Cisco Secure PIX Firewall と Checkpoint NG Firewall 間のIPSec トンネル設定

内容

概要

このドキュメントでは、2 つのプライベート ネットワーク間で通信するために事前共有キーを使用して IPSec トンネルを設定する方法について説明します。この例では、通信するネットワークは、Cisco Secure PIX Firewall 内部の 192.168.10.x プライベート ネットワークと Checkpoint(TM) Next Generation（NG）ファイアウォール内部の 10.32.x.x プライベート ネットワークです。

前提条件

要件

この設定を行う前に、次の要件が満たされていることを確認します。

- この設定を開始する前に、PIX内部および^{CheckpointTM} NG内部からインターネット(ここでは172.18.124.xネットワークで表されます)へのトラフィックが流れる必要があります。
- ユーザが IPsec のネゴシエーションに精通している必要があります。このプロセスは、2つのインターネットキー交換(IKE)フェーズを含む5つのステップに分けることができます。対象トラフィックによって IPsec トンネルが開始されます。IPsec ピアの間を転送されるトラフ

ィックは、対象トラフィックとみなされます。IKE フェーズ 1 では、IPsec ピア同士が、IKE セキュリティ アソシエーション（SA）ポリシーについてネゴシエートします。ピアが認証されると、Internet Security Association and Key Management Protocol（ISAKMP）を使用して安全なトンネルが作成されます。IKE フェーズ 2 では、IPsec ピア同士が認証済みの安全なトンネルを使用して、IPsec SA トランスフォームをネゴシエートします。共有ポリシーのネゴシエーションによって、IPsec トンネルの確立方法が決まります。IPsec トンネルが作成され、IPsec トランスフォーム セットに設定された IPsec パラメータに基づいて、IPsec 間でデータが伝送されます。IPsec SA が削除されるか、そのライフタイムの有効期限が切れると、IPsec トンネルは終了します。

使用するコンポーネント

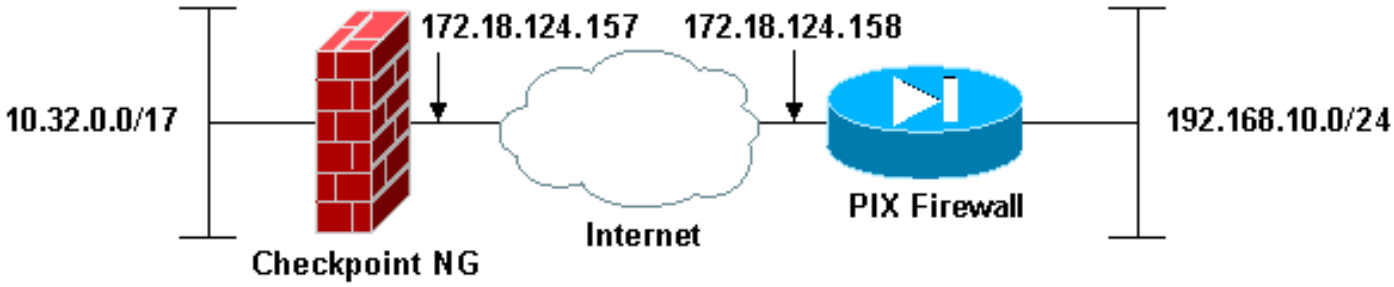
このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- PIX ソフトウェア リリース 6.2.1
- CheckpointTM NGファイアウォール

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

ネットワーク図

このドキュメントでは、次のネットワーク セットアップを使用します。



表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

PIX の設定

このセクションでは、このドキュメントで説明する機能を設定するための情報を提供します。

PIX の設定
PIX Version 6.2(1) nameif ethernet0 outside security0 nameif ethernet1 inside security100 enable password 8Ry2YjIyt7RRXU24 encrypted passwd 2KFQnbNIdI.2KYOU encrypted hostname PIXRTPVPN

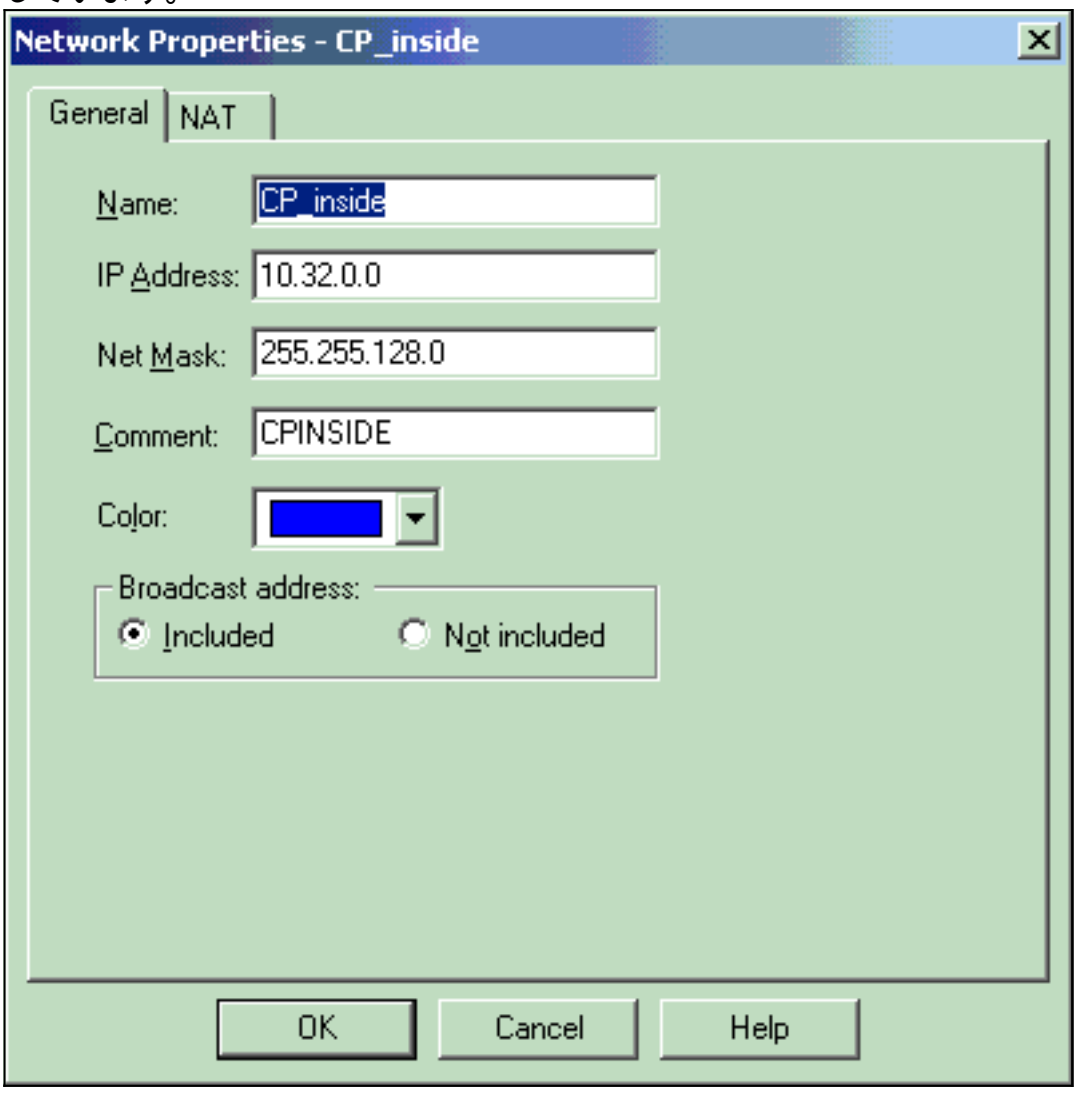
```
domain-name cisco.com
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol ils 389
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
fixup protocol skinny 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
```

