配置在Cisco路由器和检查点NG之间的一个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：

- 172.16.15.x私有网络在路由器里面。
- 192.168.10.x私有网络在Checkpoint™下一代(NG)里面。

先决条件

要求

在本文略述的步骤根据这些假设。

- Checkpoint TM NG基本策略设置。
- 所有访问、网络地址转换(NAT)和路由设置配置。
- 从路由器和里面里边的流量对互联网的Checkpoint TM NG流。

使用的组件

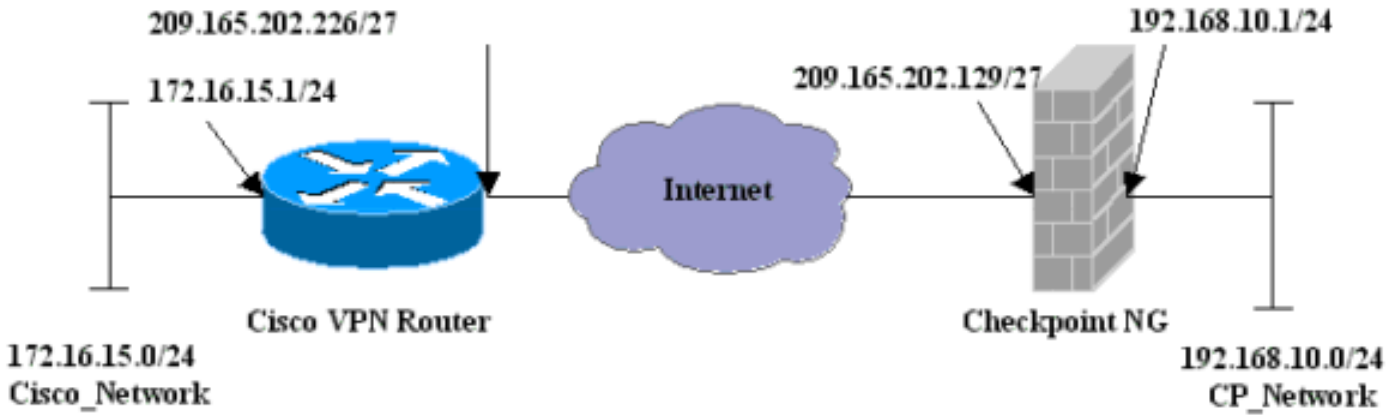
本文档中的信息基于以下软件和硬件版本：

- Cisco 1751 路由器
- Cisco IOS软件(C1700-K9O3SY7-M)，版本12.2(8)T4，发行软件(fc1)
- Checkpoint TM NG Build 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

Cisco VPN 1751路由器

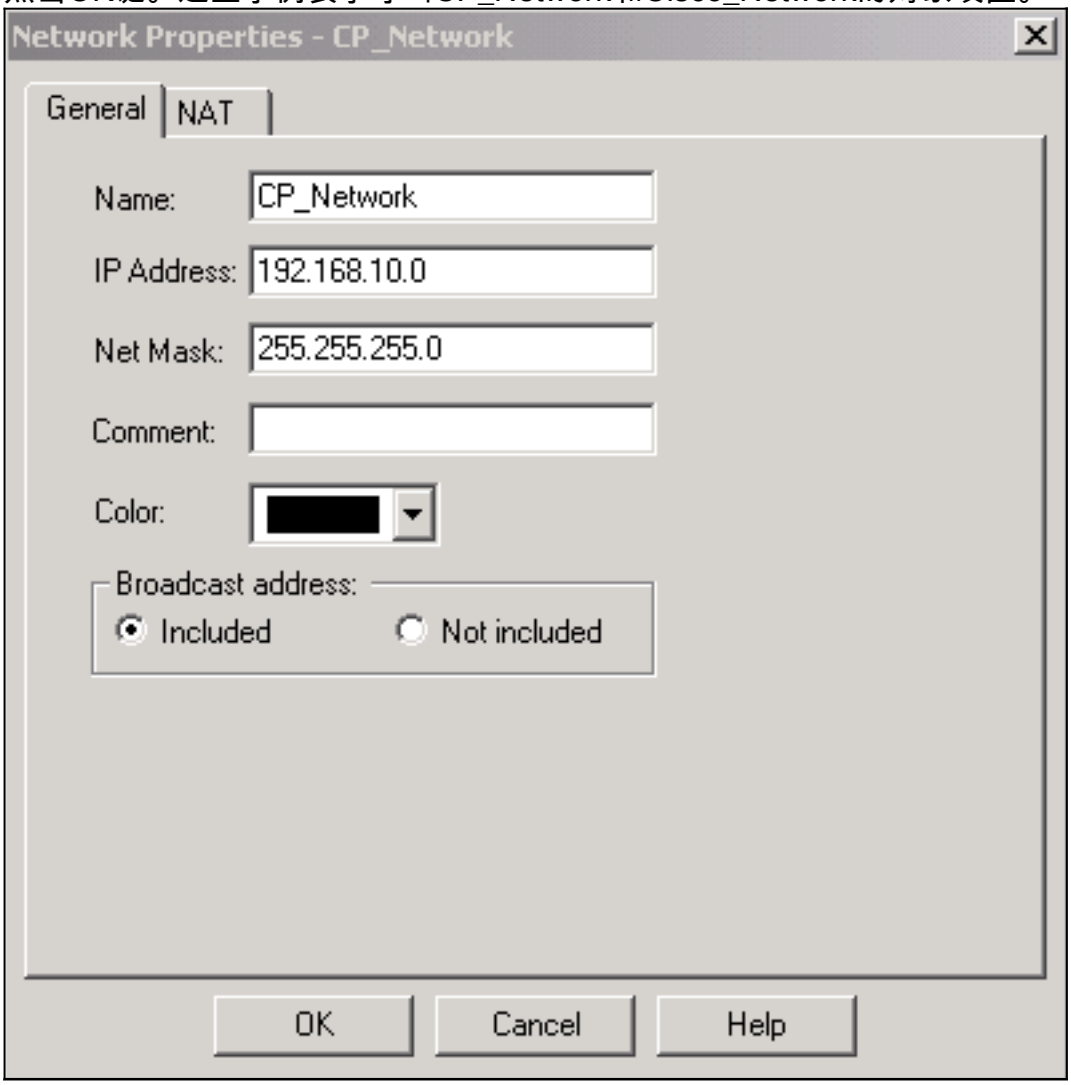
```
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
hostname sv1-6
memory-size iomem 15
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip subnet-zero
no ip domain-lookup
ip audit notify log
ip audit po max-events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

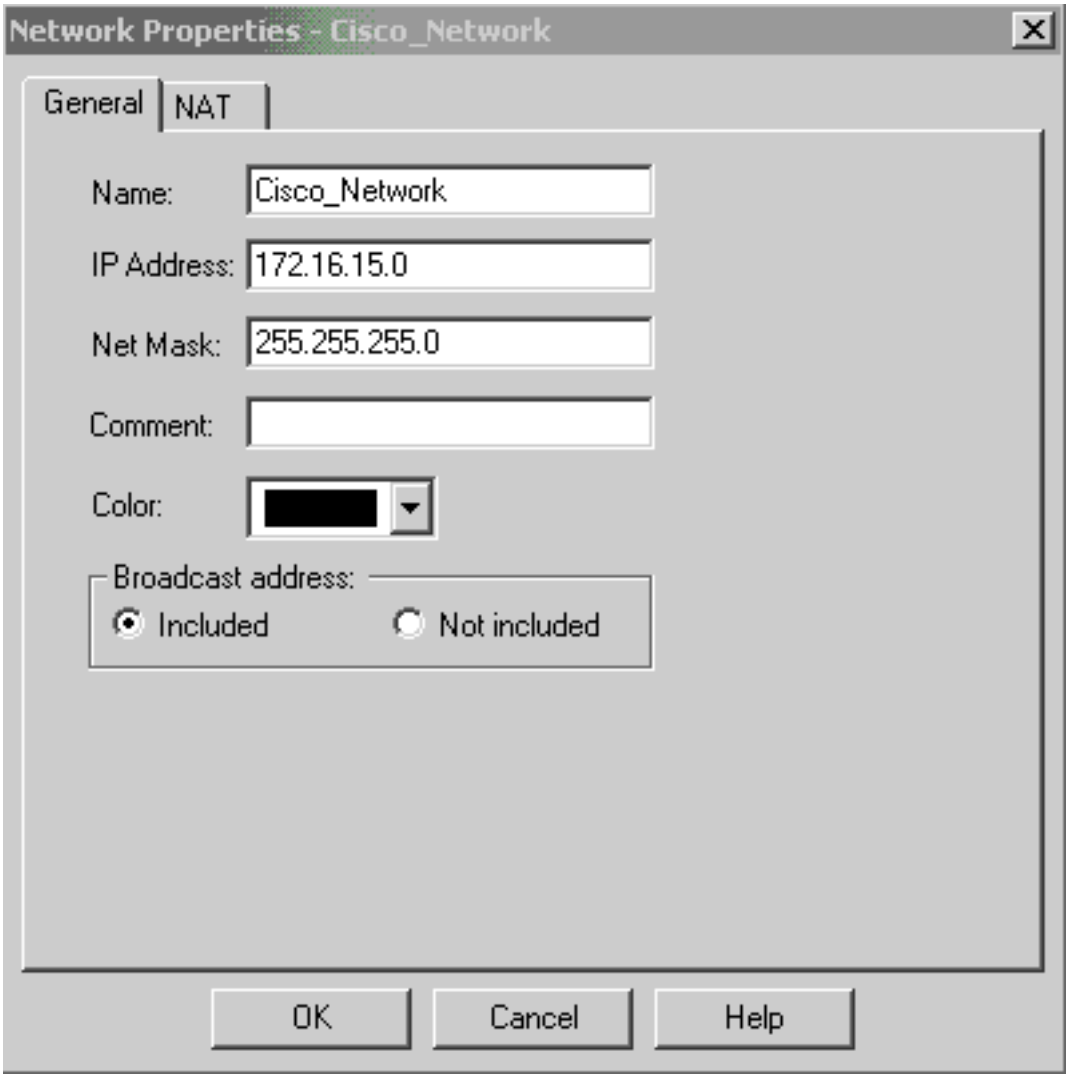
```
interface Ethernet0/0 overload ip classless ip route
0.0.0.0 0.0.0.0 209.165.202.225 no ip http server ip pim
bidir-enable !--- Encryption match address access list.
access-list 110 permit ip 172.16.15.0 0.0.0.255
192.168.10.0 0.0.0.255 !--- NAT access list. access-list
120 deny ip 172.16.15.0 0.0.0.255 192.168.10.0 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

