Configuración de un túnel IPSec - Firewall PIX seguro de Cisco para el firewall Checkpoint 4.1

Contenido

Introducción
Prerequisites
Requirements
Componentes Utilizados
Convenciones
Configurar
Diagrama de la red
Configuraciones
Punto de control de Firewall
comandos debug, show y clear
Cisco PIX Firewall
Punto de control
Troubleshoot
Resumen de la red
Ejemplo de resultado de depuración de PIX
Información Relacionada

Introducción

Esta configuración de ejemplo muestra cómo formar un túnel IPSec con 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 supone que el tráfico desde dentro del PIX y dentro del Firewall del punto de control 4.1 a Internet (representado aquí por las redes 172.18.124.X) fluye antes de comenzar esta configuración.

Prerequisites

Requirements

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Convenciones

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

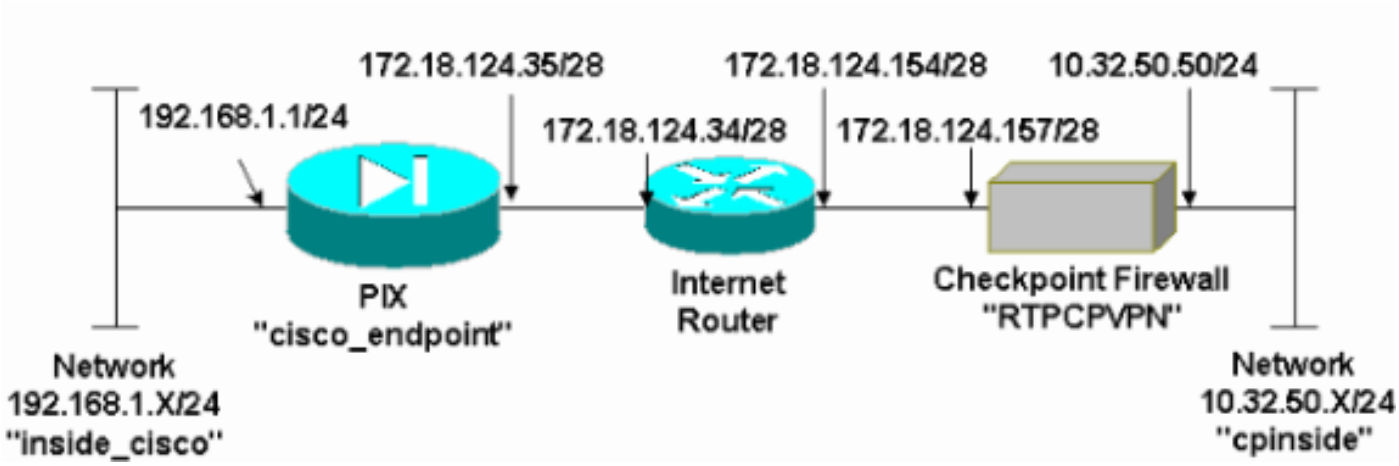
Configurar

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

Nota: Para encontrar información adicional sobre los comandos usados en este documento, utilice la Command Lookup Tool (sólo 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 que se muestran en esta sección.

Configuración de PIX

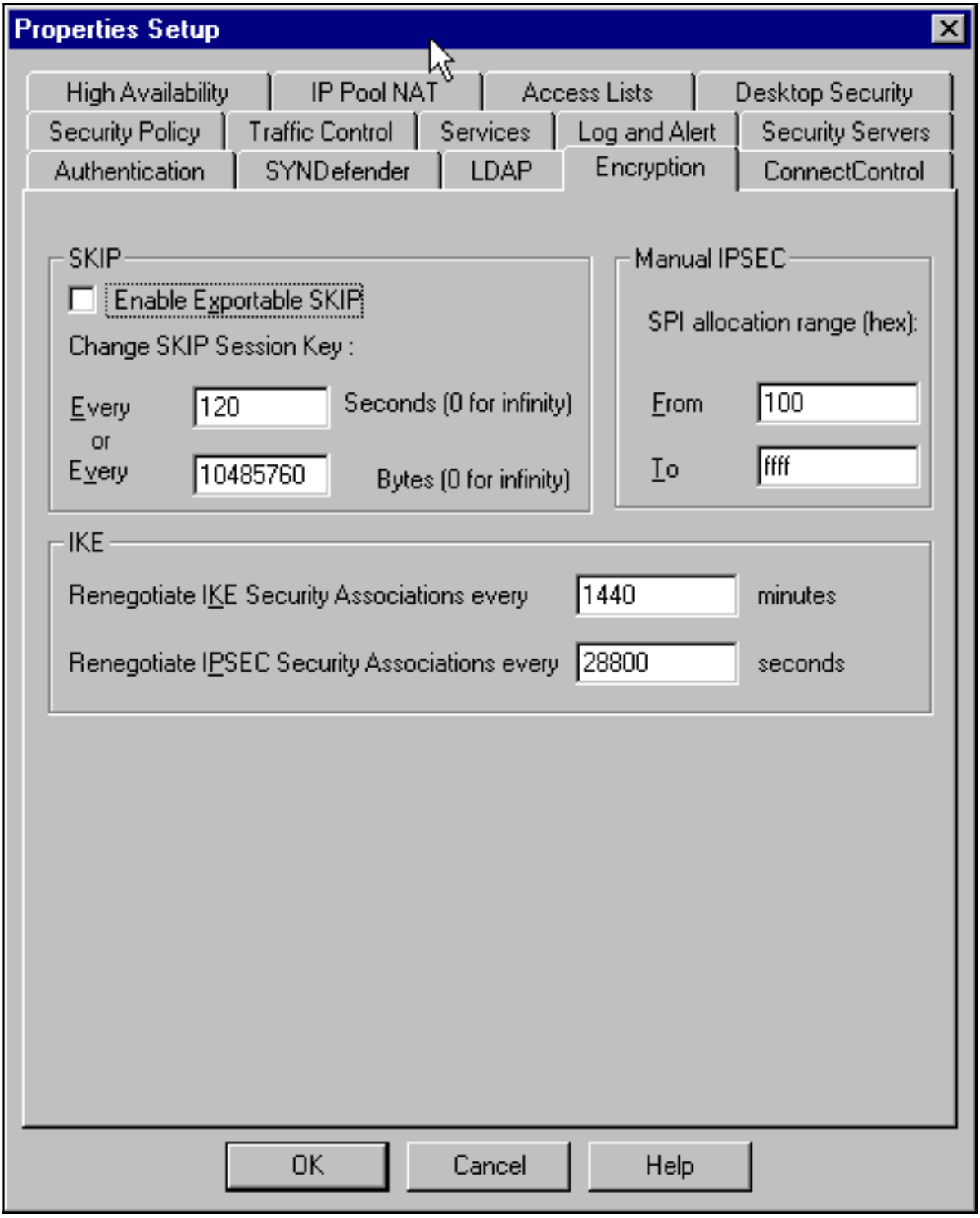
```
PIX Version 5.3(1)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname cisco_endpoint
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 1720
```

```
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
```

