在Cisco Secure PIX防火牆和檢查點NG防火牆之間配置IPSec隧道

目錄

簡介

本文檔演示如何使用預共用金鑰配置IPsec隧道以在兩個專用網路之間進行通訊。在本示例中，通訊網路是Cisco Secure PIX防火牆內部的192.168.10.x專用網路和CheckpointTM Next Generation(NG)防火牆內部的10.32.x.x專用網路。

必要條件

需求

嘗試此組態之前，請確保符合以下要求：

- 從PIX內部和CheckpointTM NG內部到Internet（這裡由172.18.124.x網路表示）的流量應在開始此配置之前流動。
- 使用者應熟悉IPsec交涉。此過程可分為五個步驟，包括兩個網際網路金鑰交換(IKE)階段。IPsec隧道由相關流量發起。流量在IPsec對等路由器之間傳輸時，會被視為有趣。在IKE第1階段，IPsec對等體協商已建立的IKE安全關聯(SA)策略。對等點通過驗證後，會使用網際網路安全性關聯和金鑰管理通訊協定(ISAKMP)建立安全通道。在IKE第2階段，IPsec對等使用經過身份驗證的安全隧道協商IPsec SA轉換。共用策略的協商確定如何建立IPsec隧道。將建立

IPsec隧道，並根據IPsec轉換集中配置的IPsec引數在IPsec對等體之間傳輸資料。IPsec隧道在IPsec SA被刪除或其生存期到期時終止。

採用元件

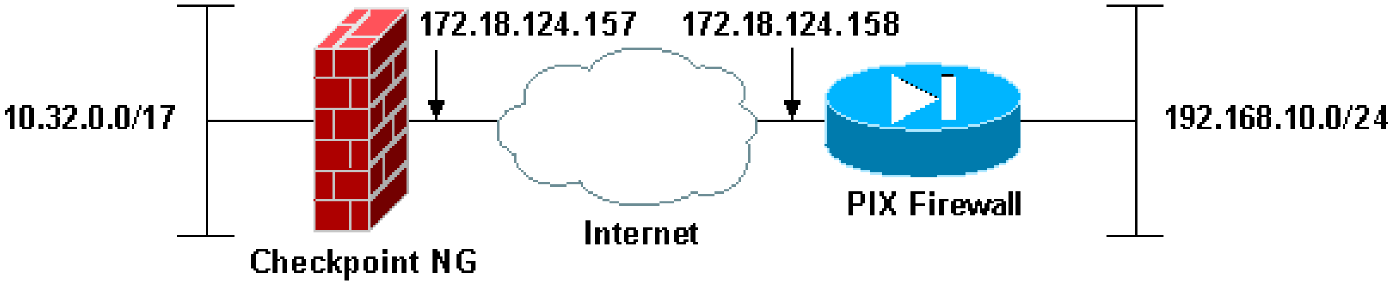
本文中的資訊係根據以下軟體和硬體版本：

- PIX軟體版本6.2.1
- CheckpointTM NG防火牆

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

網路圖表

本檔案會使用以下網路設定：



慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

配置PIX

本節提供用於設定本檔案中所述功能的資訊。

PIX配置

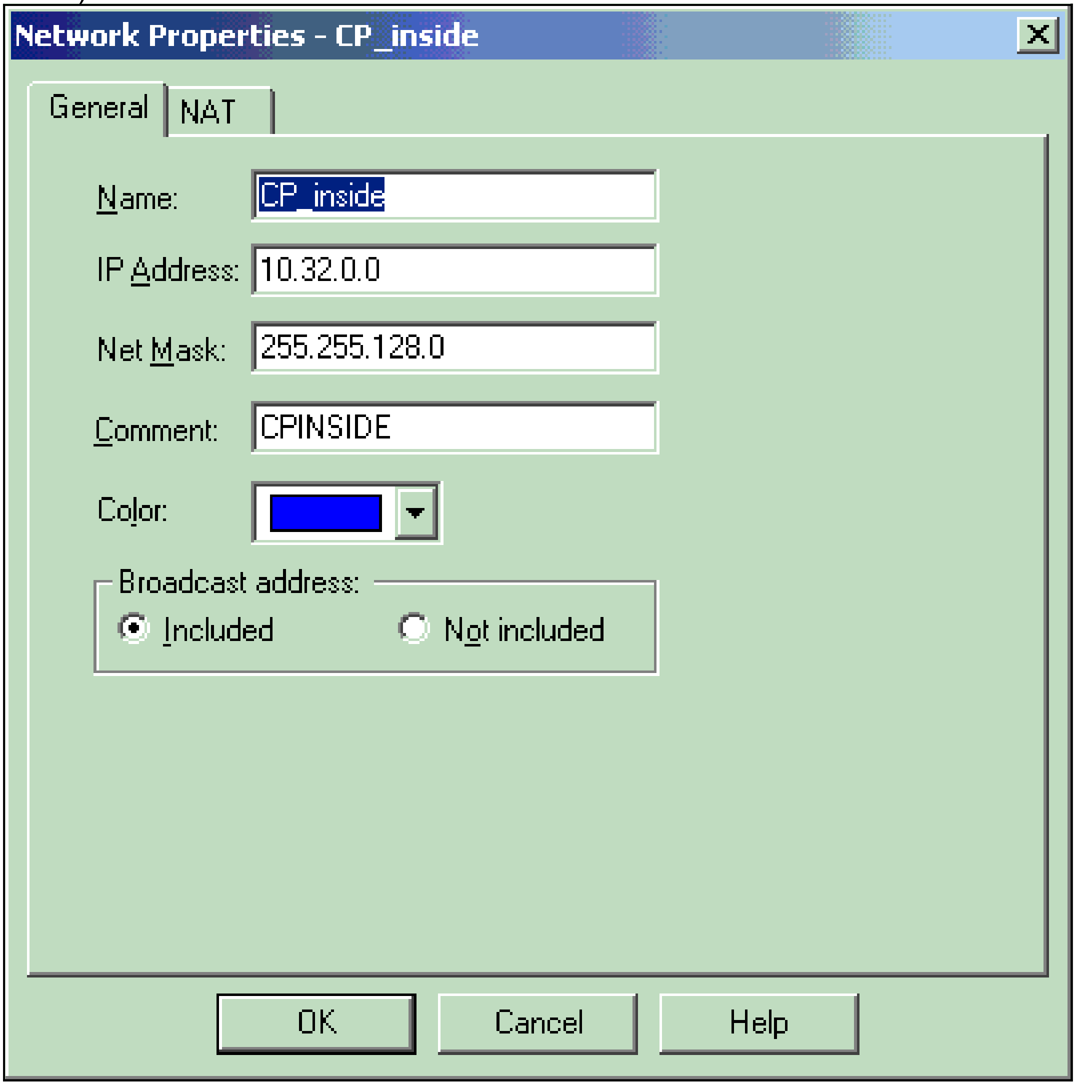
```
PIX Version 6.2(1)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname PIXRTPVPN
domain-name cisco.com
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 h225 1720
fixup protocol 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
```

配置檢查點NG

在CheckpointTM NG上定義網路對象和規則，以構成與要設定的VPN配置相關的策略。然後使用CheckpointTM NG策略編輯器安裝此策略，以完成配置的CheckpointTM NG端。

1. 為用於加密相關流量的Checkpoint網路和PIX防火牆網路建立兩個網路對象。若要執行此操作，請選擇**管理** > **網路對象**，然後選擇**新建** > **網路**。輸入相應的網路資訊，然後按一下**OK**。這些示例顯示一組名為CP_Inside（CheckpointTM NG的內部網路）和PIXINSIDE（PIX的內部網路）的網路對象。