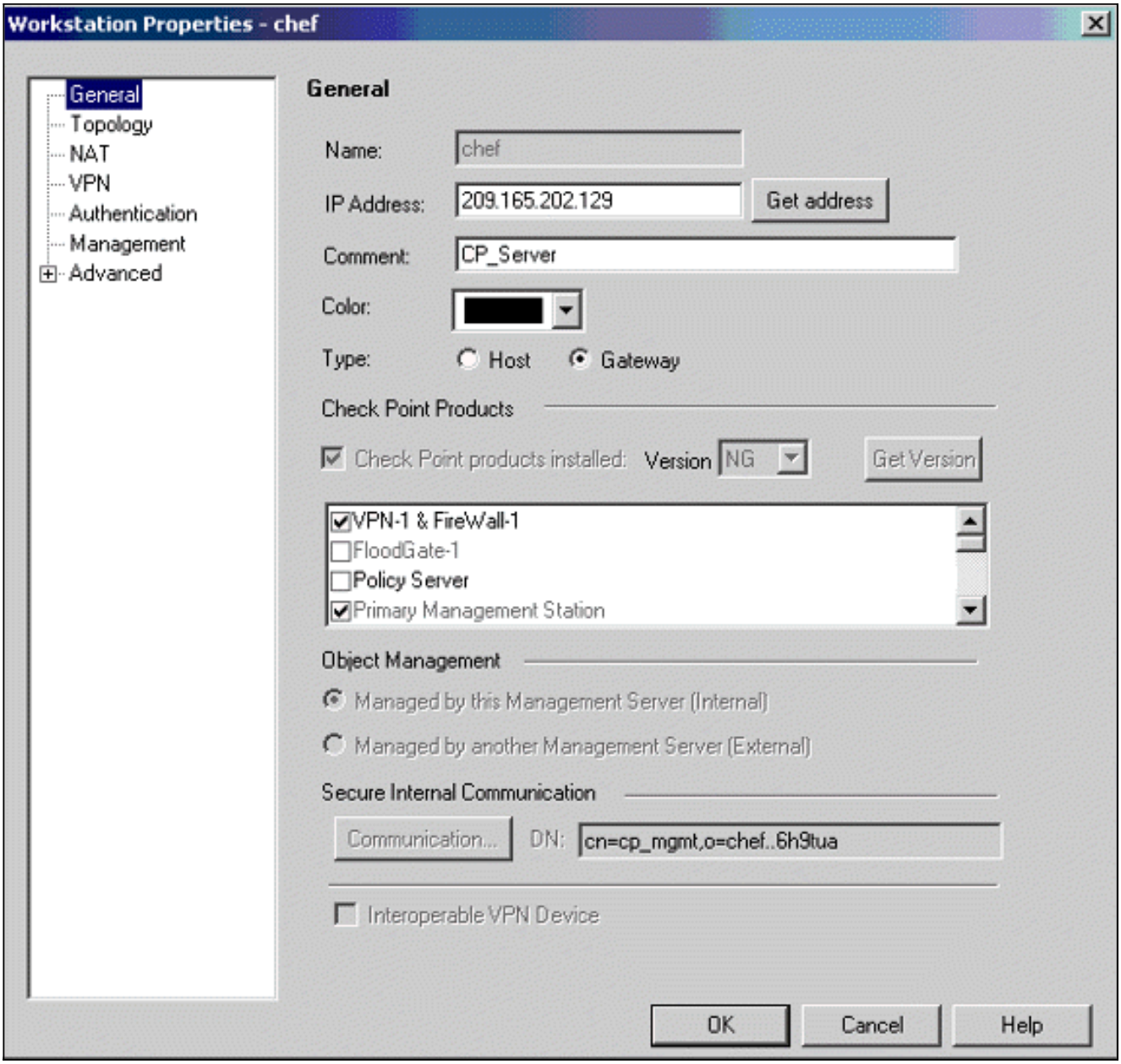
Checkpoint TM NG是一面向对象的配置。网络对象和规则定义组成适合于对将设置的VPN配置的策略。此策略然后安装使用Checkpoint TM NG策略编辑器完成VPN配置的Checkpoint TM NG侧。

