在 Cisco Secure PIX 防火墙与 Checkpoint NG 防火墙之间配置 IPSec 隧道

目录

简介

本文展示如何用预共享密钥配置IPSec隧道，从而在二个专用网络之间通信。在本例中，通信网络是Cisco安全PIX防火墙内部的192.168.10.x专用网络和CheckpointTM 下一代(NG)防火墙内部的10.32.x.x专用网络。

先决条件

要求

尝试进行此配置之前，请确保满足以下要求：

- 在开始此配置之前，从PIX内部和CheckpointTM NG内部（由172.18.124.x网络表示）到Internet的流量应该流动。
- 用户应该熟悉 IPsec 协商。此过程可分为五个步骤，包括两个互联网密钥交换(IKE)阶段。IPsec 隧道由相关数据流启动。如果数据流在 IPsec 对等体之间传输，则它会被认为是相关数据流。在 IKE 第 1 阶段中，IPsec 对等体对建立的 IKE 安全关联 (SA) 策略进行协商。对等体经过身份验证后，会使用 Internet 安全关联和密钥管理协议 (ISAKMP) 创建安全隧道。在 IKE 第 2 阶段中，IPsec 对等体使用经身份验证的安全隧道对 IPsec SA 转换进行协商。共享策略的

协商决定建立 IPsec 隧道的方式。根据 IPsec 转换集中配置的 IPsec 参数，将在 IPsec 对等体之间创建 IPsec 隧道并传输数据。如果删除了 IPsec SA，或者 IPsec SA 的生存时间到期，则 IPsec 隧道将终止。

使用的组件

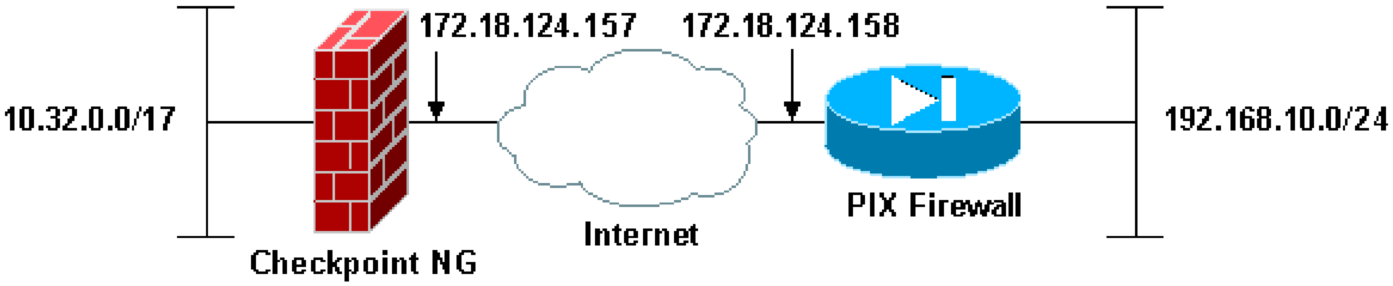
本文档中的信息基于以下软件和硬件版本：

- PIX软件版本6.2.1
- CheckpointTM NG防火墙

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 PIX

本部分为您提供配置本文档中描述功能的信息。

PIX 配置

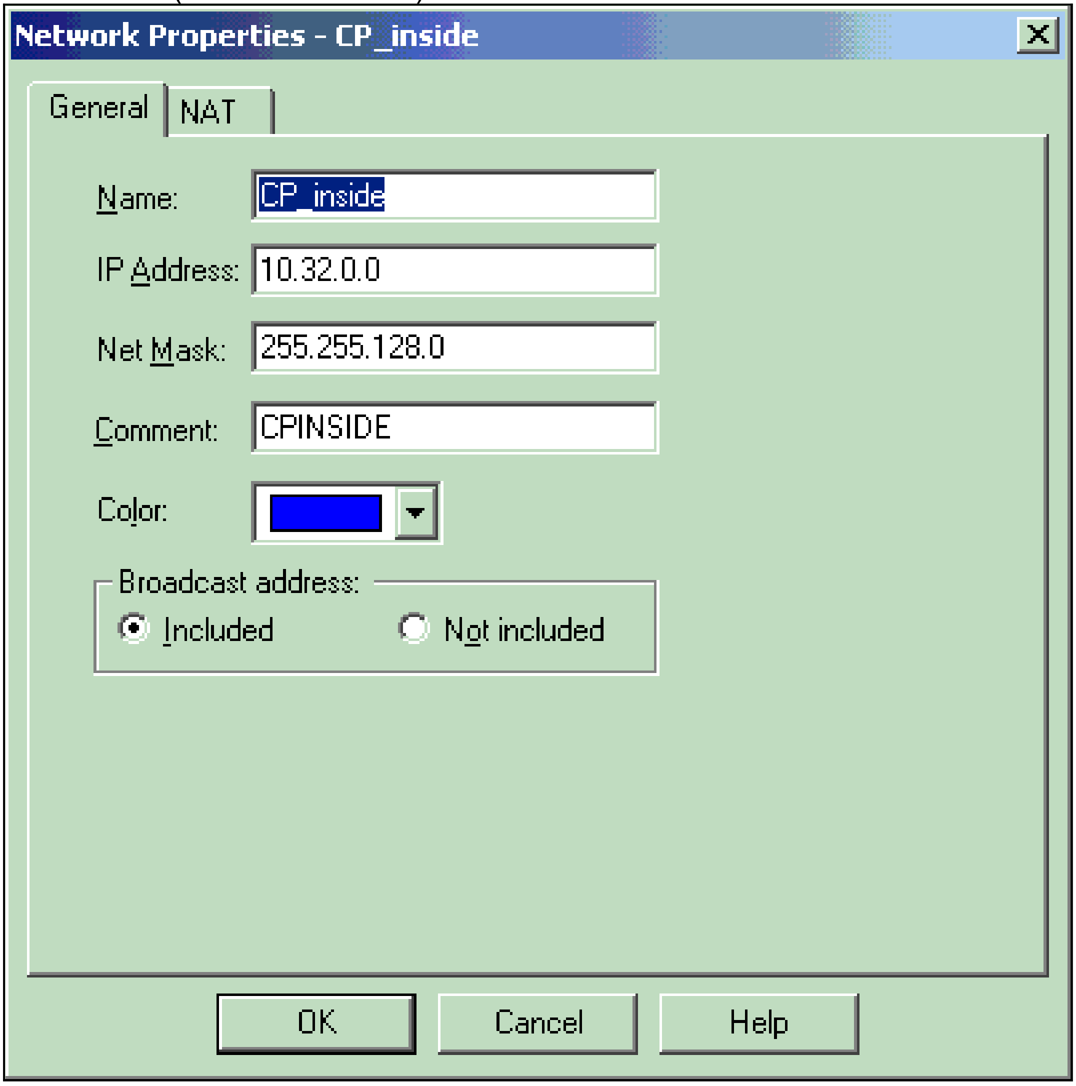
```
PIX Version 6.2(1)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname PIXRTPVPN
domain-name cisco.com
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol ils 389
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
fixup protocol skinny 2000
names
!--- Interesting traffic to be encrypted to the
Checkpoint™ NG. access-list 101 permit ip 192.168.10.0
255.255.255.0 10.32.0.0 255.255.128.0
!--- Do not perform Network Address Translation (NAT) on
traffic to the Checkpoint™ NG. access-list nonat permit
ip 192.168.10.0 255.255.255.0 10.32.0.0 255.255.128.0
pager lines 24
interface ethernet0 10baset
interface ethernet1 10full
mtu outside 1500
mtu inside 1500
ip address outside 172.18.124.158 255.255.255.0
ip address inside 192.168.10.1 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
pdm history enable
arp timeout 14400
global (outside) 1 interface
!--- Do not perform NAT on traffic to the Checkpoint™
NG. nat (inside) 0 access-list nonat
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
route outside 0.0.0.0 0.0.0.0 172.18.124.1 1
timeout xlate 3:00:00
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
aaa-server LOCAL protocol local
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
!--- Permit all inbound IPsec authenticated cipher
sessions. sysopt connection permit-ipsec
no sysopt route dnat
!--- Defines IPsec encryption and authentication
algorithms. crypto ipsec transform-set rtptac esp-3des
esp-md5-hmac
!--- Defines crypto map. crypto map rtprules 10 ipsec-
isakmp
crypto map rtprules 10 match address 101
crypto map rtprules 10 set peer 172.18.124.157
crypto map rtprules 10 set transform-set rtptac
!--- Apply crypto map on the outside interface. crypto
map rtprules interface outside
isakmp enable outside
!--- Defines pre-shared secret used for IKE
authentication. isakmp key ******** address
172.18.124.157 netmask 255.255.255.255
!--- Defines ISAKMP policy. isakmp policy 1
authentication pre-share
isakmp policy 1 encryption 3des
isakmp policy 1 hash md5
isakmp policy 1 group 2
isakmp policy 1 lifetime 86400
telnet timeout 5
ssh timeout 5
terminal width 80
Cryptochecksum:089b038c8e0dbc38d8ce5ca72cf920a5
```

```
: end
```

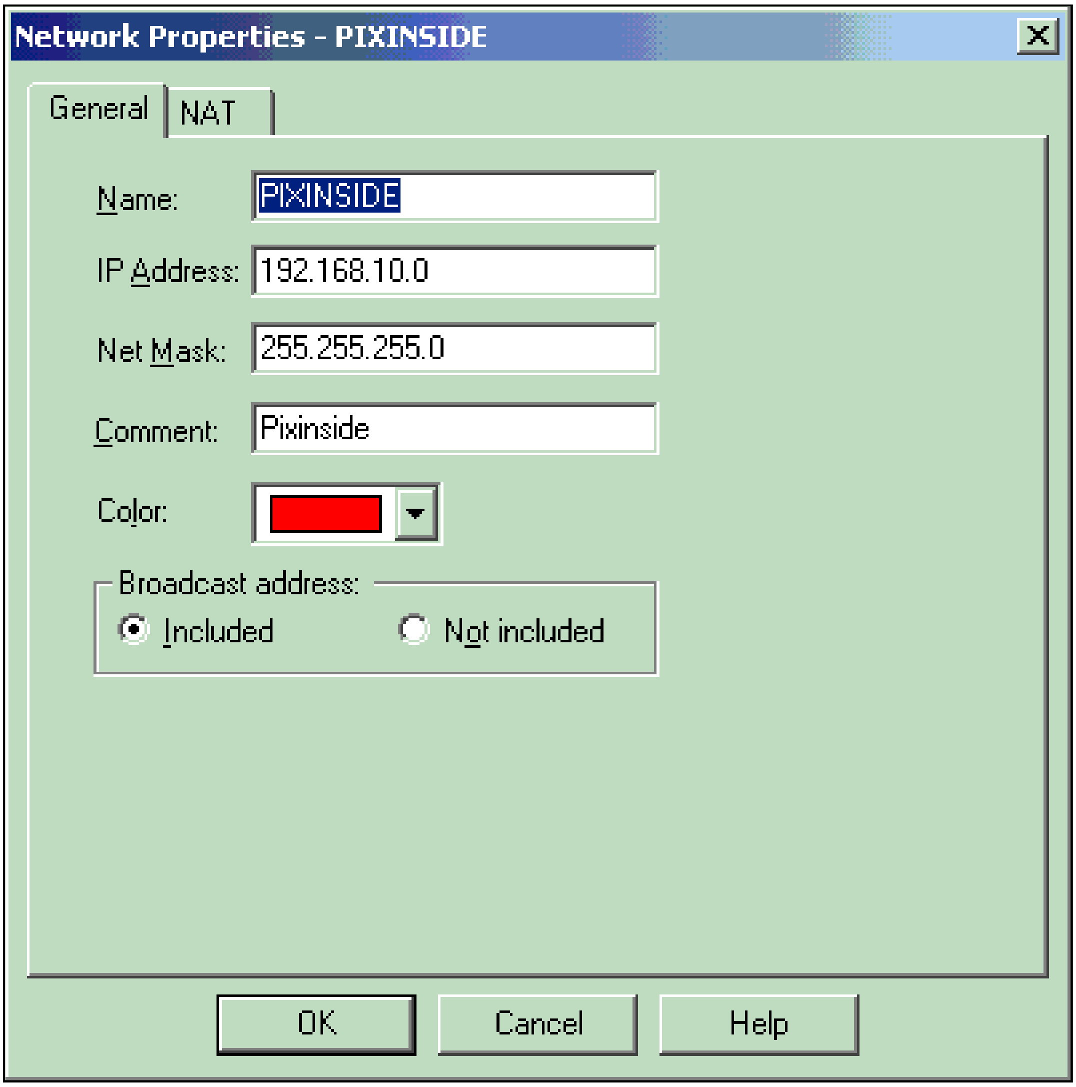
配置检查点NG

在CheckpointTM NG上定义网络对象和规则，组成适合建立VPN配置所需的策略。使用CheckpointTM NG策略编辑器，安装这一策略，完成CheckpointTM NG端的配置。

