在检查点NG和路由器之间配置IPSec隧道

目录

简介

本文档说明如何使用预共享密钥来构建 IPSec 隧道以加入两个专用网络：

- 路由器内的172.16.15.x专用网络。
- CheckpointTM下一代(NG)内的192.168.10.x专用网络。

先决条件

要求

本文档中概述的程序基于这些假设。

- 已设置CheckpointTM NG基本策略。
- 配置了所有访问、网络地址转换(NAT)和路由设置。
- 从路由器内部和CheckpointTM NG内部到Internet的流量。

使用的组件

本文档中的信息基于以下软件和硬件版本：

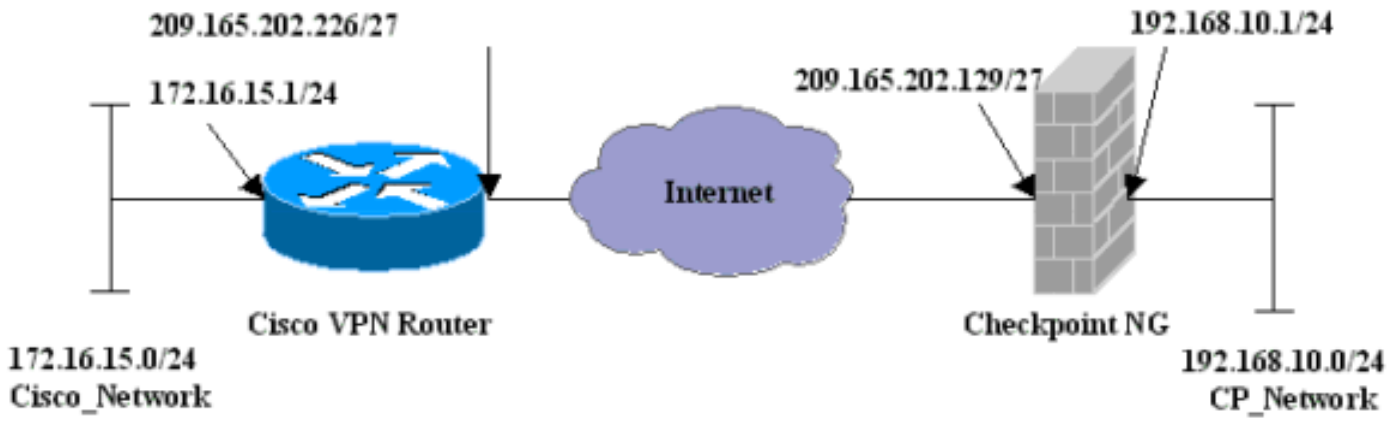
- Cisco 1751 路由器
- 思科IOS®软件(C1700-K9O3SY7-M)，版本12.2(8)T4，版本软件(fc1)

- CheckpointTM NG内部版本50027

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

网络图

本文档使用以下网络设置：



规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

配置Cisco 1751 VPN路由器

思科VPN 1751路由器

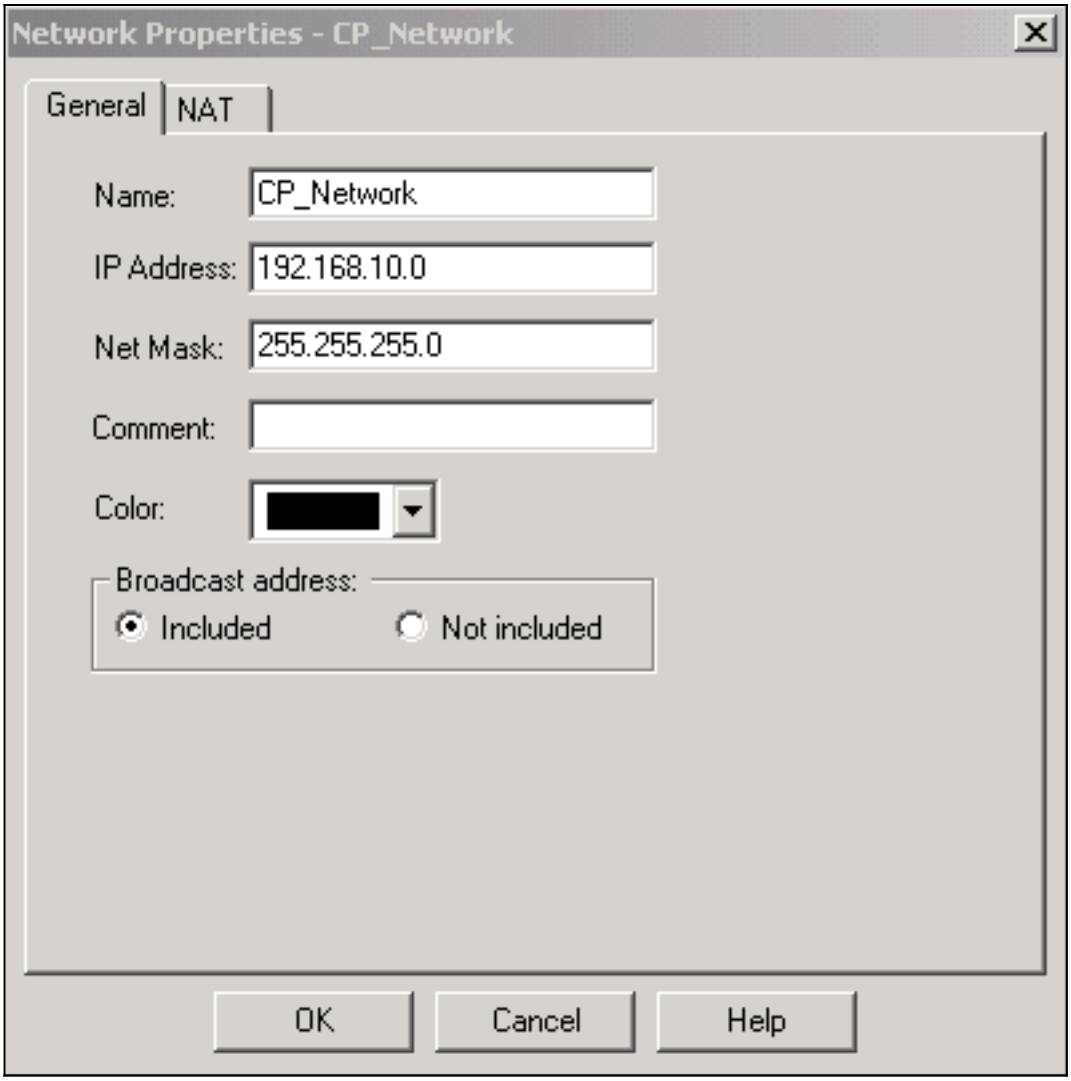
```
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
hostname sv1-6
memory-size iomem 15
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip subnet-zero
no ip domain-lookup
ip audit notify log
ip audit po max-events 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
```