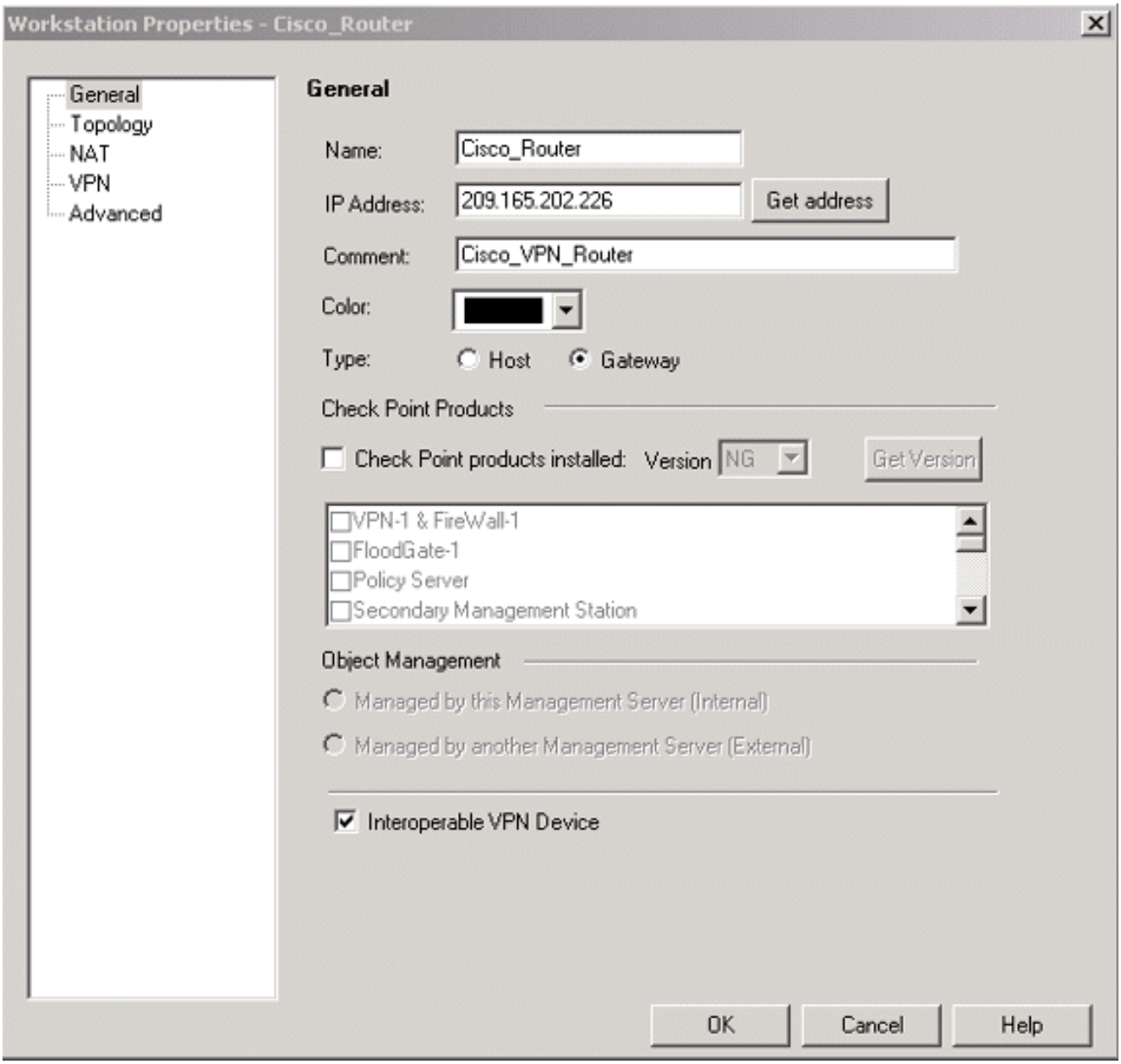
1. 创建Cisco网络子网和Checkpoint TM NG网络子网作为网络对象。这是什么加密。要创建对象，请选择**Manage > Network Objects**，然后选择**New > Network**。输入适当的网络信息，然后点击OK键。这些示例表示呼叫CP_Network和Cisco_Network的对象设置。