1. 为Checkpoint网络和PIX防火墙网络创建两个网络对象，以加密相关流量。为此，请选择**Manage** > **Network Objects**，然后选择**New** > **Network**。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_Inside（CheckpointTM NG的内部网络）和PIXINSIDE（PIX的内部网络）的网络对象。



Name: CP_inside
IP Address: 10.32.0.0
Net Mask: 255.255.128.0
Comment: CPINSIDE
Color: 🟦
Broadcast address: ● Included ○ Not included



Network Properties - PIXINSIDE

General | NAT

Name: PIXINSIDE

IP Address: 192.168.10.0

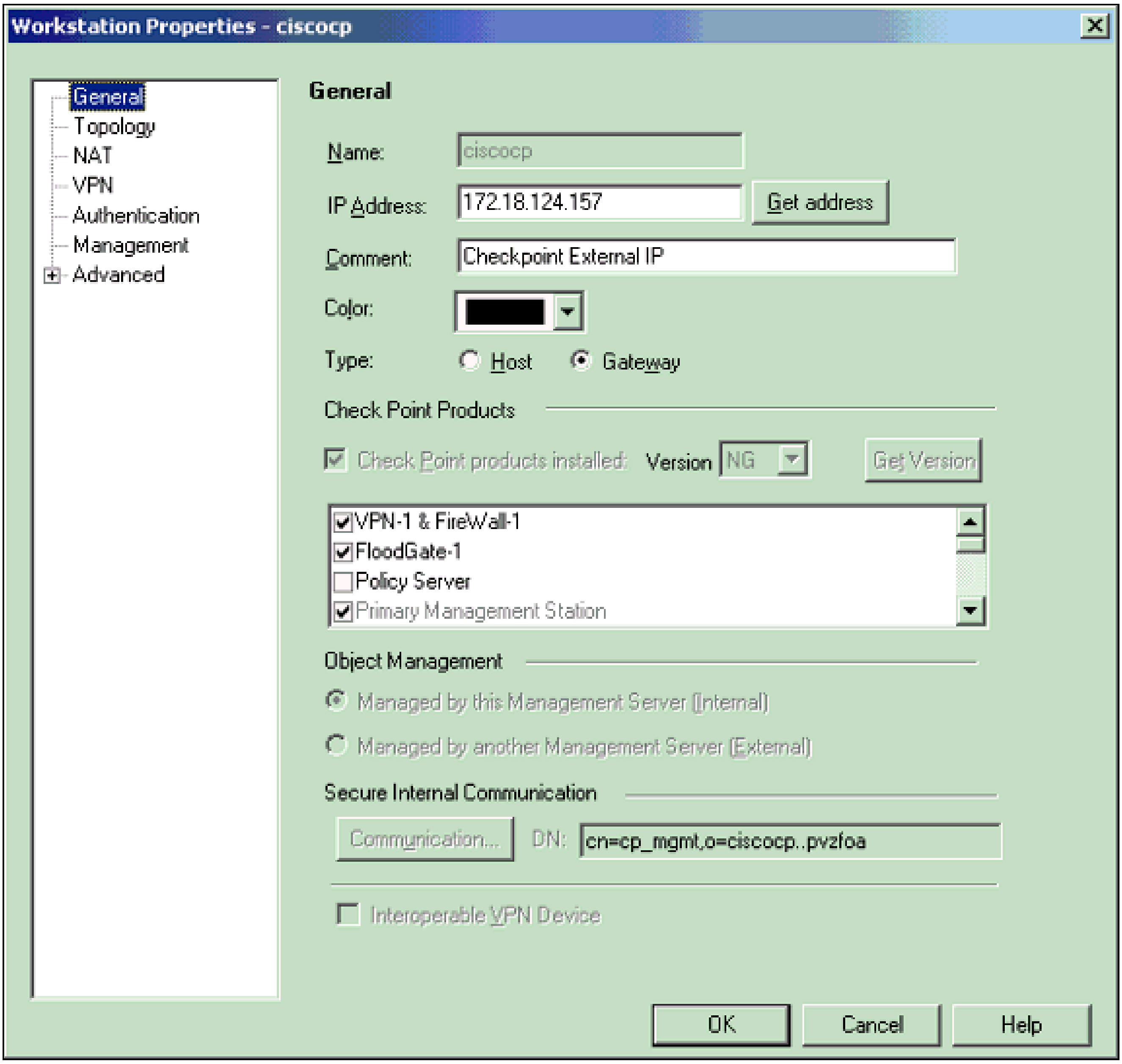
Net Mask: 255.255.255.0

Comment: Pixinside

Color: 🟥

Broadcast address: ● Included ○ Not included

2. 为CheckpointTM NG和PIX创建工作站对象。为此，请选择**Manage** > **Network Objects** > **New** > **Workstation**。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。选择将工作站设置为网关和可互操作的VPN设备选项，然后点击OK。这些示例显示了一组名为ciscocp(CheckpointTM NG)和PIX（PIX防火墙）的对象。



Workstation Properties - ciscocp

General

Name: ciscocp

IP Address: 172.18.124.157

Comment: Checkpoint External IP

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

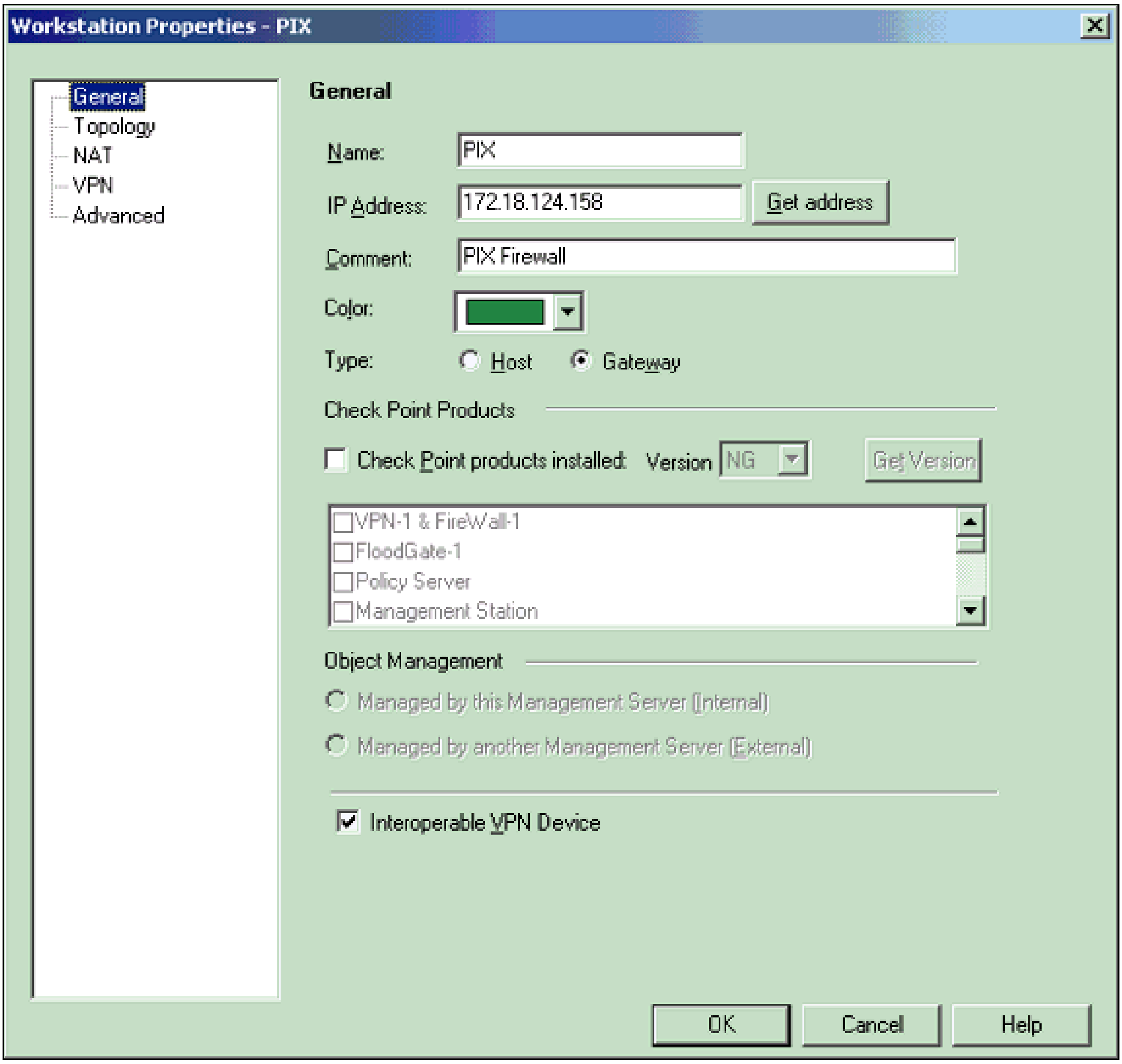
● Managed by this Management Server (Internal)

○ Managed by another Management Server (External)

Secure Internal Communication

DN: cn=cp_mgmt,o=ciscocp..pvzfoa

□ Interoperable VPN Device



General

Name: PIX

IP Address: 172.18.124.158

Comment: PIX Firewall

Color: 🟩

Type: ○ Host ● Gateway

Check Point Products

☐ Check Point products installed: Version NG

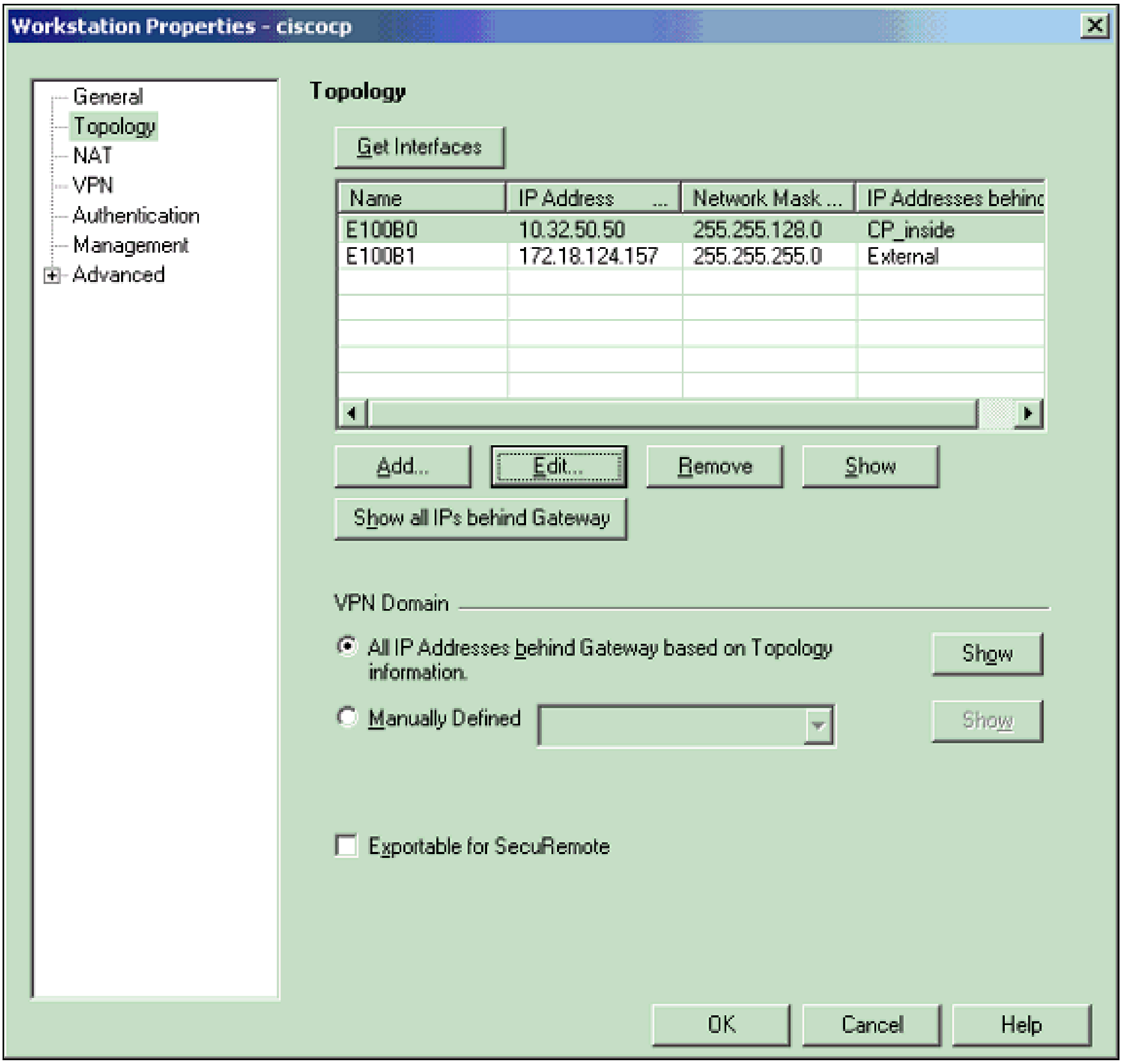
☐ VPN-1 & FireWall-1
☐ FloodGate-1
☐ Policy Server
☐ Management Station