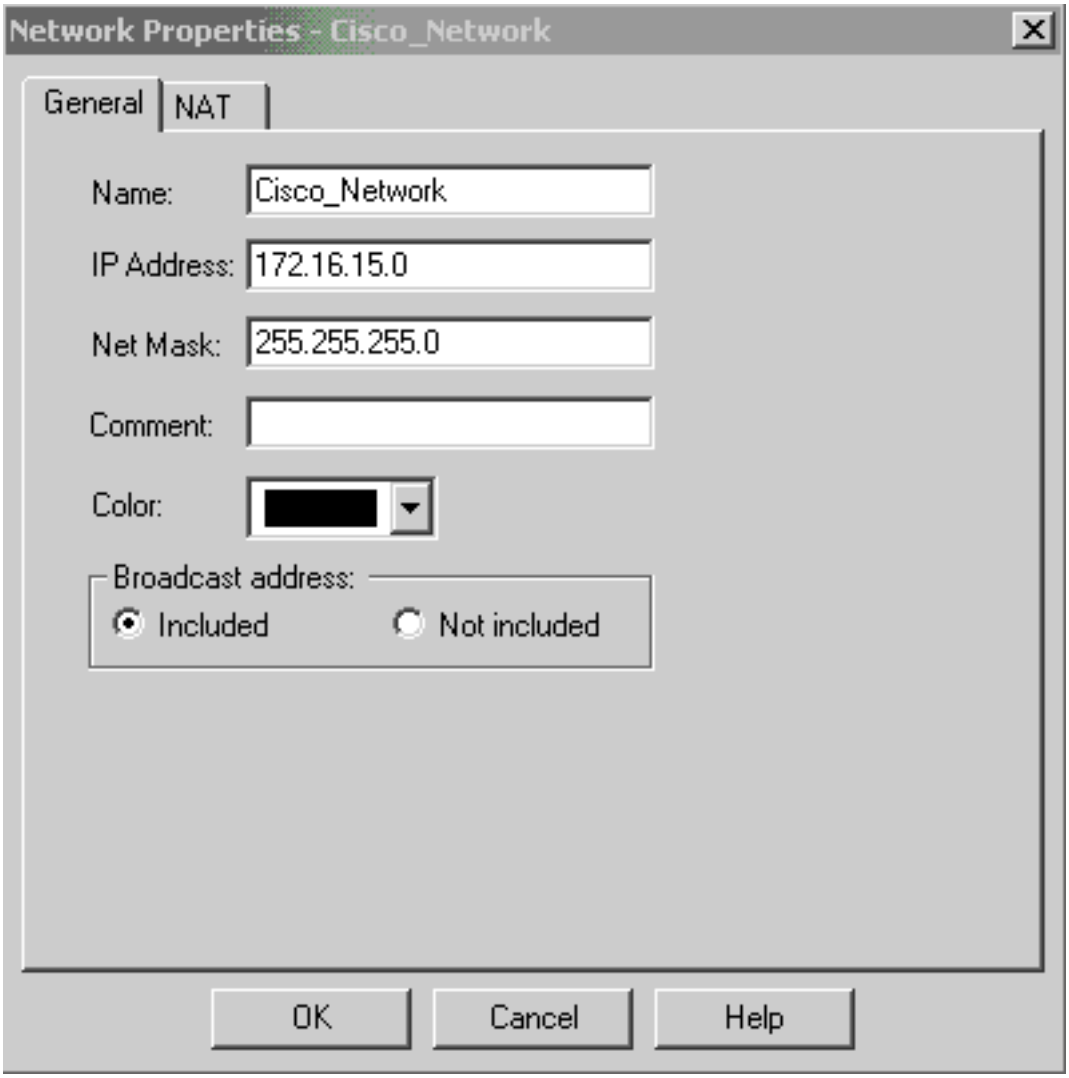
```
  set peer 209.165.202.129
  set transform-set aptset
  match address 110
!
interface Ethernet0/0
  ip address 209.165.202.226 255.255.255.224
  ip nat outside
  half-duplex
  crypto map aptmap
!
interface FastEthernet0/0
  ip address 172.16.15.1 255.255.255.0
  ip nat inside
  speed auto
!--- NAT 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
```

配置检查点NG

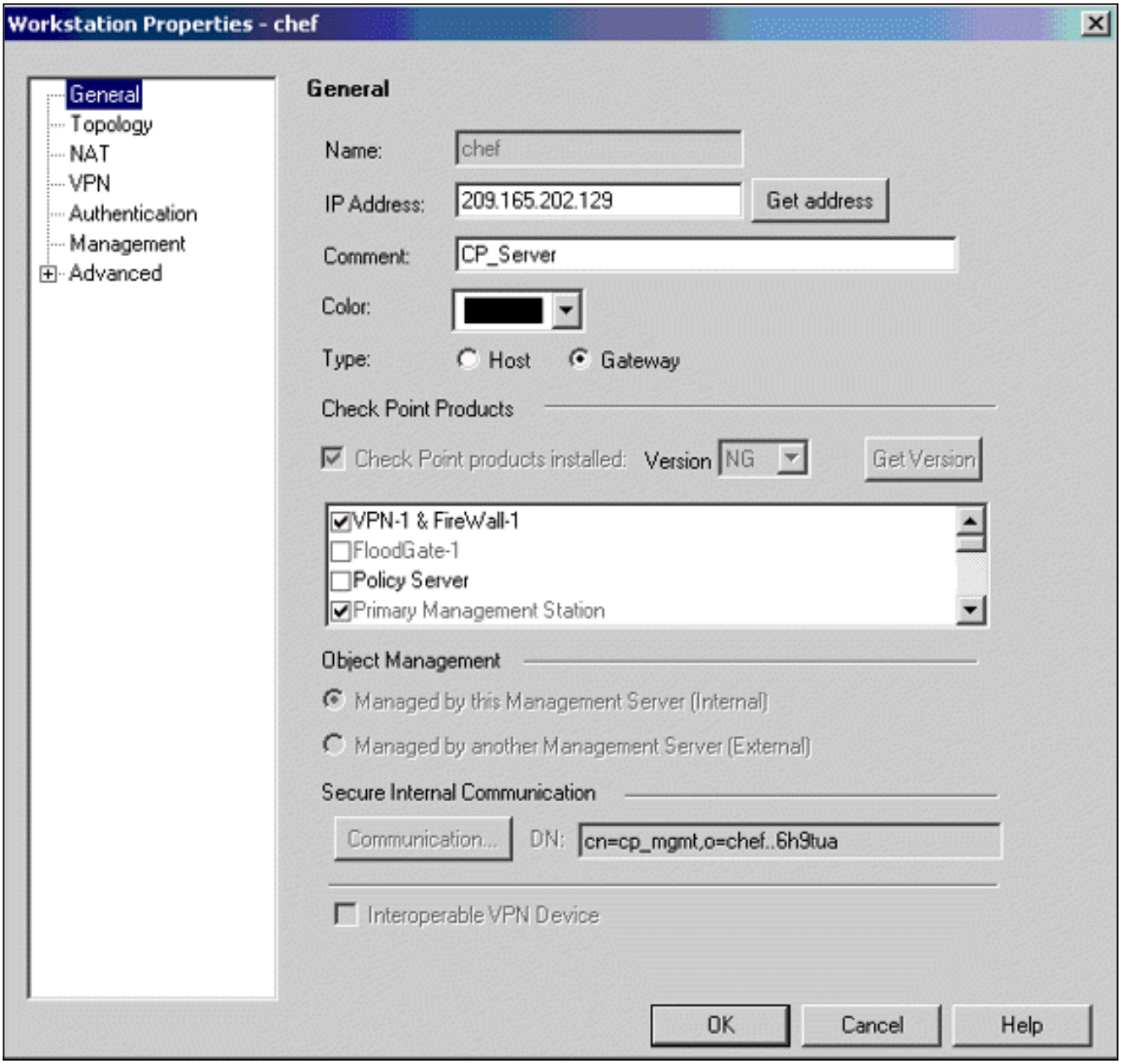
CheckpointTM NG是面向对象的配置。定义网络对象和规则以组成与要设置的VPN配置相关的策略。然后，使用CheckpointTM NG策略编辑器安装此策略，以完成VPN配置的CheckpointTM NG端。