Name: CP_inside

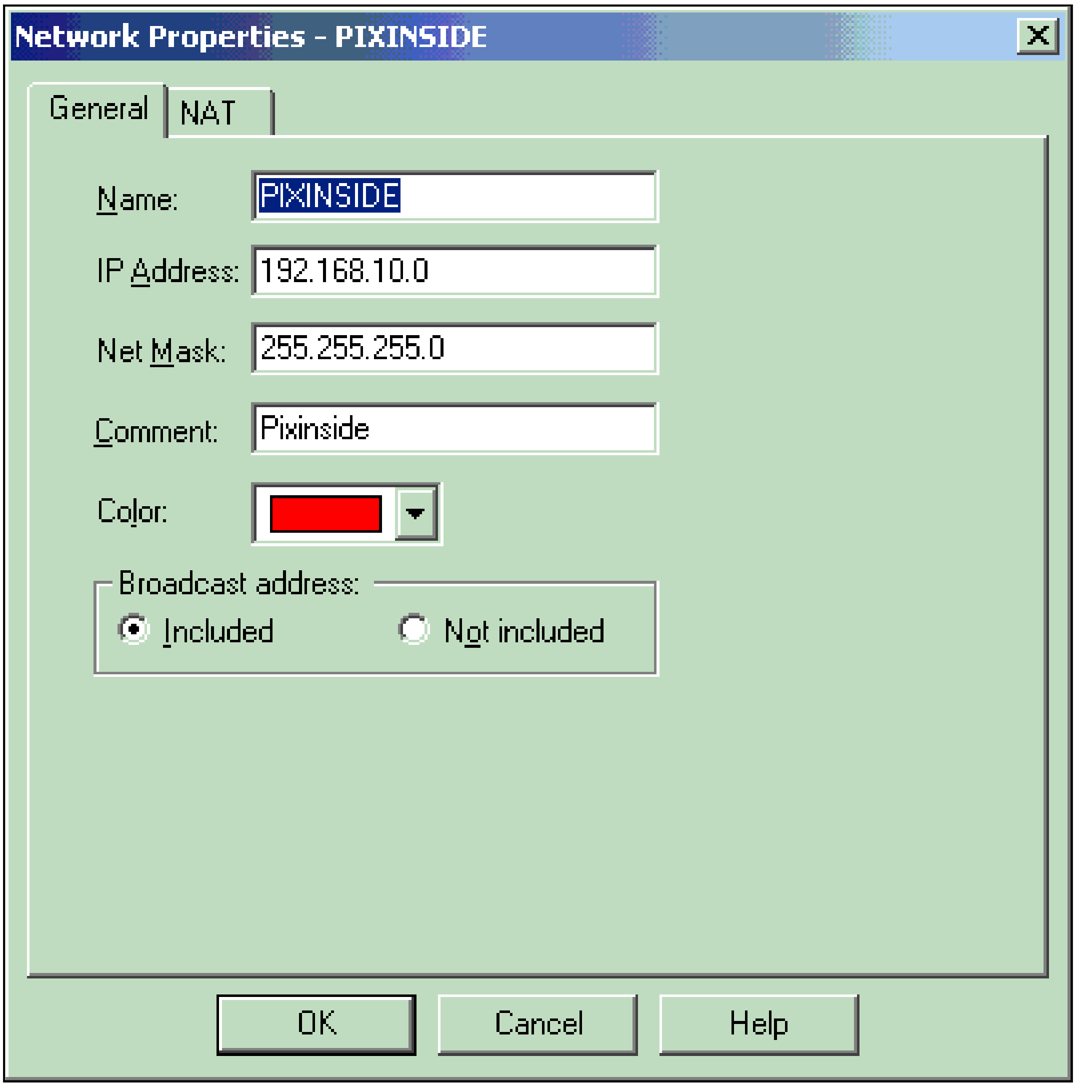
IP Address: 10.32.0.0

Net Mask: 255.255.128.0

Comment: CPINSIDE

Color: 🟦

Broadcast address: ● Included ○ Not included



Name: PIXINSIDE

IP Address: 192.168.10.0

Net Mask: 255.255.255.0

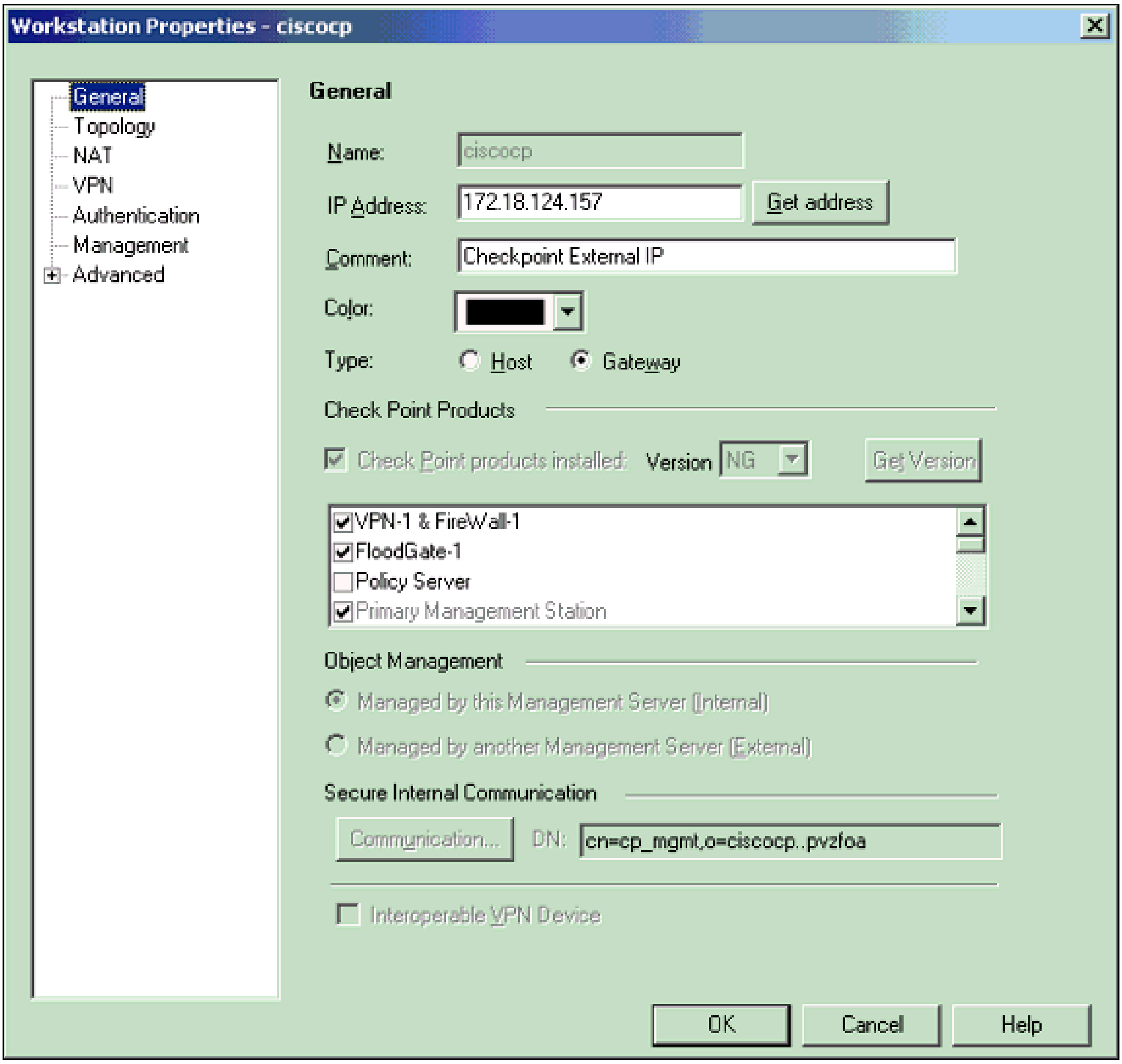
Comment: Pixinside

Color: 🟥

Broadcast address:

● Included ○ Not included

2. 為CheckpointTM NG和PIX建立工作站對象。為此，請選擇**管理** > **網路對象** > **新建** > **工作站**。請注意，您可以使用初始CheckpointTM NG設定期間建立的CheckpointTM NG工作站對象。選擇選項將工作站設定為Gateway and Interoperable VPN Device，然後按一下**OK**。這些示例顯示一組名為ciscocp(**CheckpointTM** NG**)和**PIX（PIX防火牆）的對象。



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

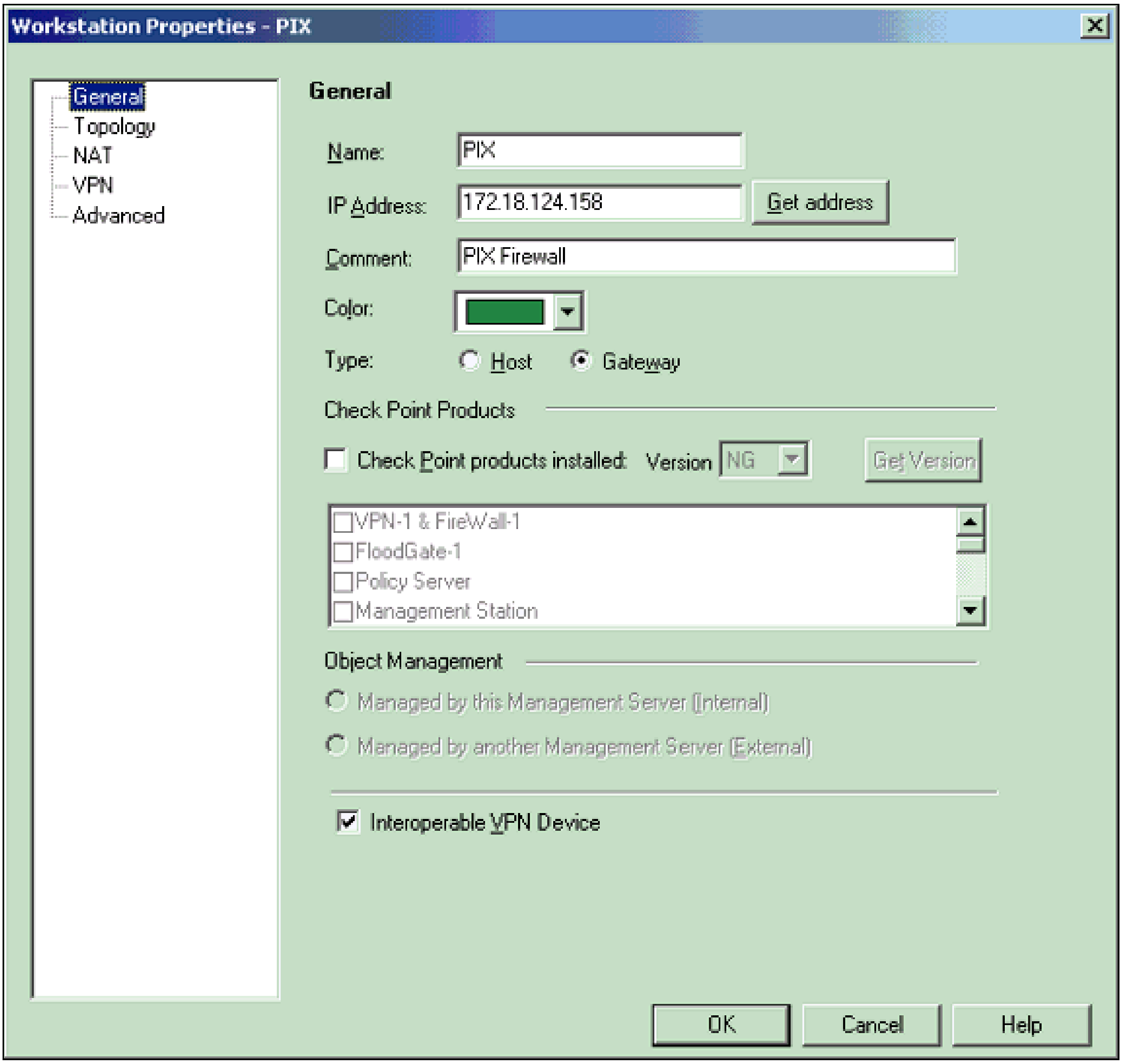
● Managed by this Management Server (Internal)

○ 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 installed: Version NG

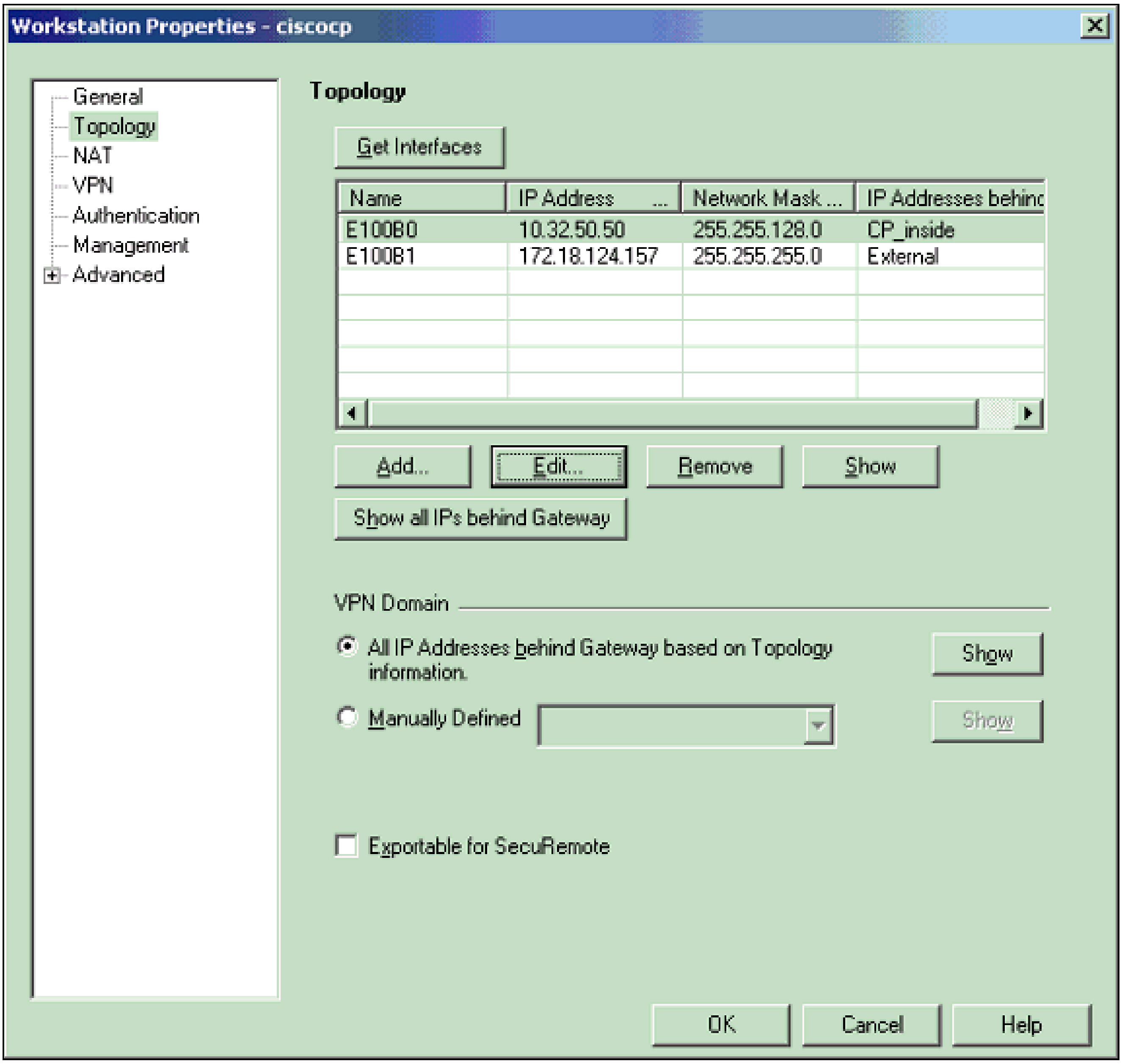
□ VPN-1 & FireWall-1
□ FloodGate-1
□ Policy Server
□ Management Station