Object Management

○ Managed by this Management Server (Internal)
○ Managed by another Management Server (External)

☑ Interoperable VPN Device

3. 选择**Manage** > **Network objects** > **Edit** 以打开CheckpointTM NG工作站（本例中为ciscocp）的“工作站属性”窗口。从窗口左边选择拓朴，然后选择要加密的网络。单击**Edit**以设置接口属性。



Name	IP Address ...	Network Mask ...	IP Addresses behinc
E100B0	10.32.50.50	255.255.128.0	CP_inside
E100B1	172.18.124.157	255.255.255.0	External

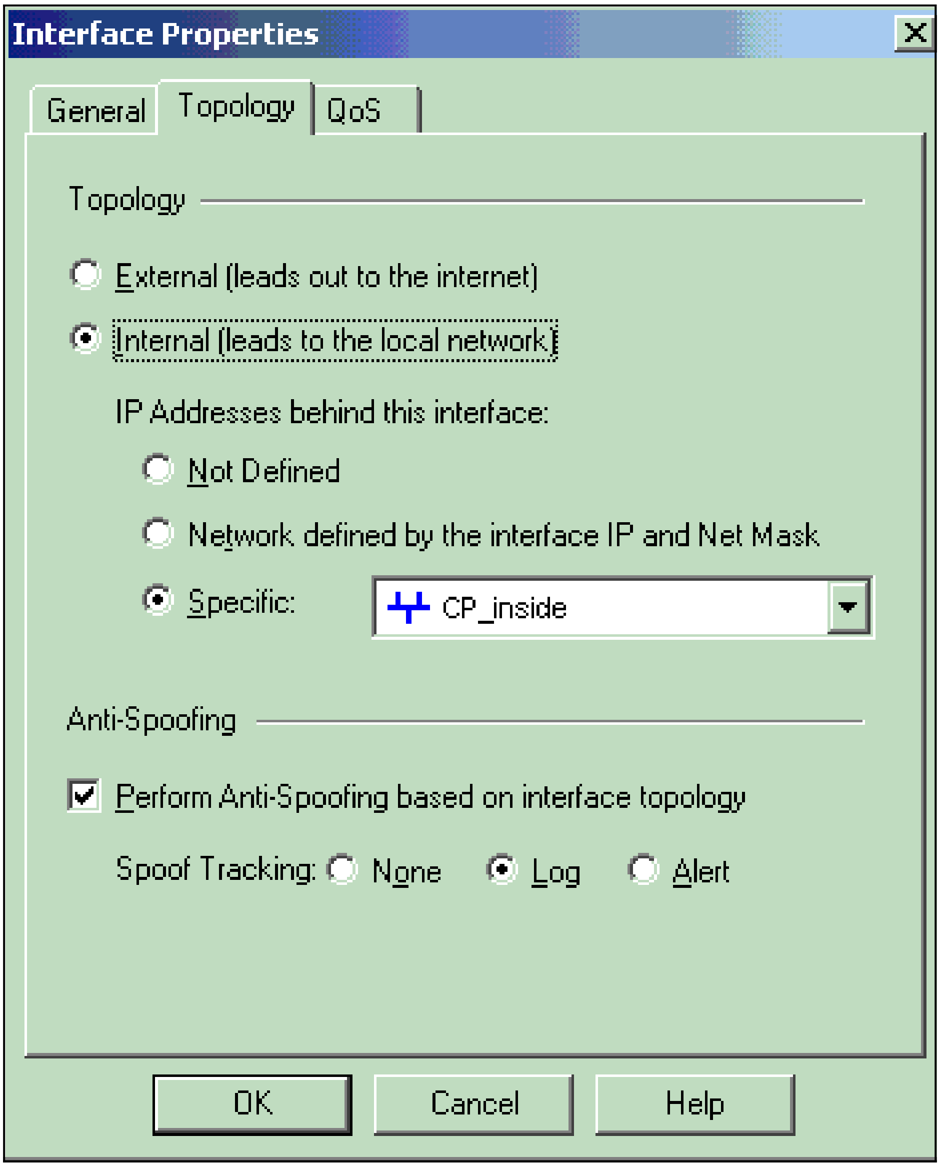
VPN Domain

● All IP Addresses behind Gateway based on Topology information.

○ Manually Defined

□ Exportable for SecuRemote

4. 选择指定工作站为内部选项，然后指定合适的IP地址。Click **OK**.在此配置中，CP_inside是CheckpointTM NG的内部网络。此处显示的拓扑选择将工作站指定为内部，并将地址指定为



Topology

○ External (leads out to the internet)

● Internal (leads to the local network)

IP Addresses behind this interface:

○ Not Defined

○ Network defined by the interface IP and Net Mask

● Specific: CP_inside

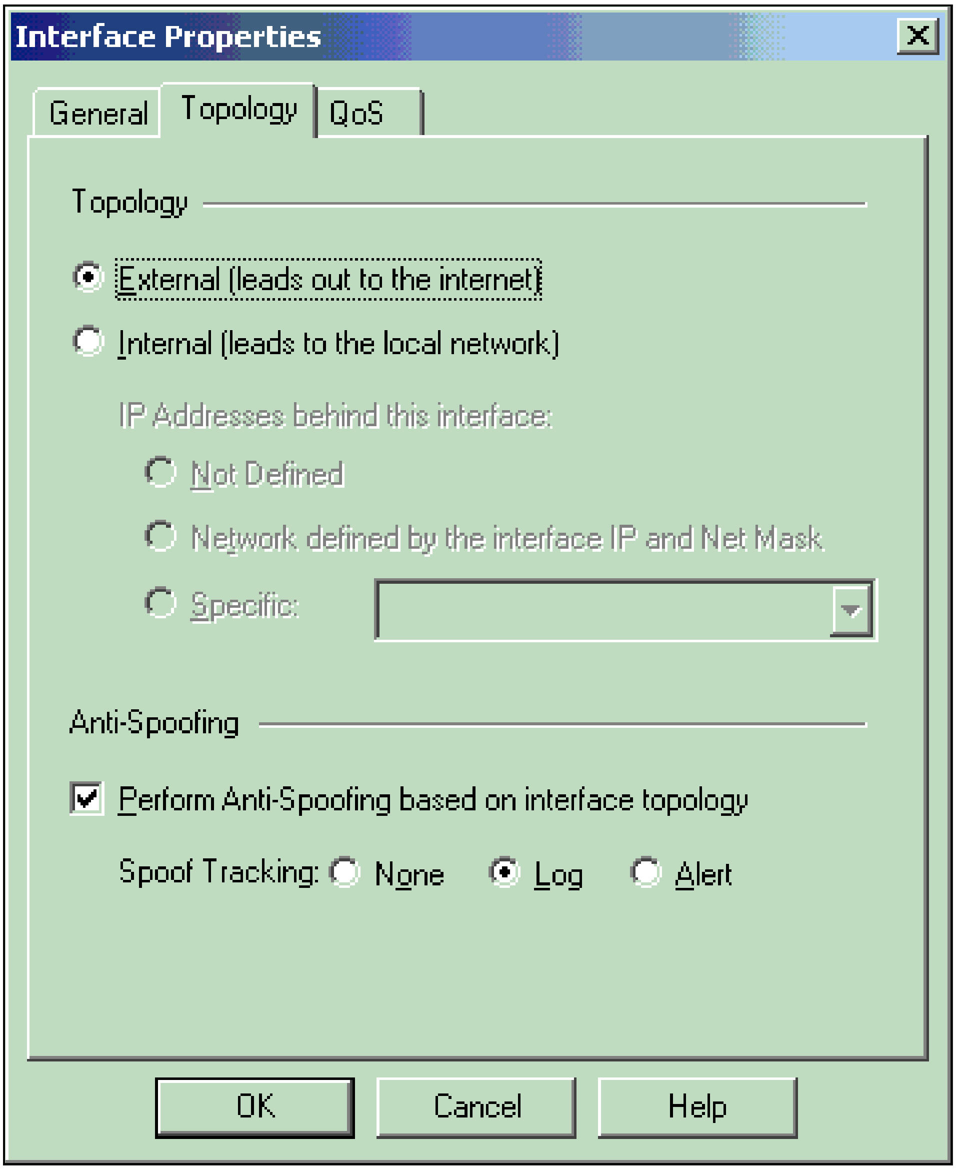
Anti-Spoofing

☑ Perform Anti-Spoofing based on interface topology

Spoof Tracking: ○ None ● Log ○ Alert

CP_inside。

5. 在工作站属性窗口，从导向互联网的CheckpointTM NG上选择外部接口，然后点击“Edit”设置接口属性。选择选项以将拓扑指定为外部拓扑，然后单击**确定**。



Topology

● External (leads out to the internet)

○ Internal (leads to the local network)

IP Addresses behind this interface:

○ Not Defined

○ Network defined by the interface IP and Net Mask

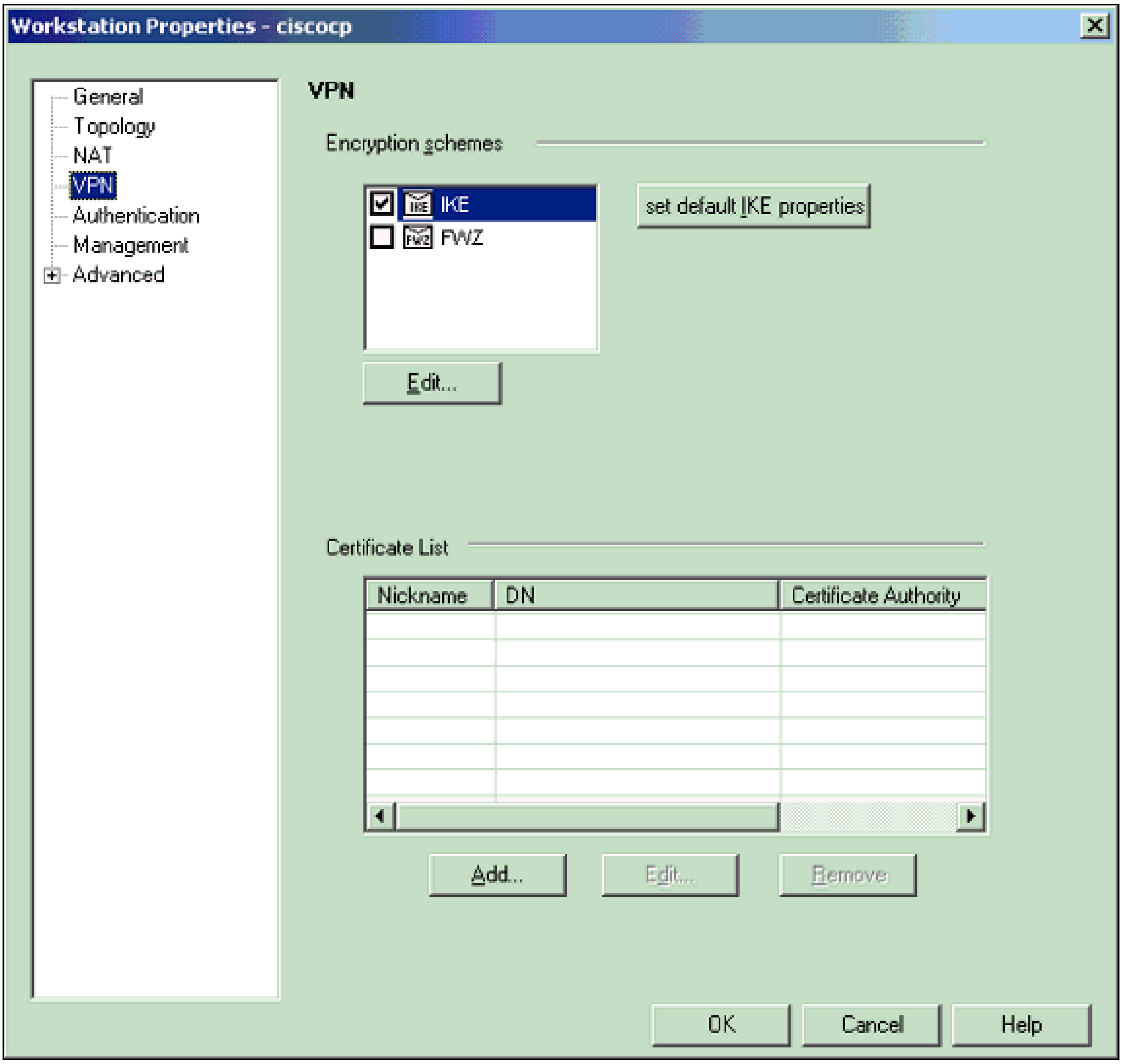
○ Specific:

Anti-Spoofing

☑ Perform Anti-Spoofing based on interface topology

Spoof Tracking: ○ None ● Log ○ Alert

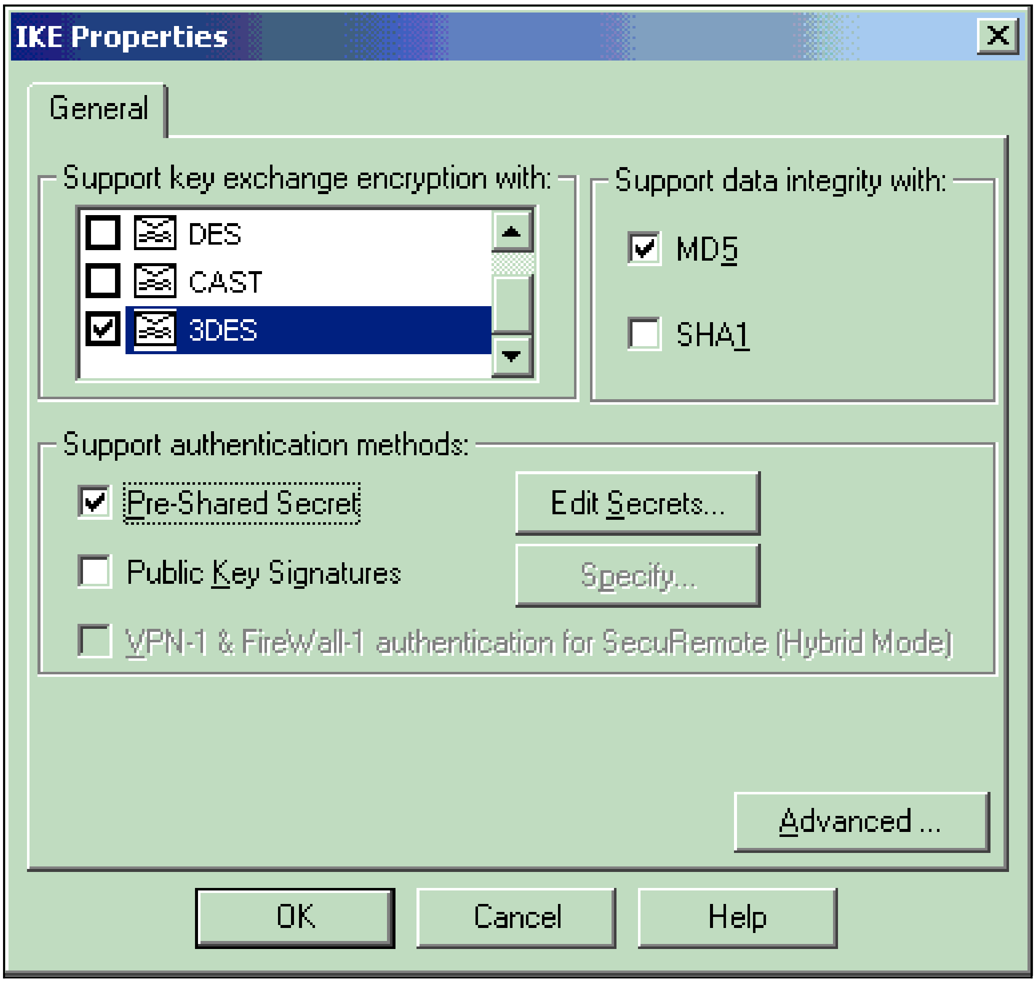
6. 在CheckpointTM NG的工作站属性窗口上，从窗口左边的选项中选择VPN，然后选择IKE参数执行加密和认证算法。单击**Edit**以配置IKE属性。



☑ IKE
□ FWZ

Nickname	DN	Certificate Authority

7. 配置IKE属性：选择3DES加密**的选**项，以便IKE属性与isakmp policy # encryption 3des**命令兼容**。选择MD5的选项，以便IKE属性与crypto isakmp policy # hash md5命令兼容。



IKE Properties

General

Support key exchange encryption with:

□ DES

□ CAST

☑ 3DES

Support data integrity with:

☑ MD5

□ SHA1

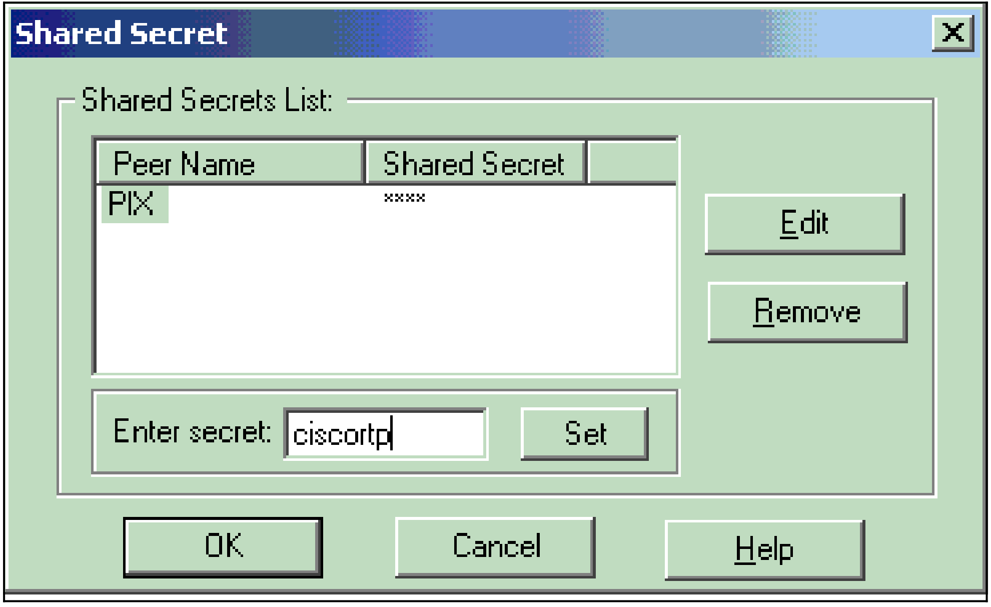
Support authentication methods:

☑ Pre-Shared Secret

□ Public Key Signatures

□ VPN-1 & FireWall-1 authentication for SecuRemote (Hybrid Mode)

8. 选择Pre-Shared Secrets（预共享秘密）的认证选项，然后点击Edit Secrets，将预共享密钥设置来与PIX命令isakmp key key address address netmask netmask兼容。单击**Edit**以输入您的密钥，如图所示，然**后单击Set， OK**。



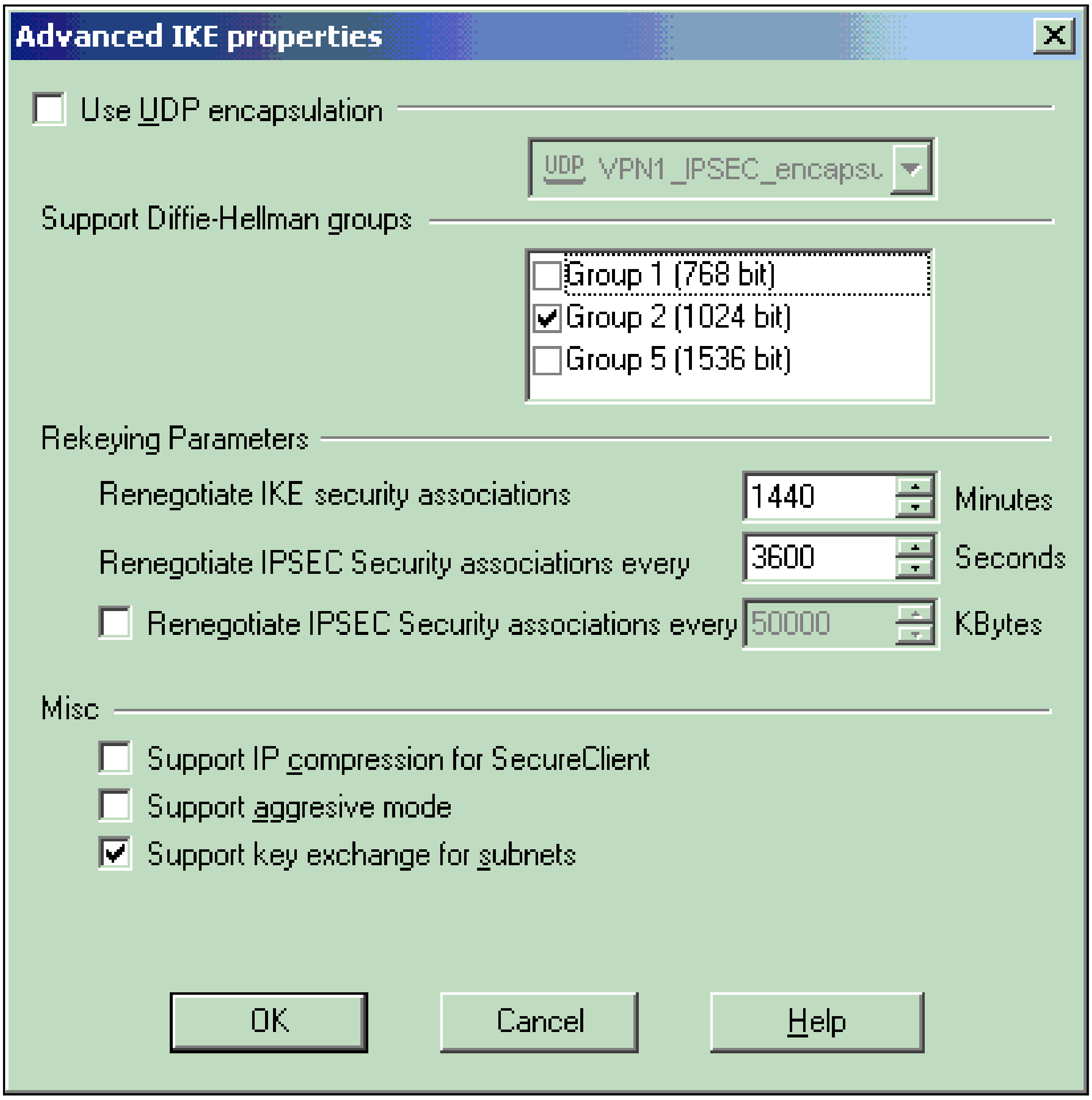
Shared Secret

Shared Secrets List:

Peer Name	Shared Secret
PIX	****

Enter secret: ciscortp

9. 在IKE属性窗口中，单击**Advanced...并**更改以下设置：取消选择“支持主动**模式”选项**。选择“支持子网**密钥交换”选项**。完成后单击 **OK。**



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 1440 Minutes

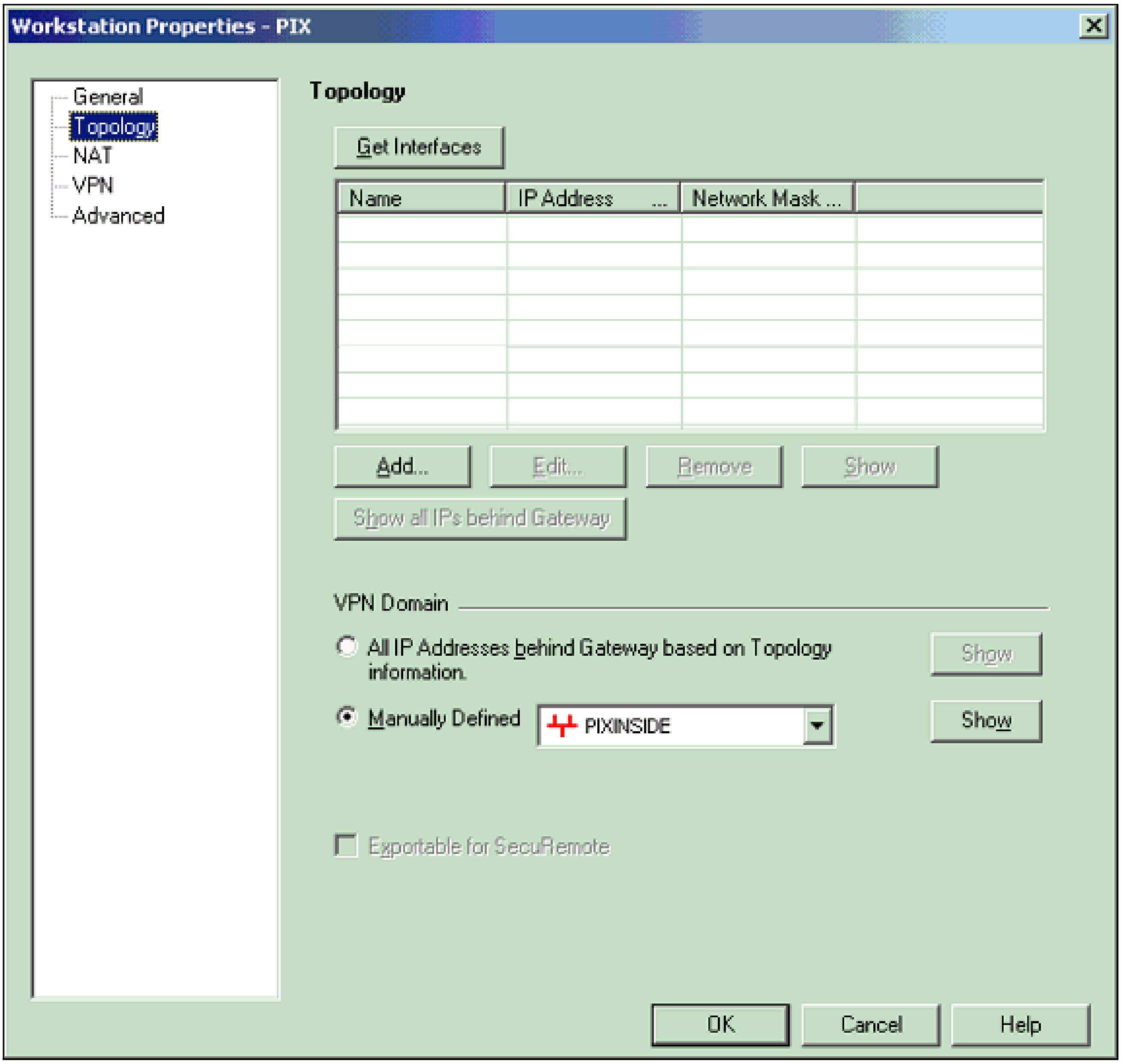
Renegotiate IPSEC Security associations every 3600 Seconds