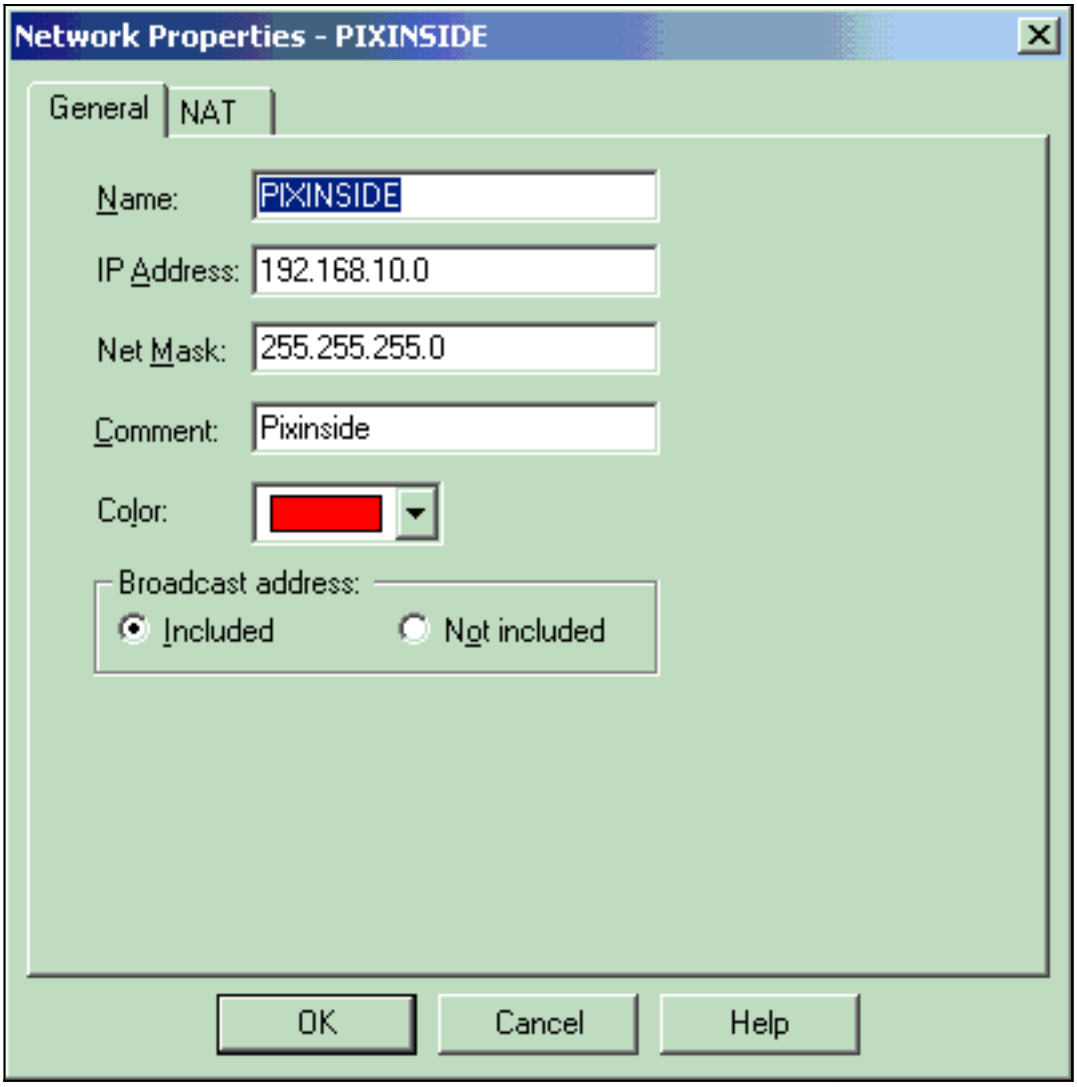
```
172.18.124.157 netmask 255.255.255.255
!--- Defines ISAKMP policy. isakmp policy 1
authentication pre-share
isakmp policy 1 encryption 3des
isakmp policy 1 hash md5
isakmp policy 1 group 2
isakmp policy 1 lifetime 86400
telnet timeout 5
ssh timeout 5
terminal width 80
Cryptochecksum:089b038c8e0dbc38d8ce5ca72cf920a5
: end
```