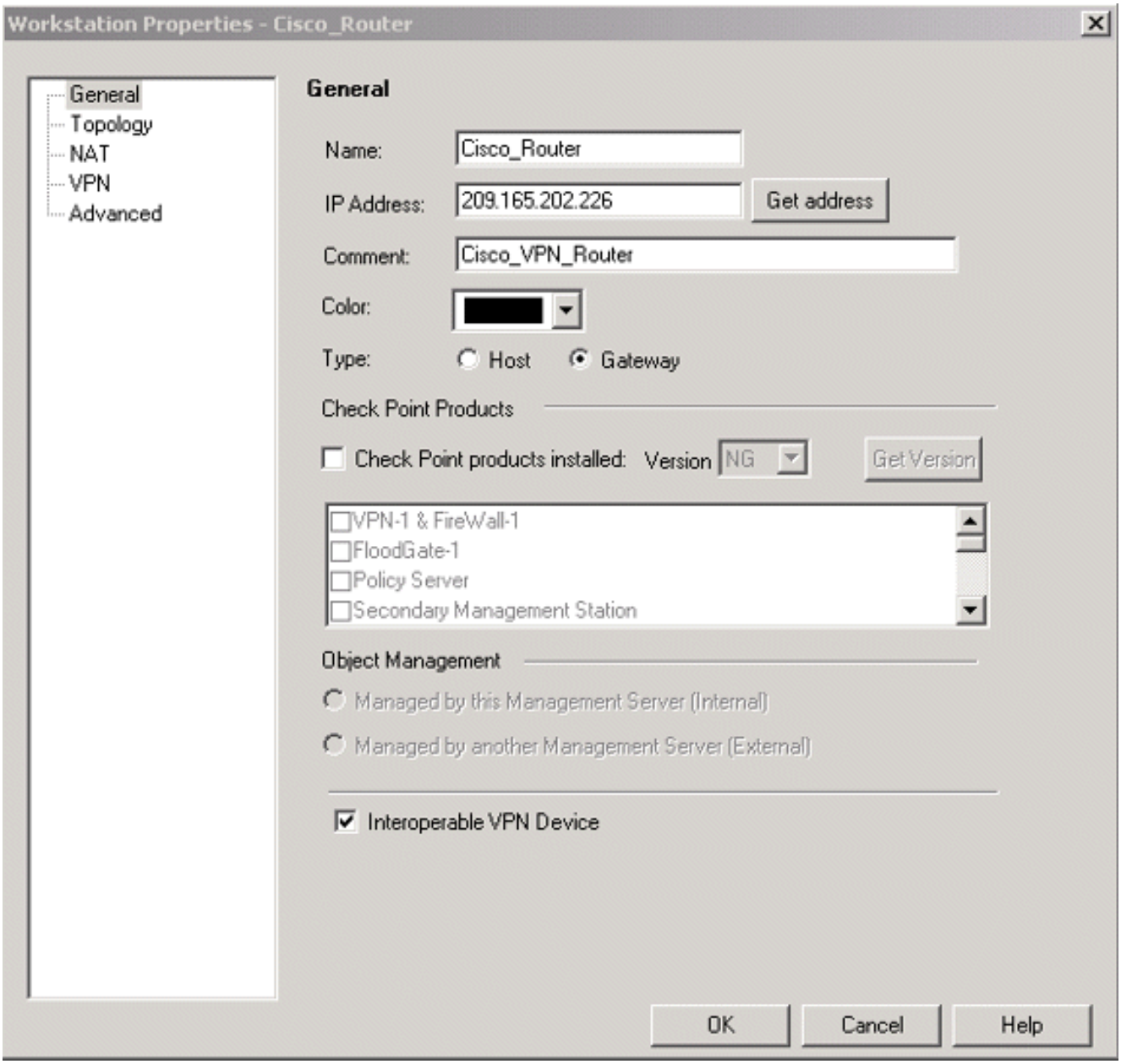
1. 创建Cisco网络子网和CheckpointTM NG网络子网作为网络对象。这是加密的。要创建对象，请选择“管理”>“网络对象”，然后选择“新建”>“网络”。输入适当的网络信息，然后单击OK。这些示例显示一组名为CP_Network和Cisco_Network的对象。


Network Properties - CP_Network
General
NAT
Name:
CP_Network
IP Address:
192.168.10.0
Net Mask:
255.255.255.0
Comment:
Color:
Broadcast address:
Included
Not included
OK
Cancel
Help

