Configuración de un túnel IPSec entre un punto de control NG y un router

Contenido

Introducción

Este documento muestra cómo formar un túnel IPSec con claves previamente compartidas para incorporar dos redes privadas:

- La red privada 172.16.15.x dentro del router.
- La red privada 192.168.10.x dentro de la última generación CheckpointTM (NG).

Prerequisites

Requirements

Los procedimientos esbozados en este documento se basan en esas hipótesis.

- Se configura la política básica CheckpointTM NG.
- Se configuran todas las configuraciones de acceso, traducción de direcciones de red (NAT) y routing.
- El tráfico desde dentro del router y dentro del NG CheckpointTM a Internet fluye.

Componentes Utilizados

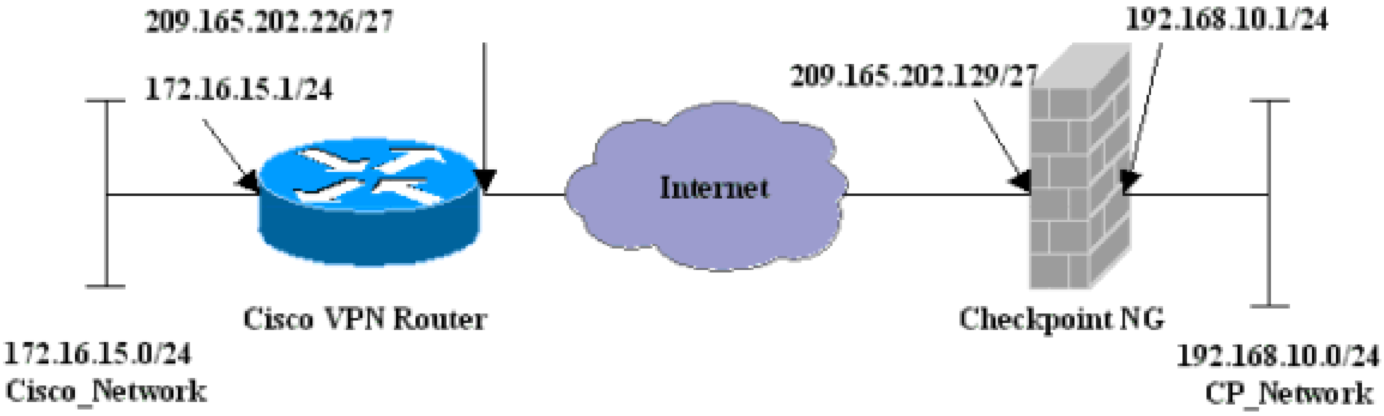
La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco 1751 Router
- Software Cisco IOS® (C1700-K9O3SY7-M), versión 12.2(8)T4, SOFTWARE DE VERSIÓN (fc1)
- CheckpointTM NG Build 50027

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.

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Convenciones

Para obtener más información sobre las convenciones del documento, consulte Convenciones de Consejos Técnicos de Cisco.

Configuración del router VPN Cisco 1751

Router Cisco VPN 1751

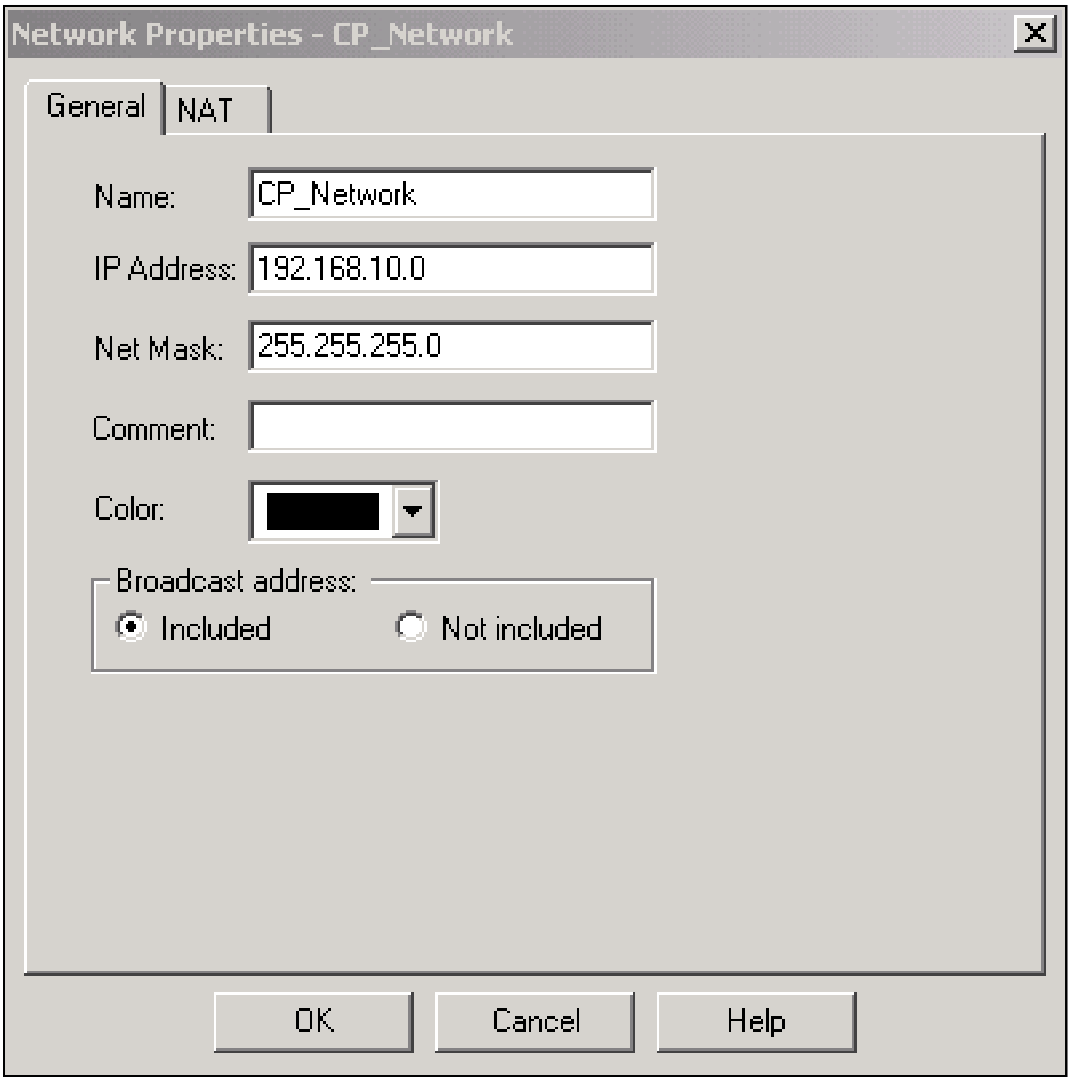
```
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
hostname sv1-6
memory-size iomem 15
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip subnet-zero
no ip domain-lookup
ip audit notify log
ip audit po max-events 100
!--- Internet Key Exchange (IKE) configuration. crypto
isakmp policy 1
  encr 3des
  hash md5
  authentication pre-share
  group 2
  lifetime 1800
!--- IPSec configuration. crypto isakmp key aptrules
address 209.165.202.129
!
crypto ipsec transform-set aptset esp-3des esp-md5-hmac
!
crypto map aptmap 1 ipsec-isakmp
  set peer 209.165.202.129
  set transform-set aptset
  match address 110
!
interface Ethernet0/0
  ip address 209.165.202.226 255.255.255.224
  ip nat outside
  half-duplex
  crypto map aptmap
!
interface FastEthernet0/0
  ip address 172.16.15.1 255.255.255.0
  ip nat inside
  speed auto
!--- NAT configuration. ip nat inside source route-map
nonat interface Ethernet0/0 overload
ip classless
ip route 0.0.0.0 0.0.0.0 209.165.202.225
no ip http server
ip pim bidir-enable
!--- Encryption match address access list. access-list
110 permit ip 172.16.15.0 0.0.0.255 192.168.10.0
0.0.0.255
!--- NAT access list. access-list 120 deny ip
172.16.15.0 0.0.0.255 192.168.10.0 0.0.0.255
access-list 120 permit ip 172.16.15.0 0.0.0.255 any
route-map nonat permit 10
  match ip address 120
line con 0
  exec-timeout 0 0
line aux 0
line vty 0 4
  password cisco
 login
end
```

Configuración del punto de control NG

CheckpointTM NG es una configuración orientada a objetos. Los objetos de red y las reglas se definen para formar la política que pertenece a la configuración de VPN que se va a configurar. A continuación, esta política se instala mediante el Editor de políticas de NG CheckpointTM para completar el lado de NG CheckpointTM de la configuración de VPN.

1. Cree una subred de red de Cisco y una subred de red NG CheckpointTM como objetos de red. Esto es lo que está cifrado. Para crear los objetos, seleccione **Administrar > Objetos de red** y, a continuación, seleccione **Nuevo > Red**. Ingrese la información de red adecuada y luego haga clic en **Aceptar**.Estos ejemplos muestran una configuración de objetos llamada CP_Network y

Cisco_Network.