Checkpoint NG の設定

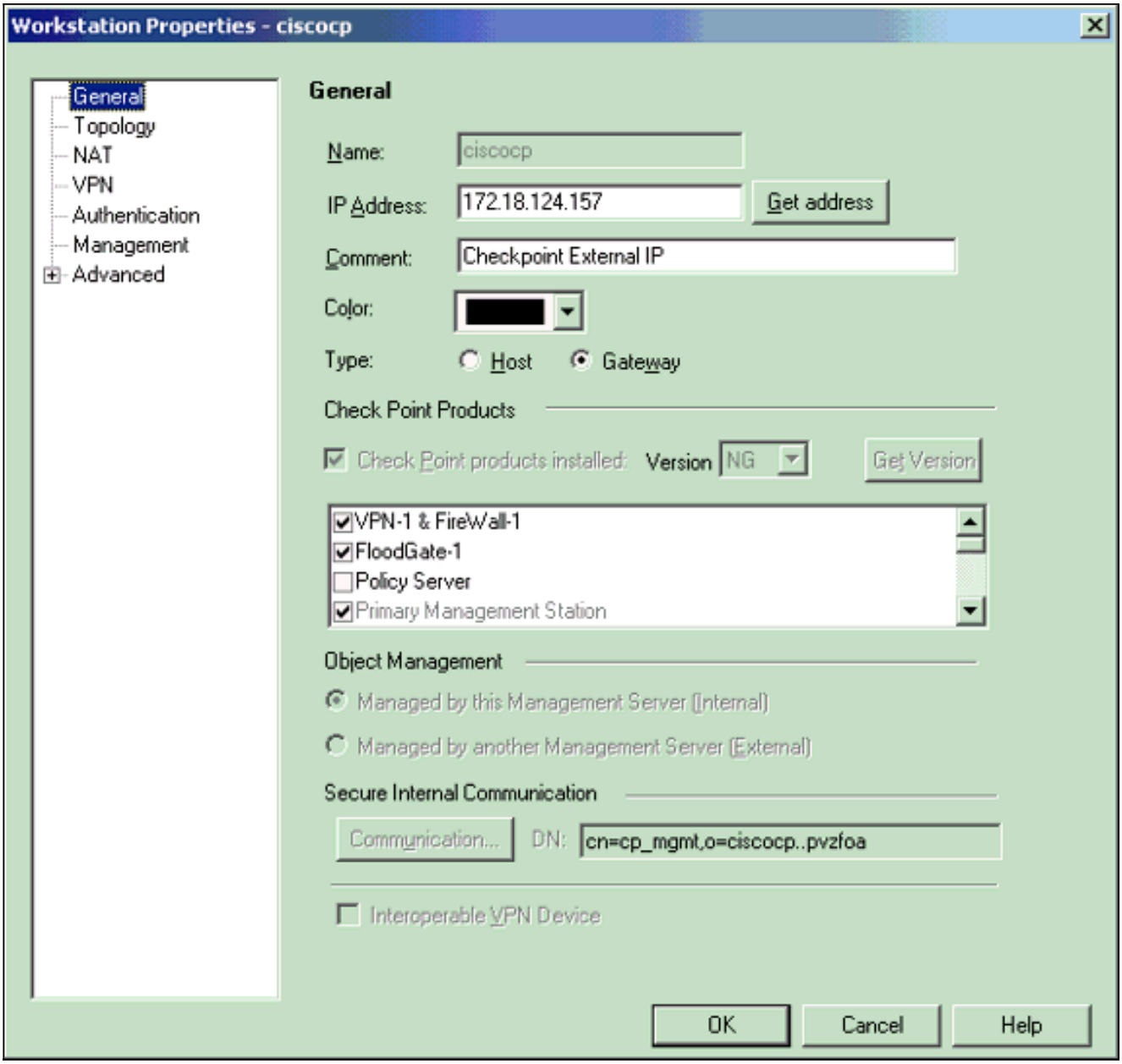
CheckpointTM NGでネットワークオブジェクトとルールが定義され、設定するVPN設定に関連するポリシーが作成されます。このポリシーは、CheckpointTM NG Policy Editorを使用してインストールされ、構成のCheckpointTM NG側を完了します。

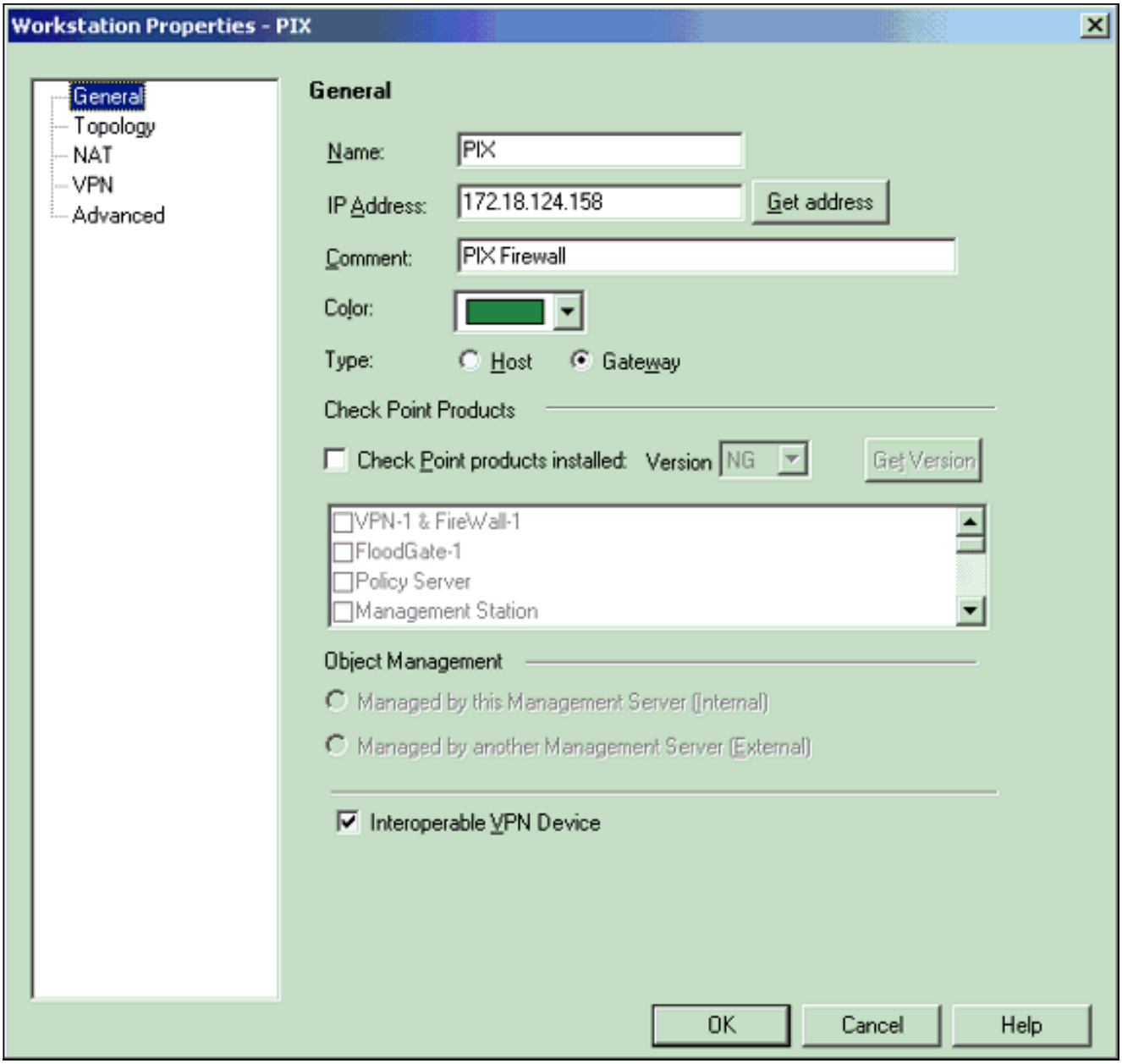
1. 対象トラフィックを暗号化するCheckpointネットワークとPIX Firewallネットワークの2つのネットワークオブジェクトを作成します。これを行うには、[**Manage**] > [**Network Objects**]の順に選択し、[**New**] > [**Network**]を選択します。適切なネットワーク情報を入力して、[OK] をクリックします。次の例は、CP_Inside(CheckpointTM NGの内部ネットワーク)およびPIXINSIDE（PIXの内部ネットワーク）と呼ばれるネットワークオブジェクトのセットを示しています。