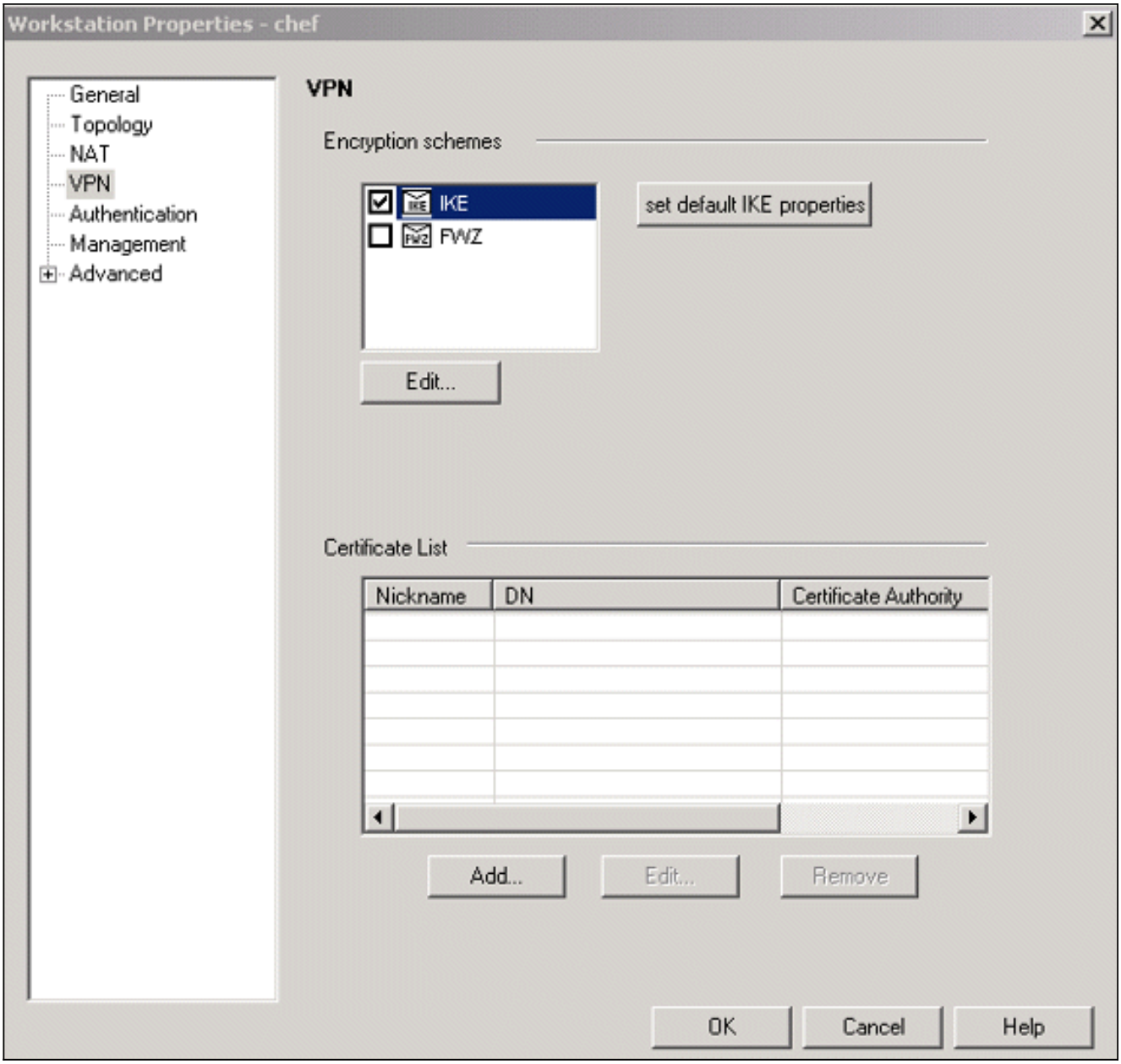


2. 将Cisco_Router和Checkpoint_NG对象创建为工作站对象。这些是VPN设备。要创建对象，请选择“**管理**”>“**网络对象**”，然后选择“**新建**”>“**工作站**”。注意您能使用在最初的CheckpointTM NG设置期间创建的CheckpointTM NG工作站对象。选择选项，将工作站设置为**网关**和可**互操作VPN设备**。这些示例显示一组名为chef和Cisco_Router的对象。

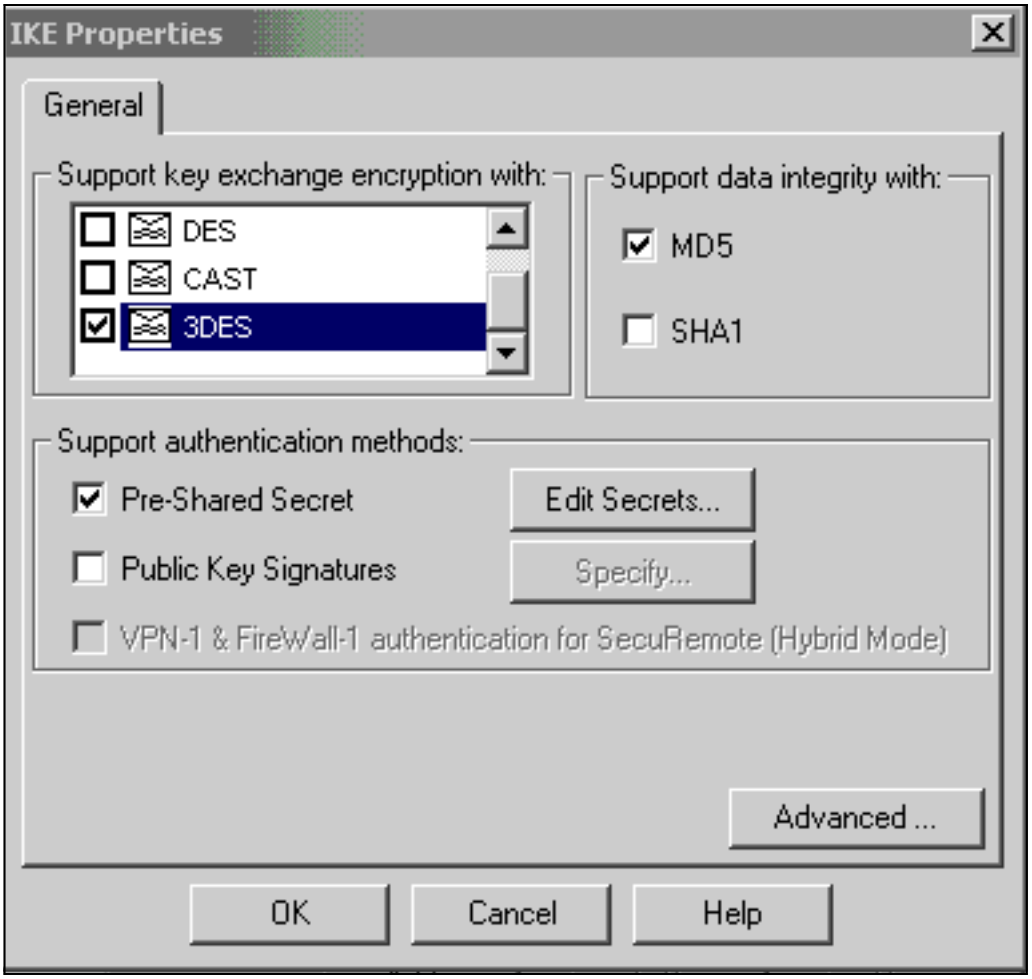

Workstation Properties - chef
General
Topology
NAT
VPN
Authentication
Management
Advanced
General
Name:
chef
IP Address:
209.165.202.129
Get address
Comment:
CP_Server
Color:
Type:
Host
Gateway
Check Point Products
Check Point products installed:
Version
NG
Get Version
VPN-1 & FireWall-1
FloodGate-1
Policy Server
Primary Management Station
Object Management
Managed by this Management Server (Internal)
Managed by another Management Server (External)
Secure Internal Communication
Communication...
DN:
cn=cp_mgmt,o=chef..6h9tua
Interoperable VPN Device
OK
Cancel
Help