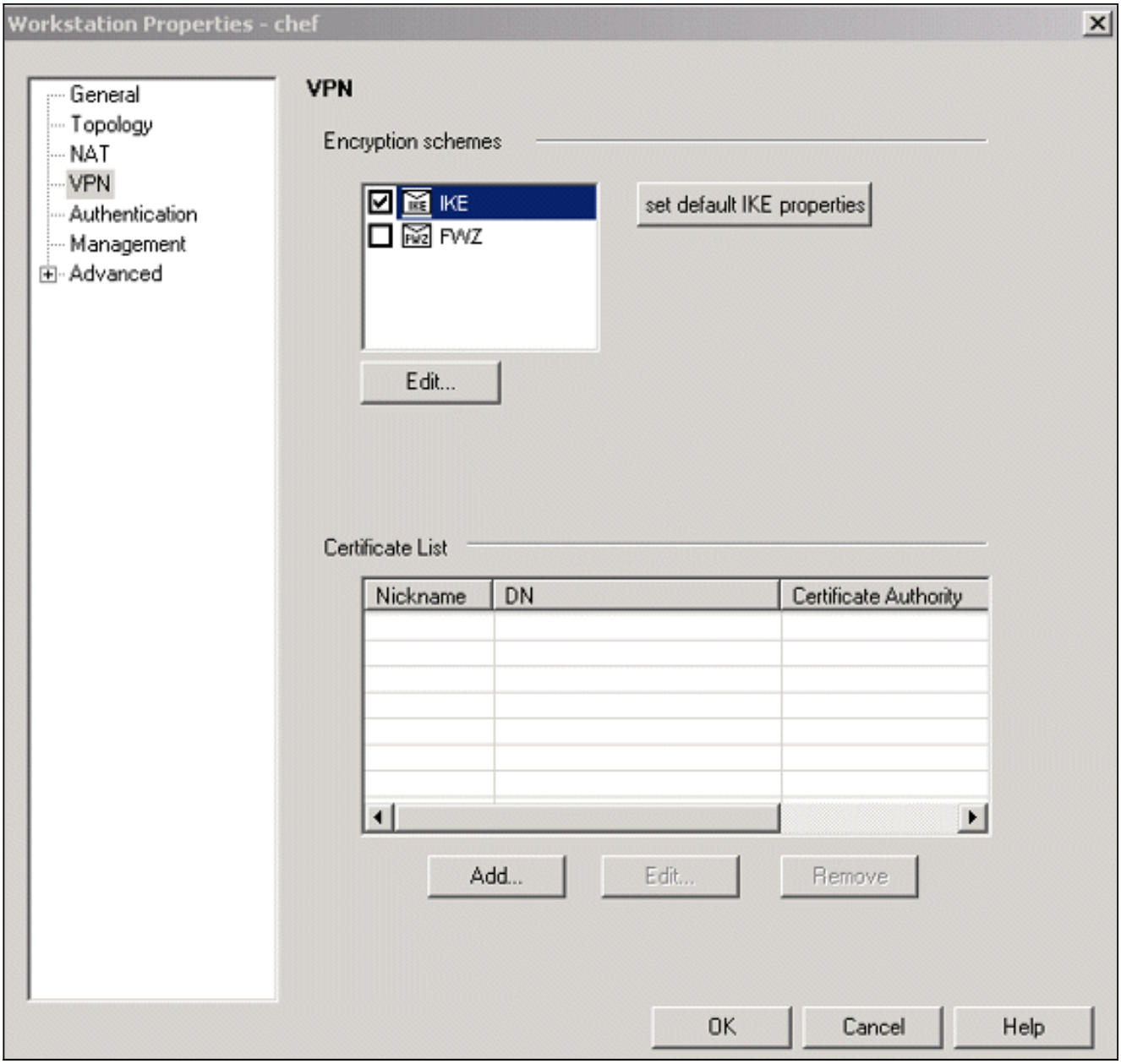


2. 创建Cisco_Router和Checkpoint_NG对象作为工作站对象。这些是VPN设备。要创建对象，请选择**Manage > Network Objects**，然后选择**New > Workstation**。注意您能使用在初始检查点 TM NG设置期间创建的Checkpoint TM NG工作站对象。选择选项设置工作站作为**网关**和**相互可操作的VPN设备**。这些示例表示呼叫主厨和Cisco_Router的对象设置。

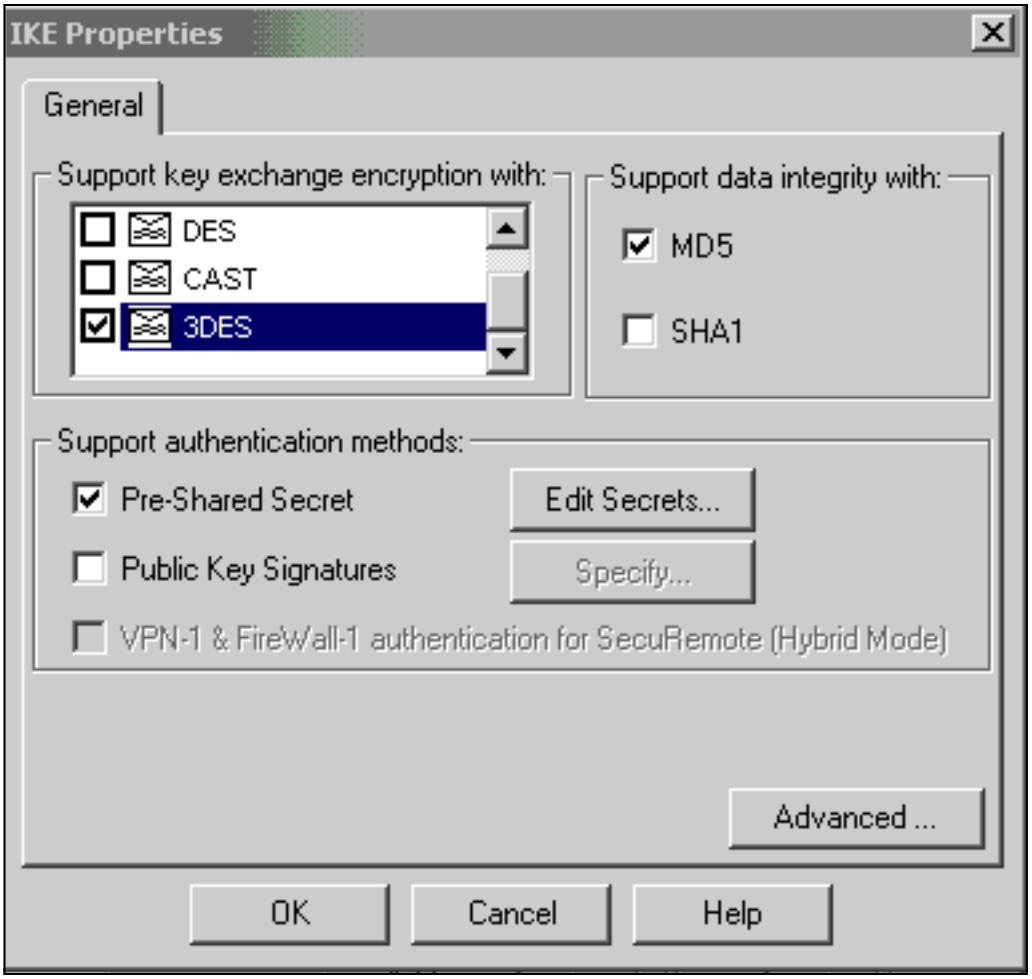

Workstation Properties - chef
General
Topology
NAT
VPN
Authentication
Management
Advanced
General
Name:
chef
IP Address:
209.165.202.129
Get address
Comment:
CP_Server
Color:
Type:
Host
Gateway
Check Point Products
Check Point products installed:
Version
NG
Get Version
VPN-1 & FireWall-1
FloodGate-1
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