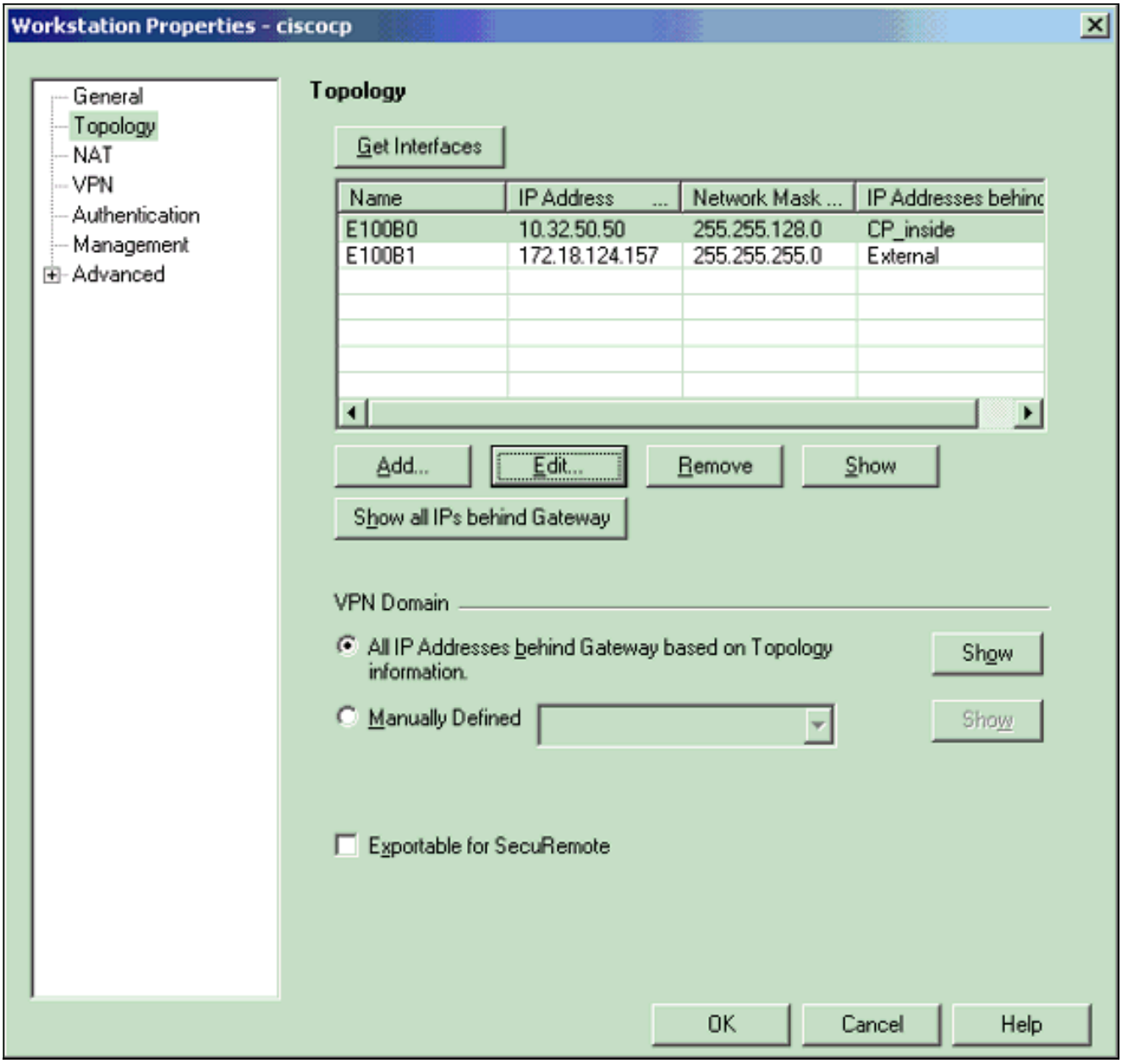


2. CheckpointTM NGおよびPIX用のワークステーションのオブジェクトを作成します。これを行うには、[Manage] > [Network Objects] > [New] > [Workstation] の順に選択します。Checkpoint TM NG の初期設定の際に作成した CheckpointTM NG ワークステーション オブジェクトを使用できます。ワークステーションをゲートウェイおよび相互運用可能VPNデバイスとして設定するオプションを選択し、[OK]をクリックします。次の例は、ciscocp(CheckpointTM NG)およびPIX(PIX Firewall)と呼ばれるオブジェクトのセットを示しています。