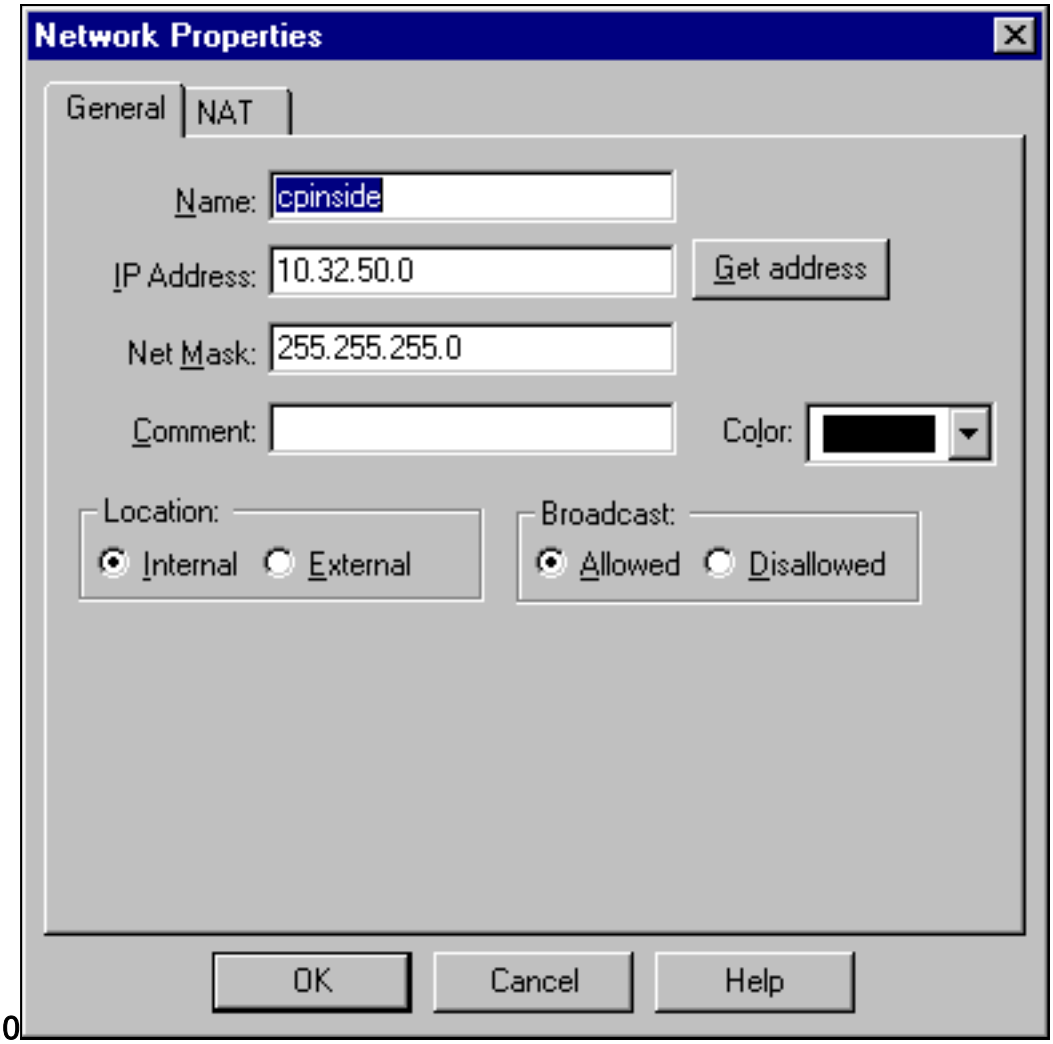
```
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption des
isakmp policy 10 hash sha
isakmp policy 10 group 1
isakmp policy 10 lifetime 86400
telnet timeout 5
ssh timeout 5
terminal width 80
Cryptochecksum:dc43c44e4513d3633a3fc7b1c3802c79
: end
[OK]
```

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.La duración IKE predeterminada de PIX es 86400 segundos (=1440 minutos), modificable por este comando: **isakmp policy # lifetime 86400**La duración de PIX IKE puede configurarse entre 60-86400 segundos.La duración predeterminada de IPSec de PIX es 28800 segundos, modificable por este comando: **crypto ipsec security-association lifetime seconds #**Puede configurar una duración de IPSec PIX entre 120-86400 segundos.