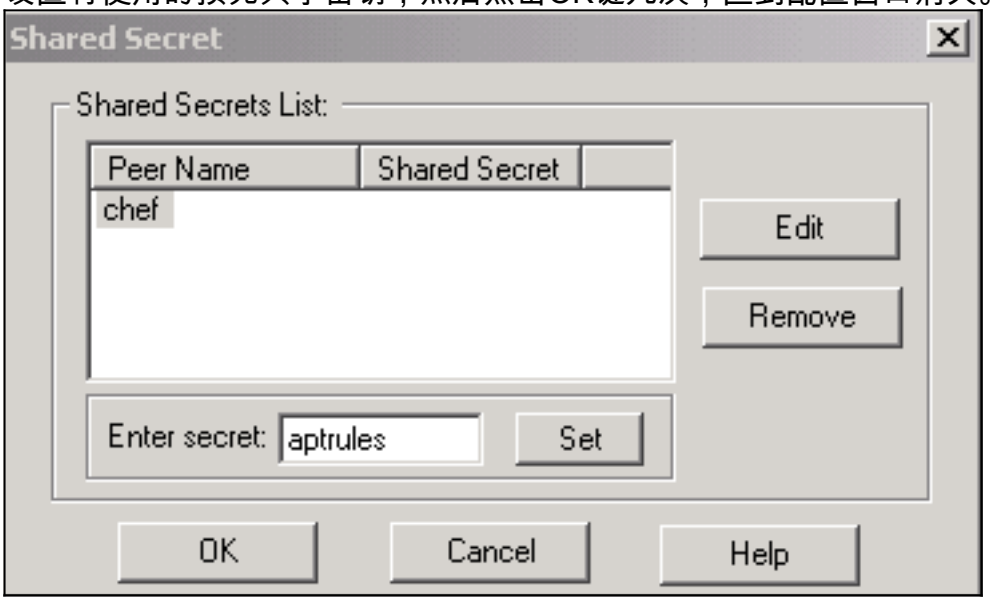
3. 配置在VPN选项的IKE，然后单击**编辑**。



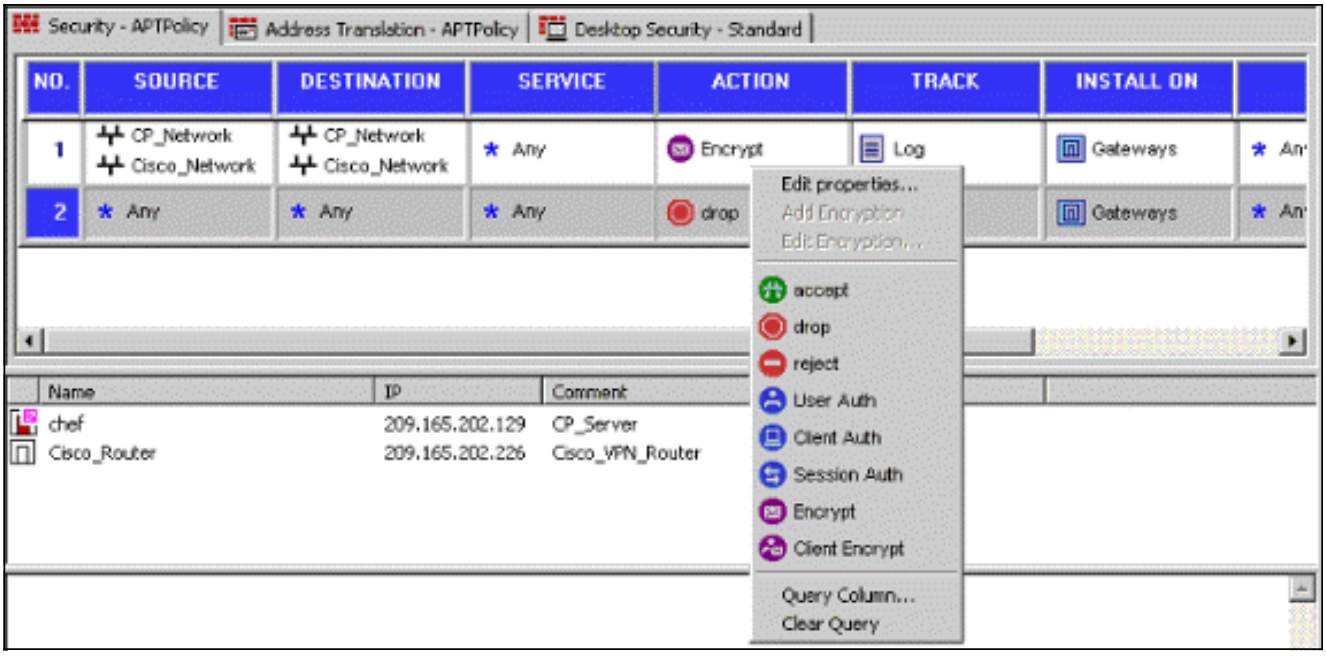
4. 配置密钥交换策略，并且单击**编辑秘密**。



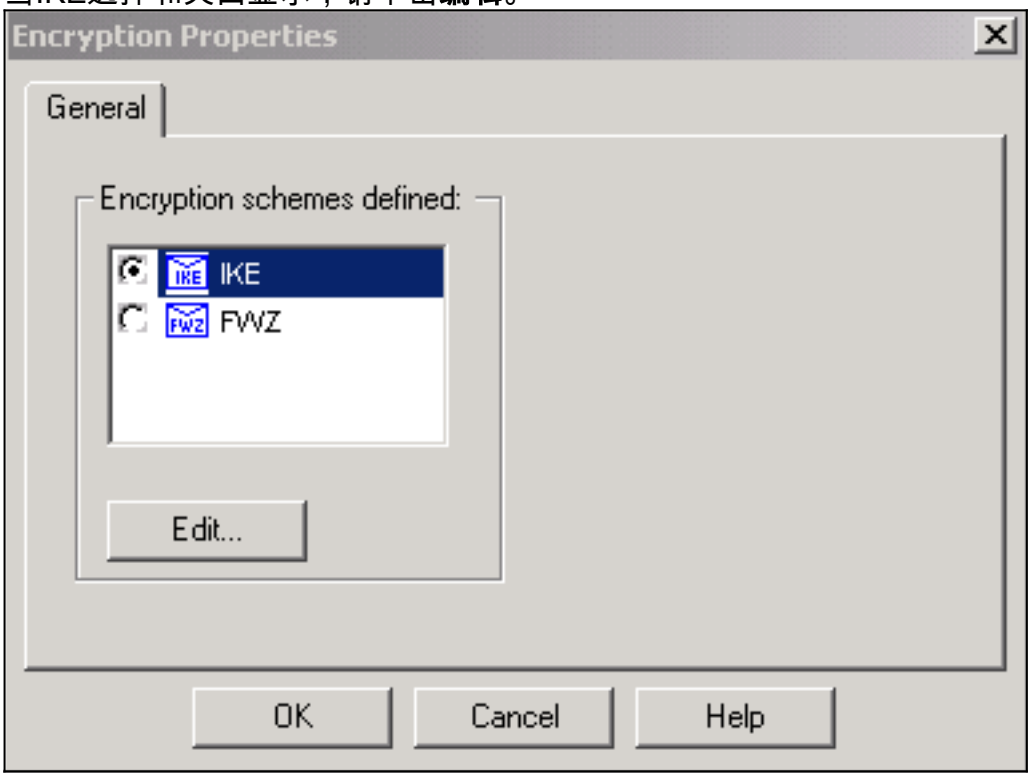
5. 设置将使用的预先共享密钥，然后点击OK键几次，直到配置窗口消失。