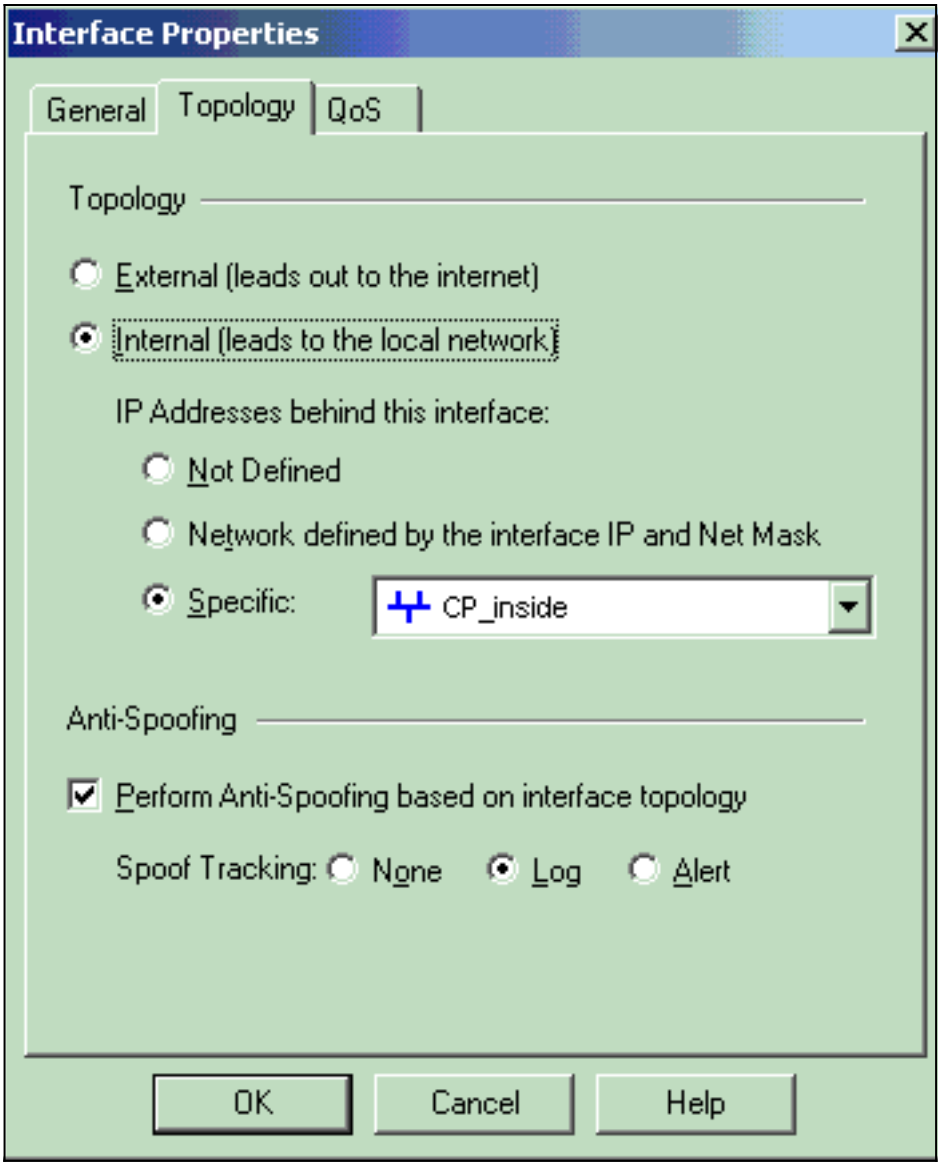

Workstation Properties - ciscocp
General
Topology
NAT
VPN
Authentication
Management
Advanced
General
Name:
ciscocp
IP Address:
172.18.124.157
Get address
Comment:
Checkpoint External IP
Color:
Type:
Host
Gateway
Check Point Products
Check Point products installed:
Version
NG
Get Version
VPN-1 & FireWall-1
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=ciscocp..pvzfoa
Interoperable VPN Device
OK
Cancel
Help



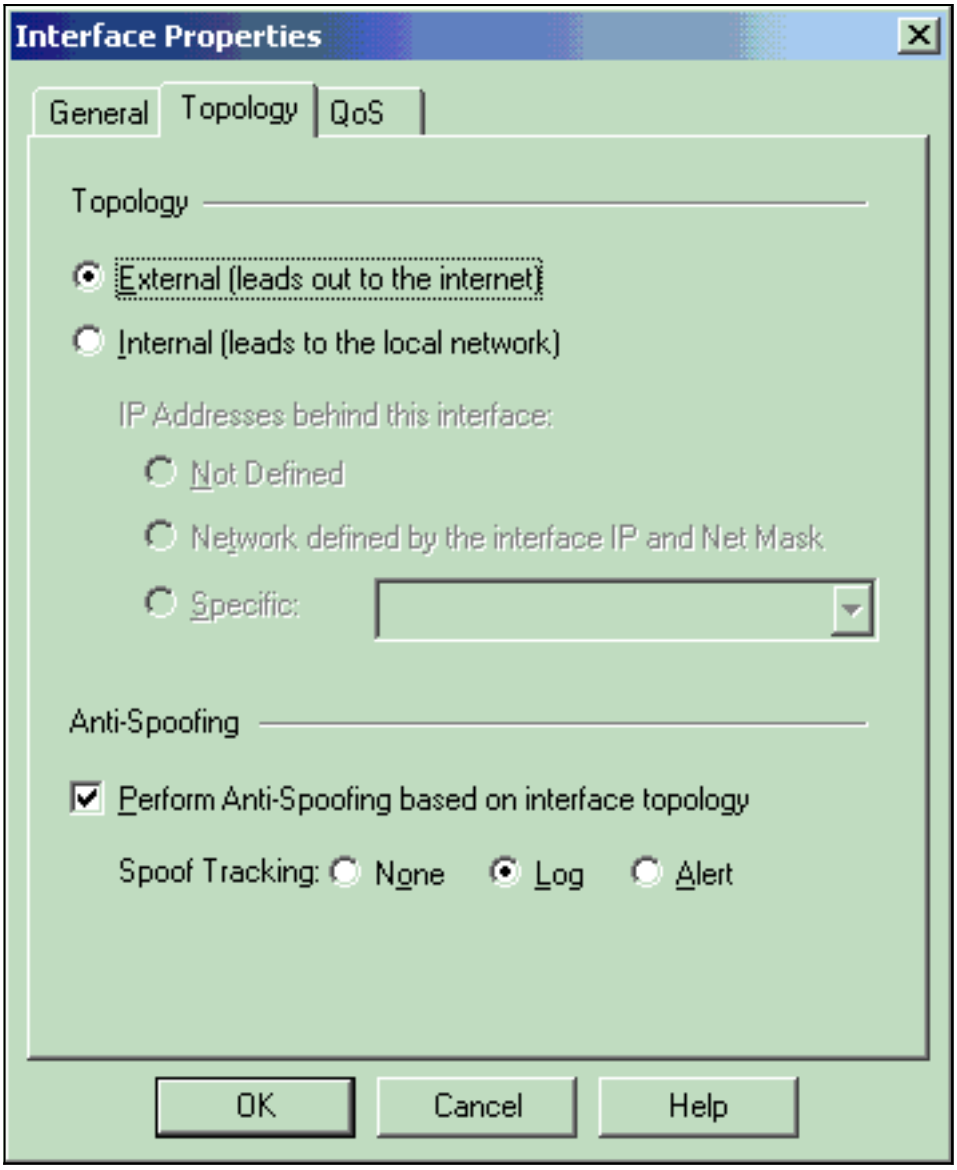
3. [Manage] > [Network objects] > [Edit] を選択し、**CheckpointTM** NGワークステーション（この例ではciscocp）の[Workstation Properties]ウィンドウを開きます。ウィンドウの左側の選択肢から**[Topology]**を選択し、暗号化するネットワークを選択します。[編集]をクリックして、インターフェイスのプロパティを設定します。