Network Properties - CP_Network

Name: CP_Network

IP Address: 192.168.10.0

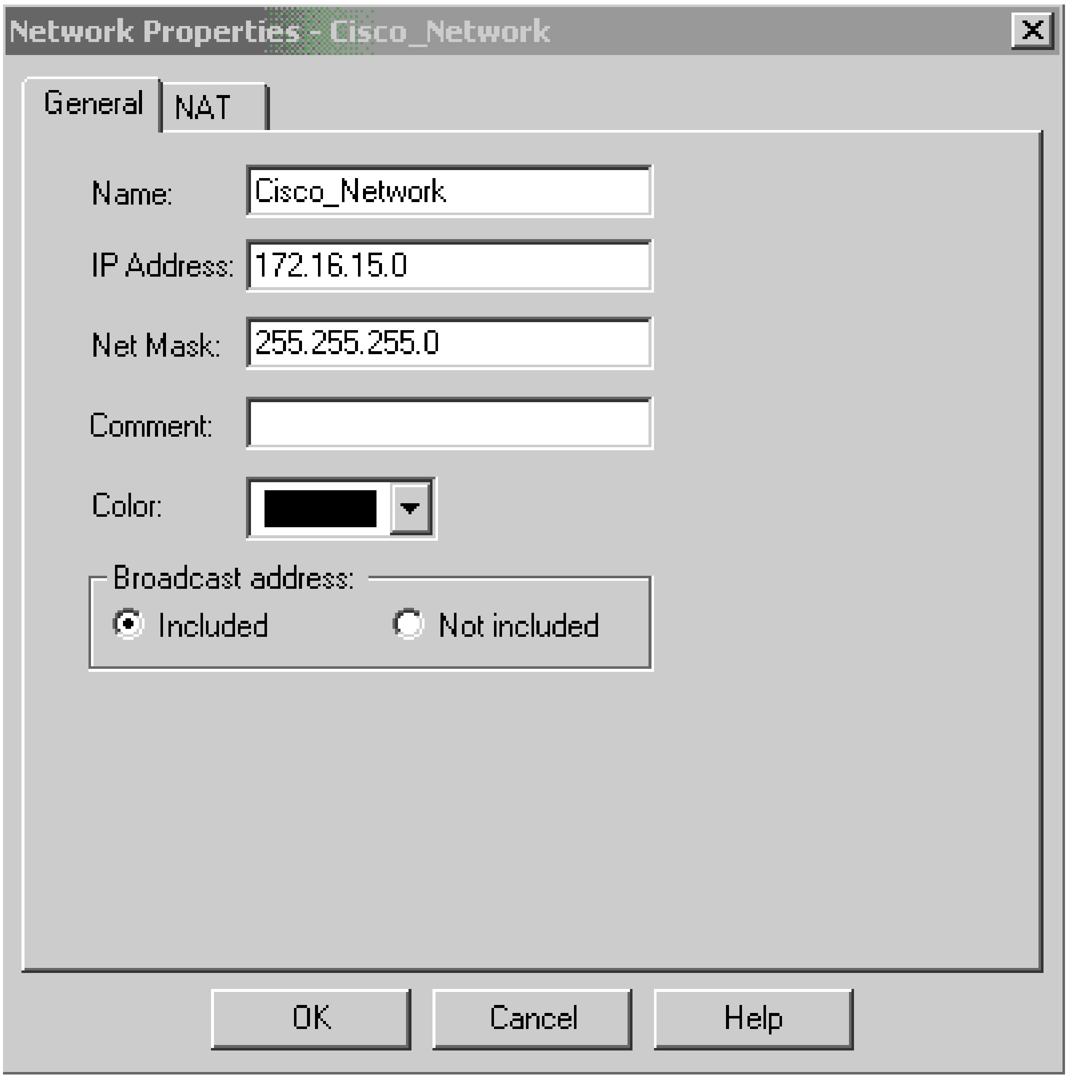
Net Mask: 255.255.255.0

Comment:

Color: ■

Broadcast address:

● Included ○ Not included



Network Properties - Cisco_Network

Name: Cisco_Network

IP Address: 172.16.15.0

Net Mask: 255.255.255.0

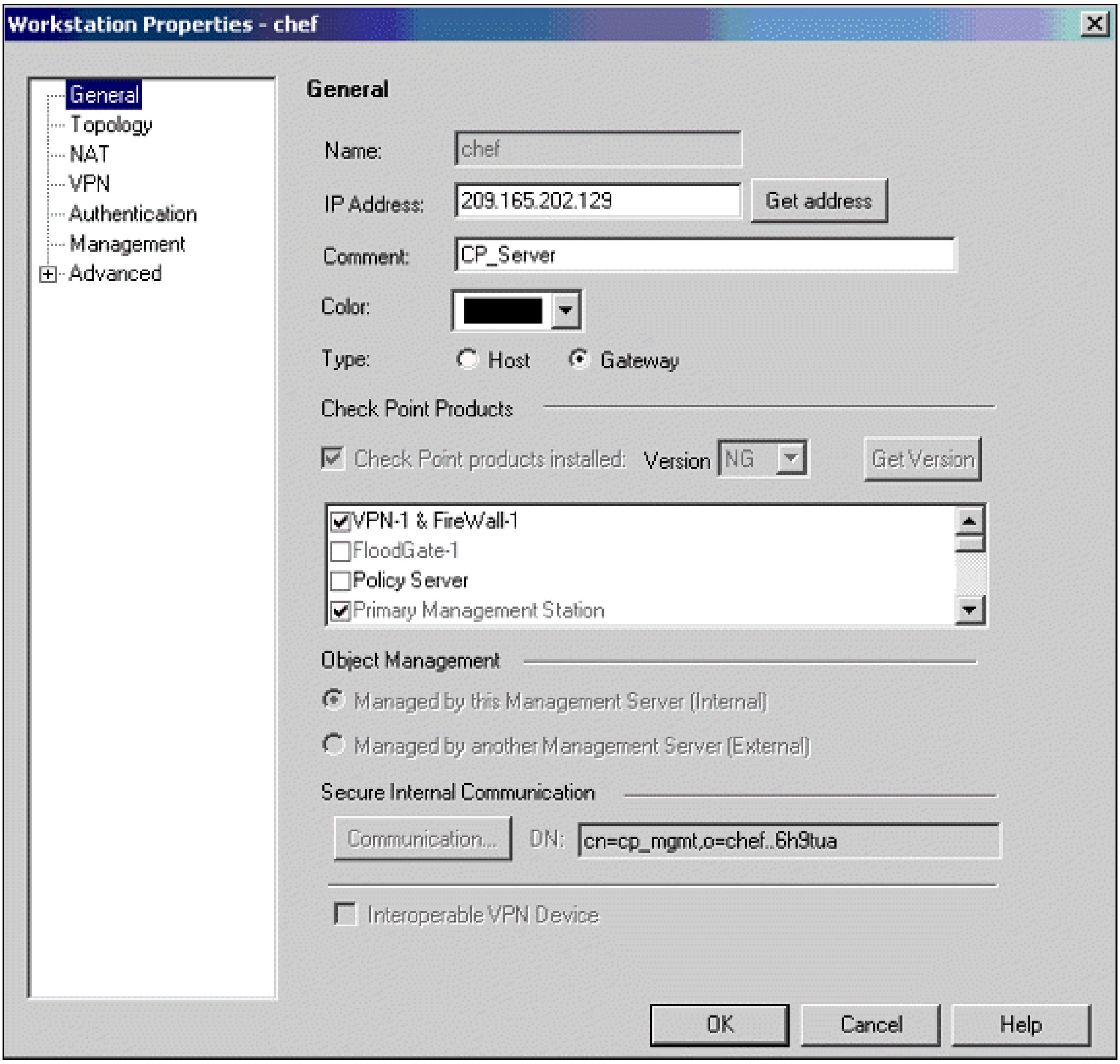
Comment:

Color: ■

Broadcast address:

● Included ○ Not included

2. Cree los objetos Cisco_Router y Checkpoint_NG como objetos de estación de trabajo. Estos son los dispositivos VPN. Para crear los objetos, seleccione **Administrar > Objetos de red** y, a continuación, seleccione **Nuevo > Estación de trabajo**.Tenga en cuenta que puede utilizar el objeto de estación de trabajo NG CheckpointTM creado durante la configuración NG inicial de CheckpointTM. Seleccione las opciones para configurar la estación de trabajo como **Gateway** y **dispositivo VPN interoperable**.Estos ejemplos muestran una configuración de objetos llamada chef y
Cisco_Router.