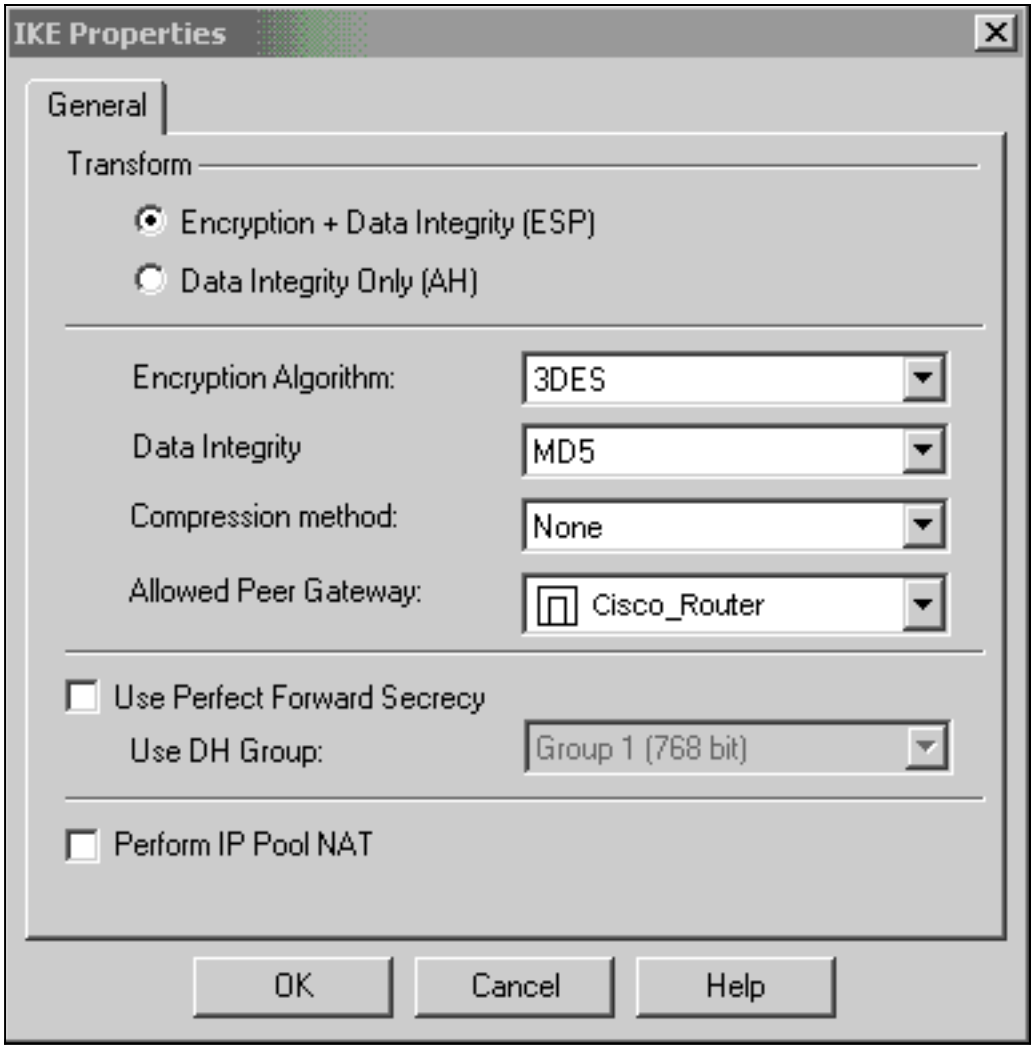


6. 选择**Rules > Add Rules > Top**配置策略的加密规则。在上面的规则是在可能绕过加密的其他规则前执行的第一个规则。配置源和目的包括CP_Network和Cisco_Network，如显示此处。一旦添加了规则的加密行为部分，请用鼠标右键单击**操作**并且选择**Edit Properties**。