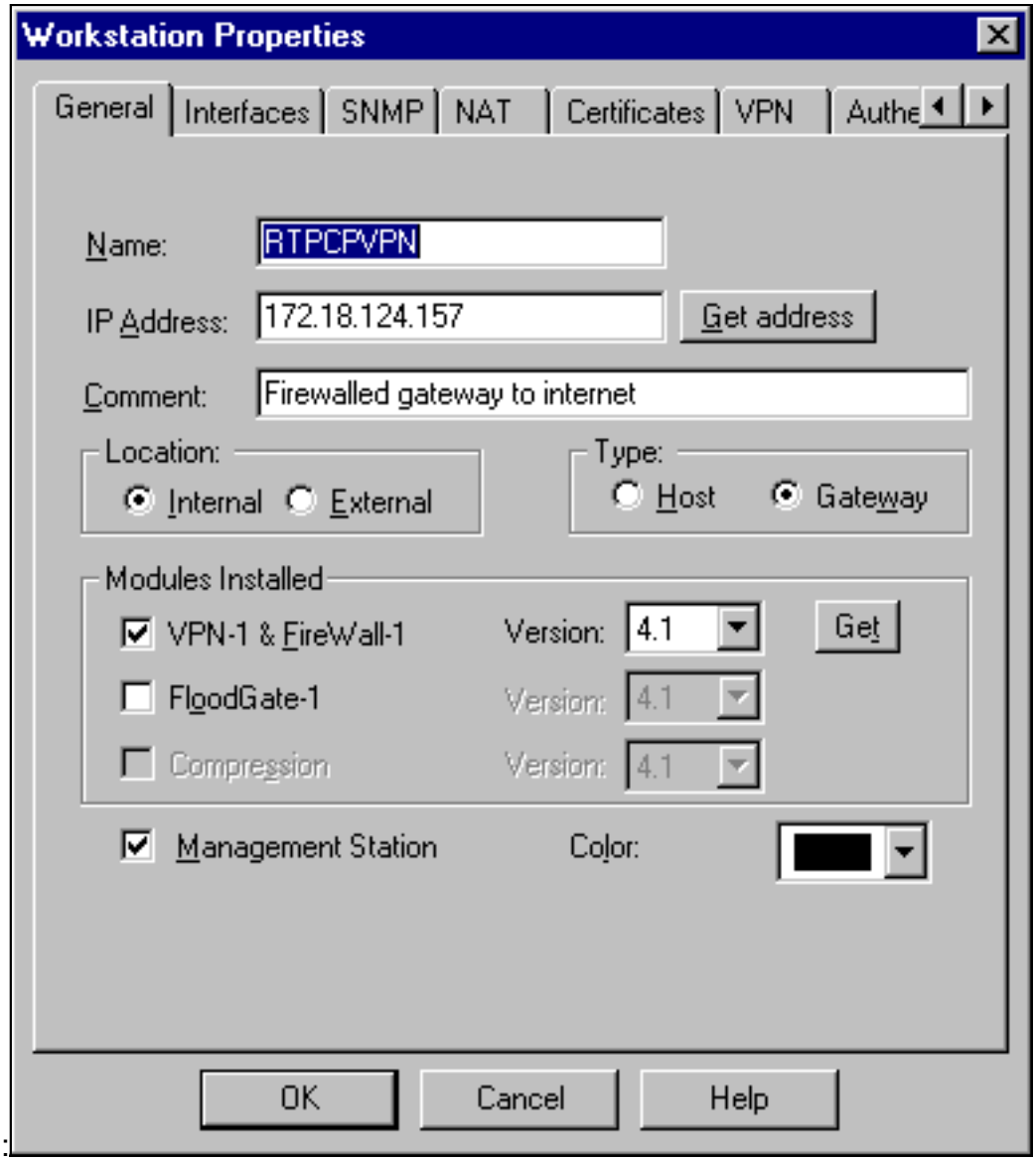


2. Seleccione Manage (Administración) > Network Objects (Objetos de red) > New (o Edit) Nuevo (o Editar) > Network (Red) para configurar el objeto para la red interna ("cpinside") detrás del punto de control.Esto debe coincidir con la red de destino (segunda) en este comando PIX: **access-list 115 permit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



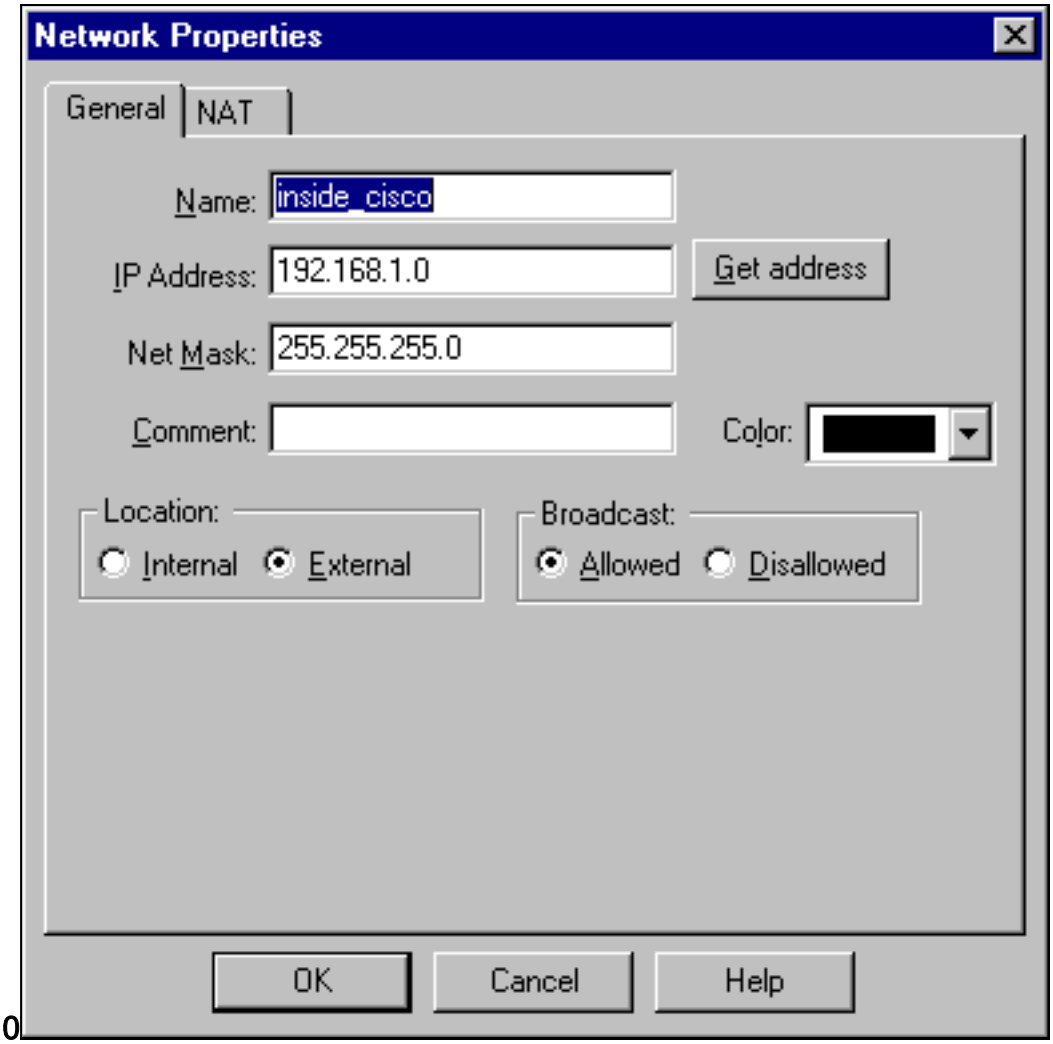
255.255.255.0

3. Seleccione **Manage > Network Objects > Edit** para editar el objeto para el punto de control de gateway ("RTPCPVPN" Checkpoint) al que el PIX señala en este comando: **crypto map name # set peer ip_address**En Location (Ubicación), seleccione Internal (Interna). En Type (Tipo), seleccione Gateway. En Modules Installed (Módulos instalados), seleccione la casilla de verificación **VPN-1 y FireWall-1**, y también seleccione la **casilla de verificación Management**