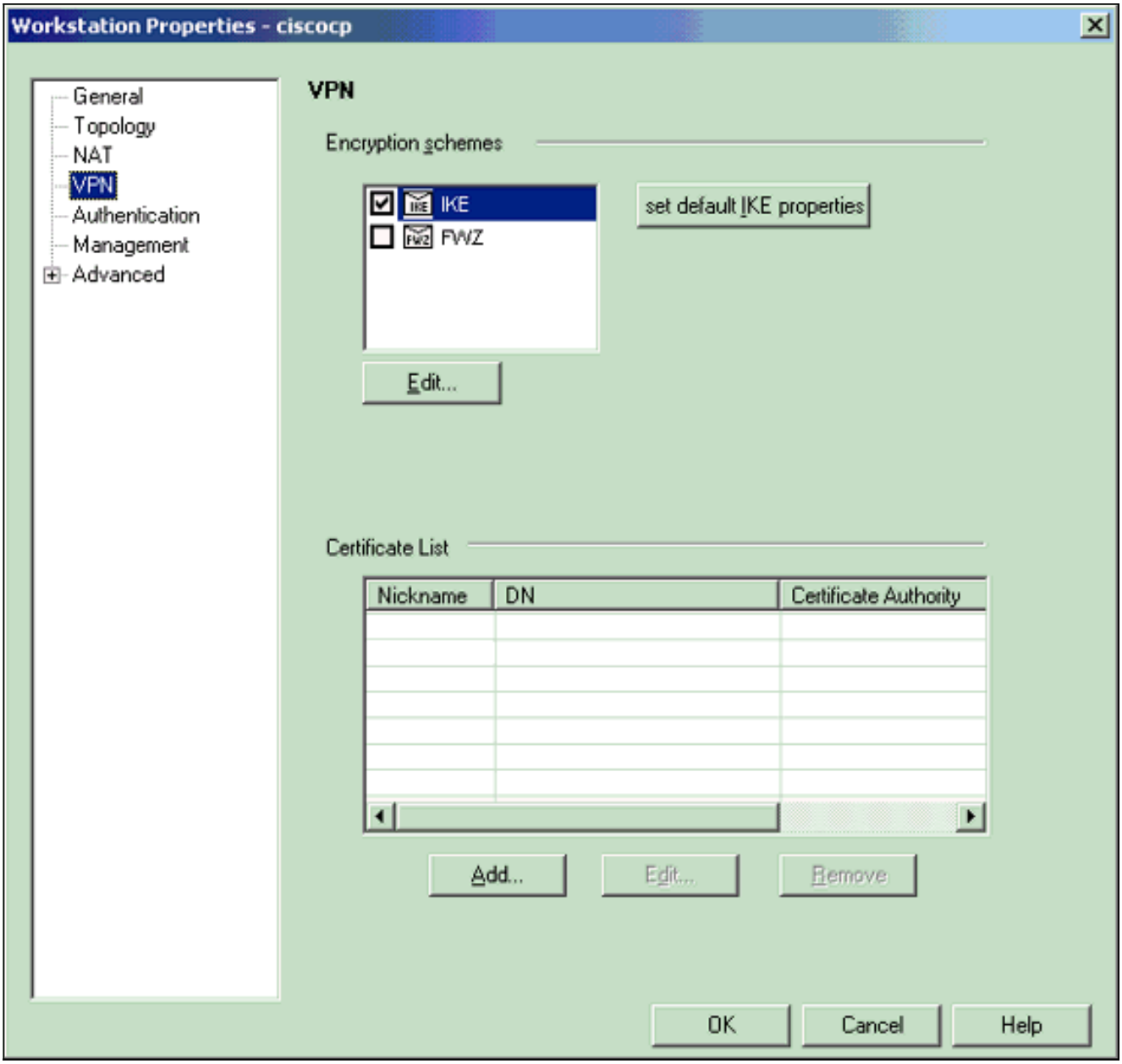
4. ワークステーションを内部として指定するオプションを選択し、適切なIPアドレスを指定します。[OK] をクリックします。この設定では、CP_insideはCheckpointTM NGの内部ネットワークです。ここに示すトポロジ選択では、ワークステーションを内部として指定し、アドレスをCP_insideとして指定します。



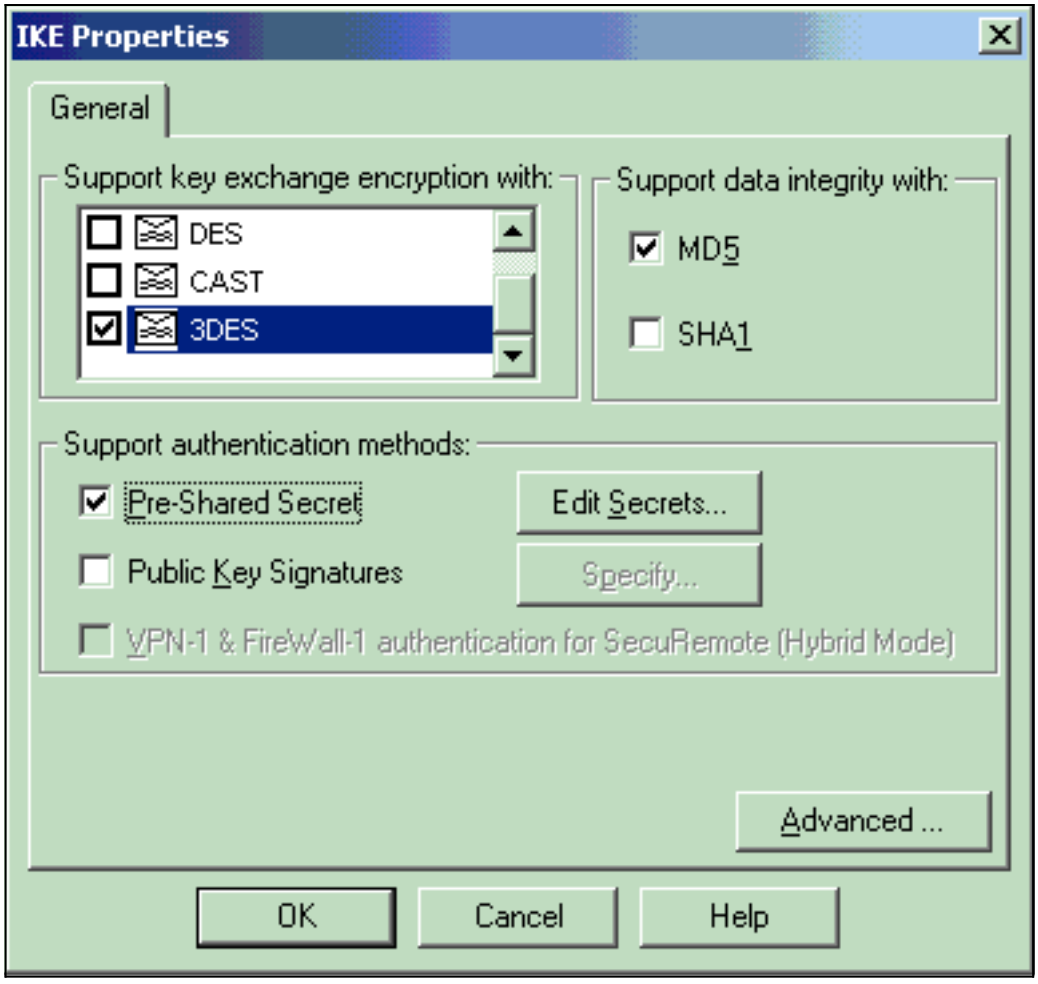
5. [Workstation Properties]ウィンドウで、インターネットに接続するCheckpointTM NGの外部インターフェイスを選択し、[**Edit**]をクリックしてインターフェイスのプロパティを設定します。トポロジを外部として指定するオプションを選択し、[**OK**]をクリックします。



6. CheckpointTM NGのWorkstation Propertiesウィンドウで、ウィンドウの左側にある選択肢から**VPN**を選択し、次に暗号化および認証アルゴリズムのIKEパラメータを選択します。**[Edit]**をクリックしてIKEプロパティを設定します。