○ Managed by this Management Server (Internal)

○ Managed by another Management Server (External)

☑ Interoperable VPN Device

3. 選擇**Manage** > **Network objects** > **Edit**，開啟**CheckpointTM** NG工作站（本例中為 ciscocp）的工作站的「工作站屬性」視窗。從視窗左側的選項中選擇**Topology**，然後選擇要加密的網路。按一下**Edit**以設定介面屬性。



Topology

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

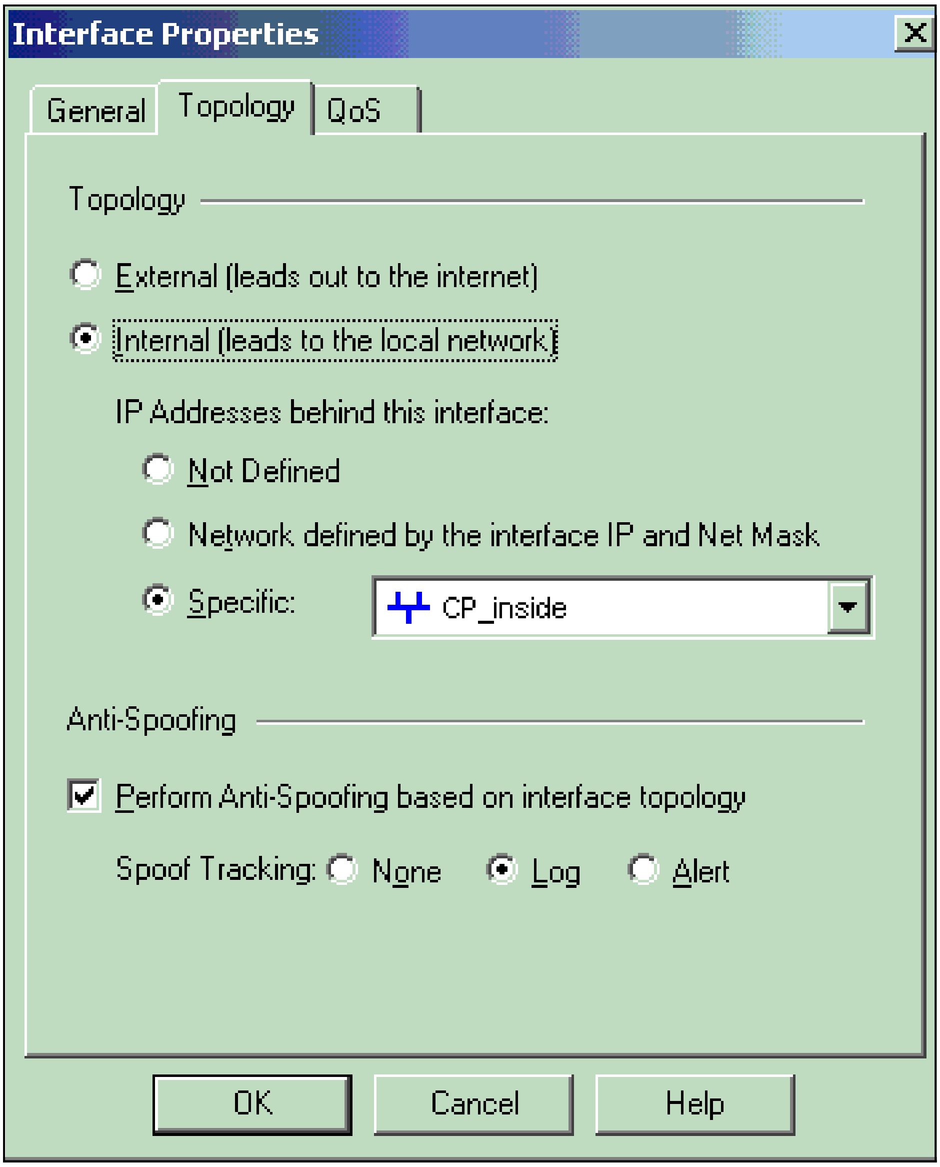
VPN Domain

● All IP Addresses behind Gateway based on Topology information.

○ Manually Defined

□ Exportable for SecuRemote

4. 選擇將工作站指定為內部工作站的選項，然後指定適當的IP地址。按一下「**OK**」（確定）。在此配置中，CP_inside是CheckpointTM NG的內部網絡。此處顯示的拓撲選擇將工作站指定為內部，並將地址指定為CP_inside。



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

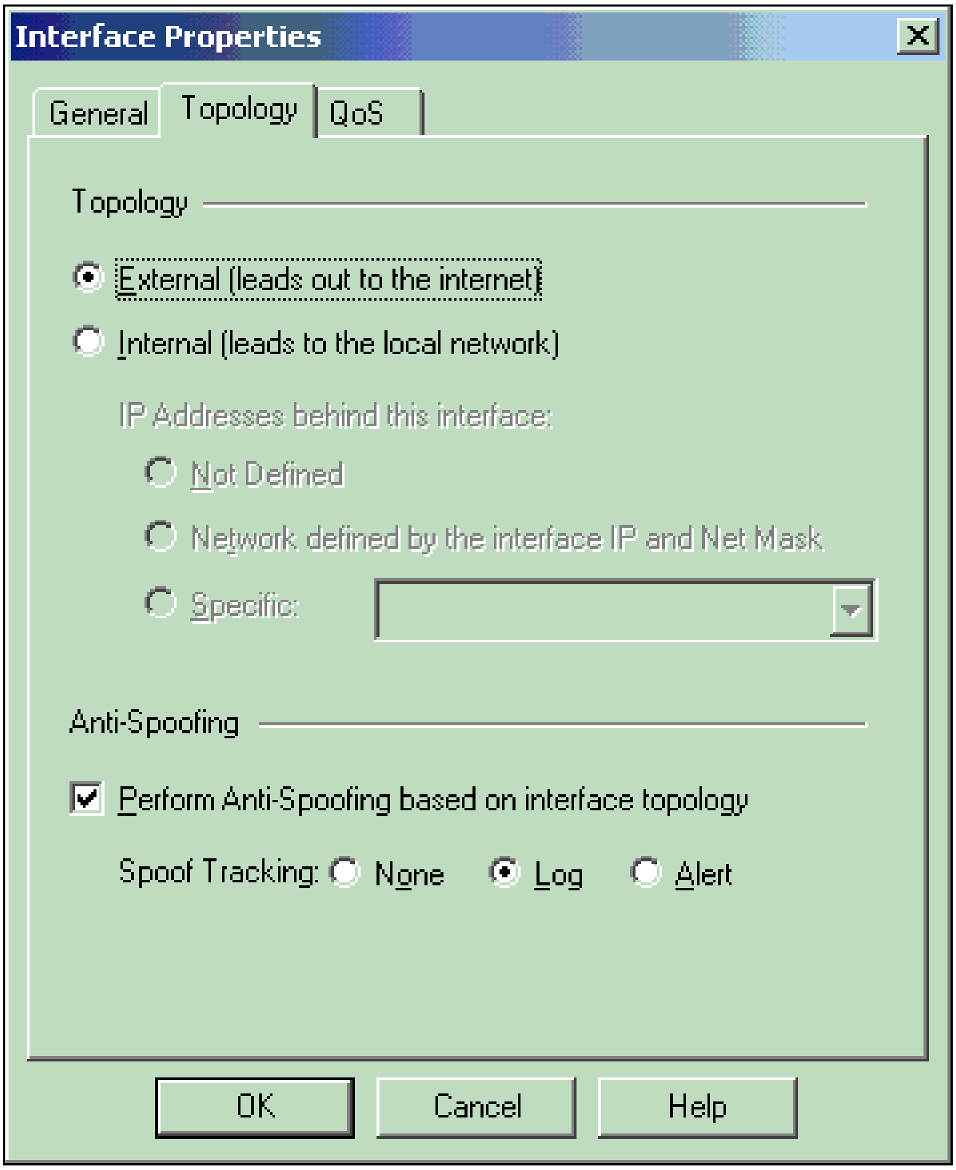
● Specific: CP_inside

Anti-Spoofing

☑ Perform Anti-Spoofing based on interface topology

Spoof Tracking: ○ None ● Log ○ Alert

5. 在「工作站屬性」視窗中，選擇指向Internet的CheckpointTM NG上的外部介面，然後按一下**編輯**以設定介面屬性。選擇該選項將拓撲指定為外部拓撲，然後按一下**確定**。



Interface Properties

General | Topology | QoS

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

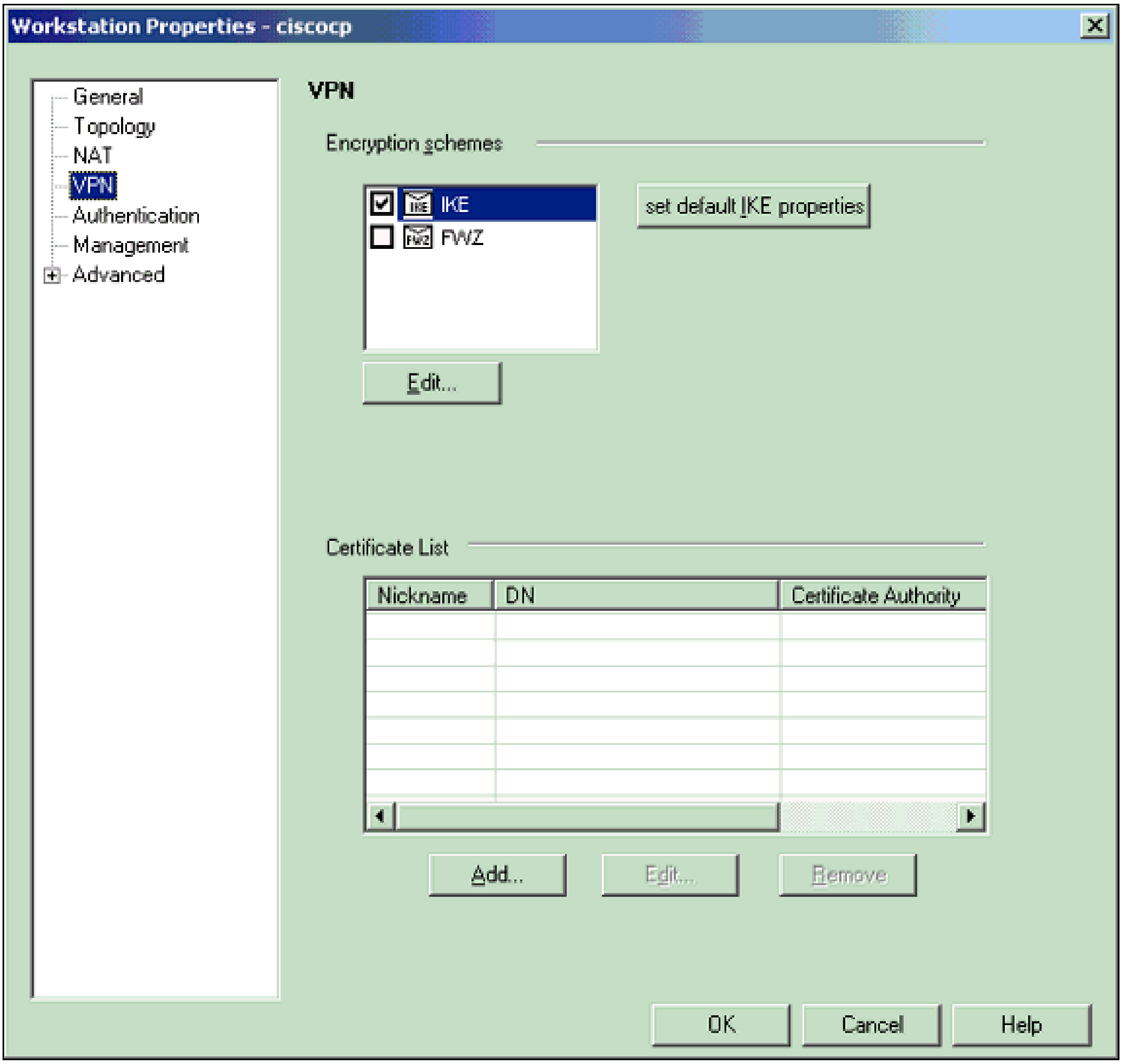
○ Specific:

Anti-Spoofing

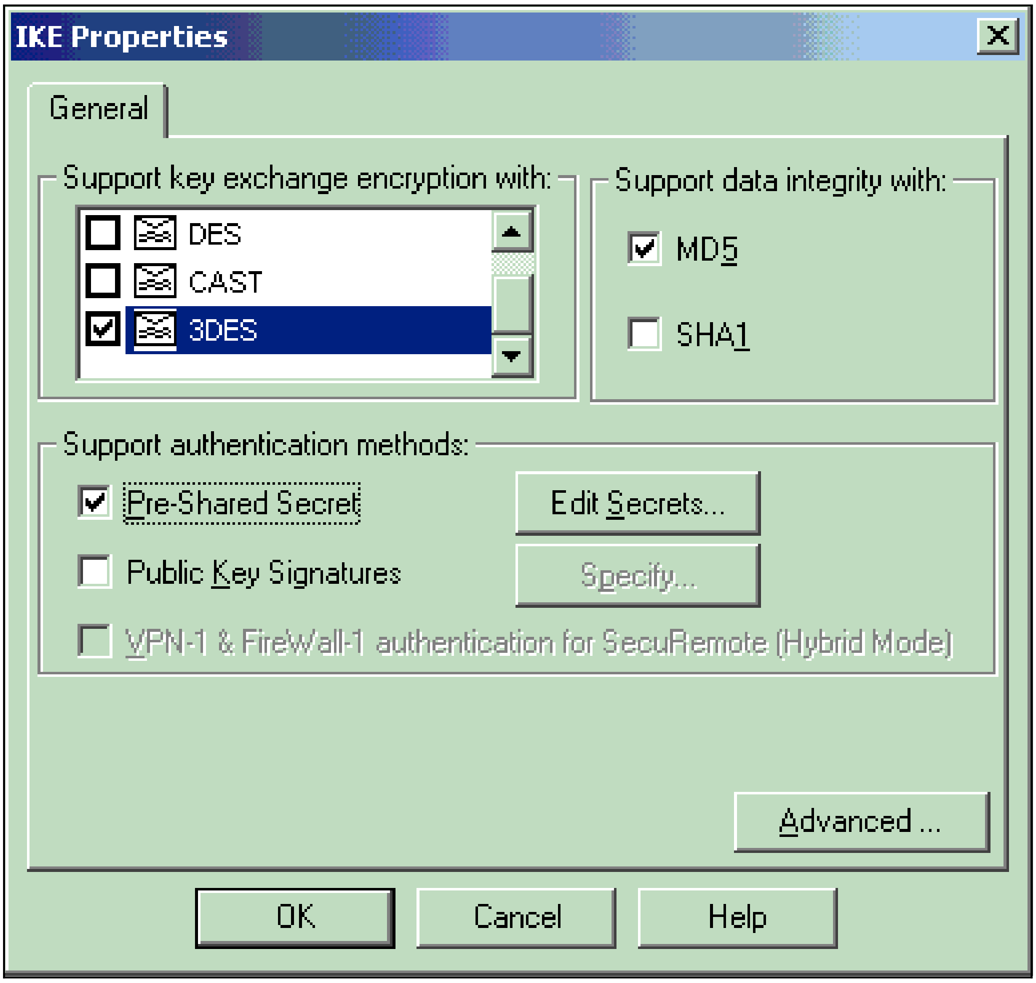
☑ Perform Anti-Spoofing based on interface topology

Spoof Tracking: ○ None ● Log ○ Alert

6. 在CheckpointTM NG上的「工作站屬性」視窗中，從視窗左側的選項中選擇**VPN**，然後選擇IKE引數以用於加密和身份驗證演算法。按一下**Edit**配置IKE屬性。



7. 配置IKE屬性：選擇**3DES**加密的選項，使IKE屬性與**isakmp policy # encryption 3des**命令相容。選擇**MD5**的選項，使IKE屬性與**crypto isakmp policy # hash md5**命令相容。



IKE Properties

General

Support key exchange encryption with:

- □ DES
- □ CAST
- ☑ 3DES

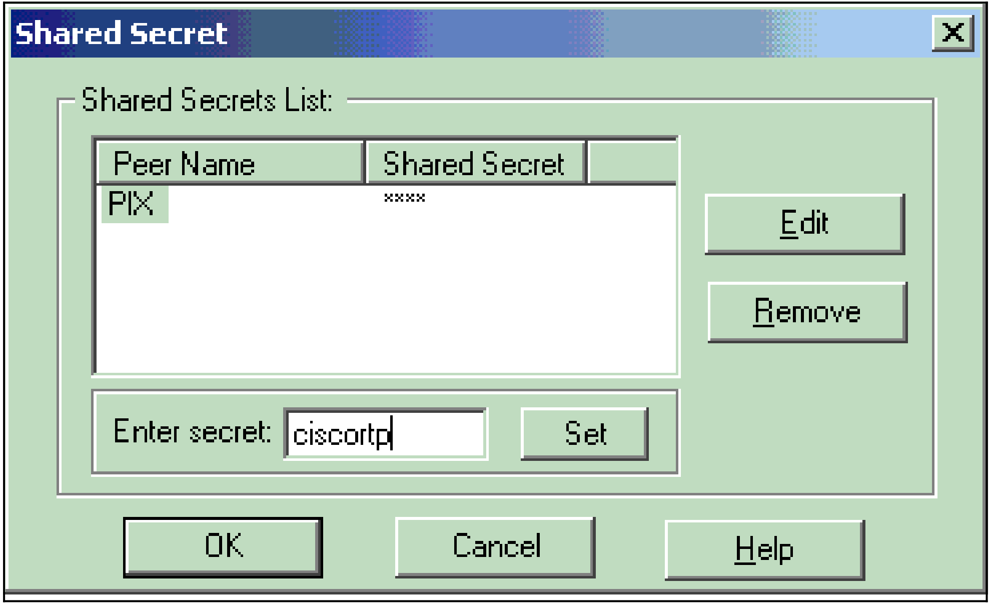
Support data integrity with:

- ☑ MD5
- □ SHA1

Support authentication methods:

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

8. 選擇Pre-Shared Secrets的身份驗證選項，然後單擊Edit Secrets，將預共用金鑰設定為與PIX命令**isakmp key *key key* address** address **netmask**相容。按一下**Edit**以輸入您的金鑰，如下圖所示，然後按一下**Set**，**OK**。



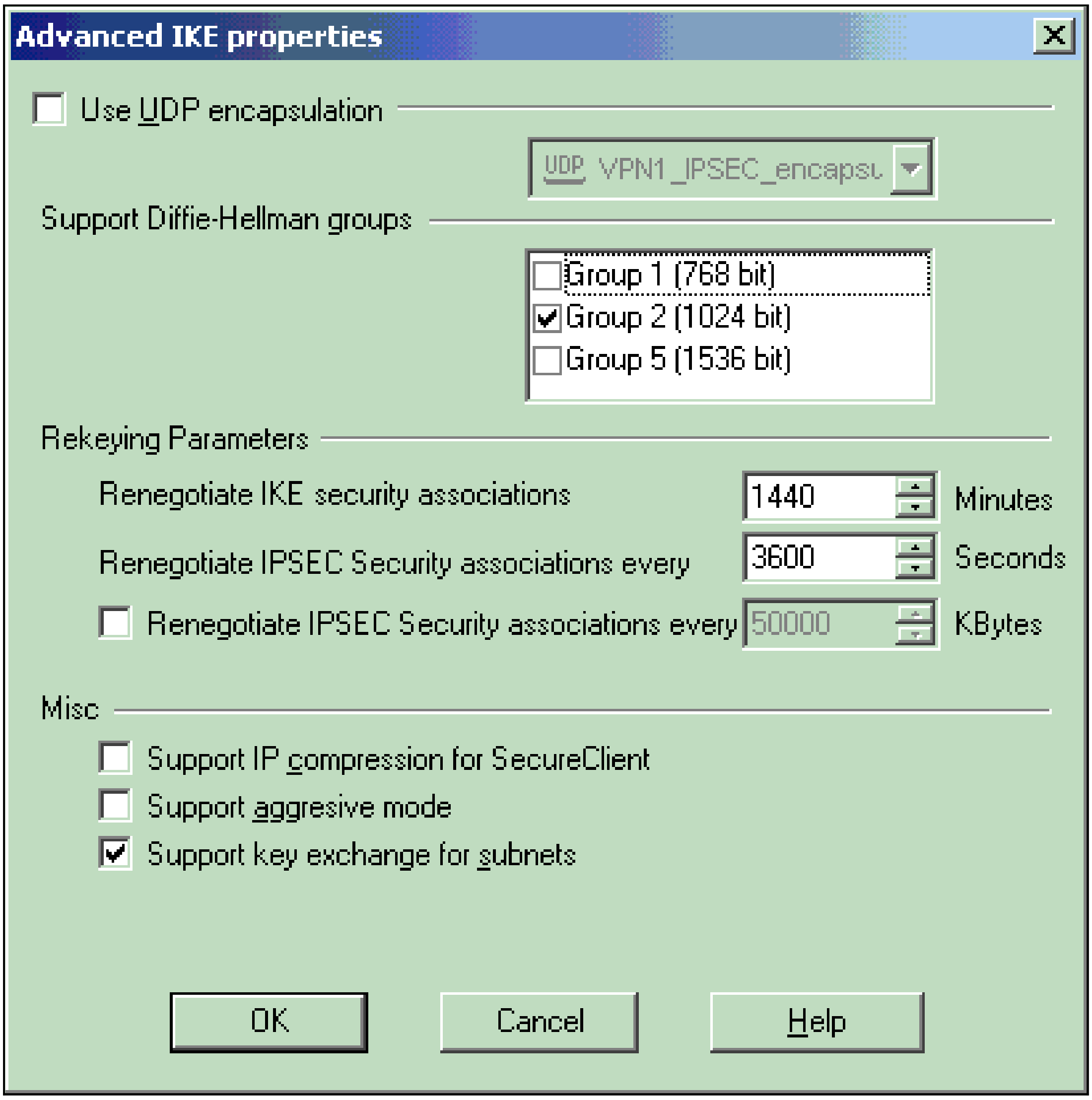
Shared Secret

Shared Secrets List:

Peer Name	Shared Secret
PIX	****

Enter secret: ciscortp

9. 在IKE屬性視窗中，按一下**Advanced...**並更改以下設定：取消選擇**Support aggressive mode**選項。選擇支援子網**金鑰交換的選項**。完成後按一下**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

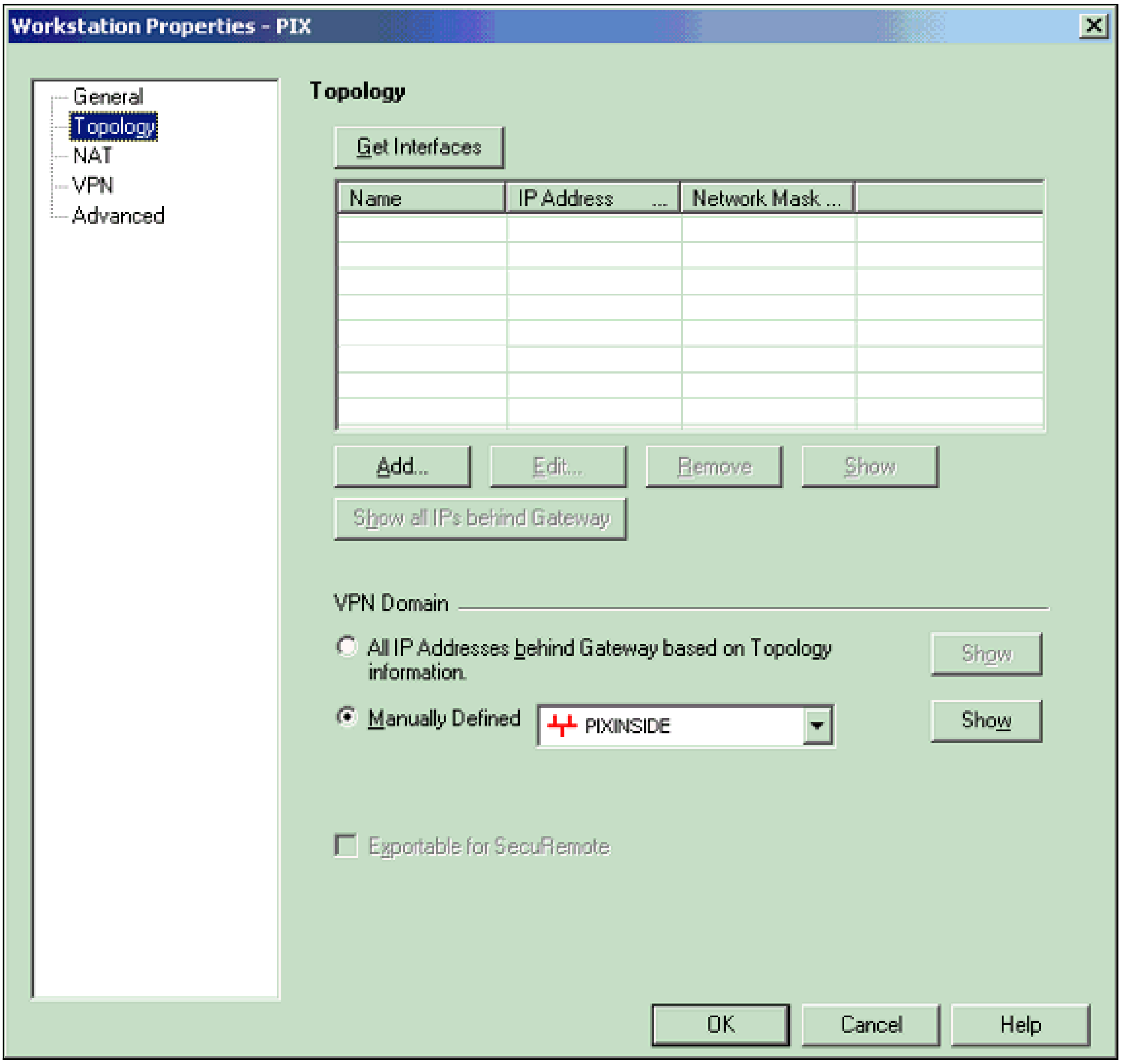
Renegotiate IPSEC Security associations every 3600 Seconds

☐ Renegotiate IPSEC Security associations every 50000 KBytes

Misc

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

10. 選擇**Manage** > **Network objects** > **Edit**以開啟PIX的工作站屬性視窗。從視窗左側的選項中選擇**Topology**，以手動定義VPN域。在此配置中，PIXINSIDE（PIX的內部網路）定義為VPN域。



Workstation Properties - PIX

Topology

Name	IP Address ...	Network Mask ...	

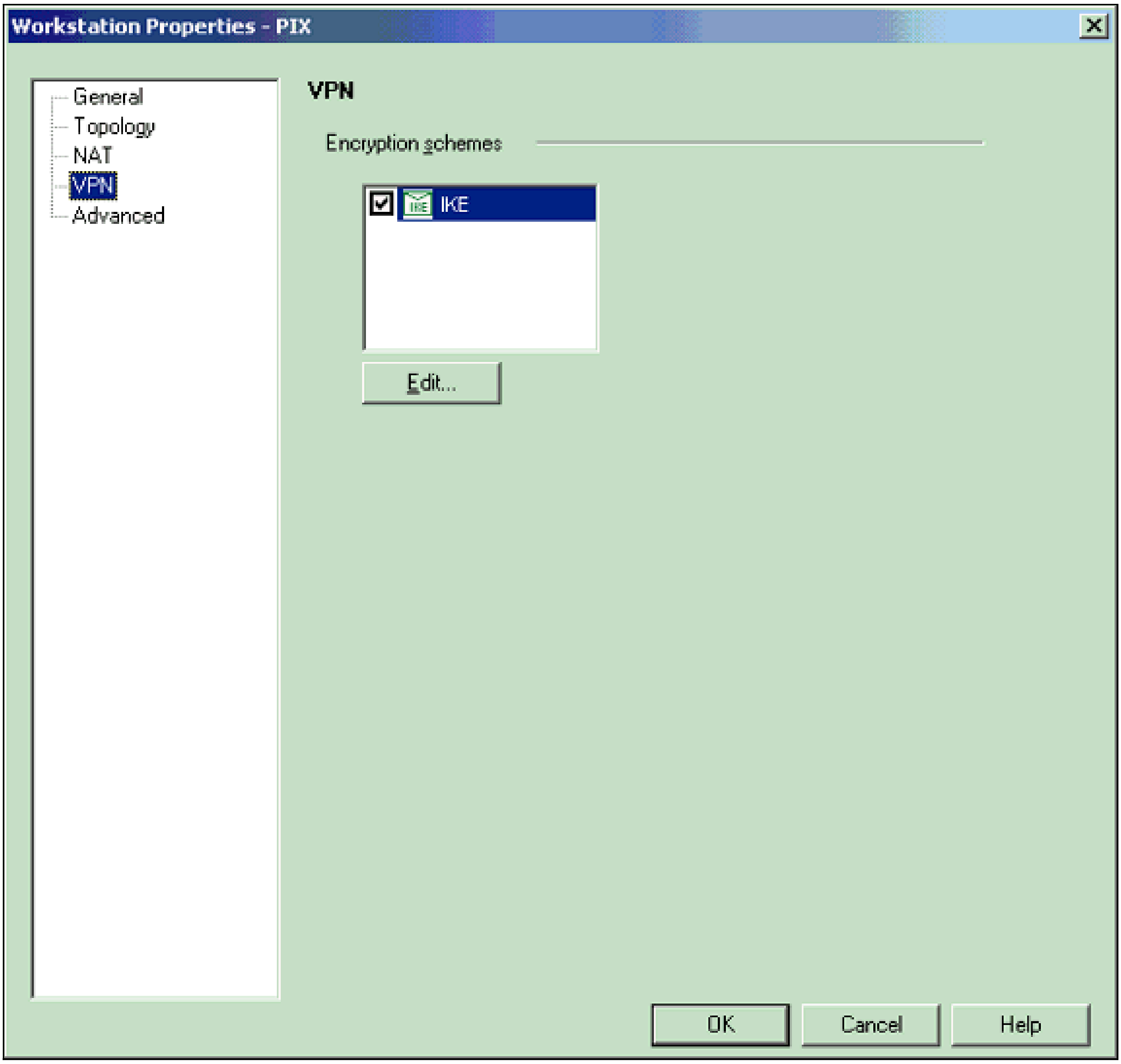
VPN Domain

○ All IP Addresses behind Gateway based on Topology information.

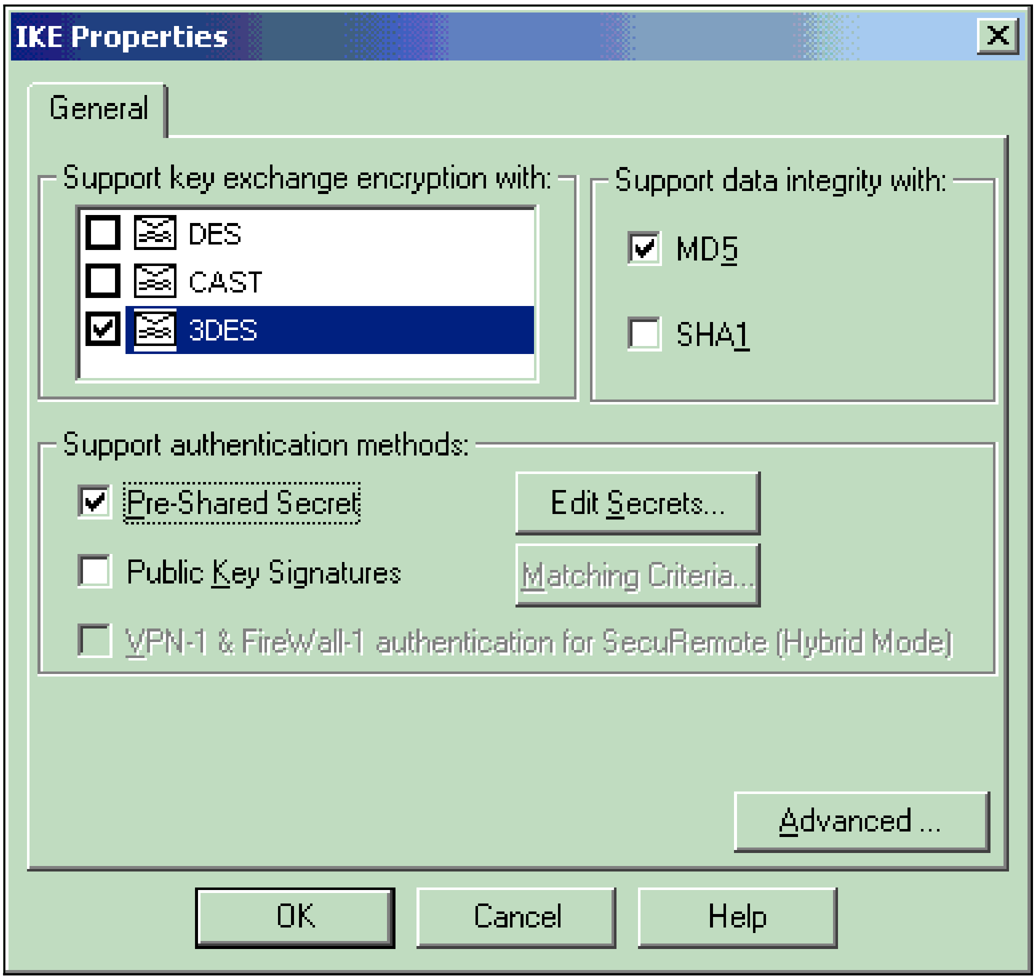
● Manually Defined: PIXINSIDE

□ Exportable for SecuRemote

11. 從視窗左側的選項中選擇**VPN**，然後選擇IKE作為加密方案。按一下**Edit**配置IKE屬性。



12. 配置IKE屬性，如下所示：選擇3DES加密的選項，使IKE屬性與isakmp policy # encryption 3des命令相容。選擇MD5的選項，使IKE屬性與crypto isakmp policy # hash md5命令相容。