☐ Renegotiate IPSEC Security associations every 50000 KBytes

Misc

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

10. 选择**Manage** > **Network objects** > **Edit** 以打开PIX的Workstation Properties窗口。从窗口的左边的选项中选择Topology，手工定义VPN域。在此配置中，PIXINSIDE（PIX的内部网络）定义为VPN域。



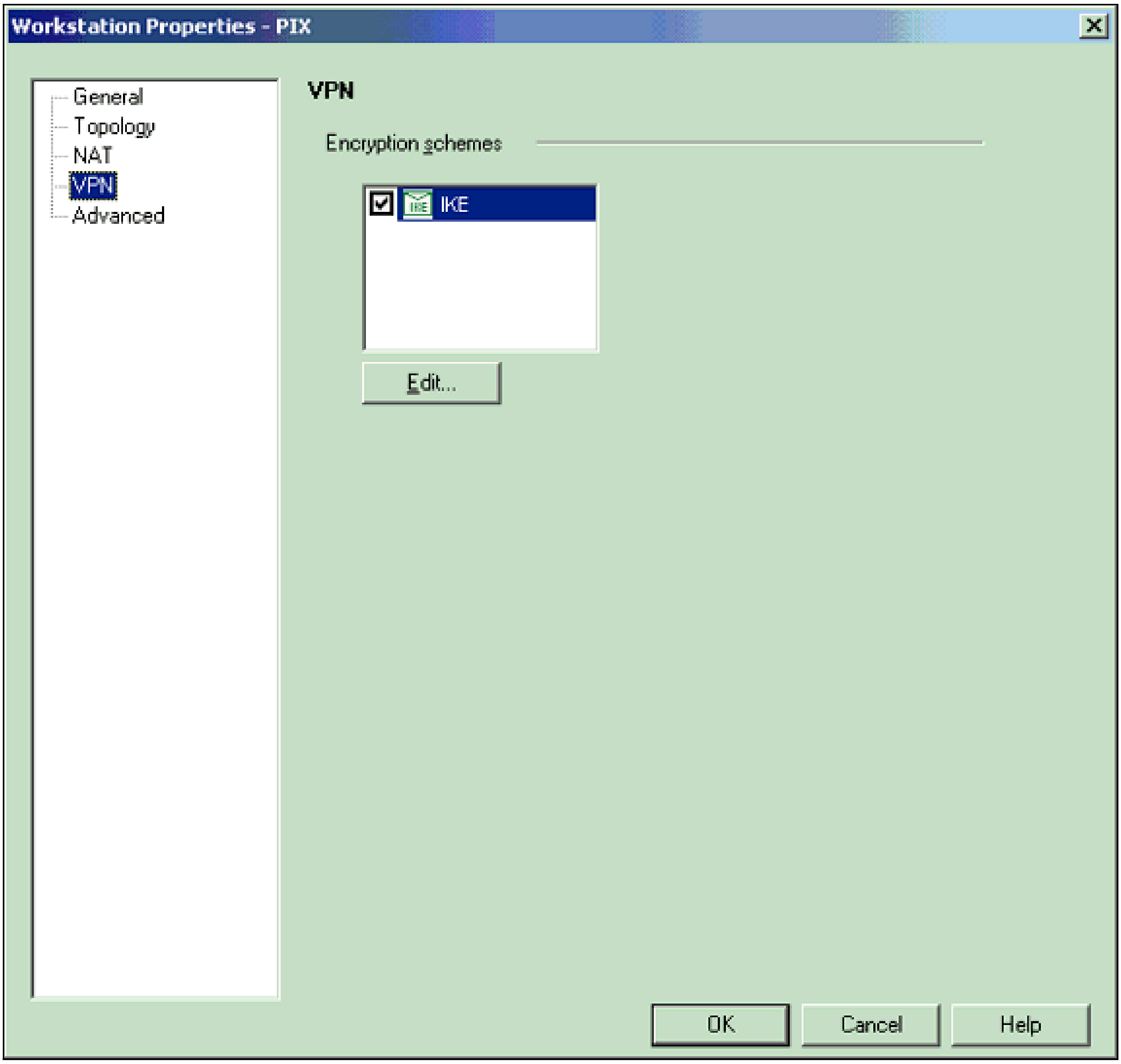
VPN Domain

○ All IP Addresses behind Gateway based on Topology information.

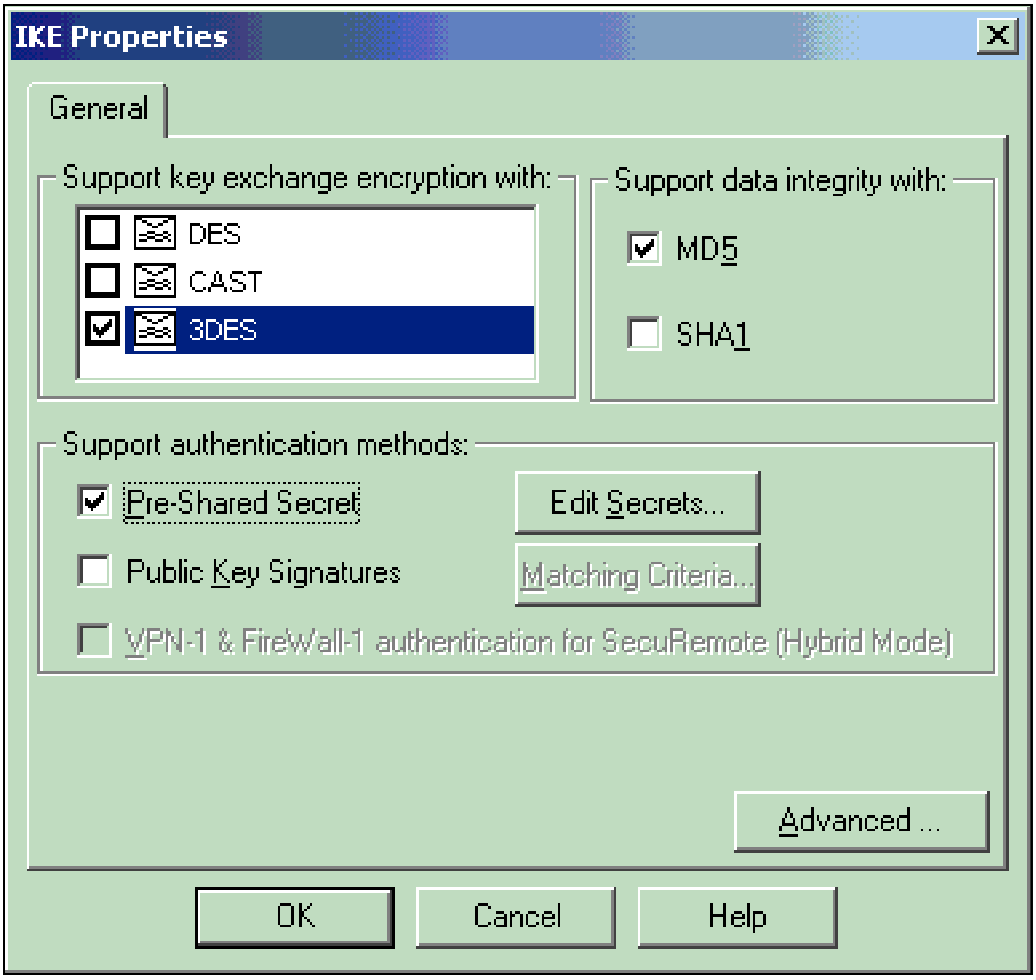
● Manually Defined: PIXINSIDE

□ Exportable for SecuRemote

11. 从窗口左边选择VPN，然后选择IKE作为加密机制。单击**Edit**以配置IKE属性。



12. 配置IKE属性，如下所示：选择3DES加密**的选**项，以便IKE属性与isakmp policy # encryption 3des**命令兼容**。选择MD5的选项，以便IKE属性与crypto isakmp policy # hash md5命令兼容



Support key exchange encryption with:

☐ DES
☐ CAST
☑ 3DES

Support data integrity with:

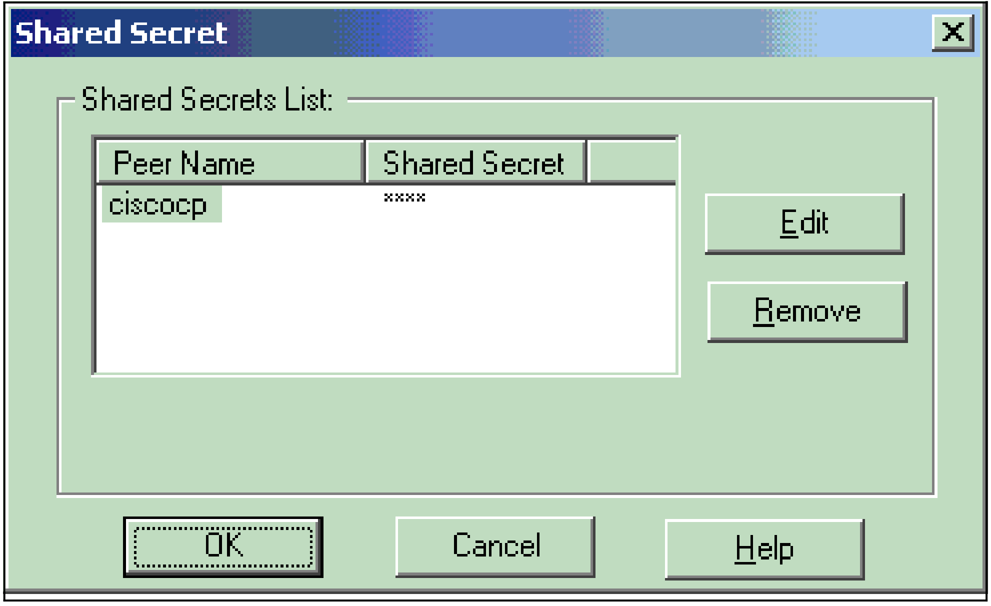
☑ MD5
☐ SHA1

Support authentication methods:

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

。

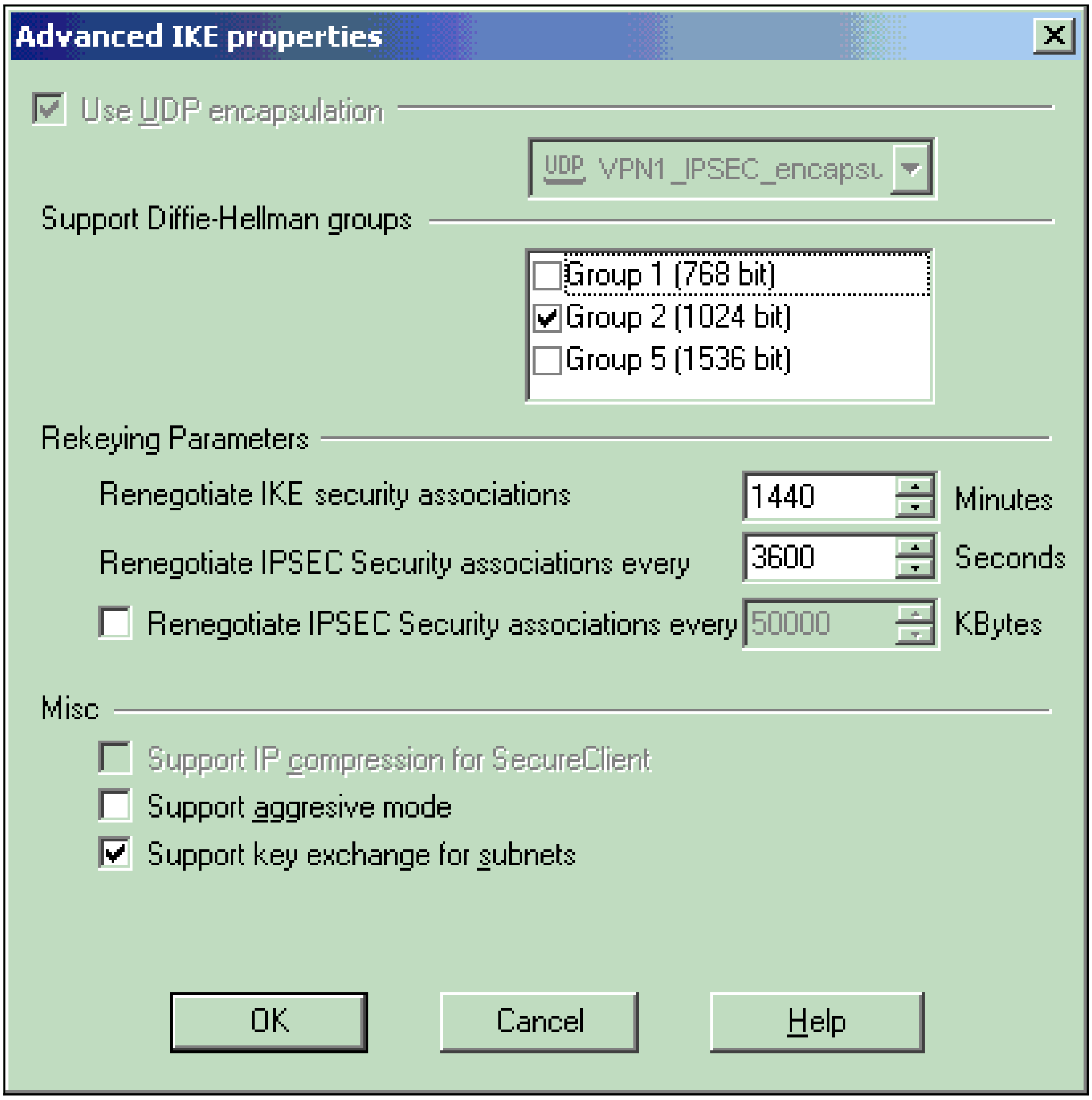
13. 选择Pre-Shared Secrets（预共享秘密）的认证选项，然后点击Edit Secrets，将预共享密钥设置来与PIX命令isakmp key key address address netmask netmask兼容。单击**Edit**以输入密钥，然后单击**Set**， **OK**。



Shared Secrets List:

Peer Name	Shared Secret
ciscocp	****

14. 在IKE属性窗口中，单击**Advanced...并**更改这些设置。选择适合IKE属性的Diffie-Hellman组。取消选择“支持主动**模式”选项**。选择“支持子网**密钥交换”选项**。完成**后，单**击“确定”。



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 1440 Minutes

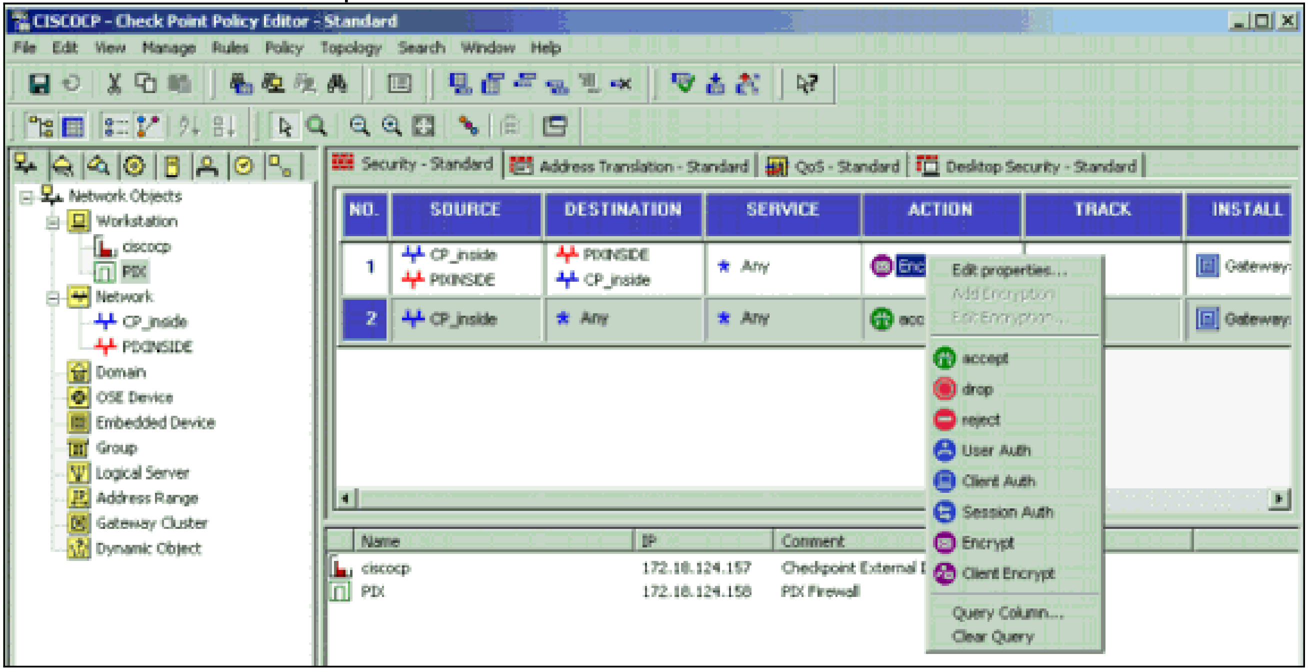
Renegotiate IPSEC Security associations every 3600 Seconds

□ Renegotiate IPSEC Security associations every 50000 KBytes

Misc

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

15. 选择**Rules** > **Add Rules** > **Top**为策略配置加密规则。在Policy Editor窗口，在源及目的两列插入带CP_inside (在Checkpoint TM NG网络内部)规则的源和PIXINSIDE (在PIX的网络内部)。设置服务**=任意、操作=加密和**跟踪**=日志的值**。当您添加了规则的加密行为部分时，点击Action 并且选择Edit Properties。

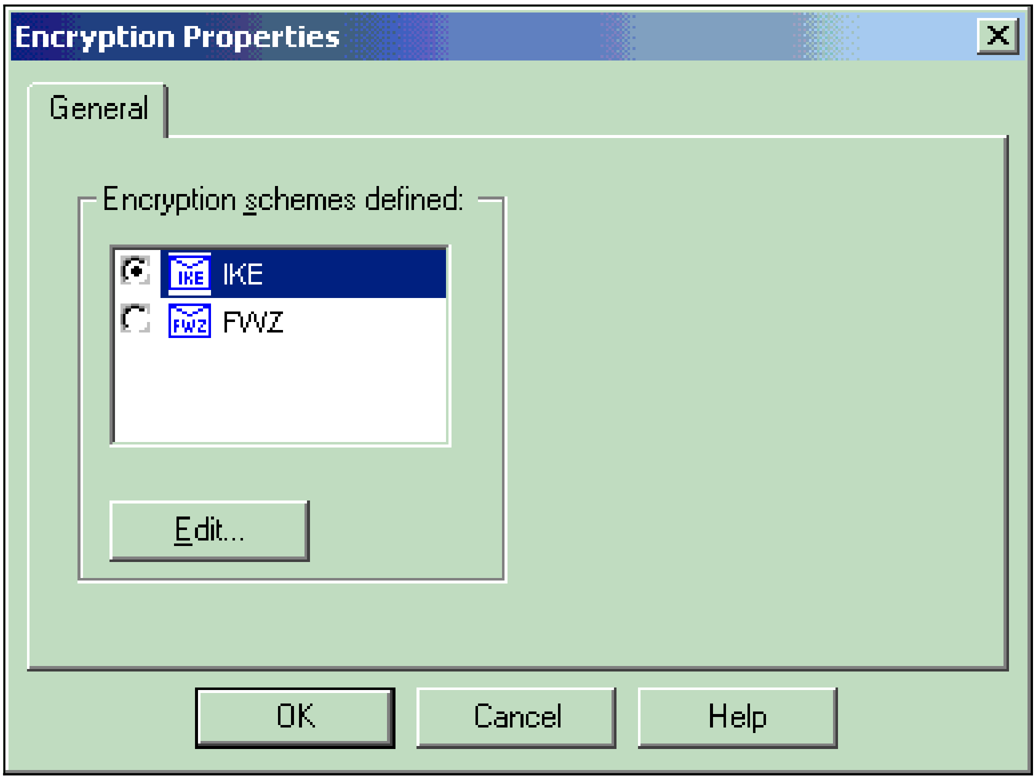


CISCOCP - Check Point Policy Editor - Standard

NO.	SOURCE	DESTINATION	SERVICE	ACTION	TRACK	INSTALL
1	CP_inside PIXINSIDE	PIXINSIDE CP_inside	Any	Enc		Gateway:
2	CP_inside	Any	Any	acc		Gateway:

Name	IP	Comment
ciscocp	172.18.124.157	Checkpoint External I
PIX	172.18.124.158	PIX Firewall

16. 选中并突出显示IKE后，单击**Edit**。



Encryption Properties

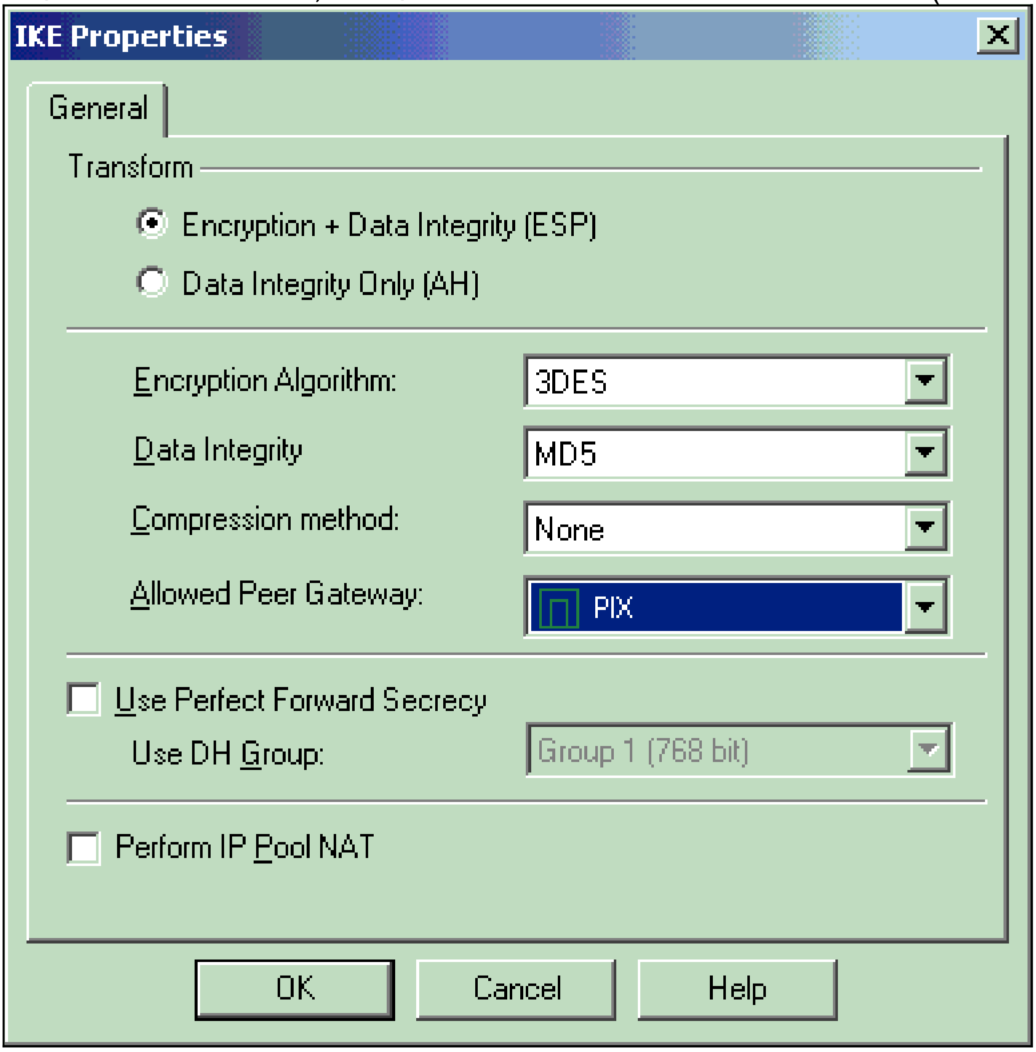
General

Encryption schemes defined:

● IKE

○ FWZ

17. 在“IKE属性”窗口中，更改属性以与**crypto ipsec transform-set rtptac esp-3des esp-md5-hmac命令中的PIX IPsec转换**一致。将Transform选项设置为加密+数据完整性(ESP)，设置3DES加密算法，设置MD5数据完整性，并设置允许的对等网关来匹配外部PIX网关(此处称为PIX)。 Click **OK**.