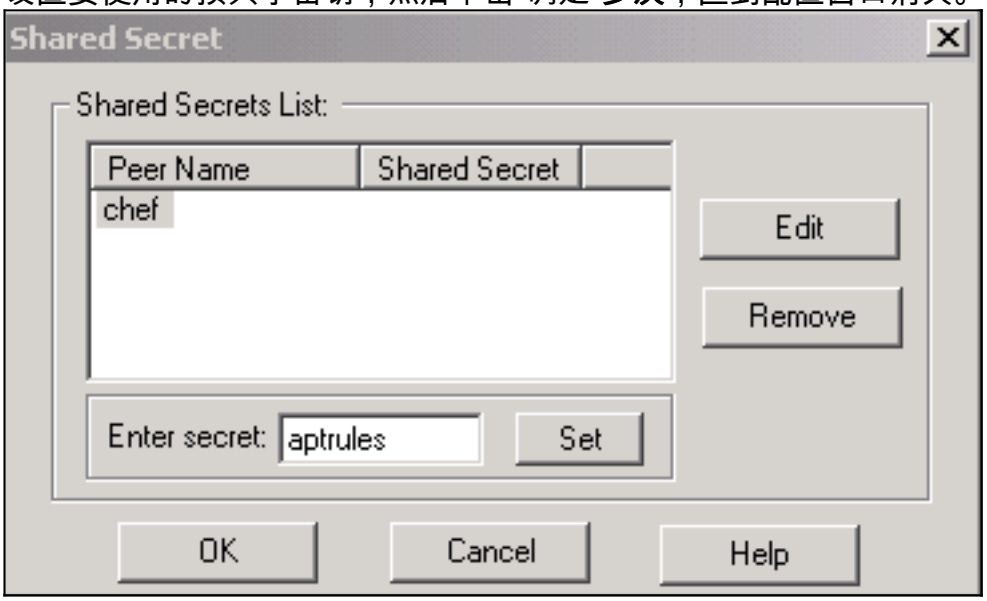
3. 在VPN选项卡上配置IKE，然后单击**Edit**。



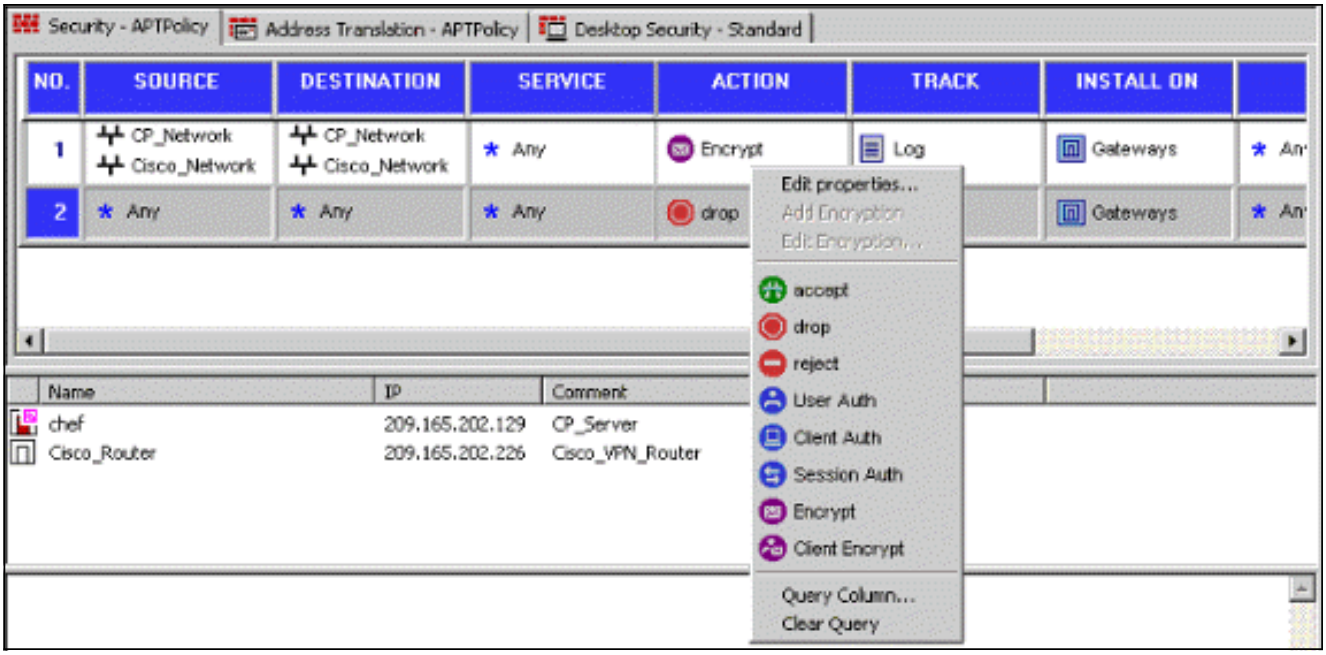
4. 配置密钥交换策略，然后单击“编辑**密钥**”。



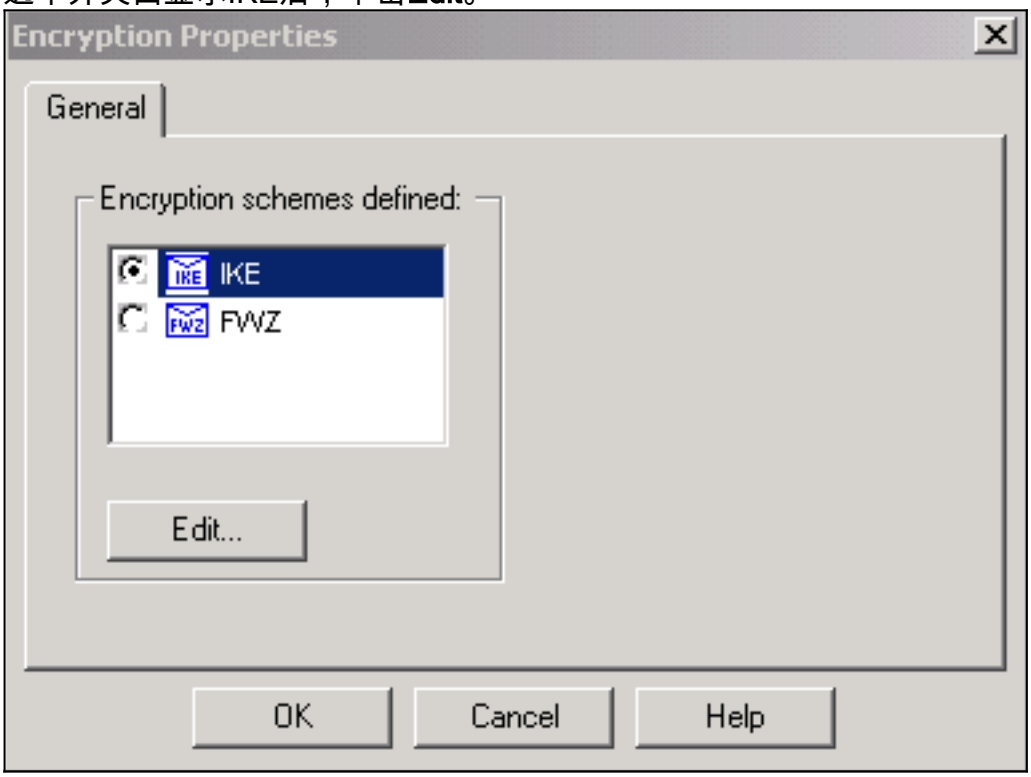
5. 设置要使用的预共享密钥，然后单击“确定”**多次**，直到配置窗口消失。