Workstation Properties - chef

General

Name: chef

IP Address: 209.165.202.129

Comment: CP_Server

Color: ■

Type: ○ Host ● Gateway

Check Point Products

☑ Check Point products installed: Version NG

☑ VPN-1 & FireWall-1
☐ FloodGate-1
☐ Policy Server
☑ Primary Management Station

Object Management

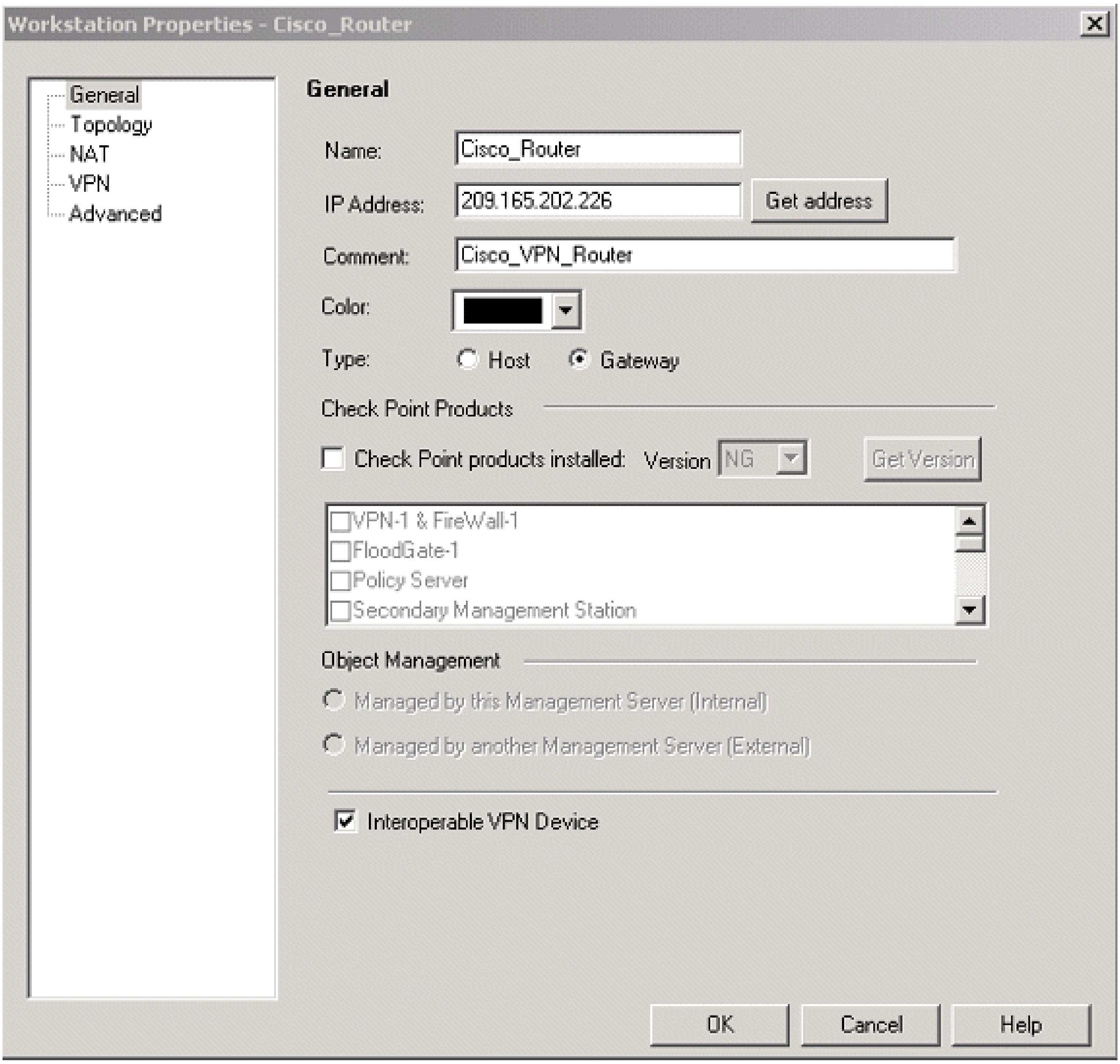
● Managed by this Management Server (Internal)

○ Managed by another Management Server (External)

Secure Internal Communication

DN: cn=cp_mgmt,o=chef..6h9tua

☐ Interoperable VPN Device



Workstation Properties - Cisco_Router

General

Name: Cisco_Router

IP Address: 209.165.202.226

Comment: Cisco_VPN_Router

Color: ■

Type: ○ Host ● Gateway

Check Point Products

□ Check Point products installed: Version NG

□ VPN-1 & FireWall-1
□ FloodGate-1
□ Policy Server
□ Secondary Management Station

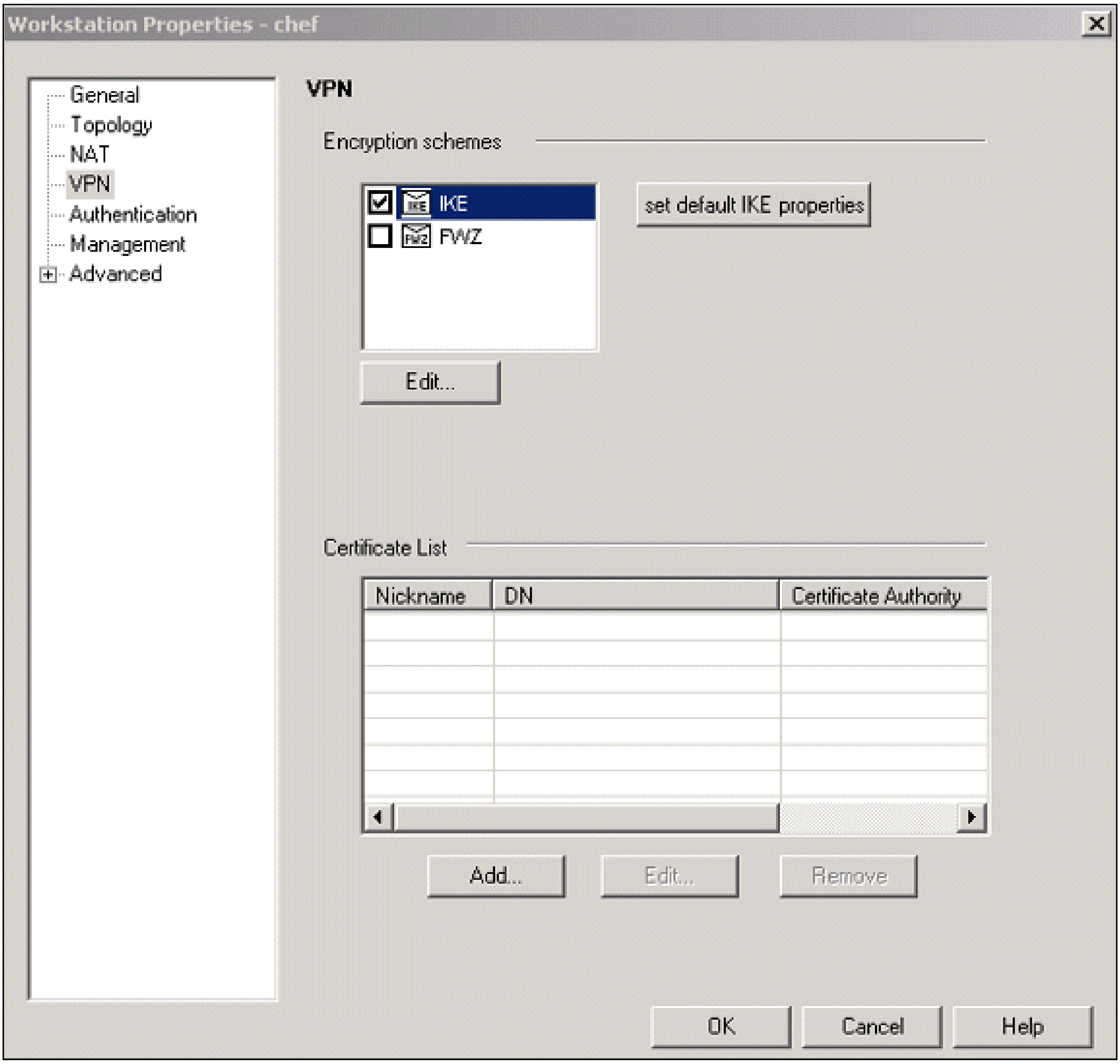
Object Management

○ Managed by this Management Server (Internal)

○ Managed by another Management Server (External)

☑ Interoperable VPN Device

3. Configure el IKE en la ficha VPN y luego haga clic en **Edit**.



VPN

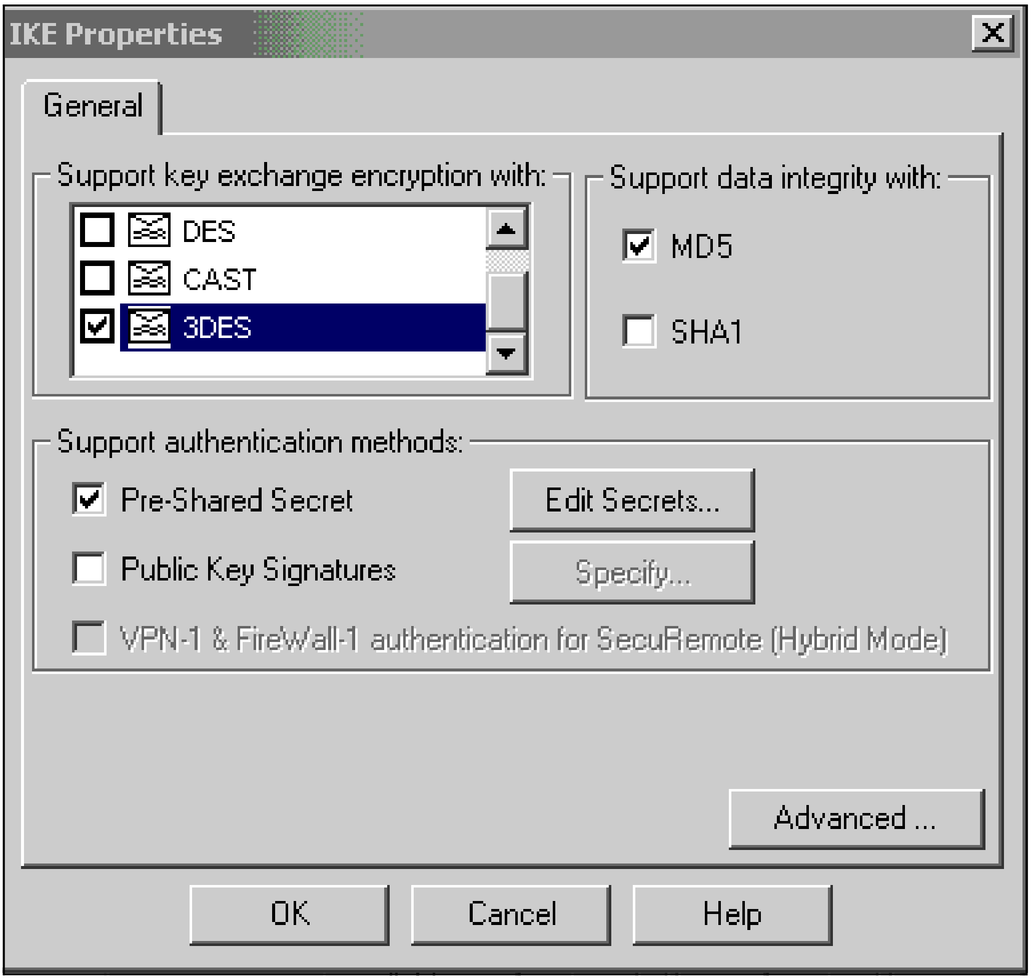
Encryption schemes

☑ IKE
□ FWZ

Certificate List

Nickname	DN	Certificate Authority

4. Configure la política de intercambio de claves y haga clic en **Editar**



IKE Properties

General

Support key exchange encryption with:

- □ DES
- □ CAST
- ☑ 3DES

Support data integrity with:

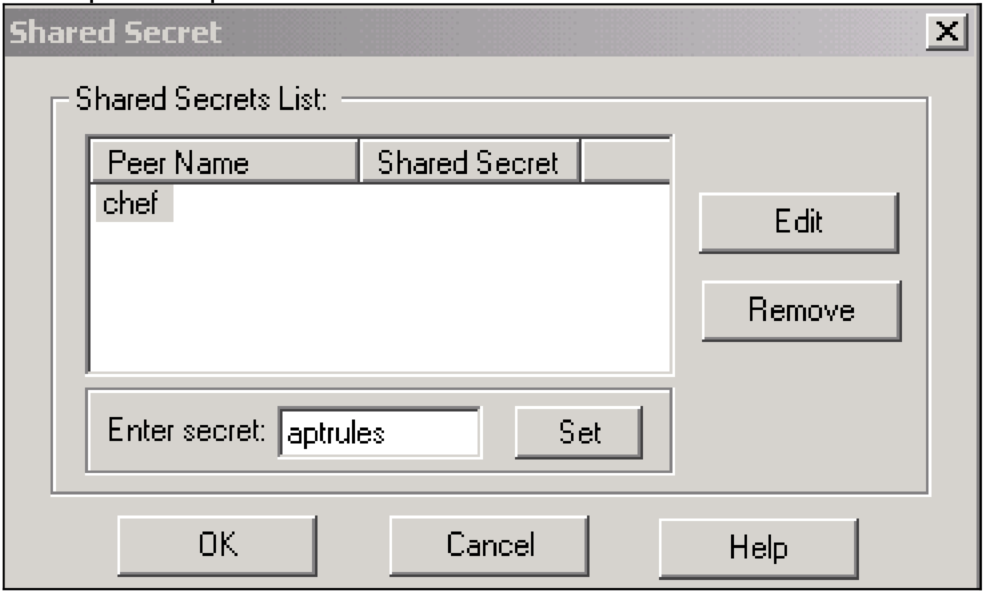
- ☑ MD5
- □ SHA1

Support authentication methods:

- ☑ Pre-Shared Secret
- □ Public Key Signatures
- □ VPN-1 & FireWall-1 authentication for SecuRemote (Hybrid Mode)

secretos.

5. Configure las claves previamente compartidas que se van a utilizar y haga clic en **Aceptar** varias veces hasta que desaparezcan las ventanas de configuración.



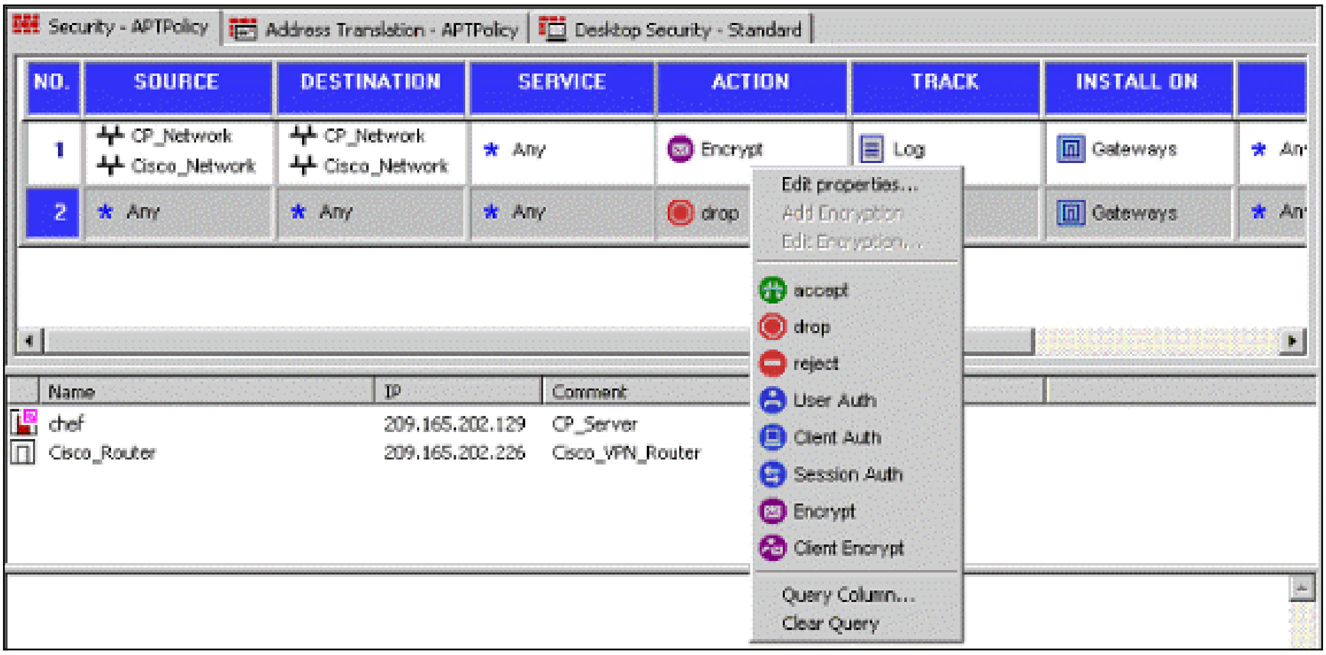
Shared Secret

Shared Secrets List:

Peer Name	Shared Secret
chef	

Enter secret: aptrules

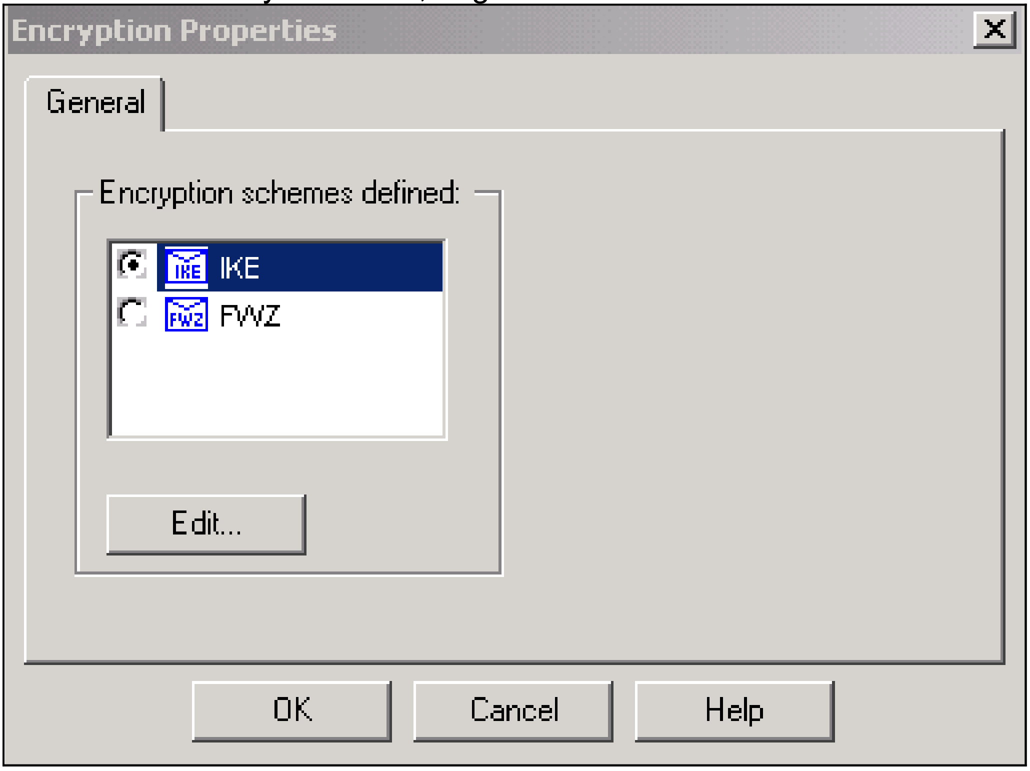
6. Seleccione **Rules > Add Rules > Top** para configurar las reglas de cifrado para la política.La regla de la parte superior es la primera que se realiza antes de cualquier otra regla que pueda eludir el cifrado. Configure el Origen y el Destino para incluir CP_Network y Cisco_Network, como se muestra aquí. Una vez que haya agregado la sección Acción de cifrado de la regla, haga clic con el botón derecho en **Acción** y seleccione **Editar propiedades**.