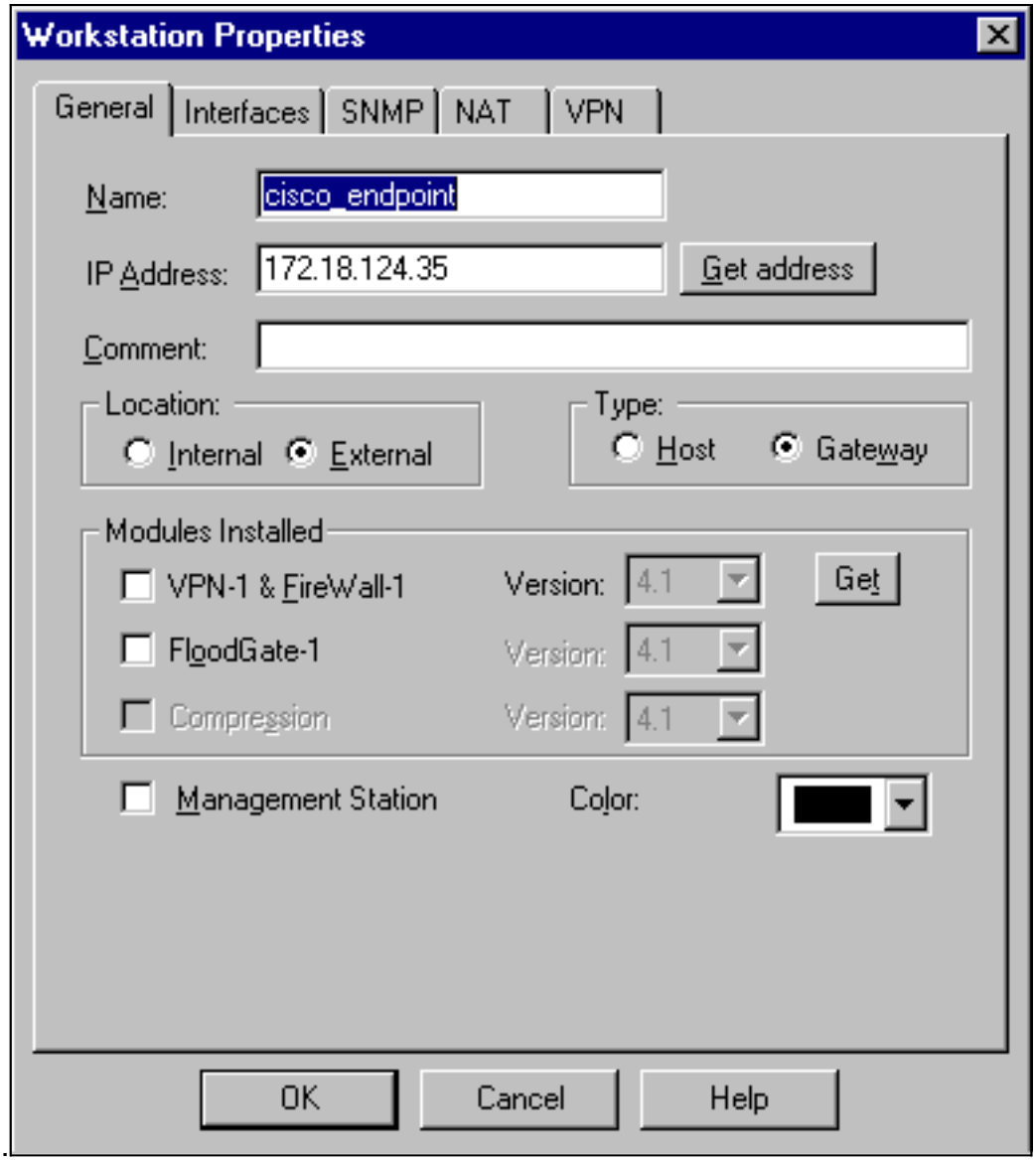
Station:

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



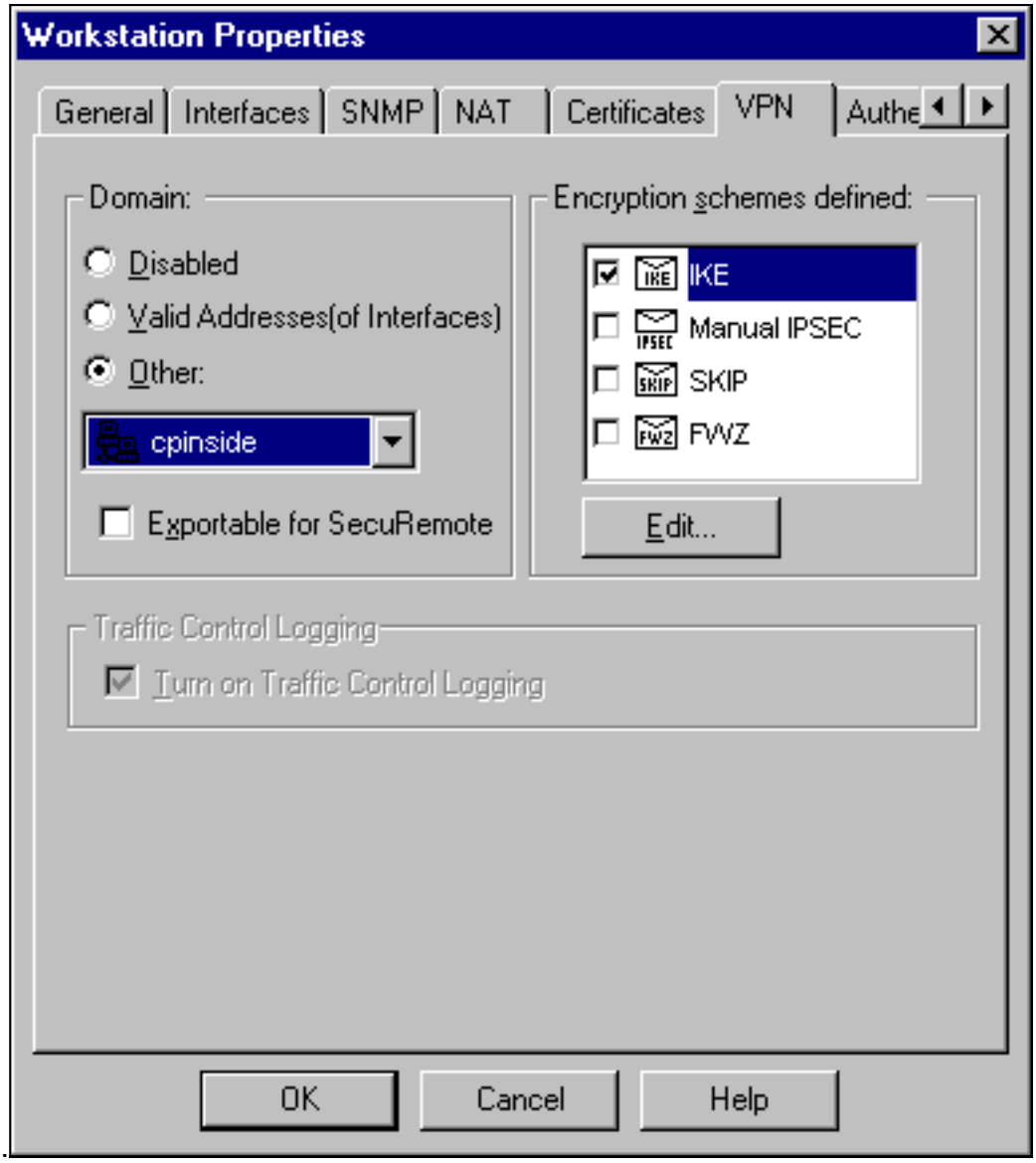
255.255.255.0

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"). Esta es la interfaz PIX a la que se aplica este comando: **interfaz *de nombre de* mapa criptográfico fuera**En Location (Ubicación), seleccione External (Externa). En Type (Tipo), seleccione Gateway.**Nota:** No seleccione la casilla de verificación VPN-