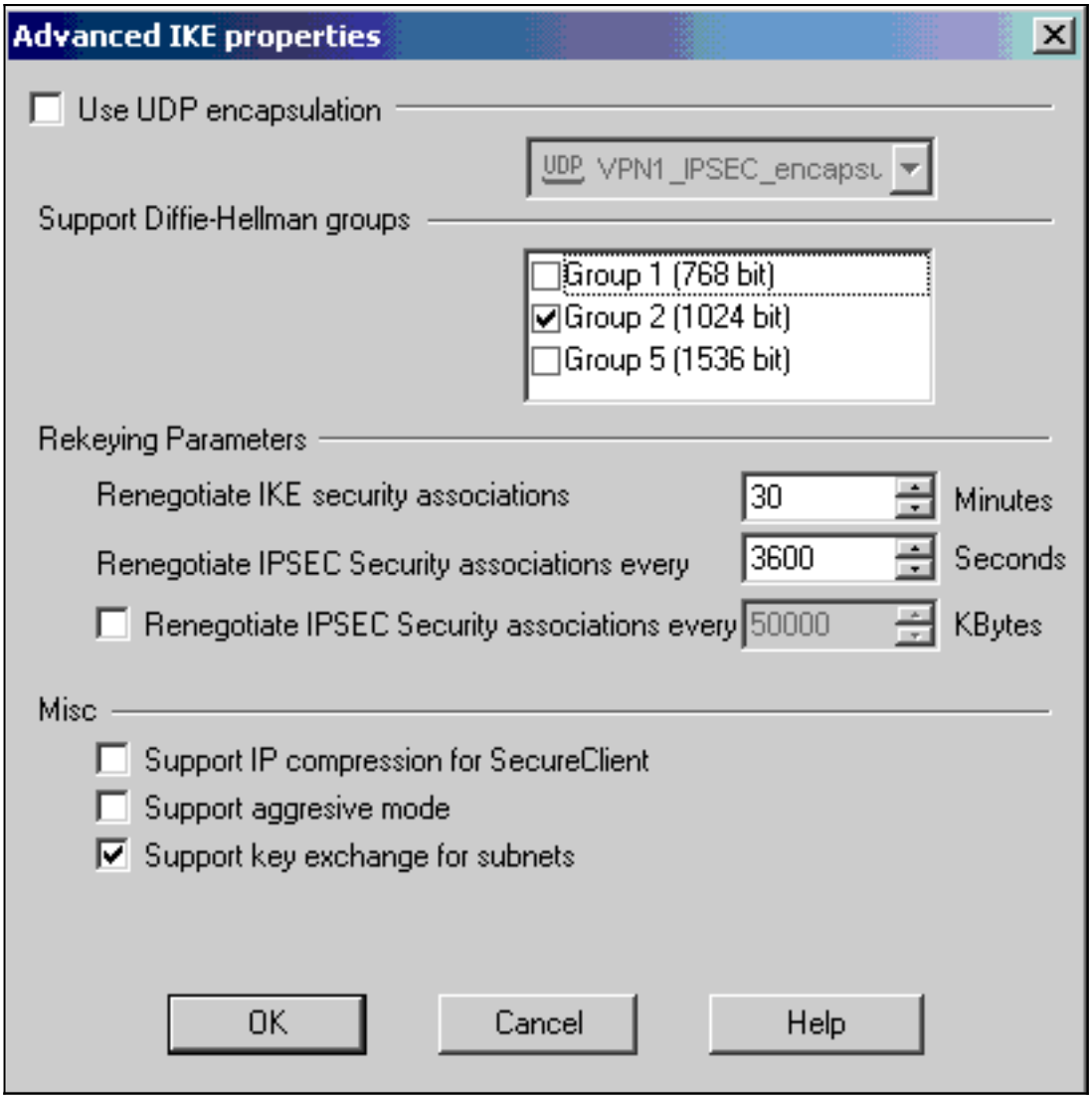


7. 当IKE选择和突出显示，请单击**编辑**。

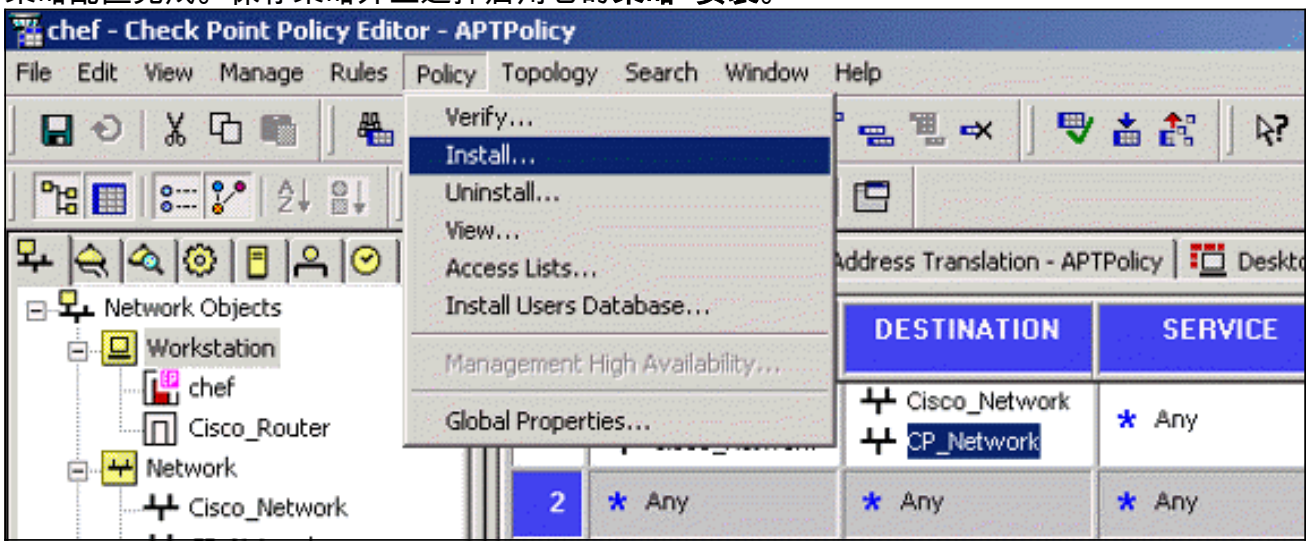




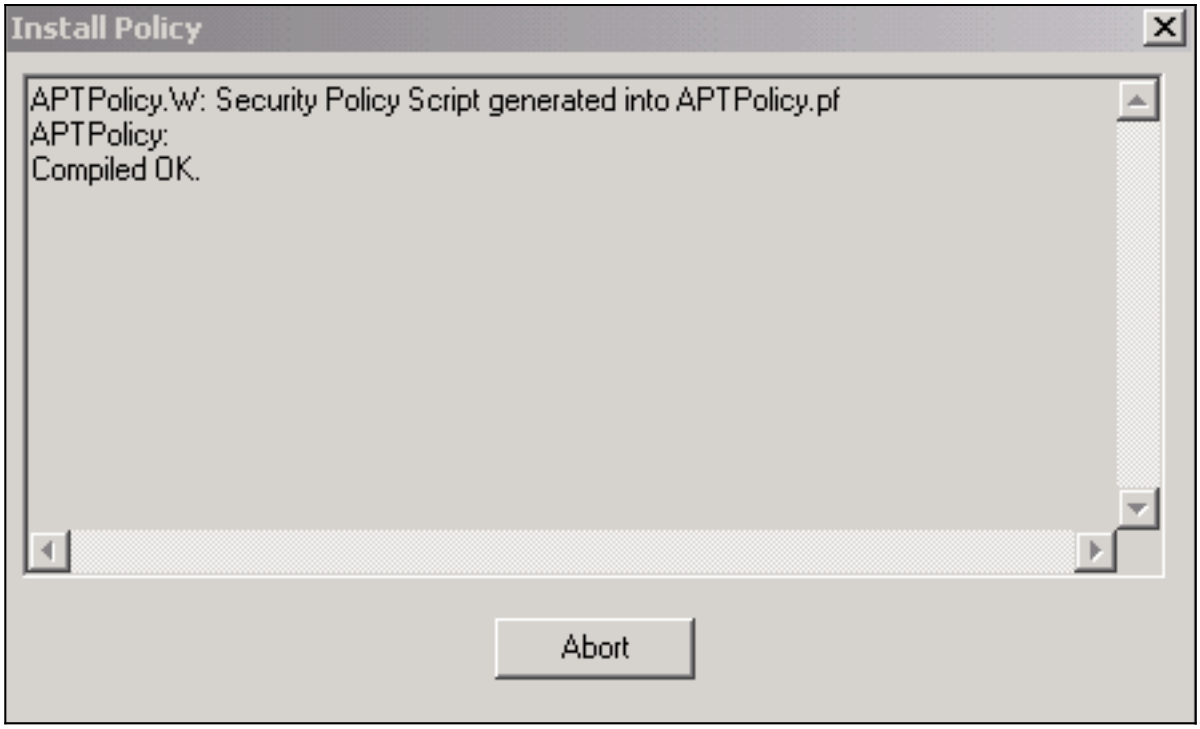
8. 确认IKE配置。
9. 其中一个关于运行VPN的主要问题在Cisco设备和其他IPSec设备之间是密钥交换重新协商。保证IKE交换的设置在Cisco路由器正确地是相同的象在Checkpoint TM NG配置的那。**注意：** 实际值此参数依靠您特定的公司安全策略。在本例中，在路由器的IKE配置设置为30分钟用**lifetime 1800命令**。同一个值在Checkpoint TM NG必须设置。要设置在Checkpoint TM NG的此值，选择请**管理网络对象**，然后选择Checkpoint TM NG对象并且单击**编辑**。然后请选择**VPN**，并且编辑IKE。选择**预付款**并且配置重新生成密钥的参数。在您配置Checkpoint TM NG网络对象的后密钥交换，请执行密钥交换重新协商的相同的配置Cisco_Router网络对象的。**注意：** 保证您让正确迪菲–赫尔曼组选择匹配在路由器配置的那。