NO.	SOURCE	DESTINATION	SERVICE	ACTION	TRACK	INSTALL ON	
1	CP_Network Cisco_Network	CP_Network Cisco_Network	* Any	Encrypt	Log	Gateways	* An
2	* Any	* Any	* Any	drop		Gateways	* An

Name	IP	Comment
chef	209.165.202.129	CP_Server
Cisco_Router	209.165.202.226	Cisco_VPN_Router

7. Con IKE seleccionado y resaltado, haga clic en **Edit.**

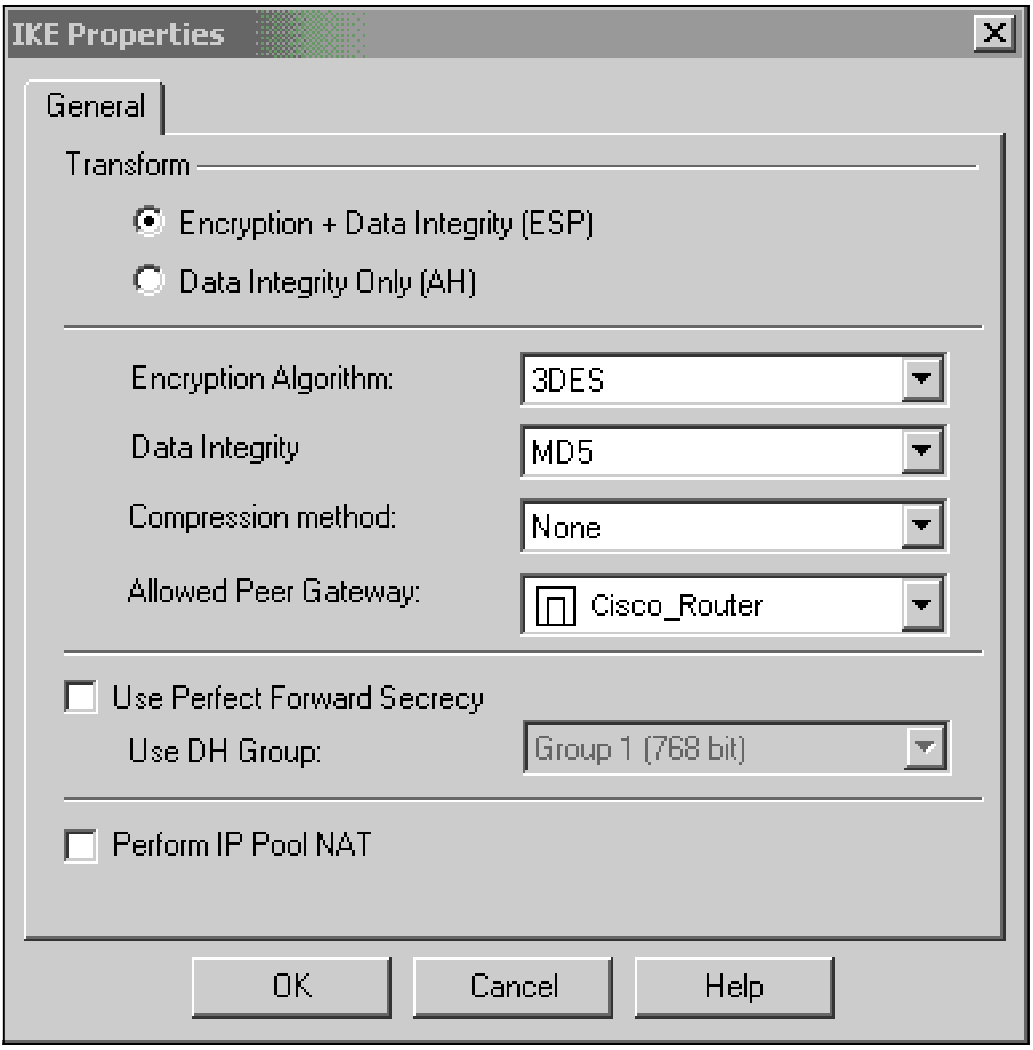


Encryption schemes defined:

● IKE

○ FWZ

8. Confirme la configuración



IKE Properties

General

Transform

● Encryption + Data Integrity (ESP)

○ Data Integrity Only (AH)

Encryption Algorithm: 3DES

Data Integrity: MD5

Compression method: None

Allowed Peer Gateway: Cisco_Router

☐ Use Perfect Forward Secrecy

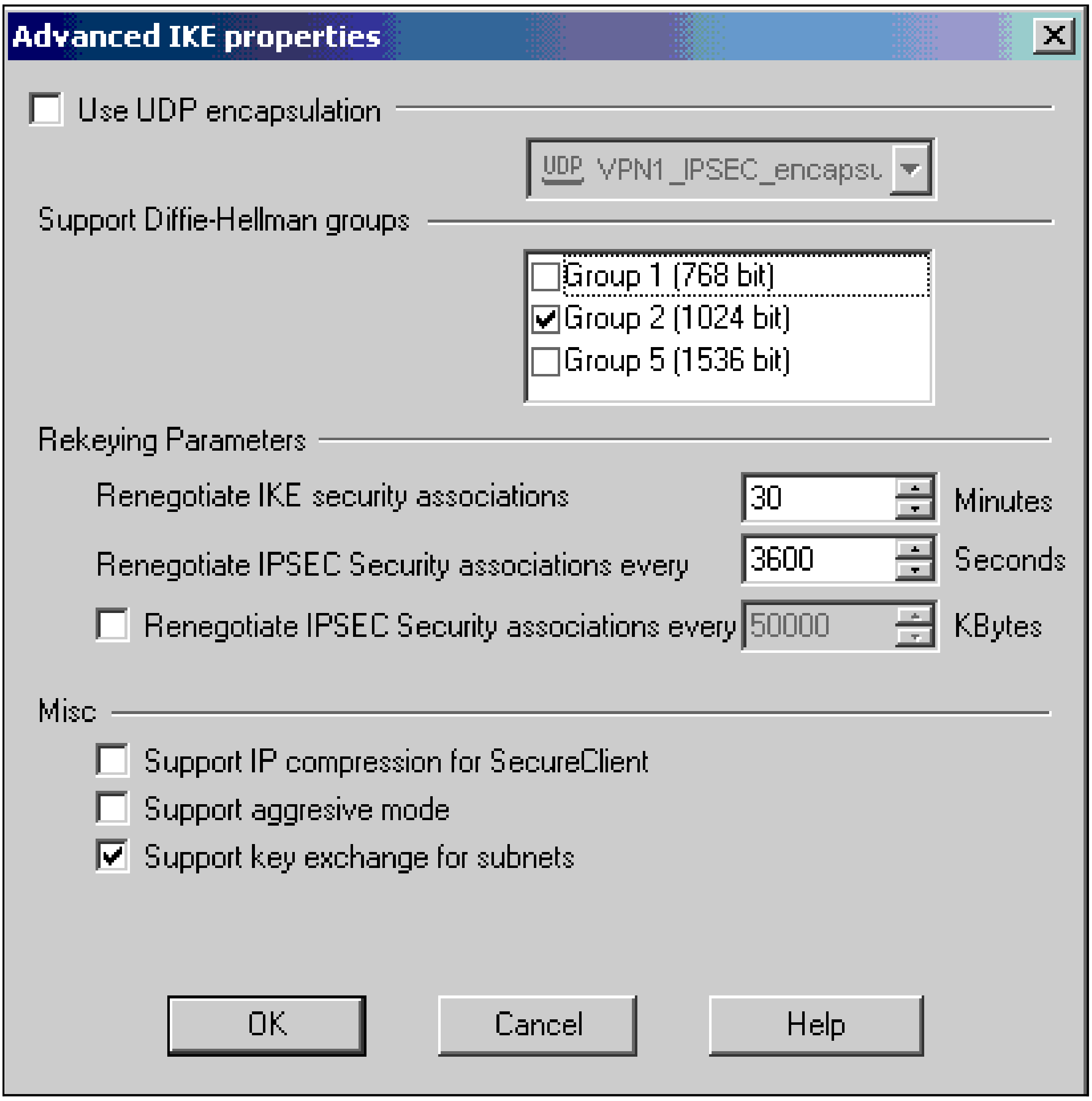
Use DH Group: Group 1 (768 bit)

☐ Perform IP Pool NAT

IKE.

9. Uno de los principales problemas con la ejecución de VPN entre los dispositivos Cisco y otros dispositivos IPSec es la renegociación del intercambio de claves. Asegúrese de que la configuración para el intercambio IKE en el router Cisco sea exactamente la misma que la configurada en el CheckpointTM NG.**Nota:** El valor real de este parámetro depende de su política de seguridad corporativa en particular.En este ejemplo, la configuración IKE en el router se ha establecido en 30 minutos con el comando **lifetime 1800**. El mismo valor se debe establecer en el NG CheckpointTM.Para establecer este valor en el NG CheckpointTM, seleccione **Manage Network Object**, luego seleccione el objeto CheckpointTM NG y haga clic en **Edit**. A continuación, seleccione **VPN** y edite el IKE. Seleccione **Advance** y configure los Parámetros de Rekeying. Después de configurar el intercambio de claves para el objeto de red CheckpointTM NG, realice la misma configuración de la renegociación del intercambio de claves para el objeto de red Cisco_Router.**Nota:** Asegúrese de que el grupo Diffie-Hellman correcto esté seleccionado para coincidir con el configurado en el

router.