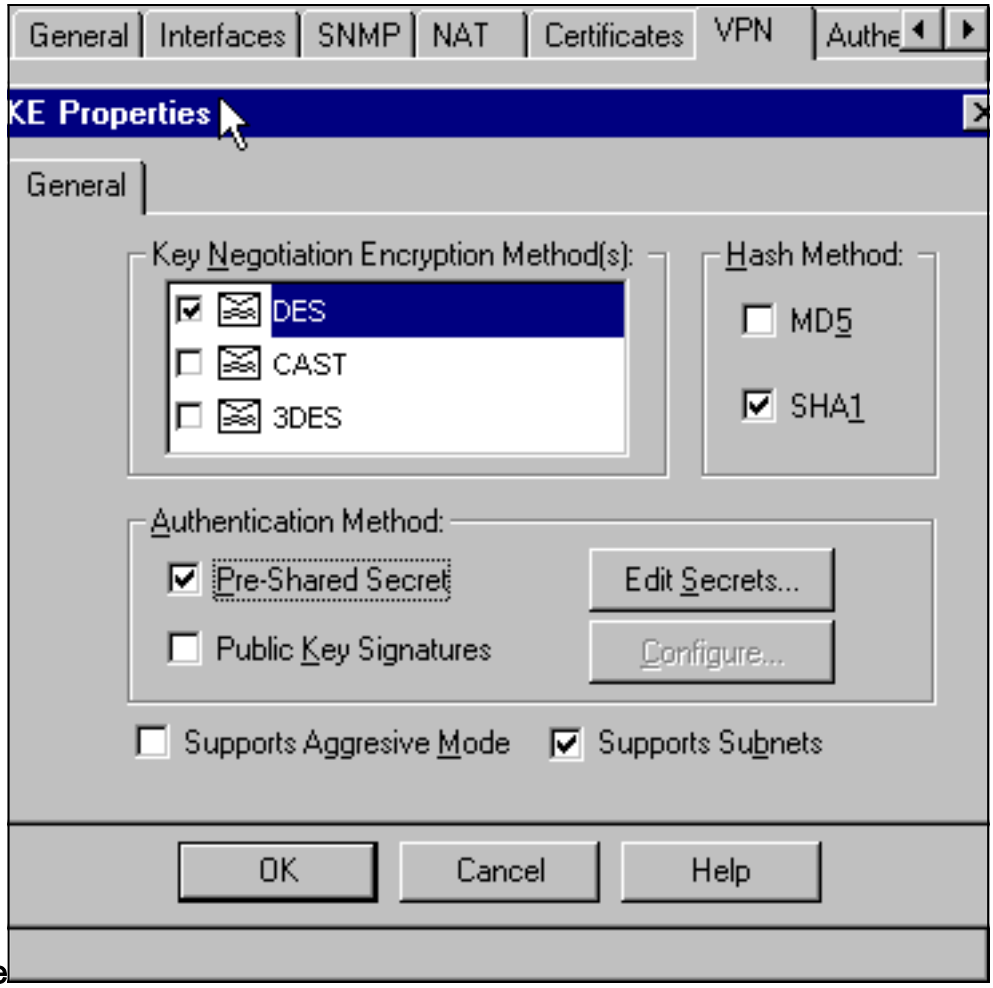
1/FireWall-1.

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



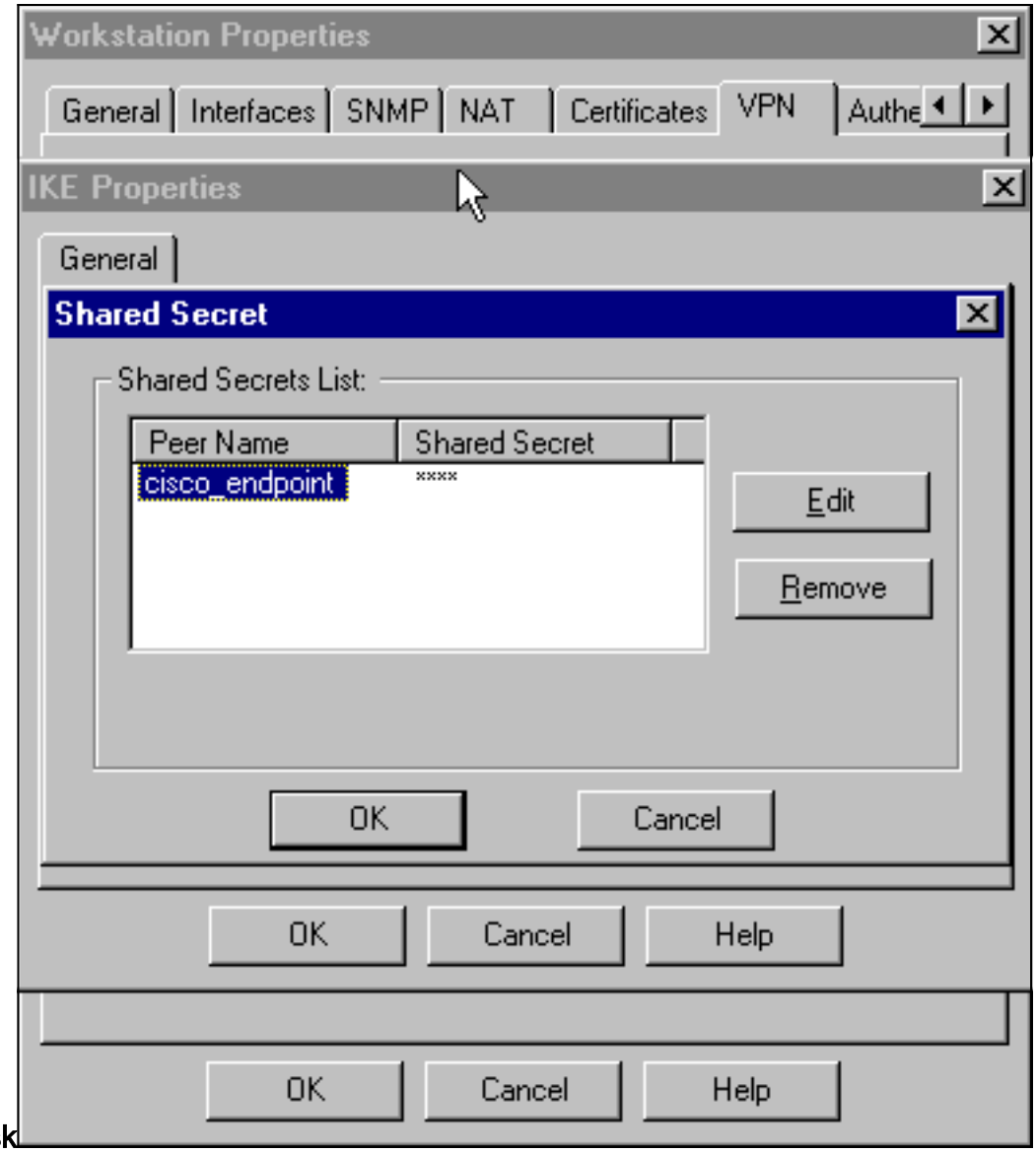
(Editar).