IKE Properties

General

Support key exchange encryption with:

□ DES
□ CAST
☑ 3DES

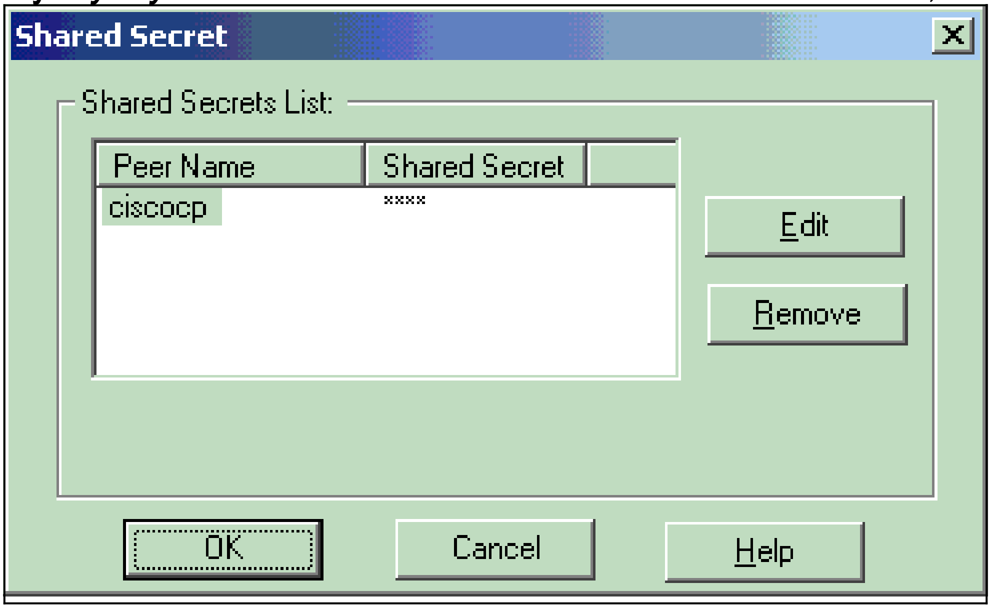
Support data integrity with:

☑ MD5
□ SHA1

Support authentication methods:

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

13. 選擇Pre-Shared Secrets的身份驗證選項，然後按一下Edit Secrets將預共用金鑰設定為與PIX命令**isakmp key *key key*** address **address netmask**相容。按一下**Edit**輸入金鑰，然後按一下**Set**， **OK**。

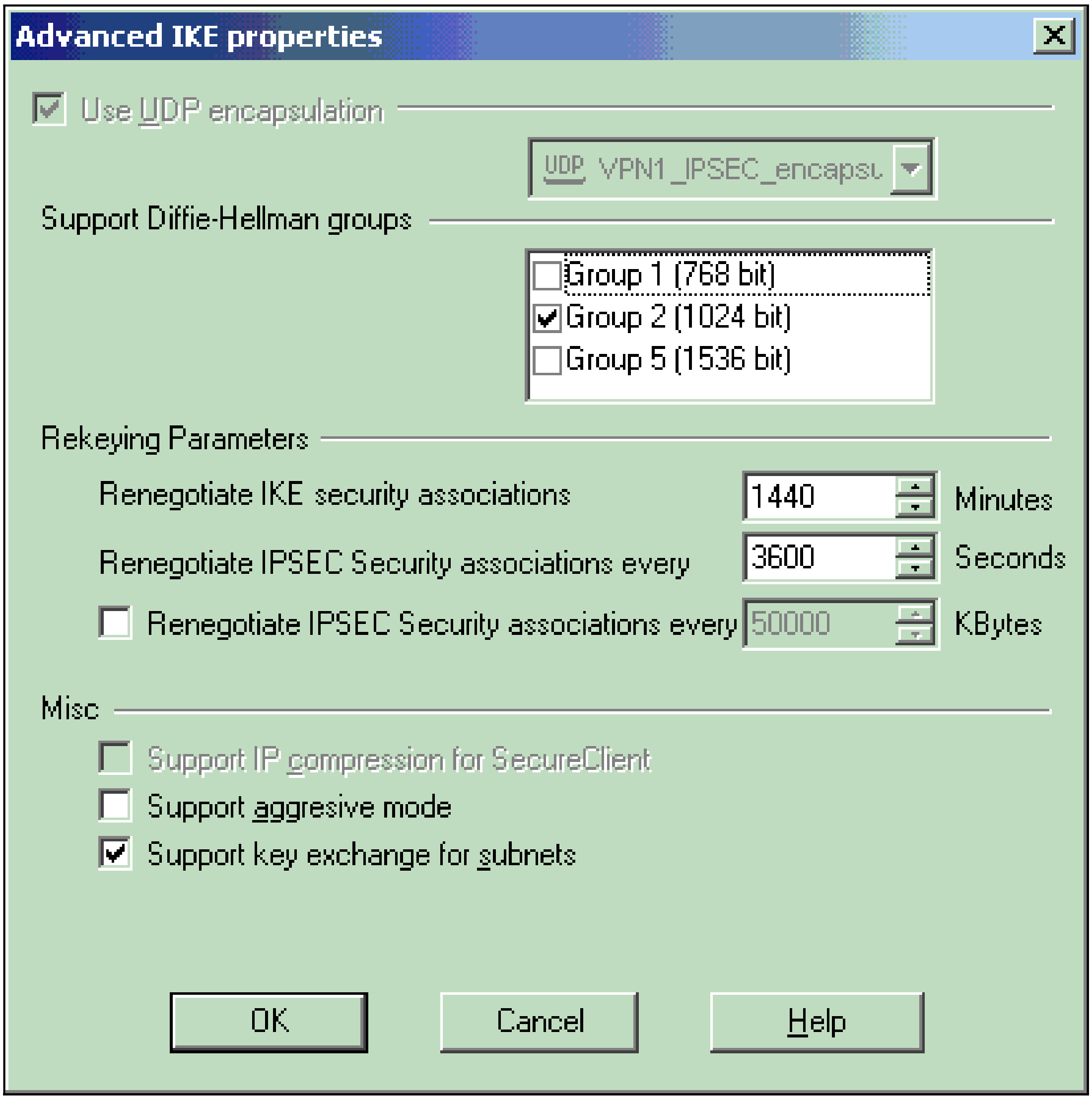


Shared Secret

Shared Secrets List:

Peer Name	Shared Secret
ciscocp	****

14. 在IKE屬性視窗中，按一下**Advanced...**並更改這些設定。選擇適用於IKE屬性的Diffie-Hellman組。取消選擇**Support aggressive mode**選項。選擇支援子網**金鑰交換的選項**。完成後，按一下**OK**、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

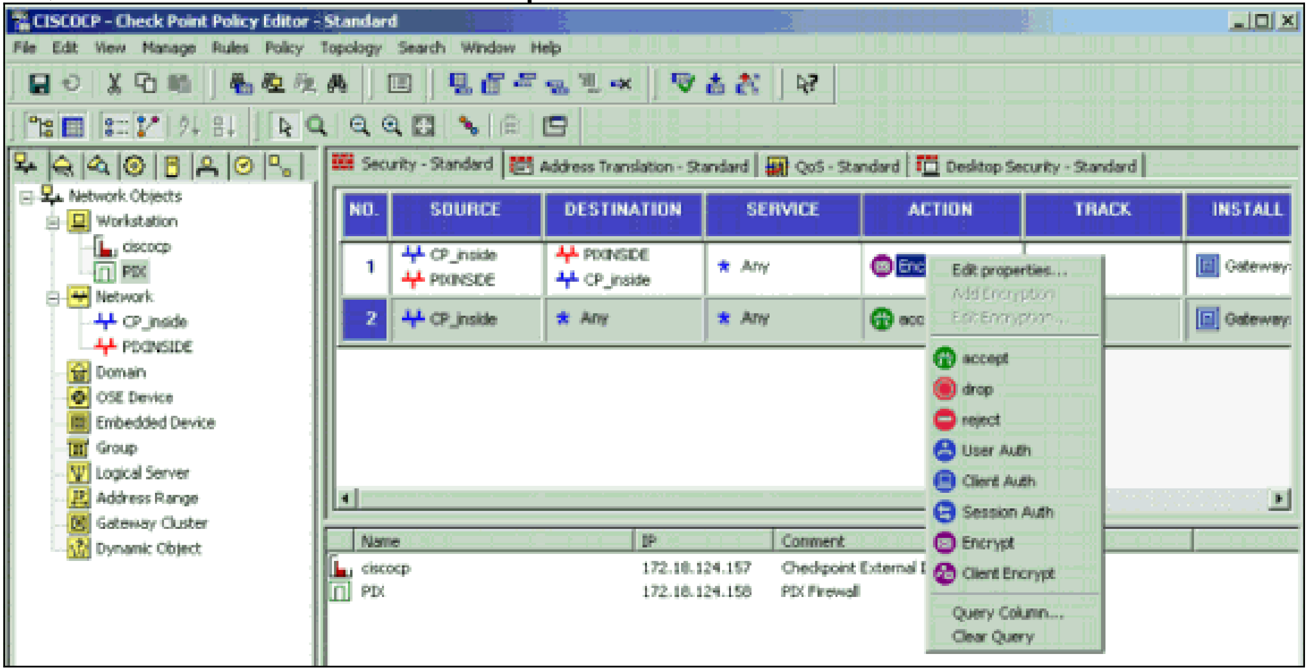
Misc

□ Support IP compression for SecureClient

□ Support aggresive mode

☑ Support key exchange for subnets

15. 選擇**Rules** > **Add Rules** > **Top**為策略配置加密規則。在「策略編輯器」視窗中，在源列和目標列上插入源為CP_inside(檢查點TM NG的內部網路)和PIXINSIDE（PIX的內部網路）的規則。設定**Service = Any**、**Action = Encrypt**和**Track = Log**的值。新增規則的Encrypt Action部分後，按一下右鍵**Action**並選擇**Edit Properties**。