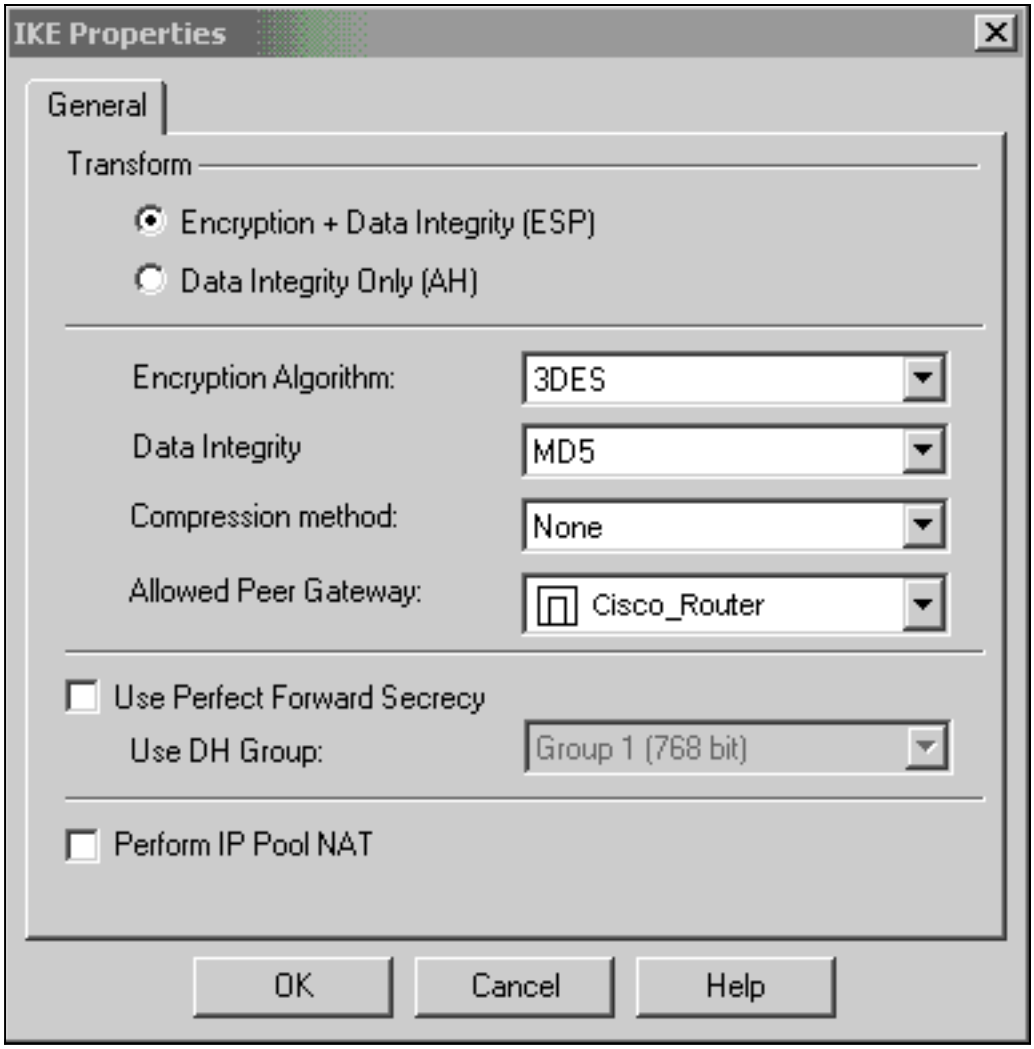
6. 选择**Rules > Add Rules > Top**以配置策略的加密规则。顶部的规则是在绕过加密的任何其他规则之前执行的第一个规则。配置源和目标以包括CP_Network和Cisco_Network，如下所示。添加规则的“加密操作”部分后，右键单击“操作”，**然后选择**“编辑**属性**”。