7. Cambie las propiedades IKE para el cifrado DES para coincidir con este comando:**isakmp policy # encryption des**
8. Cambie las propiedades IKE a Hashing SHA1 para coincidir con este comando:**isakmp policy # hash sha**Cambie esta configuración:Cancelar la selección del modo agresivoSeleccione la casilla de verificación **Support Subnets** .En Método de autenticación, seleccione la casilla de verificación **Pre-Shared Secret** . Esto coincide con este comando:**isakmp policy # authentication pre-**



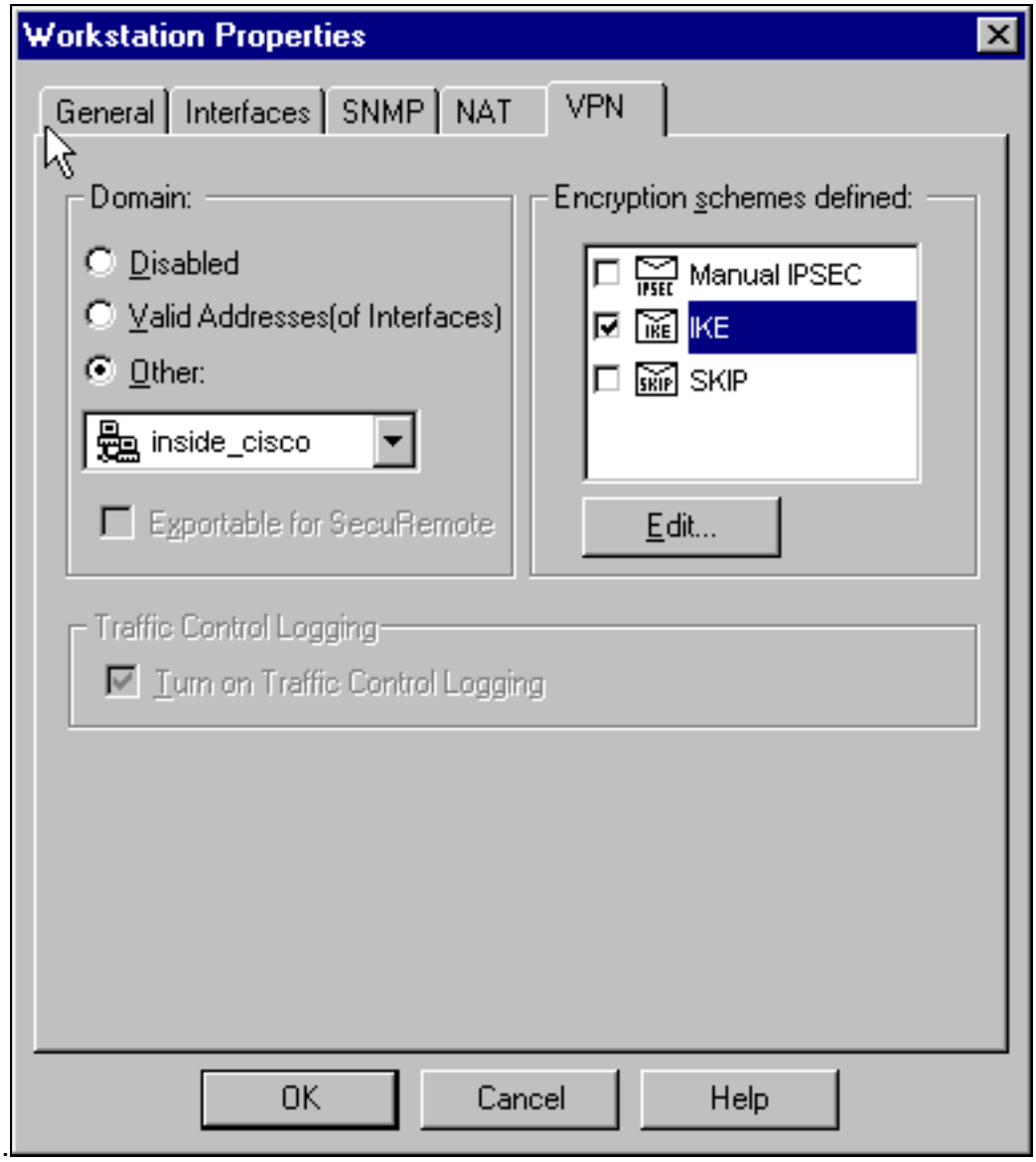
share

9. Haga clic en **Editar secretos** para configurar la clave previamente compartida para que coincida con el comando PIX:**isakmp key key address address netmask**