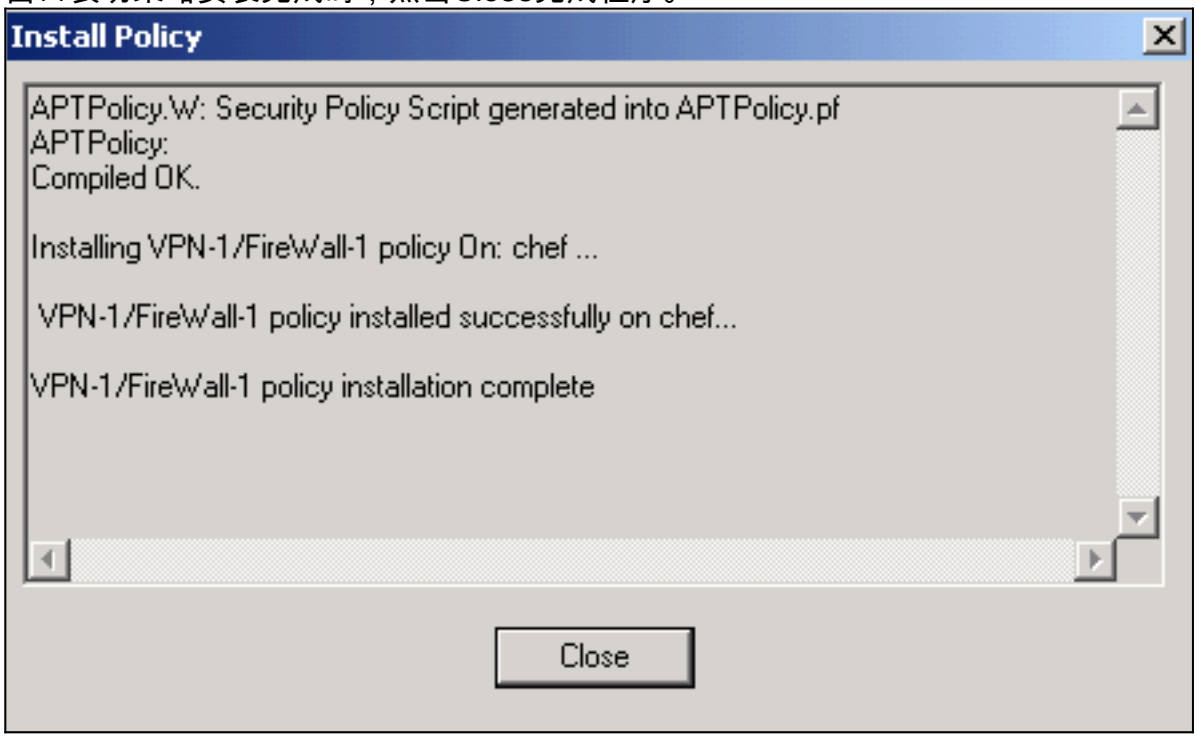
10. 策略配置完成。保存策略并且选择启用它的**策略>安装**。



当策略被编译，安装窗口显示进度注释。



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。

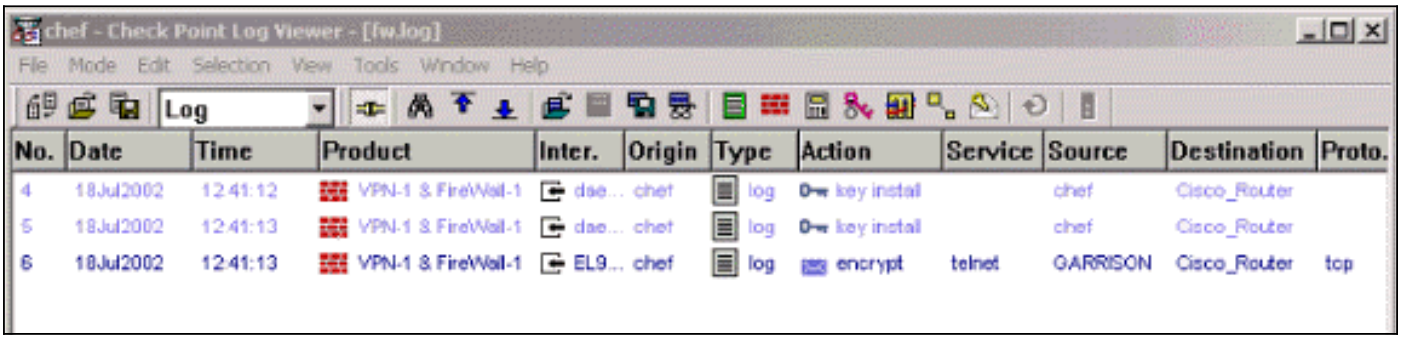
验证Cisco路由器

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。

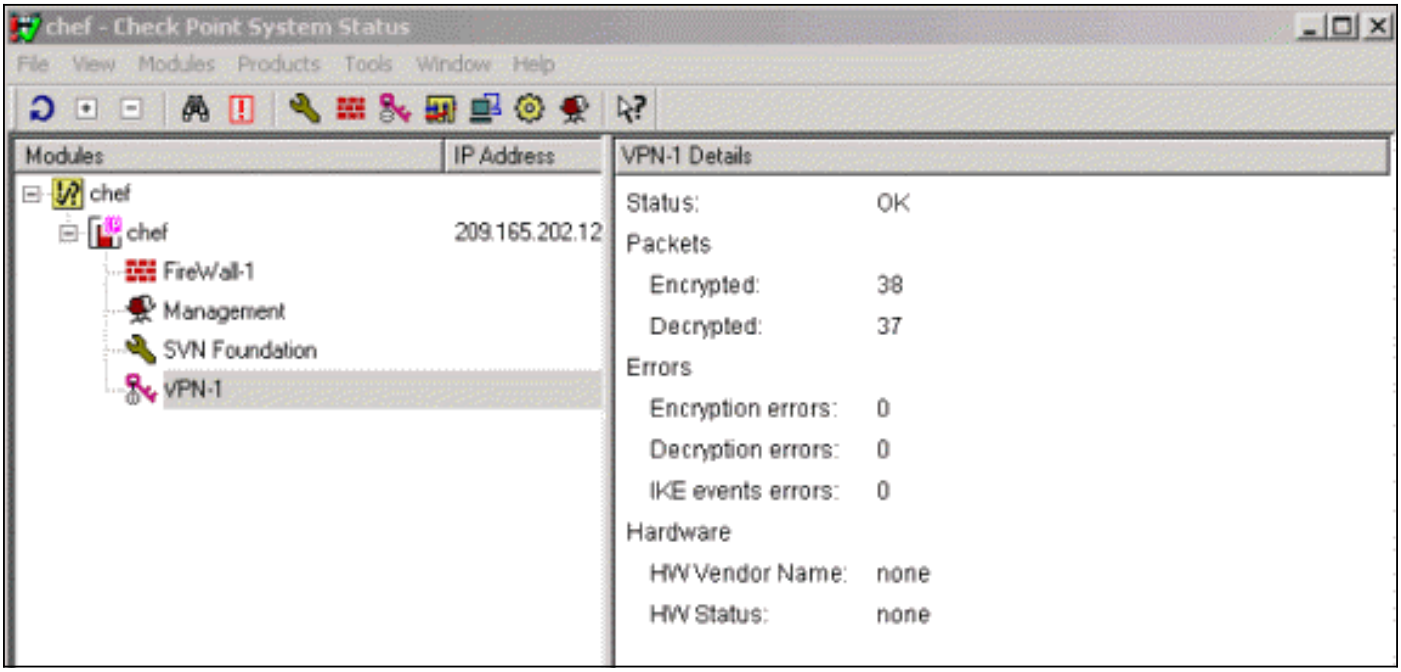
- show crypto isakmp sa - 显示对等体上的所有当前 IKE 安全关联 (SA)。
- **show crypto ipsec sa** - 显示当前 SA 使用的设置。

验证检查点NG

查看日志， Select窗口**>日志查看器**。



查看系统状态， Select窗口**>System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。

其他故障排除信息，请参考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** -显示关于加密引擎的调试消息，进行加密和解密。
- **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。

成功的调试日志输出

```
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