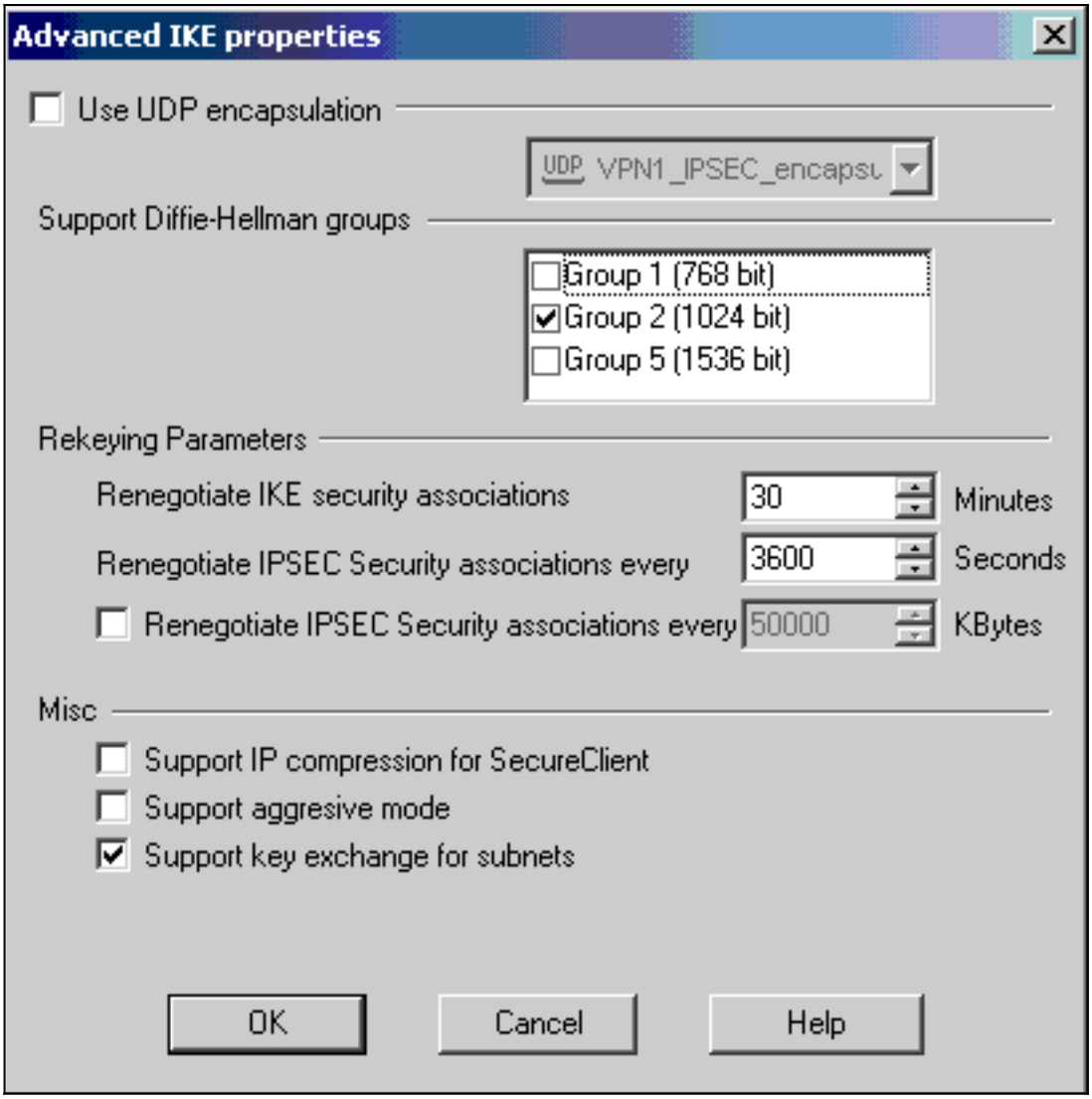
7. 选中并突出显示IKE后，单击**Edit**。



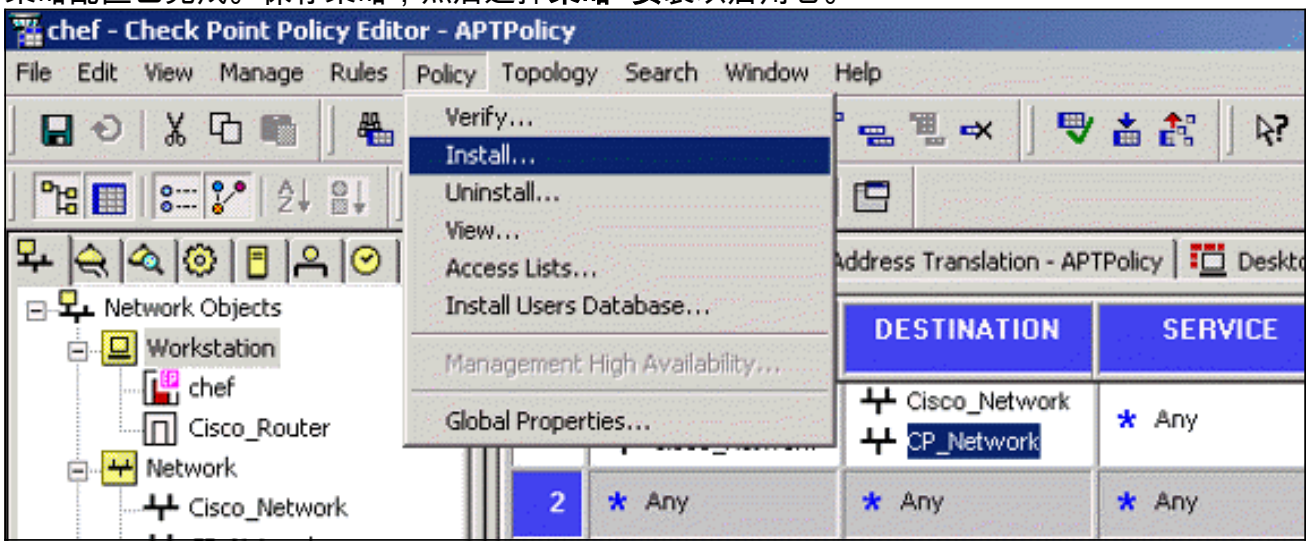
8. 确认IKE配置。



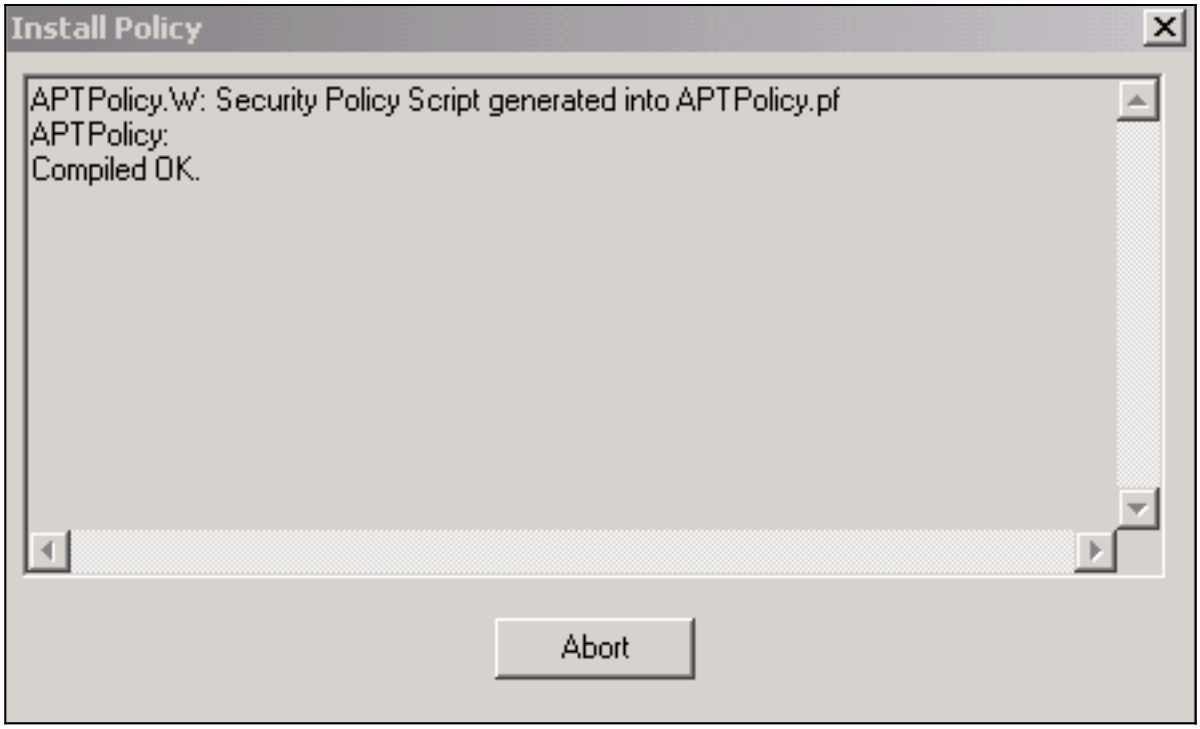
9. 在思科设备和其他IPSec设备之间运行VPN的主要问题之一是密钥交换重新协商。确保Cisco路由器上IKE交换的设置与CheckpointTM NG上配置的设置完全相同。**注：此**参数的实际值取决于您的特定公司安全策略。在本示例中，使用lifetime 1800命令将路由器上的IKE配置设**置为30**分钟。必须在CheckpointTM NG上设置相同的值。要在CheckpointTM NG上设置此值，请选**择Manage Network Object**，然后选**择CheckpointTM** NG对象，然后单击**Edit**。然后选择**VPN**，并编辑IKE。选择**Advance**并配置Rekeying Parameters。为CheckpointTM NG网络对象配置密钥交换后，请对Cisco_Router网络对象执行相同的密钥交换重新协商配置。**注：确**保选择了正确的Diffie-Hellman组，以匹配路由器上配置的组。