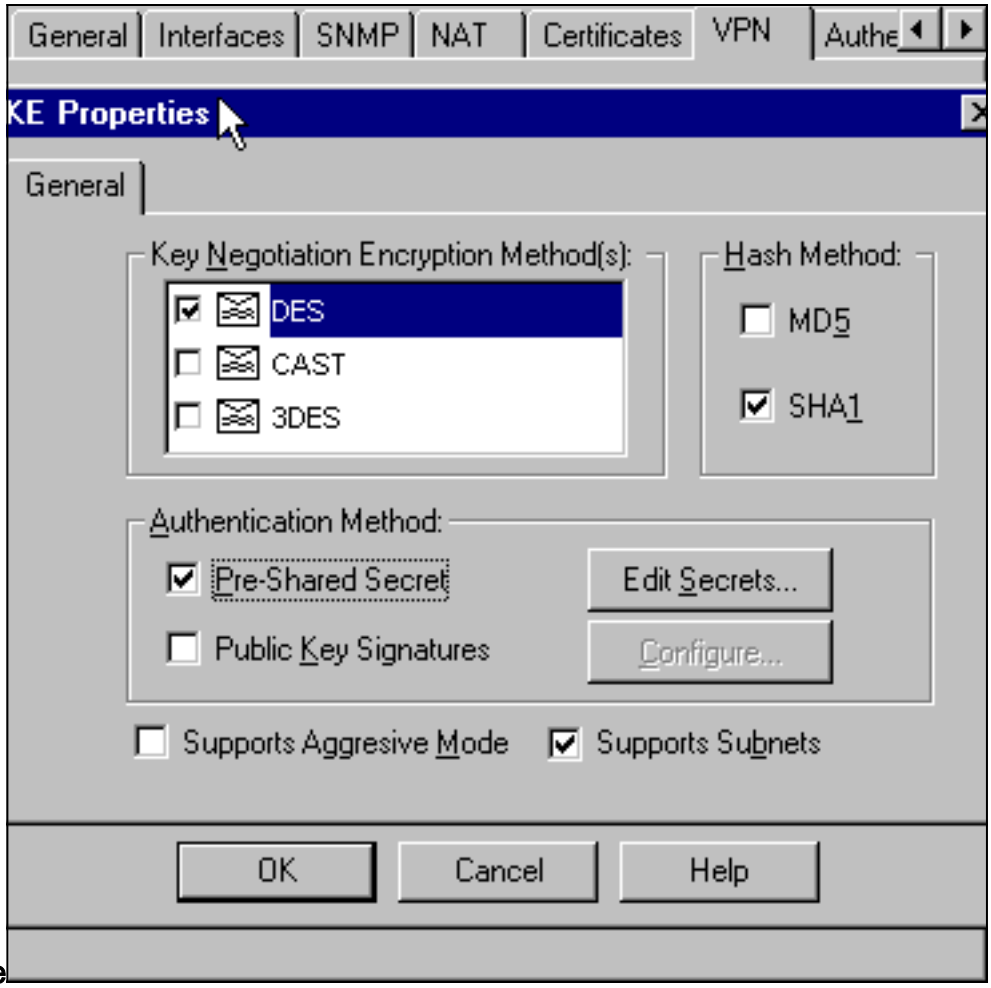
netmask

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



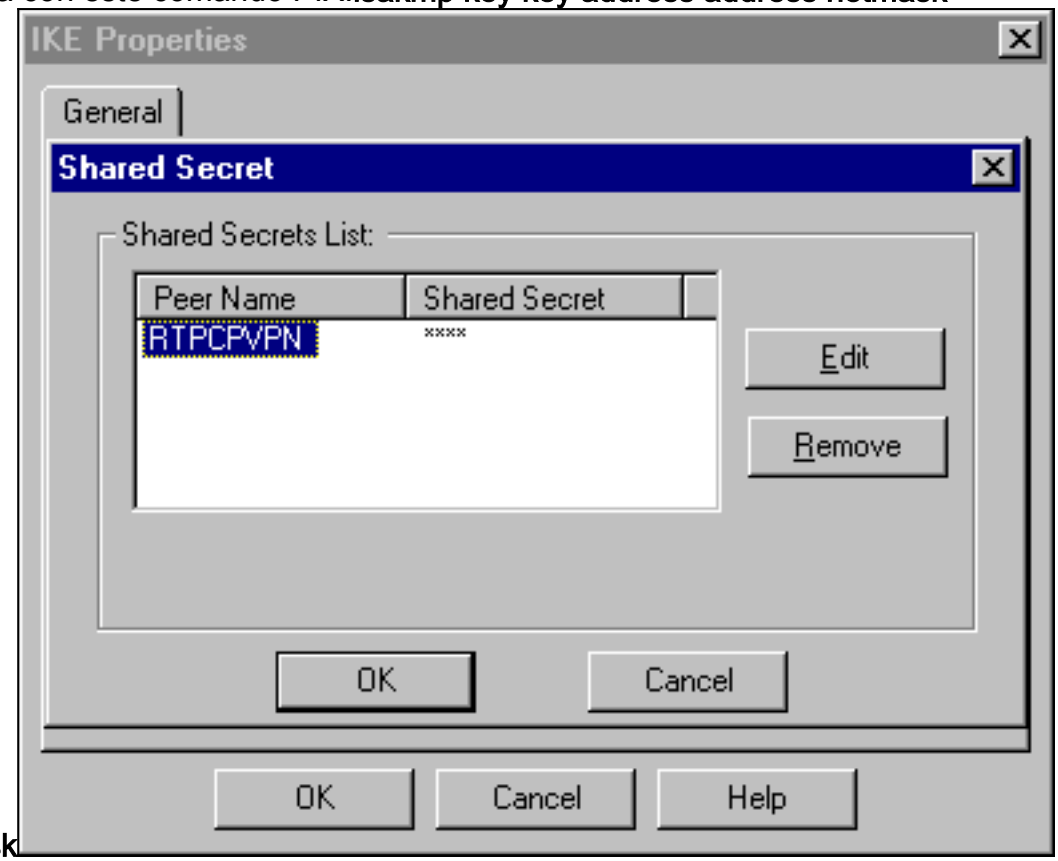
(Editar).

11. Cambie el encripción DES de propiedades IKE para coincidir con este comando:**isakmp policy # encryption des**
12. Cambie las propiedades IKE a Hashing SHA1 para coincidir con este comando:**crypto isakmp policy # hash sha**Cambie esta configuración:Cancelar la selección del modo agresivoSeleccione la casilla de verificación **Support Subnets** .En Método de autenticación, seleccione la casilla **Pre-Shared Secret**. Esta acción coincide con este comando:**isakmp policy # authentication pre-**



share

13. Haga clic en **Editar secretos** para configurar la clave previamente compartida para que coincida con este comando PIX:**isakmp key key address address netmask**