Advanced IKE properties

□ Use UDP encapsulation

UDP VPN1_IPSEC_encapsu

Support Diffie-Hellman groups

□ Group 1 (768 bit)
☑ Group 2 (1024 bit)
□ Group 5 (1536 bit)

Rekeying Parameters

Renegotiate IKE security associations 30 Minutes

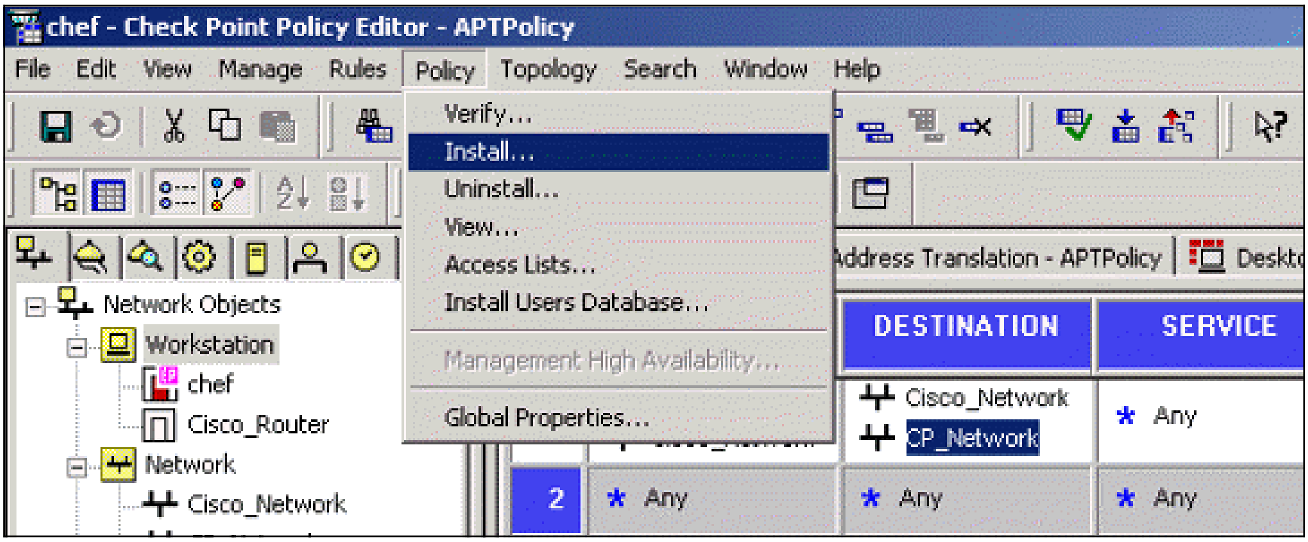
Renegotiate IPSEC Security associations every 3600 Seconds

□ Renegotiate IPSEC Security associations every 50000 KBytes

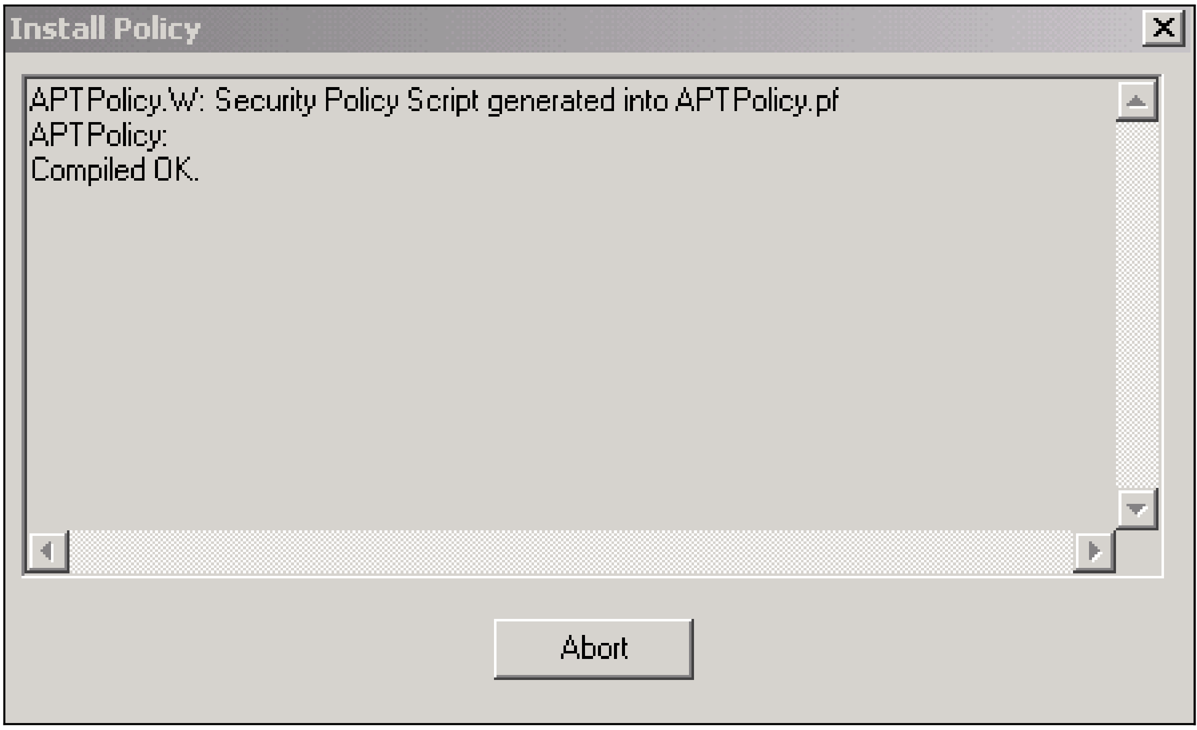
Misc

□ Support IP compression for SecureClient
□ Support aggresive mode
☑ Support key exchange for subnets

10. La configuración de la política ha finalizado. Guarde la política y seleccione **Policy > Install** para habilitarla.

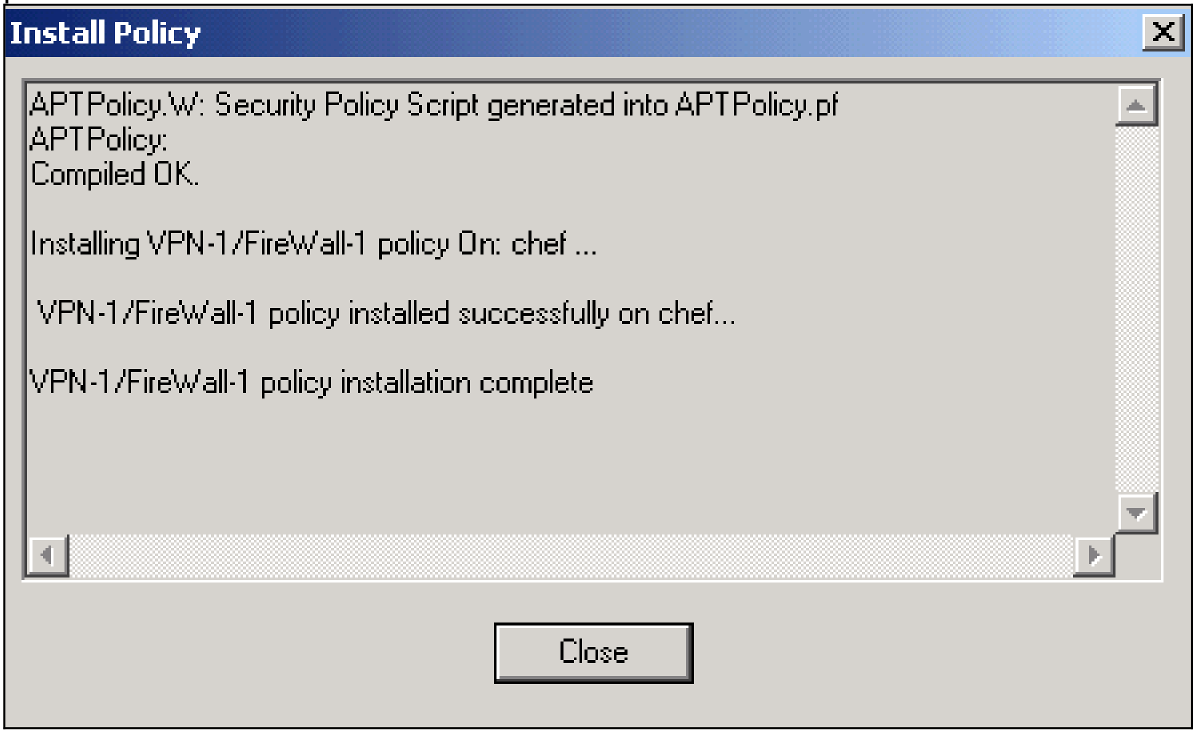


La ventana de instalación muestra las notas de progreso a medida que se compila la política.



```
APTPolicy.W: Security Policy Script generated into APTPolicy.pf
APTPolicy:
Compiled OK.
```

Cuando la ventana de instalación indique que la instalación de la política ha finalizado, haga clic en **Cerrar** para finalizar el procedimiento.



```
APTPolicy.W: Security Policy Script generated into APTPolicy.pf
APTPolicy:
Compiled OK.

Installing VPN-1/FireWall-1 policy On: chef ...

 VPN-1/FireWall-1 policy installed successfully on chef...

VPN-1/FireWall-1 policy installation complete
```