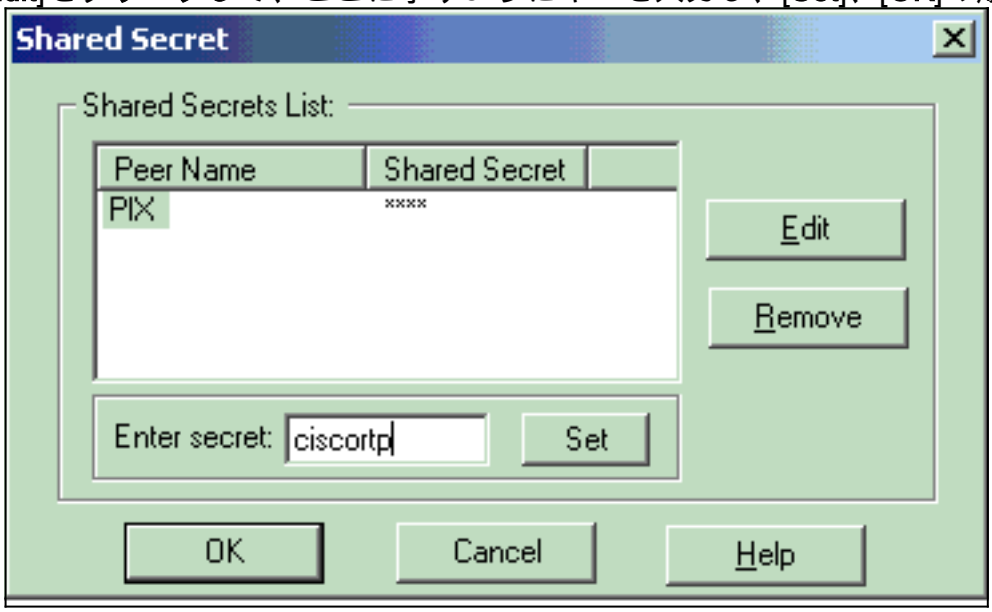


7. IKEプロパティを設定します。3DES暗号化のオプション**を選択し**て、IKEプロパティがisakmp policy # encryption 3desコマンドと互換性**を持つようにします**。IKEプロパティが**crypto isakmp policy # hash md5**コマンドと互換性を持つように、MD5の**オプションを選択**



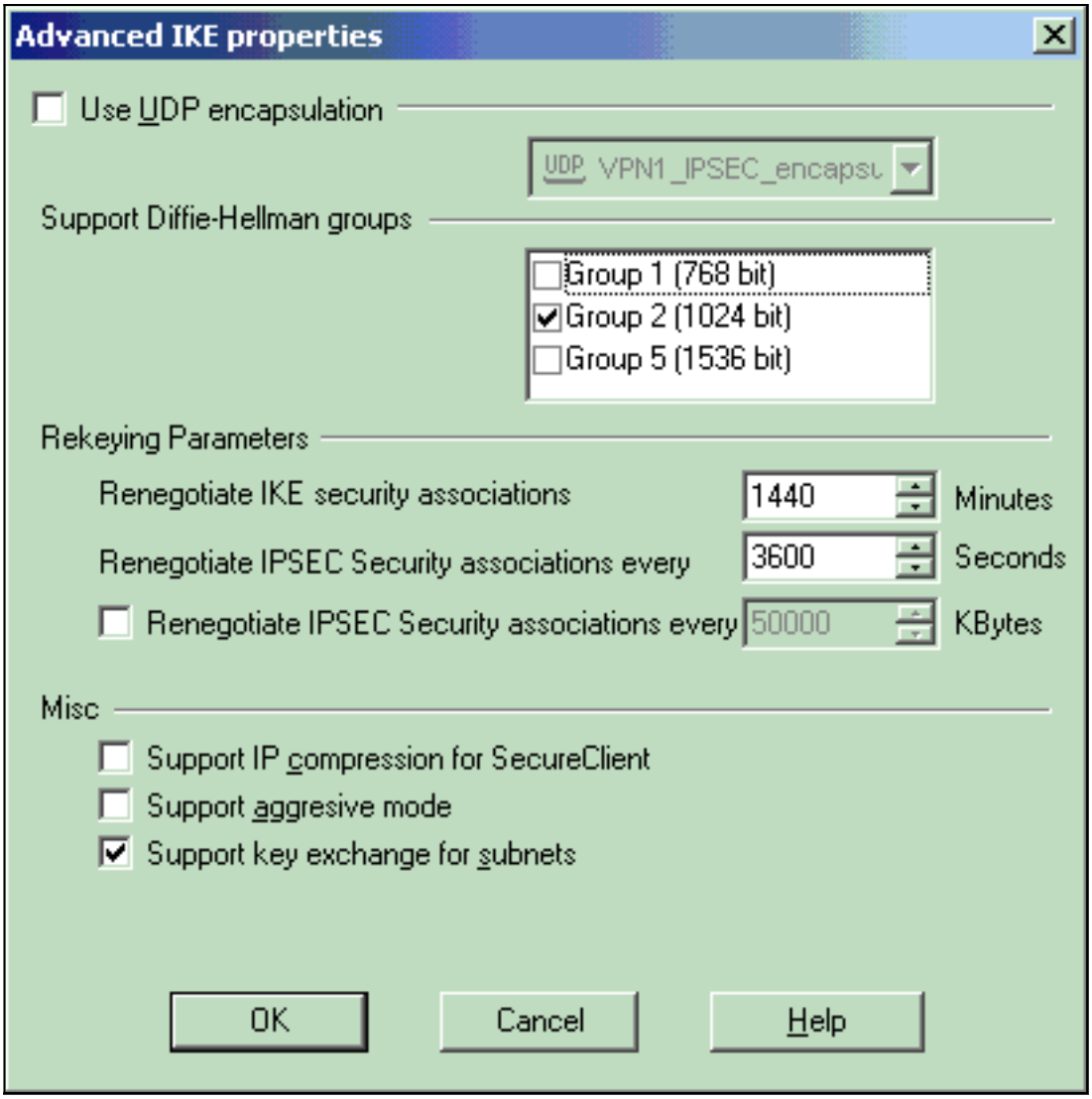
します。

8. Pre-Shared Secretsの認証オプションを選択し、Edit Secretsをクリックして、事前共有キーをPIXコマンド**isakmp key *address address* netmask *netmask*と互換性があるように設定します。**[Edit]をクリックして、ここに示すようにキーを入力し、[Set]、[OK]の順にクリック