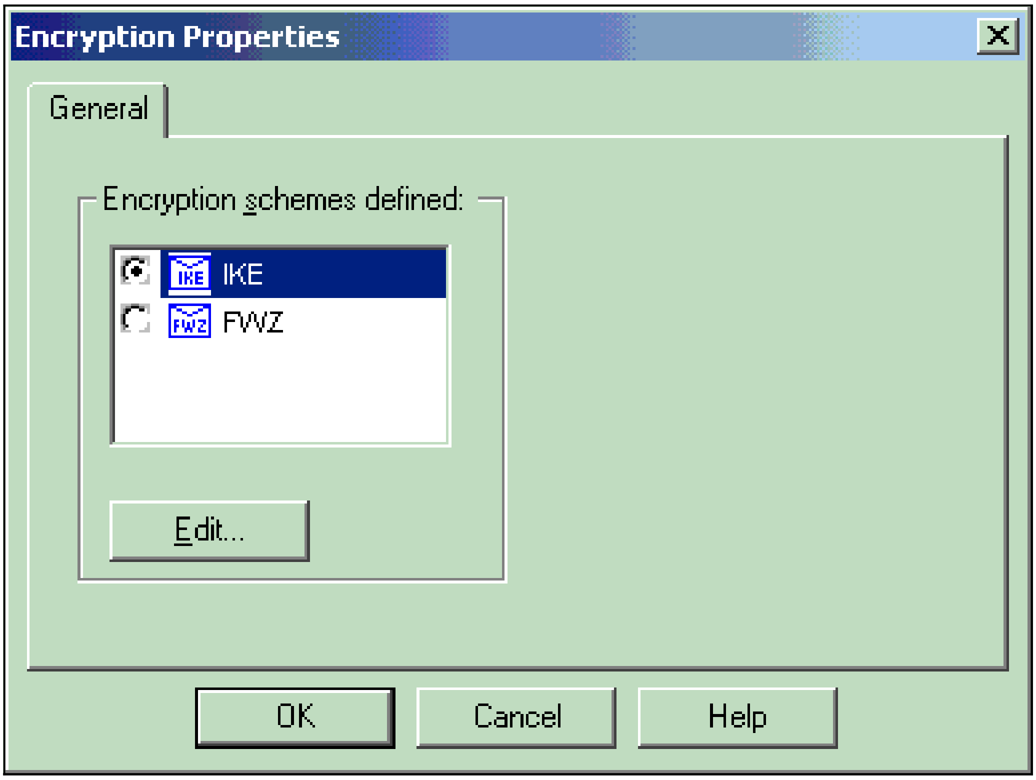


CISCOCP - Check Point Policy Editor - Standard

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. 選中並突出顯示IKE後，按一下**Edit**。



Encryption Properties

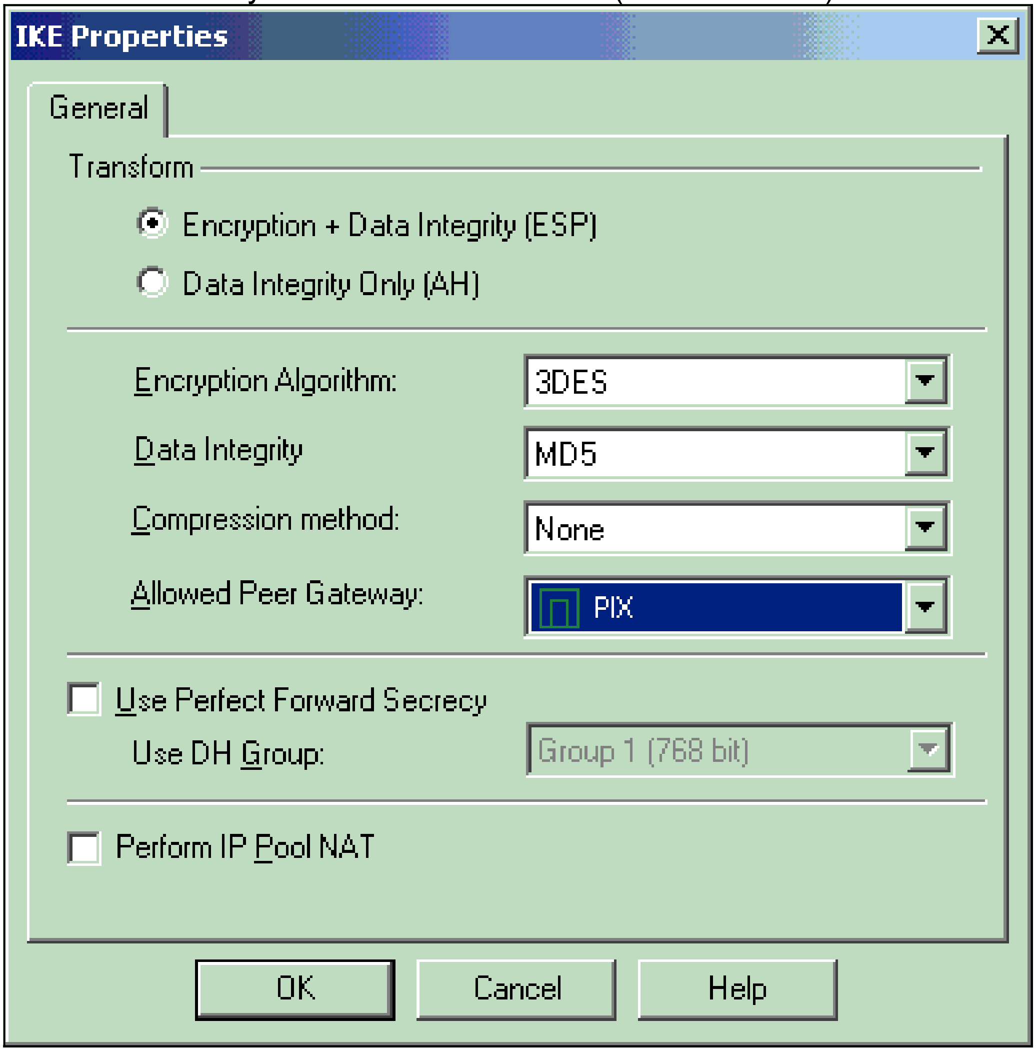
General

Encryption schemes defined:

● IKE

○ FWZ

17. 在「IKE屬性」視窗中，更改屬性以與**crypto ipsec transform-set rtptac esp-3des esp-md5-hmac**命令中的PIX IPsec轉換一致。將Transform選項設定為**Encryption + Data Integrity(ESP)**，將Encryption Algorithm設定為**3DES**，將Data Integrity設定為**MD5**，並將Allowed Peer Gateway設定為匹配外部PIX網關（此處稱為PIX）。 按一下「**OK**」（確定）。



IKE Properties

General

Transform

● Encryption + Data Integrity (ESP)

○ Data Integrity Only (AH)

Encryption Algorithm: 3DES

Data Integrity: MD5

Compression method: None

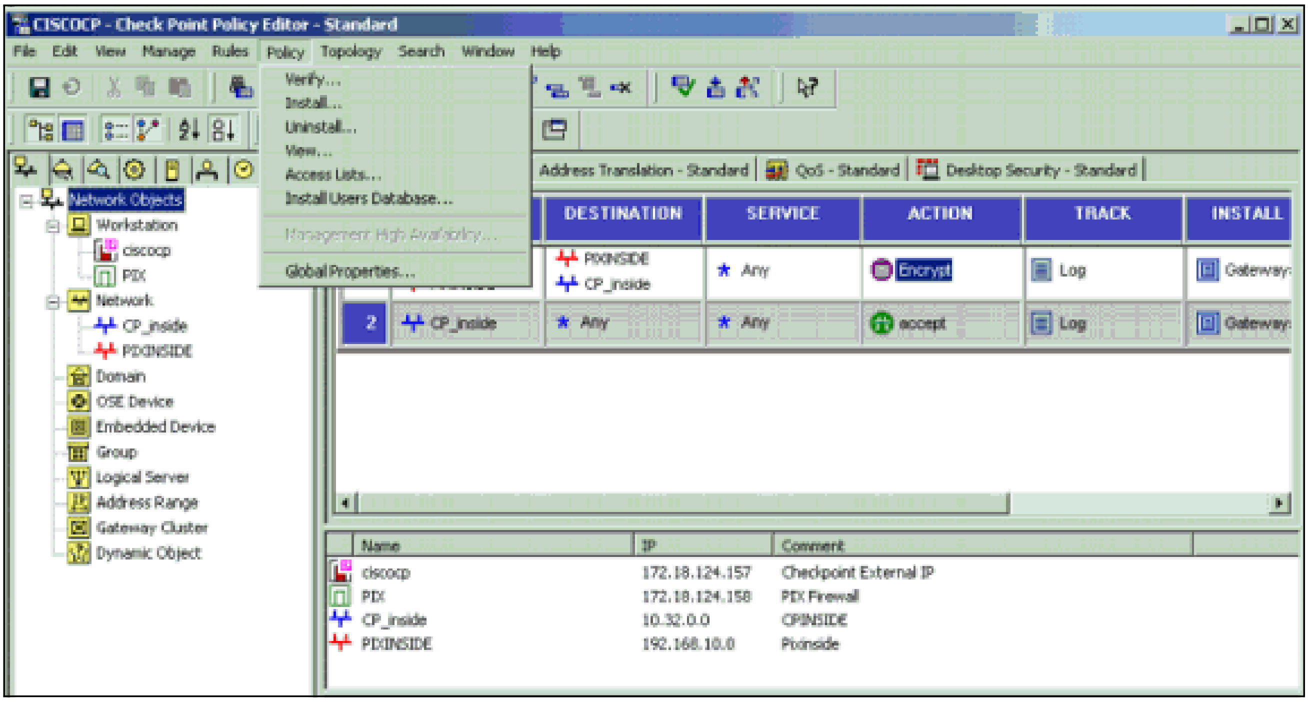
Allowed Peer Gateway: PIX

□ Use Perfect Forward Secrecy

Use DH Group: Group 1 (768 bit)

□ Perform IP Pool NAT

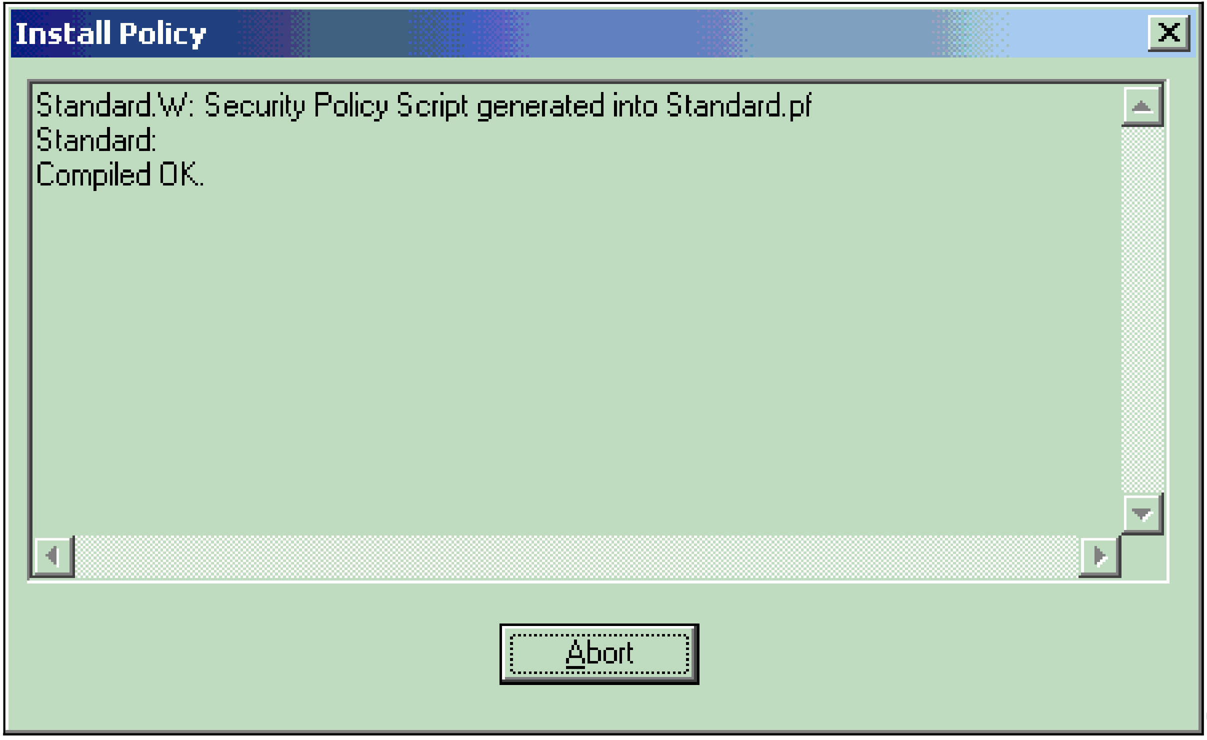
18. 配置CheckpointTM NG後，請儲存該策略並選擇**Policy** > **Install**以啟用它。