IKE Properties

General

Transform

● Encryption + Data Integrity (ESP)

○ Data Integrity Only (AH)

Encryption Algorithm: 3DES

Data Integrity: MD5

Compression method: None

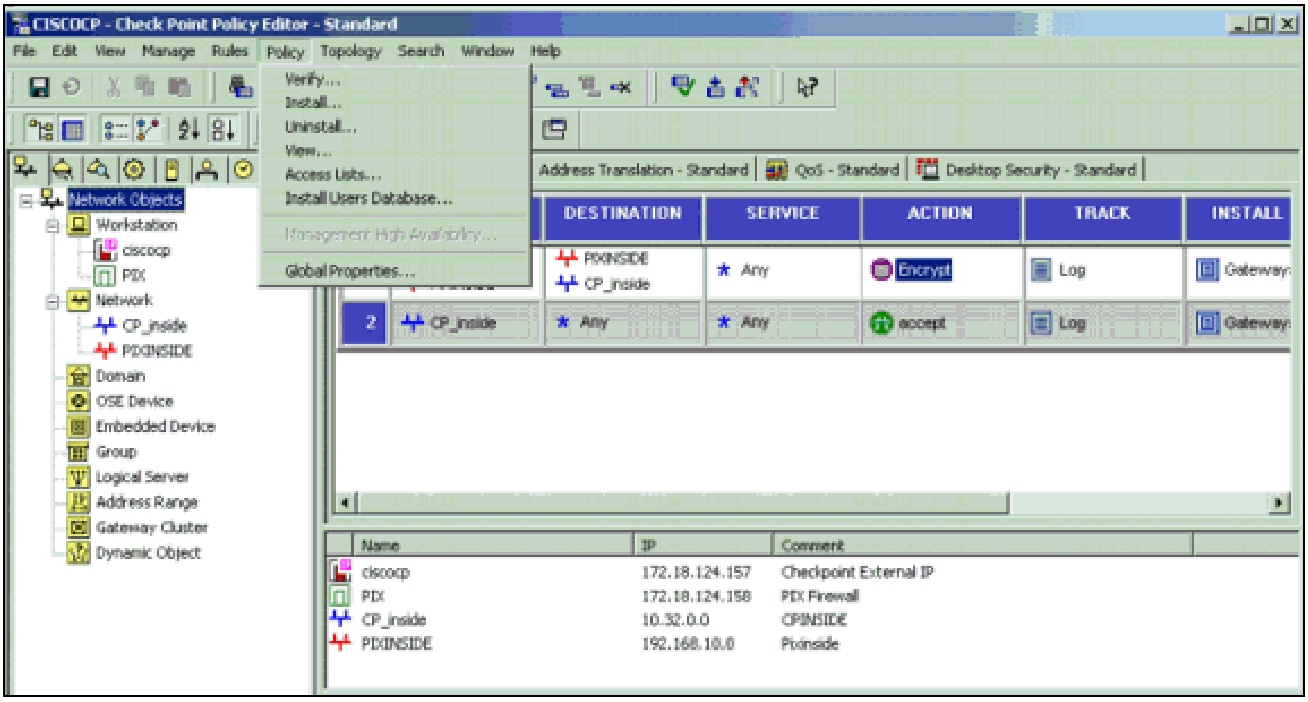
Allowed Peer Gateway: PIX

□ Use Perfect Forward Secrecy

Use DH Group: Group 1 (768 bit)

□ Perform IP Pool NAT

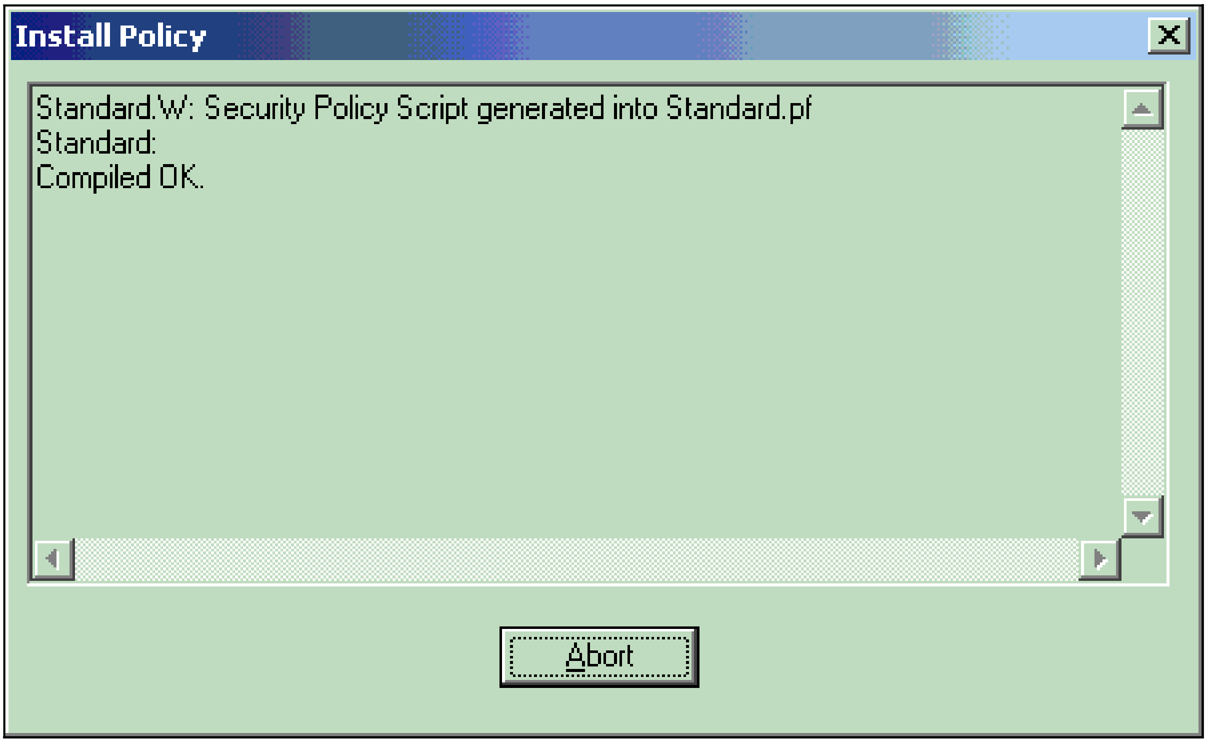
18. 配置CheckpointTM NG后，保存策略并选择**Policy** > **Install** 以启用它。



		DESTINATION	SERVICE	ACTION	TRACK	INSTALL
		PIXINSIDE CP_inside	Any	Encrypt	Log	Gateways
2	CP_inside	Any	Any	accept	Log	Gateways

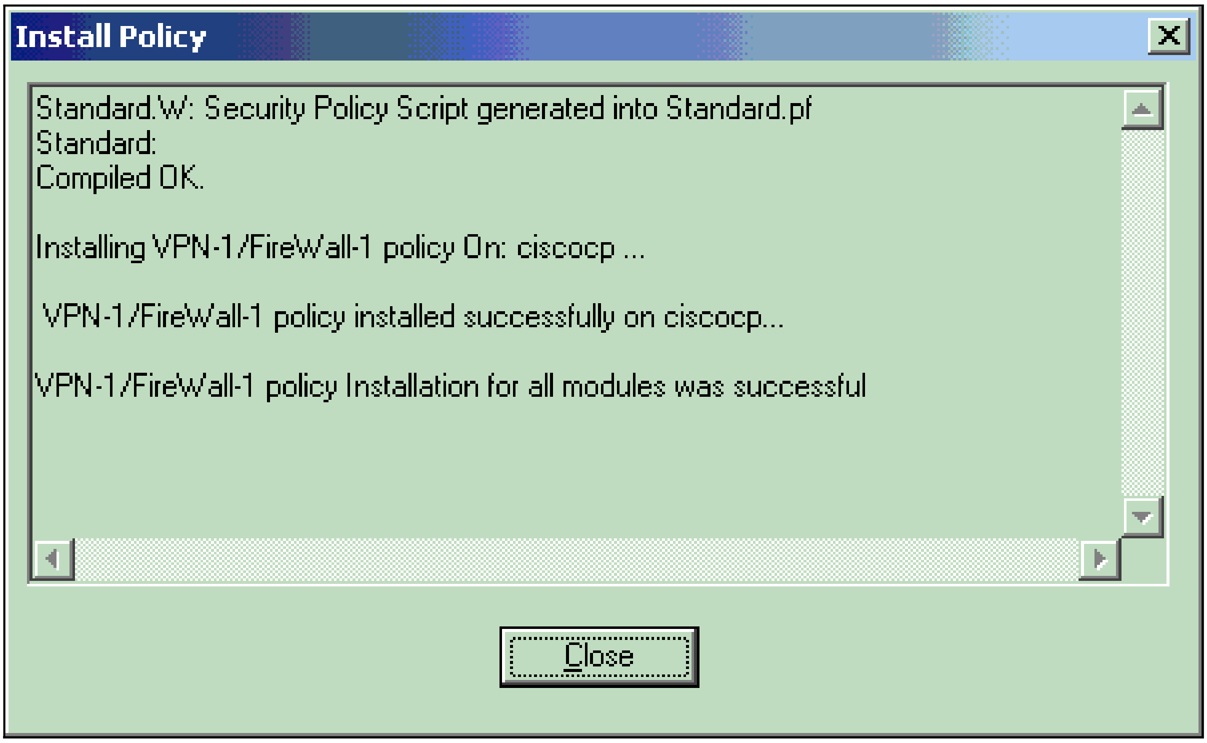
Name	IP	Comment
ciscocp	172.18.124.157	Checkpoint External IP
PIX	172.18.124.158	PIX Firewall
CP_inside	10.32.0.0	CPINSIDE
PIXINSIDE	192.168.10.0	Pixinside

安装窗口在编译策略时显示进度说明。



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

当安装窗口指示策略安装完成时。单击Close完成该过程。



Install Policy

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

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

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

VPN-1/FireWall-1 policy Installation for all modules was successful
```

验证

验证 PIX 配置

使用本部分可确认配置能否正常运行。

命令输出解释程序（仅限注册用户）(OIT) 支持某些 show 命令。使用 OIT 可查看对 show 命令输出的分析。

从其中一个专用网络向另一个专用网络发起ping，以测试两个专用网络之间的通信。在此配置中，ping从PIX端(192.168.10.2)发送到CheckpointTM NG内部网络(10.32.50.51)。

- **show crypto isakmp sa - 显示对等体上的所有当前 IKE SA。**

  ```
  show crypto isakmp sa
  Total     : 1
  Embryonic : 0
               dst                      src                     state     pending   created
    172.18.124.157   172.18.124.158   QM_IDLE         0           1
  ```

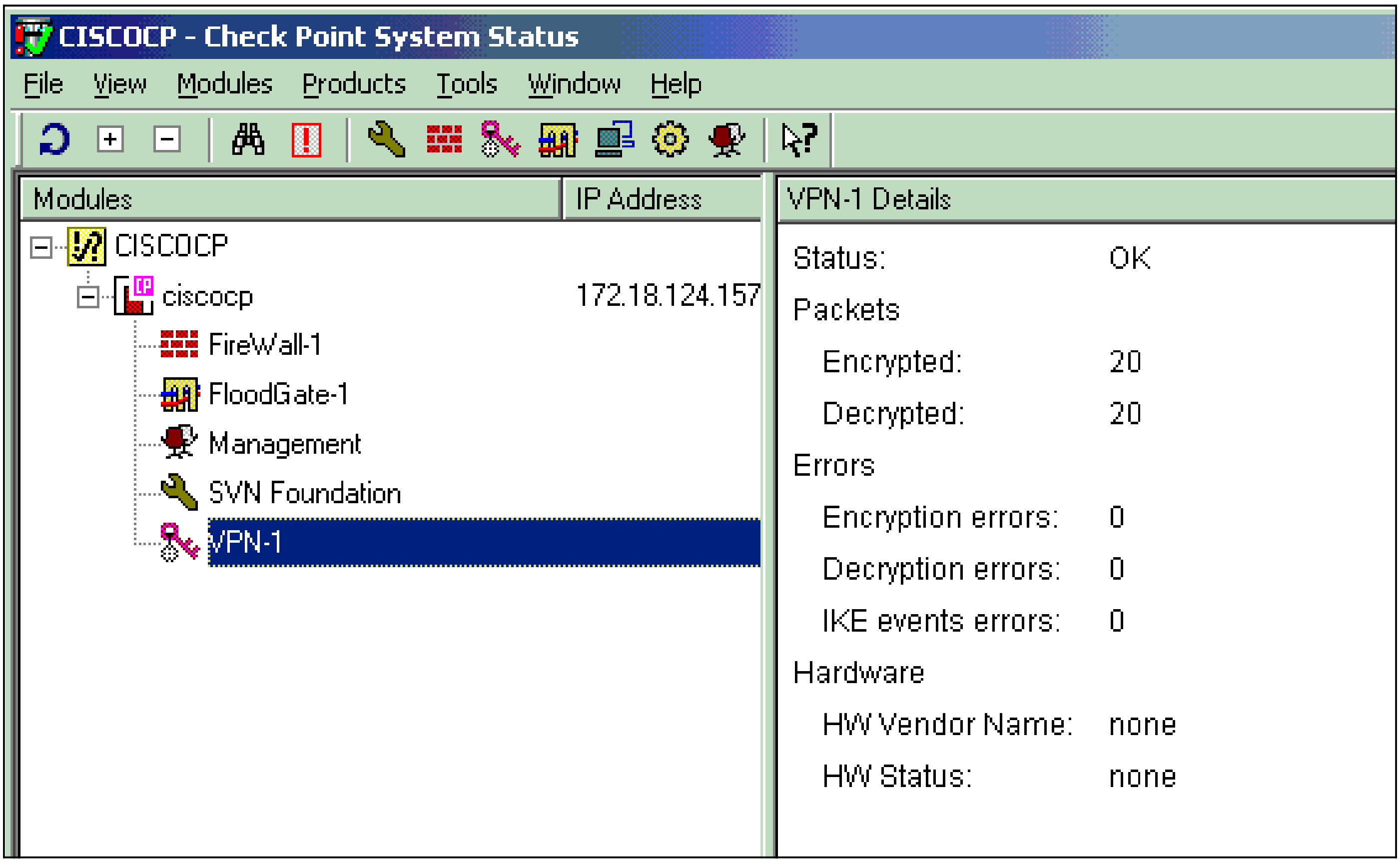
- **show crypto ipsec sa - 显示当前 SA 使用的设置。**