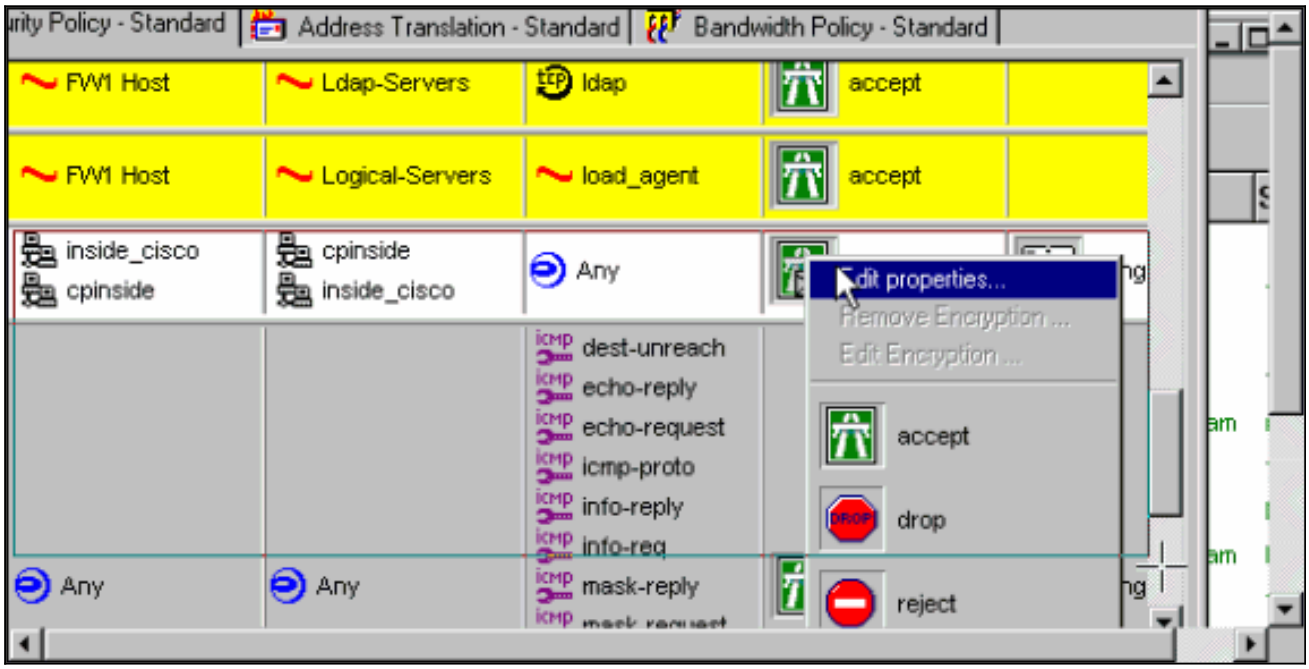


netmask

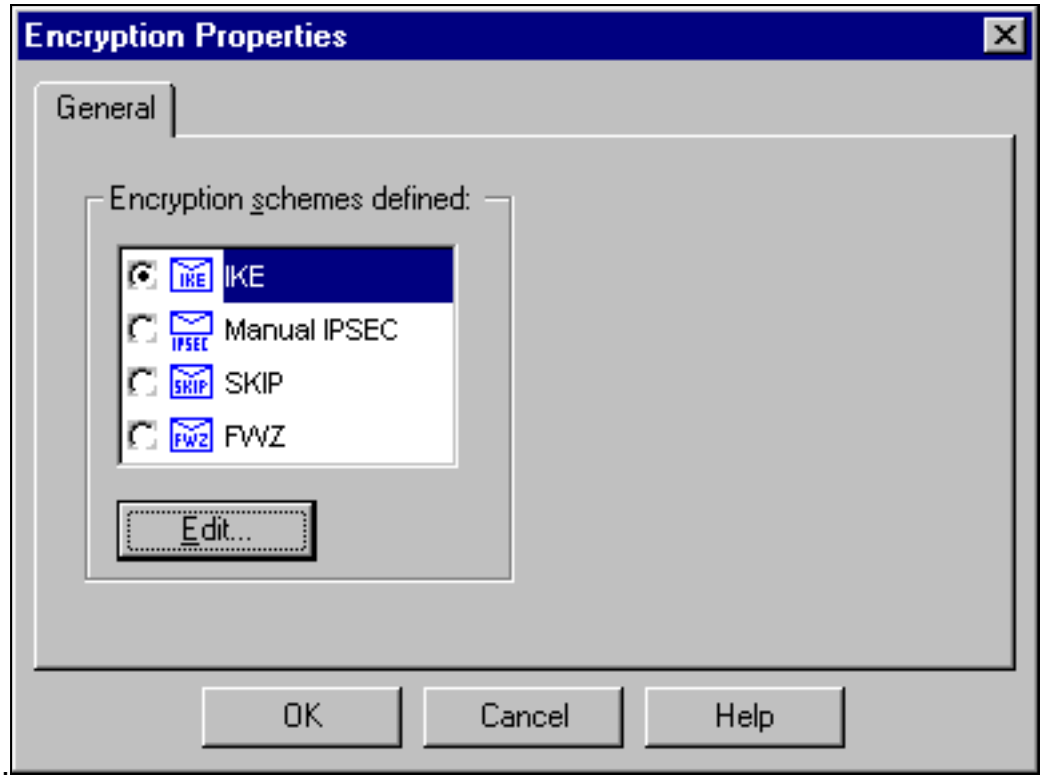
14. En la ventana del editor de políticas, ingrese una ventana tanto con el origen como con el destino, como en "inside_cisco" y "cpinside" (bidireccional). Set Service=Any, Action=Encrypt, y

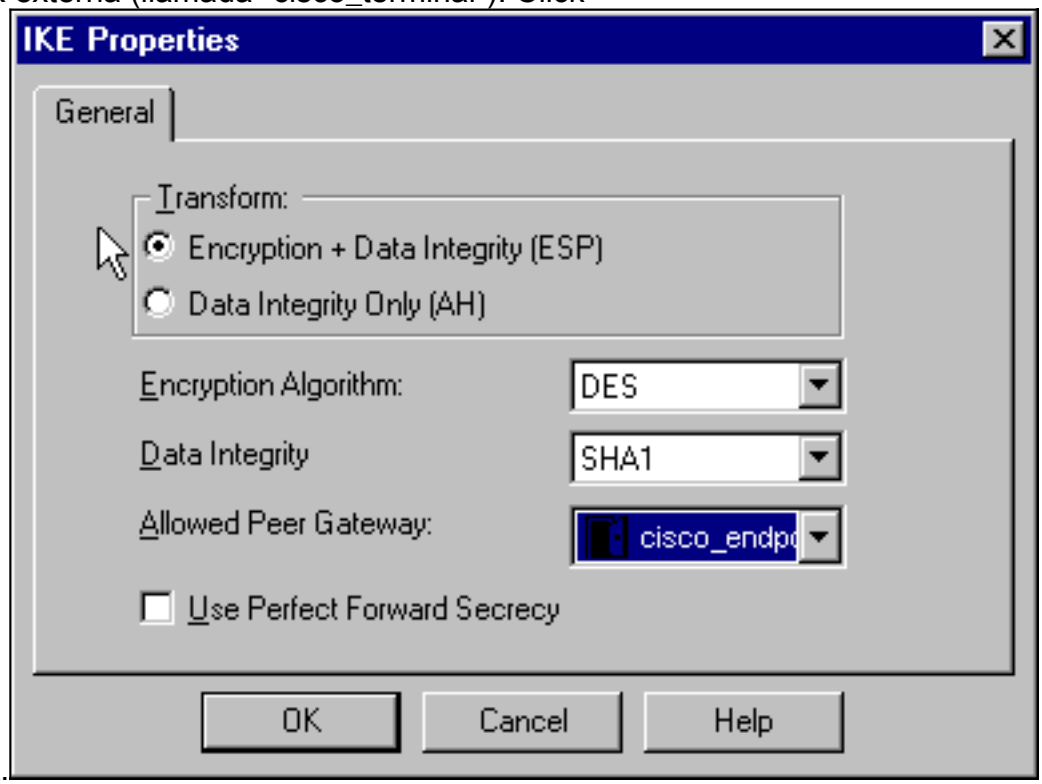
Track=Long.

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



16. Seleccione IKE y luego haga clic en Edit

(Editar). 

17. En la pantalla IKE Properties (Propiedades IKE), cambie estas propiedades para coincidir con las transformaciones de PIX IPSec 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 cifrado debe ser **DES**, la integridad de los datos debe ser **SHA1** y la gateway de par permitida debe ser la gateway PIX externa (llamada "cisco_terminal"). Click
OK. 

18. Después de configurar el punto de comprobación, seleccione **Policy > Install** en el menú Checkpoint para que los cambios surtan 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**: muestra los mensajes de depuración sobre los motores criptográficos, que realizan el cifrado y el descifrado.
- **debug crypto isakmp**: muestra mensajes sobre eventos IKE.
- **debug crypto ipsec—Muestra eventos de IPSec.**
- **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 asociaciones de seguridad actuales.
- **clear crypto isakmp sa** —(del modo de configuración) Borre todas las conexiones IKE activas.
- **clear crypto ipsec sa** —(del modo de configuración) Elimine todas las asociaciones de seguridad IPSec.

Punto de control

Debido a que el rastreo se configuró para Long en la ventana del Editor de políticas que se muestra en el paso 14, el tráfico denegado aparece en rojo en el Visor de registros. Para obtener una depuración más detallada, introduzca:

```
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.

Puede borrar las SA en el punto de control 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 respondiendo **sí** a ¿Está seguro? mensaje

Troubleshoot

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

Resumen de la red

Cuando se configuran varias redes internas adyacentes en el dominio de cifrado en el punto de control, el dispositivo puede resumirlas automáticamente con respecto al tráfico interesante. Si la ACL crypto en el PIX no está configurada 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, se pueden resumir en 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