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

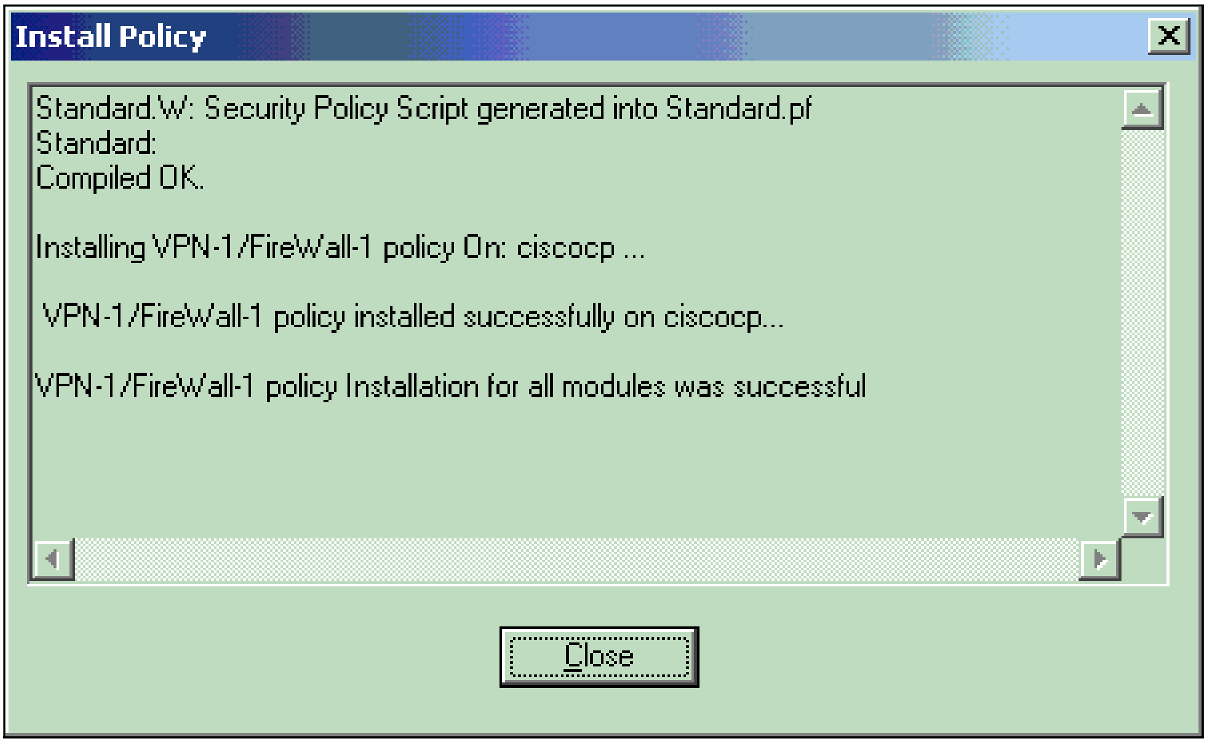
Name	IP	Comment
ciscocp	172.18.124.157	Checkpoint External IP
PIX	172.18.124.158	PIX Firewall
CP_inside	10.32.0.0	CPINSIDE
PIXINSIDE	192.168.10.0	Pixinside

編譯策略時，安裝視窗將顯示進度註釋。



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

當安裝視窗指示策略安裝完成時。按一下Close完成該過程。



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

驗證

驗證PIX配置

使用本節內容，確認您的組態是否正常運作。

輸出直譯器工具(僅供已註冊客戶使用)(OIT)支援某些**show**命令。使用OIT檢視**show**命令輸出的分析。

從其中一個專用網路向另一個專用網路發出ping命令，以測試兩個專用網路之間的通訊。在此配置中，從PIX端(192.168.10.2)向Checkpoint^{TM} NG內部網路(10.32.50.51)傳送ping。

- **show crypto isakmp sa** — 顯示對等體上的所有當前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
```

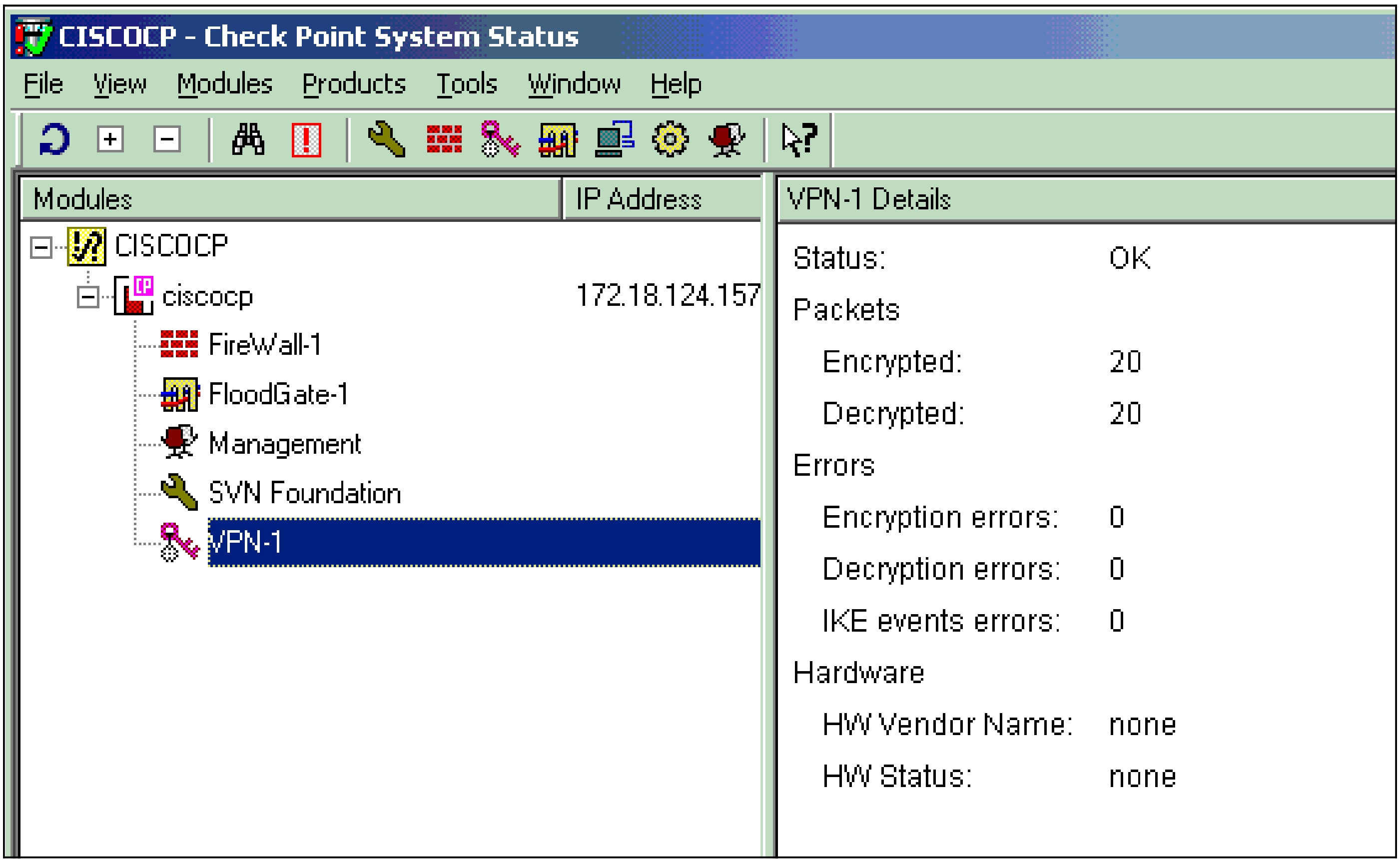
- **show crypto ipsec sa** — 顯示當前SA使用的設定。

```
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:
```

檢視檢查點NG上的隧道狀態

轉至策略編輯器，然後選擇**視窗** > **系統狀態**以檢視隧道狀態。



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

疑難排解

排除PIX配置故障

輸出直譯器工具(僅供已註冊客戶使用)(OIT)支援某些show命令。使用OIT檢視show命令輸出的分析。

附註：使用 debug 指令之前，請先參閱有關 Debug 指令的重要資訊。

使用這些命令在PIX防火牆上啟用調試。

- **debug crypto engine** — 顯示有關執行加密和解密的加密引擎的調試消息。
- **debug crypto isakmp** — 顯示有關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:
```

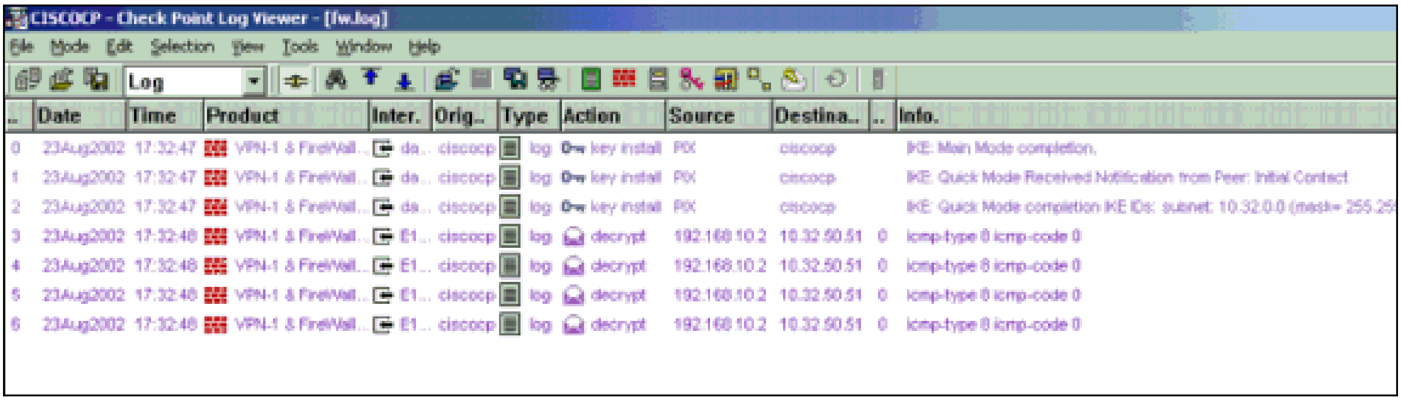
```
OAK_QM_IDLE
ISAKMP (0): processing SA payload. message ID = 322868148
ISAKMP : Checking IPSec proposal 1
ISAKMP: transform 1, ESP_3DES
ISAKMP: attributes in transform:
ISAKMP: encaps is 1
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (basic) of 28800
ISAKMP: SA life type in kilobytes
ISAKMP: 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
```

網路摘要

當在檢查點上的加密域中配置多個相鄰的內部網路時，裝置可能會根據感興趣的流量自動彙總這些網路。如果PIX上的加密訪問控制清單(ACL)未配置為匹配，則通道可能會失敗。例如，如果將10.0.0.0 /24和10.0.1.0 /24的內部網路配置為包括在隧道中，則可以將它們總結為10.0.0.0 /23。

檢視檢查點NG日誌

選擇**視窗 > 日誌檢視器**以檢視日誌。



..	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

相關資訊

- Cisco PIX防火牆軟體
- Cisco Secure PIX防火牆命令參考
- 安全產品現場通知（包括PIX）
- 要求建議 (RFC)
- 技術支援與文件 - Cisco Systems