Verificación

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

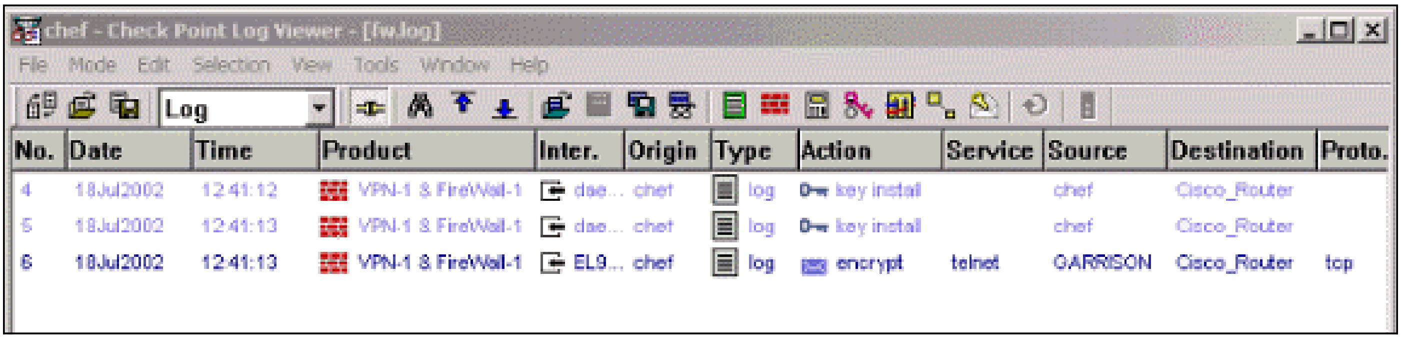
Verifique el router de Cisco

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

- show crypto isakmp sa : muestra todas las asociaciones de seguridad actuales IKE (SA) en un par.
- show crypto ipsec sa — Muestra la configuración actual utilizada por las SA actuales

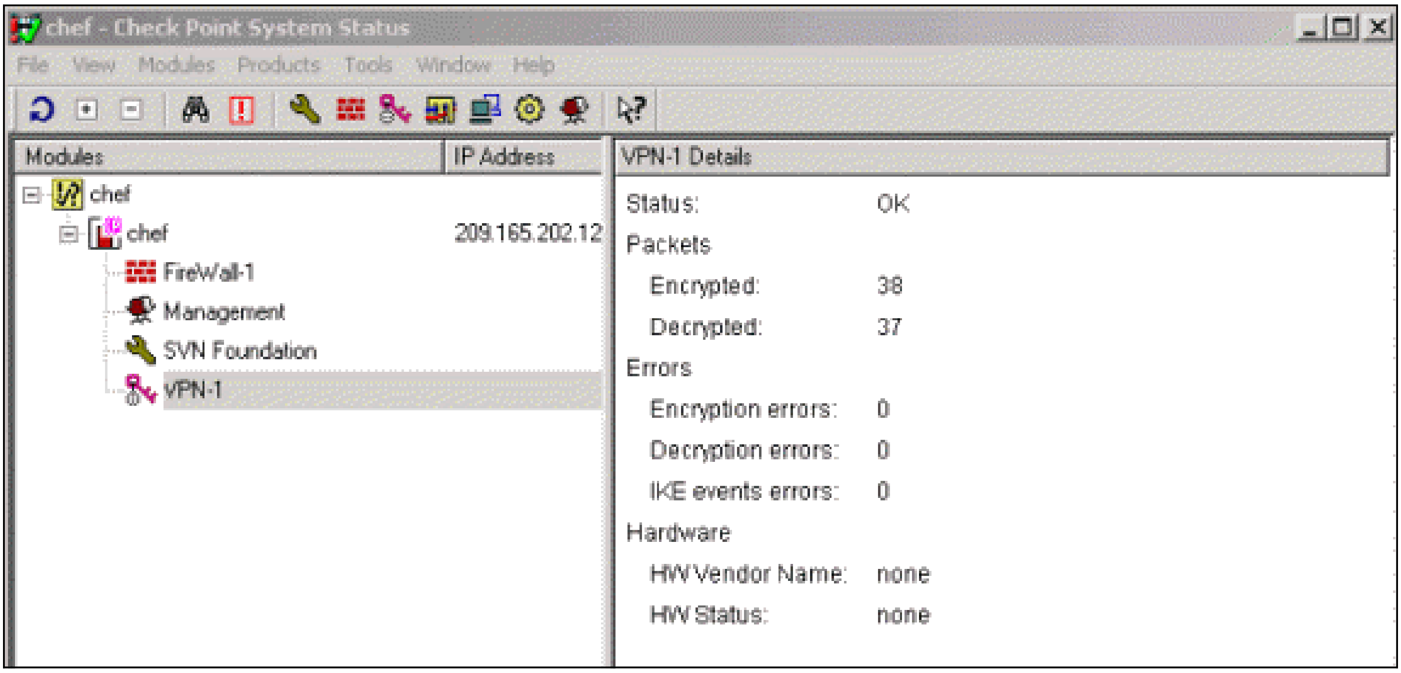
Verificar punto de control NG

Para ver los registros, seleccione **Ventana > Visor de registros**.


chef - Check Point Log Viewer - [fw.log]
File Mode Edit Selection View Tools Window Help
Log

No.	Date	Time	Product	Inter.	Origin	Type	Action	Service	Source	Destination	Proto.
4	18Jul2002	12:41:12	VPN-1 & FireWall-1	dae...	chef	log	key install		chef	Cisco_Router	
5	18Jul2002	12:41:13	VPN-1 & FireWall-1	dae...	chef	log	key install		chef	Cisco_Router	
6	18Jul2002	12:41:13	VPN-1 & FireWall-1	EL9...	chef	log	encrypt	telnet	GARRISON	Cisco_Router	tcp

Para ver el estado del sistema, seleccione **Ventana > Estado del sistema**.



```
Status:               OK
Packets
  Encrypted:          38
  Decrypted:          37
Errors
  Encryption errors:  0
  Decryption errors:  0
  IKE events errors:  0
Hardware
  HW Vendor Name:     none
  HW Status:          none
```

Troubleshoot

Router Cisco

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

Para obtener información adicional sobre la resolución de problemas, consulte Solución de problemas de seguridad IP - Introducción y uso de los comandos debug.

Nota: Antes de ejecutar un comando **debug**, consulte Información Importante sobre 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.

