser el gateway PIX externo (llamado “cisco_endpoint”). Haga clic en



OK.

18. Después de que se configure el punto de verificación, la **directiva** selecta **> instala** en el menú de punto de control para que los cambios tomen el efecto.

comandos debug, show y clear

En esta sección encontrará información que puede utilizar para confirmar que su configuración esté funcionando correctamente.

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

Antes de ejecutar un comando de depuración, consulte Información importante sobre comandos de depuración.

Cisco PIX Firewall

- debug crypto engine - Mostrar mensajes de depuración acerca del motor de criptografía, que realiza el encripción y el desencripción.
- debug crypto isakmp - Muestra mensajes acerca de eventos IKE.
- debug crypto ipsec—Muestra eventos de IPSec.
- show crypto isakmp sa: Ver todas las asociaciones actuales de seguridad IKE (SAs) de un par.
- show crypto ipsec sa - Muestra las configuraciones usadas por las asociaciones de seguridad actuales.
- **clear crypto isakmp sa** — (del modo de configuración) borre todas las conexiones del IKE activo.
- **clear crypto ipsec sa** — (del modo de configuración) borre todas las asociaciones de seguridad IPSec.

Punto de control

Porque el seguimiento fue fijado para de largo adentro la ventana de editor de políticas mostrada en el paso 14, el tráfico denegado aparece en el rojo en el Log Viewer. Un debug más prolijo puede ser obtenido ingresando:

```
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: Esto era una instalación del Microsoft Windows NT.

Usted puede borrar los SA en el punto de verificación con estos comandos:

```
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
```

¿y de contestación **sí** en es usted seguro? mensaje

Troubleshooting

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

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 puede resumirlas automáticamente con respecto al tráfico interesante. Si el ACL crypto en el PIX no se configura para hacer juego, el túnel falla probablemente. 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.

Ejemplo de resultado de depuración de PIX

```
cisco_endpoint# show debug debug crypto ipsec 1 debug crypto isakmp 1 debug crypto engine debug
fover status tx Off rx Off open Off cable Off txdmp Off rxdmp Off ifc Off rxip Off txip Off get
Off put Off verify Off switch Off fail Off fmsg Off cisco_endpoint# term mon cisco_endpoint#
ISAKMP (0): beginning Quick Mode exchange, M-ID of 2112882468:7df00724IPSEC(key_engine): got a
queue event... IPSEC(spi_response): getting spi 0x9d71f29c(2641490588) for SA from
172.18.124.157 to 172.18.124.35 for prot 3 70 crypto_isakmp_process_block: src 172.18.124.157,
dest 172.18.124.35 OAK_QM exchange oakley_process_quick_mode: OAK_QM_IDLE ISAKMP (0): processing
SA payload. message ID = 2112882468 ISAKMP : Checking IPSec proposal 1 ISAKMP: transform 1,
ESP_DES ISAKMP: attributes in transform: ISAKMP: encaps is 1 ISAKMP: SA life type in seconds
ISAKMP: SA life duration (basic) of 28800 ISAKMP: SA life type in kilobytes ISAKMP: SA life
duration (VPI) of 0x0 0x46 0x50 0x0 ISAKMP: authenticator is HMAC-SHA ISAKMP (0): atts are
acceptable.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 ISAKMP (0):
processing NONCE payload. message ID = 2112882468 ISAKMP (0): processing ID payload. message ID
= 2112882468 ISAKMP (0): processing ID payload. message ID = 2112882468map_alloc_entry:
allocating entry 3 map_alloc_entry: allocating entry 4 ISAKMP (0): Creating IPSec SAs inbound SA
from 172.18.124.157 to 172.18.124.35 (proxy 10.32.50.0 to 192.168.1.0) has spi 2641490588 and
conn_id 3 and flags 4 lifetime of 28800 seconds lifetime of 4608000 kilobytes outbound SA from
172.18.124.35 to 172.18.124.157 (proxy 192.168.1.0 to 10.32.50.0) has spi 3955804195 and conn_id
4 and flags 4 lifetime of 28800 seconds lifetime of 4608000 kilobytesIPSEC(key_engine): got a
queue event... 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=
28800s and 4608000kb, spi= 0x9d71f29c(2641490588), conn_id= 3, keysize= 0, flags= 0x4
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= 28800s and 4608000kb, spi=
0xebc8c823(3955804195), conn_id= 4, keysize= 0, flags= 0x4 return status is IKMP_NO_ERROR2303:
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= 28800s and 4608000kb, spi= 0x0(0),
conn_id= 0, keysize= 0, flags= 0x4004 602301: sa created, (sa) sa_dest= 172.18.124.35, sa_prot=
50, sa_spi= 0x9d71f29c(2641490588), sa_trans= esp-des esp-sha-hmac , sa_conn_id= 3 602301: sa
created, (sa) sa_dest= 172.18.124.157, sa_prot= 50, sa_spi= 0xebc8c823(3955804195), sa_trans=
esp-des esp-sha-hmac , sa_conn_id= 4 cisco_endpoint# sho cry ips sa interface: outside Crypto
map tag: rtpmap, 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): (0.0.0.0/0.0.0.0/0/0)
current_peer: 172.18.124.157 PERMIT, flags={origin_is_acl,} #pkts encaps: 0, #pkts encrypt: 0,
#pkts digest 0 #pkts decaps: 0, #pkts decrypt: 0, #pkts verify 0 #pkts compressed: 0, #pkts
decompressed: 0 #pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0 local crypto endpt.: 172.18.124.35, remote crypto endpt.:
172.18.124.157 path mtu 1500, ipsec overhead 0, media mtu 1500 current outbound spi: 0 inbound
esp sas: inbound ah sas: inbound pcp sas: outbound esp sas: outbound ah sas: outbound pcp sas:
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: 4, #pkts encrypt: 4, #pkts digest 4 #pkts decaps: 4, #pkts
decrypt: 4, #pkts verify 4 #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, ipsec overhead 56,
media mtu 1500 current outbound spi: ebc8c823 inbound esp sas: spi: 0x9d71f29c(2641490588)
transform: esp-des esp-sha-hmac , in use settings ={Tunnel, } slot: 0, conn id: 3, crypto map:
```

```
rtpmap sa timing: remaining key lifetime (k/sec): (4607999/28777) IV size: 8 bytes replay
detection support: Y inbound ah sas: inbound pcp sas: outbound esp sas: spi:
0xebc8c823(3955804195) transform: esp-des esp-sha-hmac , in use settings ={Tunnel, } slot: 0,
conn id: 4, crypto map: rtpmap sa timing: remaining key lifetime (k/sec): (4607999/28777) IV
size: 8 bytes replay detection support: Y outbound ah sas: outbound pcp sas: cisco_endpoint# sho
cry is sa dst src state pending created 172.18.124.157 172.18.124.35 QM_IDLE 0 2
```

Información Relacionada

- Página de Soporte de PIX
- Referencia de Comandos PIX
- Solicitudes de Comentarios (RFC)
- Configuración de seguridad de red IPSec
- Configuración del protocolo de seguridad de intercambio de claves de Internet
- PIX 5.2: Configuración del IPSec
- PIX 5.3: Configuración del IPSec
- Página de soporte de IPSec
- Soporte Técnico - Cisco Systems