10. 策略配置已完成。保存策略，然后选择**策略>安**装以启用它。



安装窗口在编译策略时显示进度说明。



当安装窗口表明策略安装完成时，点击Close完成程序。

验证

本部分所提供的信息可用于确认您的配置是否正常工作。

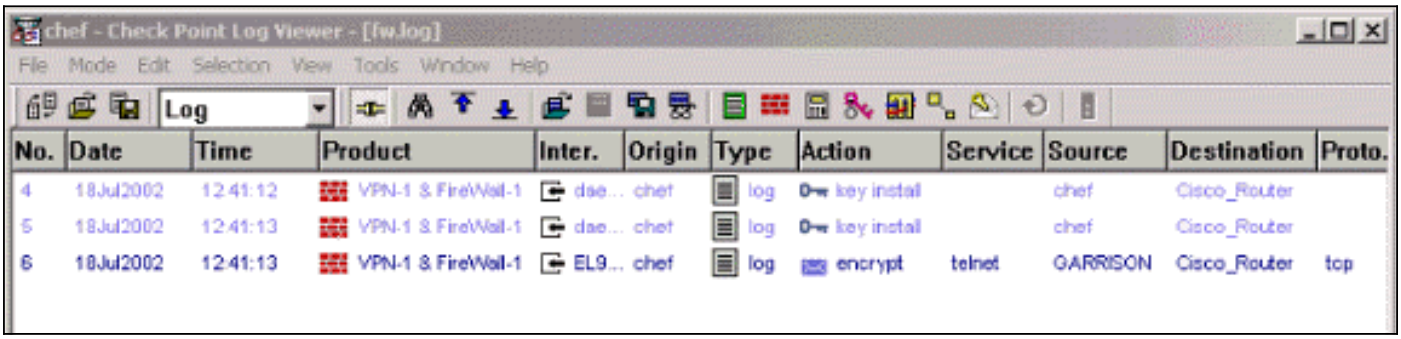
检验Cisco路由器

命令输出解释程序工具（仅限注册用户）支持某些 show 命令，使用此工具可以查看对 show 命令输出的分析。

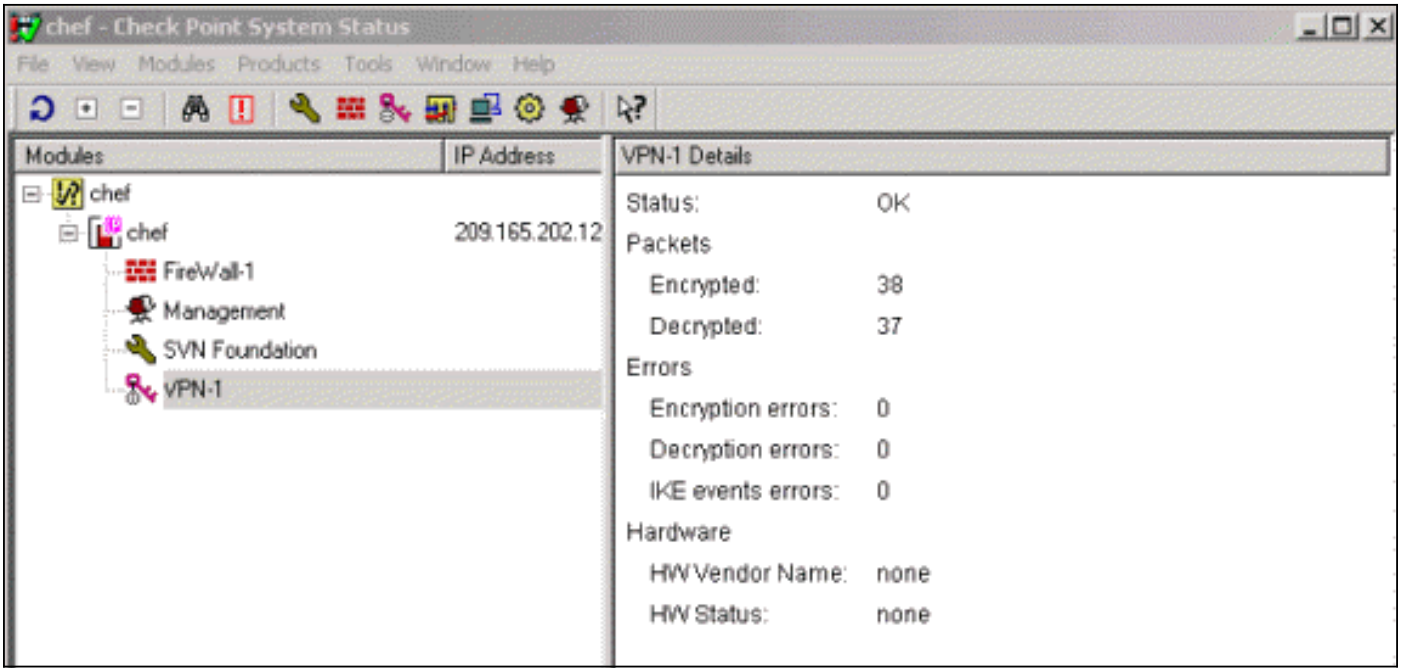
- show crypto isakmp sa - 显示对等体上的所有当前 IKE 安全关联 (SA)。
- show crypto ipsec sa - 显示当前 SA 使用的设置。

检验检查点NG

要查看日志，请选择“窗口”>“日志查看器”。



要查看系统状态，请选择“窗口”>“系统状态”。



故障排除

Cisco 路由器

本部分提供的信息可用于对配置进行故障排除。

有关其他故障排除信息，请参阅IP安全故障排除 — 了解和使用debug命令。

注意：在发出debug命令之前，请参阅有关Debug命令的重要信息。

- debug crypto engine - 显示有关执行加密和解密的加密引擎的 debug 消息。
- debug crypto isakmp — 显示关于 IKE 事件的消息。
- debug crypto ipsec — 显示 IPSec 事件。
- clear crypto isakmp - 清除所有活动的 IKE 连接。
- clear crypto sa - 清除所有 IPSec SA。

调试日志输出成功

```
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
```

相关信息

- IPSec 支持页面
- 技术支持 - Cisco Systems