Salida exitosa del registro de depuración

```
18:05:32: ISAKMP (0:0): received packet from
   209.165.202.129 (N) NEW SA
18:05:32: ISAKMP: local port 500, remote port 500
18:05:32: ISAKMP (0:1): Input = IKE_MESG_FROM_PEER,
   IKE_MM_EXCH
Old State = IKE_READY New State = IKE_R_MM1
18:05:32: ISAKMP (0:1): processing SA payload. message ID = 0
18:05:32: ISAKMP (0:1): processing vendor id payload
18:05:32: ISAKMP (0:1): vendor ID seems Unity/DPD
   but bad major
18:05:32: ISAKMP (0:1): found peer pre-shared key
   matching 209.165.202.129
18:05:32: ISAKMP (0:1): Checking ISAKMP transform 1
   against priority 1 policy
18:05:32: ISAKMP: encryption 3DES-CBC
18:05:32: ISAKMP: hash MD5
18:05:32: ISAKMP: auth pre-share
18:05:32: ISAKMP: default group 2
18:05:32: ISAKMP: life type in seconds
18:05:32: ISAKMP: life duration (VPI) of 0x0 0x0 0x7 0x8
18:05:32: ISAKMP (0:1): atts are acceptable. Next payload is 0
18:05:33: ISAKMP (0:1): processing vendor id payload
18:05:33: ISAKMP (0:1): vendor ID seems Unity/DPD but bad major
18:05:33: ISAKMP (0:1): Input = IKE_MESG_INTERNAL,
   IKE_PROCESS_MAIN_MODE
Old State = IKE_R_MM1 New State = IKE_R_MM1
18:05:33: ISAKMP (0:1): sending packet to 209.165.202.129 (R)
   MM_SA_SETUP
18:05:33: ISAKMP (0:1): Input = IKE_MESG_INTERNAL,
   IKE_PROCESS_COMPLETE
Old State = IKE_R_MM1 New State = IKE_R_MM2
18:05:33: ISAKMP (0:1): received packet from 209.165.202.129 (R)
   MM_SA_SETUP
18:05:33: ISAKMP (0:1): Input = IKE_MESG_FROM_PEER,
   IKE_MM_EXCH
Old State = IKE_R_MM2 New State = IKE_R_MM3
18:05:33: ISAKMP (0:1): processing KE payload.
   message ID = 0
18:05:33: ISAKMP (0:1): processing NONCE payload.
   message ID = 0
18:05:33: ISAKMP (0:1): found peer pre-shared key
   matching 209.165.202.129
18:05:33: ISAKMP (0:1): SKEYID state generated
18:05:33: ISAKMP (0:1): Input = IKE_MESG_INTERNAL,
   IKE_PROCESS_MAIN_MODE
Old State = IKE_R_MM3 New State = IKE_R_MM3
18:05:33: ISAKMP (0:1): sending packet to 209.165.202.129 (R)
   MM_KEY_EXCH
18:05:33: ISAKMP (0:1): Input = IKE_MESG_INTERNAL,
   IKE_PROCESS_COMPLETE
Old State = IKE_R_MM3 New State = IKE_R_MM4
18:05:33: ISAKMP (0:1): received packet from 209.165.202.129 (R)
```

```
   MM_KEY_EXCH
18:05:33: ISAKMP (0:1): Input = IKE_MESG_FROM_PEER,
   IKE_MM_EXCH
Old State = IKE_R_MM4 New State = IKE_R_MM5
18:05:33: ISAKMP (0:1): processing ID payload.
   message ID = 0
18:05:33: ISAKMP (0:1): processing HASH payload.
   message ID = 0
18:05:33: ISAKMP (0:1): SA has been authenticated
   with 209.165.202.129
18:05:33: ISAKMP (0:1): Input = IKE_MESG_INTERNAL,
   IKE_PROCESS_MAIN_MODE
Old State = IKE_R_MM5 New State = IKE_R_MM5
18:05:33: ISAKMP (0:1): SA is doing pre-shared key authentication
using id type ID_IPV4_ADDR
18:05:33: ISAKMP (1): ID payload
next-payload : 8
type : 1
protocol : 17
port : 500
length : 8
18:05:33: ISAKMP (1): Total payload length: 12
18:05:33: ISAKMP (0:1): sending packet to 209.165.202.129
(R) QM_IDLE
18:05:33: ISAKMP (0:1): Input = IKE_MESG_INTERNAL,
IKE_PROCESS_COMPLETE
Old State = IKE_R_MM5 New State = IKE_P1_COMPLETE
18:05:33: ISAKMP (0:1): Input = IKE_MESG_INTERNAL,
   IKE_PHASE1_COMPLETE
Old State = IKE_P1_COMPLETE
   New State = IKE_P1_COMPLETE
18:05:33: ISAKMP (0:1): received packet from 209.165.202.129 (R)
   QM_IDLE
18:05:33: ISAKMP (0:1): processing HASH payload.
   message ID = -1335371103
18:05:33: ISAKMP (0:1): processing SA payload.
   message ID = -1335371103
18:05:33: ISAKMP (0:1): Checking IPSec proposal 1
18:05:33: ISAKMP: transform 1, ESP_3DES
18:05:33: ISAKMP: attributes in transform:
18:05:33: ISAKMP: SA life type in seconds
18:05:33: ISAKMP: SA life duration (VPI) of 0x0 0x0 0xE 0x10
18:05:33: ISAKMP: authenticator is HMAC-MD5
18:05:33: ISAKMP: encaps is 1
18:05:33: ISAKMP (0:1): atts are acceptable.
18:05:33: IPSEC(validate_proposal_request): proposal part #1,
(key eng. msg.) INBOUND local= 209.165.202.226, remote= 209.165.202.129,
local_proxy= 172.16.15.0/255.255.255.0/0/0 (type=4),
remote_proxy= 192.168.10.0/255.255.255.0/0/0 (type=4),
protocol= ESP, transform= esp-3des esp-md5-hmac ,
   lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
18:05:33: ISAKMP (0:1): processing NONCE payload.
   message ID = -1335371103
18:05:33: ISAKMP (0:1): processing ID payload.
   message ID = -1335371103
18:05:33: ISAKMP (0:1): processing ID payload.
   message ID = -1335371103
18:05:33: ISAKMP (0:1): asking for 1 spis from ipsec
18:05:33: ISAKMP (0:1): Node -1335371103,
   Input = IKE_MESG_FROM_PEER, IKE_QM_EXCH
Old State = IKE_QM_READY New State = IKE_QM_SPI_STARVE
18:05:33: IPSEC(key_engine): got a queue event...
18:05:33: IPSEC(spi_response): getting spi 2147492563 for SA
```

```
from 209.165.202.226 to 209.165.202.129 for prot 3
18:05:33: ISAKMP: received ke message (2/1)
18:05:33: ISAKMP (0:1): sending packet to
   209.165.202.129 (R) QM_IDLE
18:05:33: ISAKMP (0:1): Node -1335371103,
   Input = IKE_MESG_FROM_IPSEC, IKE_SPI_REPLY
Old State = IKE_QM_SPI_STARVE New State = IKE_QM_R_QM2
18:05:33: ISAKMP (0:1): received packet
   from 209.165.202.129 (R) QM_IDLE
18:05:33: ISAKMP (0:1): Creating IPSec SAs
18:05:33: inbound SA from 209.165.202.129 to 209.165.202.226
   (proxy 192.168.10.0 to 172.16.15.0)
18:05:33: has spi 0x800022D3 and conn_id 200 and flags 4
18:05:33: lifetime of 3600 seconds
18:05:33: outbound SA from 209.165.202.226 to 209.165.202.129
   (proxy 172.16.15.0 to 192.168.10.0 )
18:05:33: has spi -2006413528 and conn_id 201 and flags C
18:05:33: lifetime of 3600 seconds
18:05:33: ISAKMP (0:1): deleting node -1335371103 error
   FALSE reason "quick mode done (await()"
18:05:33: ISAKMP (0:1): Node -1335371103, Input = IKE_MESG_FROM_PEER,
   IKE_QM_EXCH
Old State = IKE_QM_R_QM2 New State = IKE_QM_PHASE2_COMPLETE
18:05:33: IPSEC(key_engine): got a queue event...
18:05:33: IPSEC(initialize_sas): ,
(key eng. msg.) INBOUND local= 209.165.202.226,
   remote=209.165.202.129,
local_proxy= 172.16.15.0/255.255.255.0/0/0 (type=4),
remote_proxy= 192.168.10.0/255.255.255.0/0/0 (type=4),
protocol= ESP, transform= esp-3des esp-md5-hmac ,
   lifedur= 3600s and 0kb,
spi= 0x800022D3(2147492563), conn_id= 200, keysize= 0,
   flags= 0x4
18:05:33: IPSEC(initialize_sas): ,
(key eng. msg.) OUTBOUND local= 209.165.202.226,
   remote=209.165.202.129,
local_proxy= 172.16.15.0/255.255.255.0/0/0 (type=4),
remote_proxy= 192.168.10.0/255.255.255.0/0/0 (type=4),
protocol= ESP, transform= esp-3des esp-md5-hmac ,
   lifedur= 3600s and 0kb,
```

```
spi= 0x88688F28(2288553768), conn_id= 201, keysize= 0,
   flags= 0xC
18:05:33: IPSEC(create_sa): sa created,
(sa) sa_dest= 209.165.202.226, sa_prot= 50,
sa_spi= 0x800022D3(2147492563),
sa_trans= esp-3des esp-md5-hmac , sa_conn_id= 200
18:05:33: IPSEC(create_sa): sa created,
(sa) sa_dest= 209.165.202.129, sa_prot= 50,
sa_spi= 0x88688F28(2288553768),
sa_trans= esp-3des esp-md5-hmac , sa_conn_id= 201
18:05:34: ISAKMP (0:1): received packet
   from 209.165.202.129 (R) QM_IDLE
18:05:34: ISAKMP (0:1): phase 2 packet is a duplicate
   of a previous packet.
18:05:34: ISAKMP (0:1): retransmitting due to retransmit phase 2
18:05:34: ISAKMP (0:1): ignoring retransmission, because phase2
   node marked dead -1335371103
18:05:34: ISAKMP (0:1): received packet
   from 209.165.202.129 (R) QM_IDLE
18:05:34: ISAKMP (0:1): phase 2 packet is a duplicate
   of a previous packet.
```

```
18:05:34: ISAKMP (0:1): retransmitting due to retransmit phase 2
18:05:34: ISAKMP (0:1): ignoring retransmission, because phase2
   node marked dead -1335371103

sv1-6#show crypto isakmp sa
dst src state conn-id slot
209.165.202.226 209.165.202.129 QM_IDLE 1 0

sv1-6#show crypto ipsec sa
interface: Ethernet0/0
Crypto map tag: aptmap, local addr. 209.165.202.226
local ident (addr/mask/prot/port): (172.16.15.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (192.168.10.0/255.255.255.0/0/0)
current_peer: 209.165.202.129
PERMIT, flags={origin_is_acl,}
#pkts encaps: 21, #pkts encrypt: 21, #pkts digest 21
#pkts decaps: 24, #pkts decrypt: 24, #pkts verify 24
#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.: 209.165.202.226, remote crypto endpt.: 209.165.202.129
path mtu 1500, media mtu 1500
current outbound spi: 88688F28
inbound esp sas:
spi: 0x800022D3(2147492563)
transform: esp-3des esp-md5-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 200, flow_id: 1, crypto map: aptmap
sa timing: remaining key lifetime (k/sec): (4607997/3559)
IV size: 8 bytes
replay detection support: Y
inbound ah sas:
inbound pcp sas:
outbound esp sas:
spi: 0x88688F28(2288553768)
transform: esp-3des esp-md5-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 201, flow_id: 2, crypto map: aptmap
sa timing: remaining key lifetime (k/sec): (4607997/3550)
IV size: 8 bytes
replay detection support: Y
outbound ah sas:
outbound pcp sas:

sv1-6#show crypto engine conn act
ID Interface IP-                  Address State Algorithm  Encrypt  Decrypt
1 Ethernet0/0 209.165.202.226    set HMAC_MD5+3DES_56_C      0        0
200 Ethernet0/0 209.165.202.226  set HMAC_MD5+3DES_56_C      0        24
201 Ethernet0/0 209.165.202.226  set HMAC_MD5+3DES_56_C      21       0
```

Información Relacionada

- Página de soporte de IPSec
- Soporte Técnico - Cisco Systems