  ```
  PIX501A#show cry ipsec sa

  interface: outside
      Crypto map tag: rtprules, local addr. 172.18.124.158

     local  ident (addr/mask/prot/port): (192.168.10.0/255.255.255.0/0/0)
     remote ident (addr/mask/prot/port): (10.32.0.0/255.255.128.0/0/0)
     current_peer: 172.18.124.157
       PERMIT, flags={origin_is_acl,}
      #pkts encaps: 19, #pkts encrypt: 19, #pkts digest 19
      #pkts decaps: 19, #pkts decrypt: 19, #pkts verify 19
      #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.: 172.18.124.158, remote crypto endpt.: 172.18.124.157
path mtu 1500, ipsec overhead 56, media mtu 1500
current outbound spi: 6b15a355

inbound esp sas:
 spi: 0xced238c7(3469883591)
   transform: esp-3des esp-md5-hmac ,
   in use settings ={Tunnel, }
   slot: 0, conn id: 3, crypto map: rtprules
   sa timing: remaining key lifetime (k/sec): (4607998/27019)
   IV size: 8 bytes
   replay detection support: Y

inbound ah sas:
inbound pcp sas:

outbound esp sas:
 spi: 0x6b15a355(1796580181)
   transform: esp-3des esp-md5-hmac ,
   in use settings ={Tunnel, }
   slot: 0, conn id: 4, crypto map: rtprules
   sa timing: remaining key lifetime (k/sec): (4607998/27019)
   IV size: 8 bytes
   replay detection support: Y


outbound ah sas:

outbound pcp sas:
```

查看检查点NG上的隧道状态

转到策略编辑器，选择**窗口>系统状**态以查看隧道状态。



Modules　IP Address

CISCOCP
ciscocp　172.18.124.157
FireWall-1
FloodGate-1
Management
SVN Foundation
VPN-1

VPN-1 Details

Status: OK
Packets
Encrypted: 20
Decrypted: 20
Errors
Encryption errors: 0
Decryption errors: 0
IKE events errors: 0
Hardware
HW Vendor Name: none
HW Status: none

故障排除

排除PIX配置故障

命令输出解释程序（仅限注册用户）(OIT) 支持某些 show 命令。使用 OIT 可查看对 show 命令输出的分析。

注意：在使用debug命令之前，请参阅有关Debug命**令的**重要信息。

使用这些命令在PIX防火墙上启用调试。

- **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。**

```
VPN Peer: ISAKMP: Added new peer: ip:172.18.124.157 Total VPN Peers:1
VPN Peer: ISAKMP: Peer ip:172.18.124.157 Ref cnt incremented to:1 Total VPN Peers:1
ISAKMP (0): beginning Main Mode exchange
crypto_isakmp_process_block: src 172.18.124.157, dest 172.18.124.158
OAK_MM exchange
ISAKMP (0): processing SA payload. message ID = 0
ISAKMP (0): Checking ISAKMP transform 1 against priority 1 policy
ISAKMP: encryption 3DES-CBC
ISAKMP: hash MD5
ISAKMP: default group 2
ISAKMP: auth pre-share
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x0 0x1 0x51 0x80
ISAKMP (0): atts are acceptable. Next payload is 0
ISAKMP (0): SA is doing pre-shared key authentication using id type ID_IPV4_ADDR
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 172.18.124.157, dest 172.18.124.158
OAK_MM exchange
ISAKMP (0): processing KE payload. message ID = 0
ISAKMP (0): processing NONCE payload. message ID = 0
ISAKMP (0): ID payload
next-payload : 8
type : 1
protocol : 17
port : 500
length : 8
ISAKMP (0): Total payload length: 12
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 172.18.124.157, dest 172.18.124.158
OAK_MM exchange
ISAKMP (0): processing ID payload. message ID = 0
ISAKMP (0): processing HASH payload. message ID = 0
ISAKMP (0): SA has been authenticated
ISAKMP (0): beginning Quick Mode exchange, M-ID of 322868148:133e93b4 IPSEC(key_engine): got a
queue event...
IPSEC(spi_response): getting spi 0xced238c7(3469883591) for SA
from 172.18.124.157 to 172.18.124.158 for prot 3
return status is IKMP_NO_ERROR
ISAKMP (0): sending INITIAL_CONTACT notify
ISAKMP (0): sending NOTIFY message 24578 protocol 1
ISAKMP (0): sending INITIAL_CONTACT notify
crypto_isakmp_process_block: src 172.18.124.157, dest 172.18.124.158
OAK_QM exchange
oakley_process_quick_mode:
```

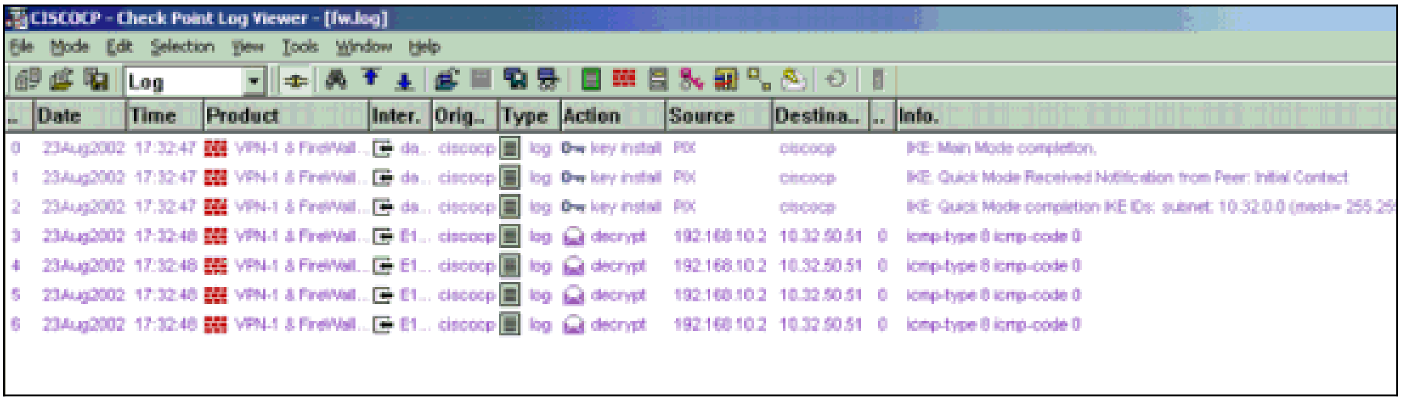
```
OAK_QM_IDLE
ISAKMP (0): processing SA payload. message ID = 322868148
ISAKMP : Checking IPSec proposal 1
ISAKMP: transform 1, ESP_3DES
ISAKMP: attributes in transform:
ISAKMP: encaps is 1
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (basic) of 28800
ISAKMP: SA life type in kilobytes
ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0
ISAKMP: authenticator is HMAC-MD5
ISAKMP (0): atts are acceptable. IPSEC(validate_proposal_request): proposal part #1,
(key eng. msg.) dest= 172.18.124.157, src= 172.18.124.158,
dest_proxy= 10.32.0.0/255.255.128.0/0/0 (type=4),
src_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
ISAKMP (0): processing NONCE payload. message ID = 322868148
ISAKMP (0): processing ID payload. message ID = 322868148
ISAKMP (0): processing ID payload. message ID = 322868148
ISAKMP (0): processing NOTIFY payload 24576 protocol 3
spi 3469883591, message ID = 322868148
ISAKMP (0): processing responder lifetime
ISAKMP (0): processing NOTIFY payload 24576 protocol 3
spi 3469883591, message ID = 322868148
ISAKMP (0): processing responder lifetime
ISAKMP (0): Creating IPSec SAs
inbound SA from 172.18.124.157 to 172.18.124.158 (proxy 10.32.0.0 to 192.168.10.0)
has spi 3469883591 and conn_id 3 and flags 4
lifetime of 28800 seconds
lifetime of 4608000 kilobytes
outbound SA from 172.18.124.158 to 172.18.124.157 (proxy 192.168.10.0 to 10.32.0.0)
has spi 1796580181 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= 172.18.124.158, src= 172.18.124.157,
dest_proxy= 192.168.10.0/255.255.255.0/0/0 (type=4),
src_proxy= 10.32.0.0/255.255.128.0/0/0 (type=4),
protocol= ESP, transform= esp-3des esp-md5-hmac ,
lifedur= 28800s and 4608000kb,
spi= 0xced238c7(3469883591), conn_id= 3, keysize= 0, flags= 0x4
IPSEC(initialize_sas): ,
(key eng. msg.) src= 172.18.124.158, dest= 172.18.124.157,
src_proxy= 192.168.10.0/255.255.255.0/0/0 (type=4),
dest_proxy= 10.32.0.0/255.255.128.0/0/0 (type=4),
protocol= ESP, transform= esp-3des esp-md5-hmac ,
lifedur= 28800s and 4608000kb,
spi= 0x6b15a355(1796580181), conn_id= 4, keysize= 0, flags= 0x4
VPN Peer: IPSEC: Peer ip:172.18.124.157 Ref cnt incremented to:2 Total VPN Peers:1
VPN Peer: IPSEC: Peer ip:172.18.124.157 Ref cnt incremented to:3 Total VPN Peers:1
return status is IKMP_NO_ERROR
```

网络汇总

当多个相邻网络内部在检查点的时加密域配置，设备也许自动地总结他们关于关注数据流的情况。如果PIX上的加密访问控制列表(ACL)未配置为匹配，隧道可能会失败。例如，如果将内部网络10.0.0.0 /24和10.0.1.0 /24配置为包含在隧道中，则可将其总结为10.0.0.0 /23。

查看检查点NG日志

选择**窗口**> **日志查**看器查看日志。


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

..	Date	Time	Product	Inter.	Orig..	Type	Action	Source	Destina..	..	Info.
0	23Aug2002	17:32:47	VPN-1 & FireWall...	da...	ciscocp	log	key install	PIX	ciscocp		IKE: Main Mode completion.
1	23Aug2002	17:32:47	VPN-1 & FireWall...	da...	ciscocp	log	key install	PIX	ciscocp		IKE: Quick Mode Received Notification from Peer: Initial Contact
2	23Aug2002	17:32:47	VPN-1 & FireWall...	da...	ciscocp	log	key install	PIX	ciscocp		IKE: Quick Mode completion IKE IDs: subnet: 10.32.0.0 (mask= 255.25
3	23Aug2002	17:32:48	VPN-1 & FireWall...	E1...	ciscocp	log	decrypt	192.168.10.2	10.32.50.51	0	icmp-type 8 icmp-code 0
4	23Aug2002	17:32:48	VPN-1 & FireWall...	E1...	ciscocp	log	decrypt	192.168.10.2	10.32.50.51	0	icmp-type 8 icmp-code 0
5	23Aug2002	17:32:48	VPN-1 & FireWall...	E1...	ciscocp	log	decrypt	192.168.10.2	10.32.50.51	0	icmp-type 8 icmp-code 0
6	23Aug2002	17:32:48	VPN-1 & FireWall...	E1...	ciscocp	log	decrypt	192.168.10.2	10.32.50.51	0	icmp-type 8 icmp-code 0

相关信息

- Cisco PIX 防火墙软件
- Cisco Secure PIX 防火墙命令参考
- 安全产品 Field Notices（包括 PIX）
- 请求注解 (RFC)
- 技术支持和文档 - Cisco Systems