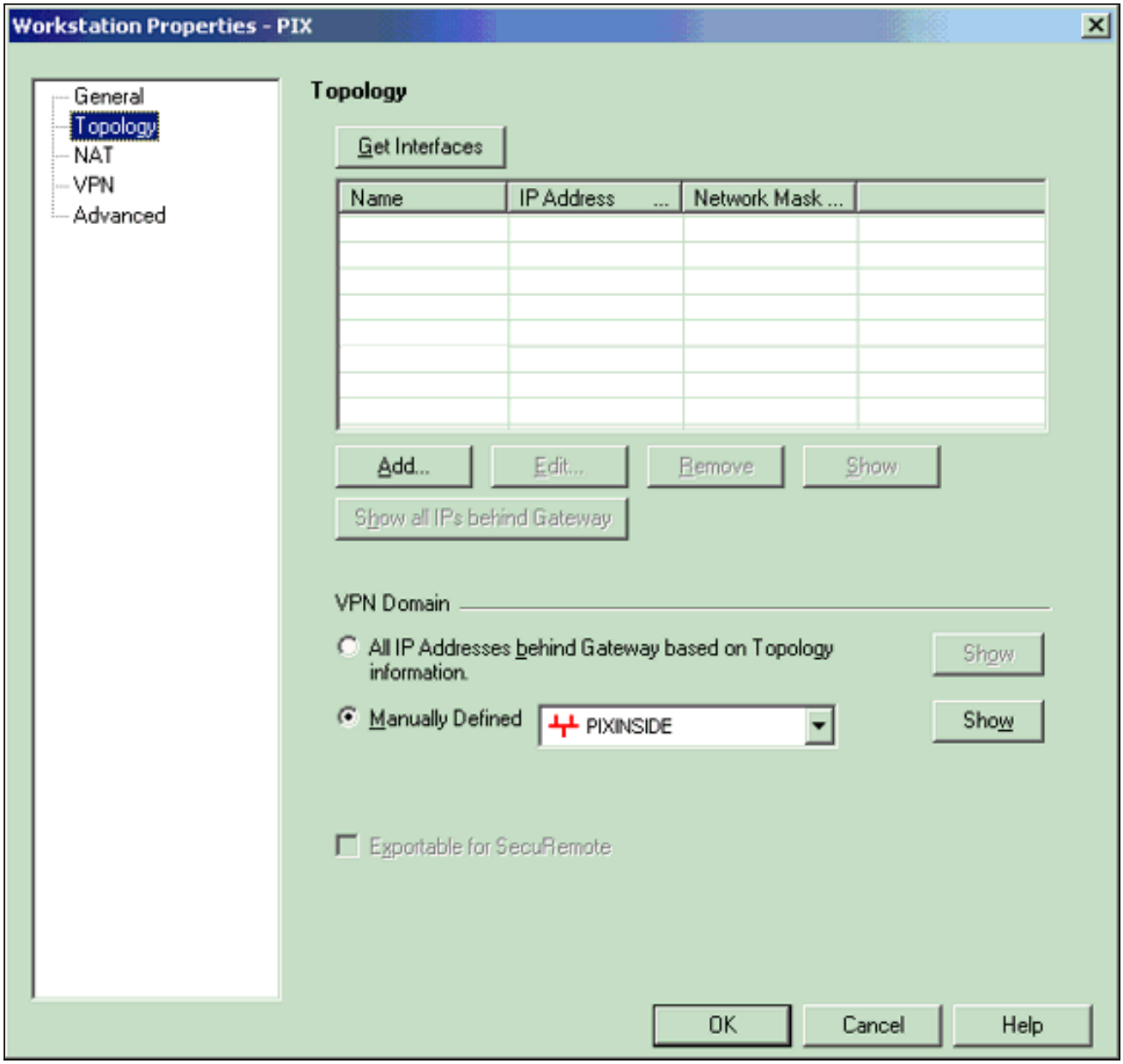


します。

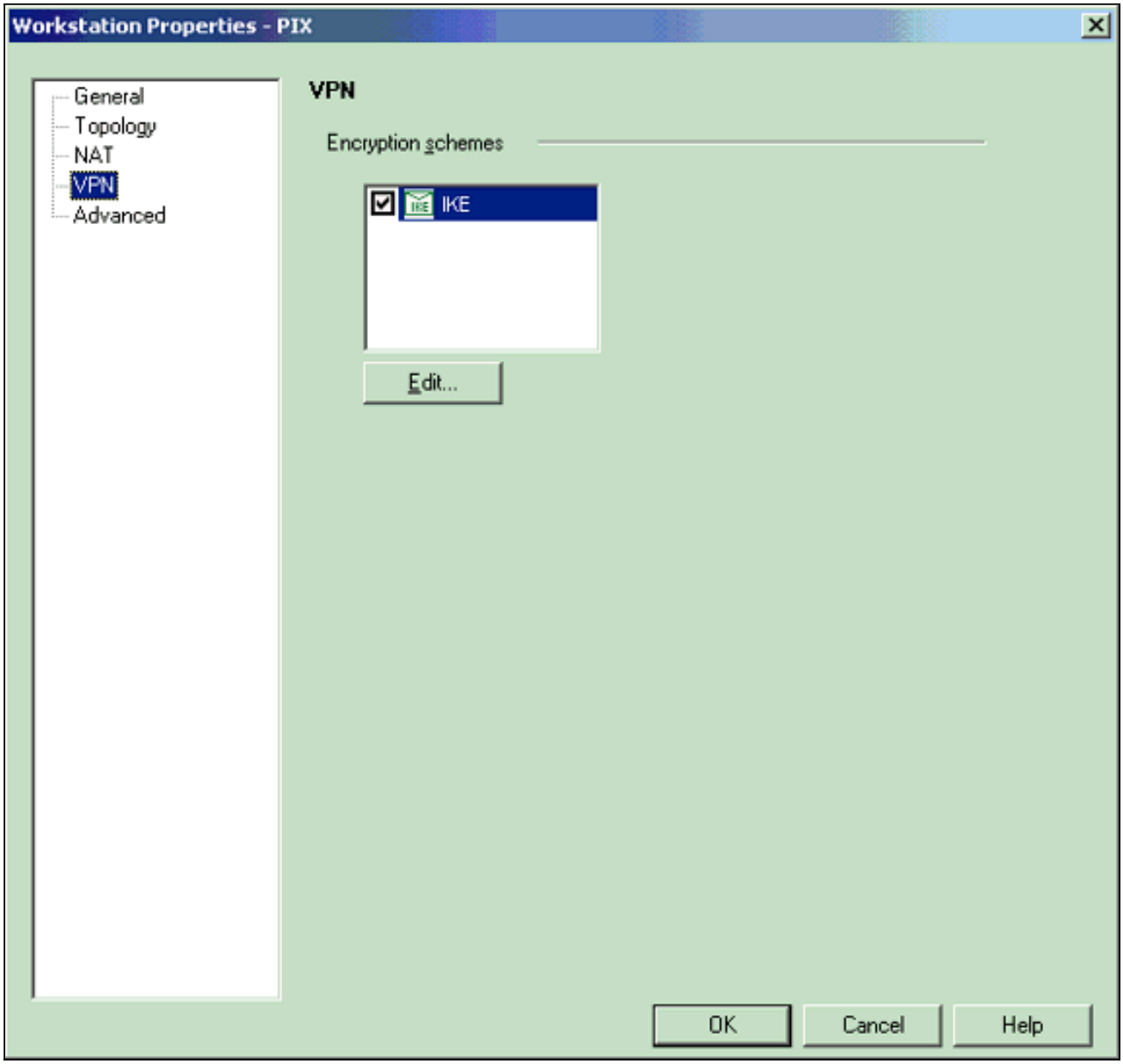
9. IKEプロパティウィンドウで、[Advanced...]をクリックし、次の設定を変更します。「アグレッシブモードをサポート」のオプションを選択解除します。[サブネットのキー交換をサポートする]オプションを選択します。完了したら、[OK] をクリックします。



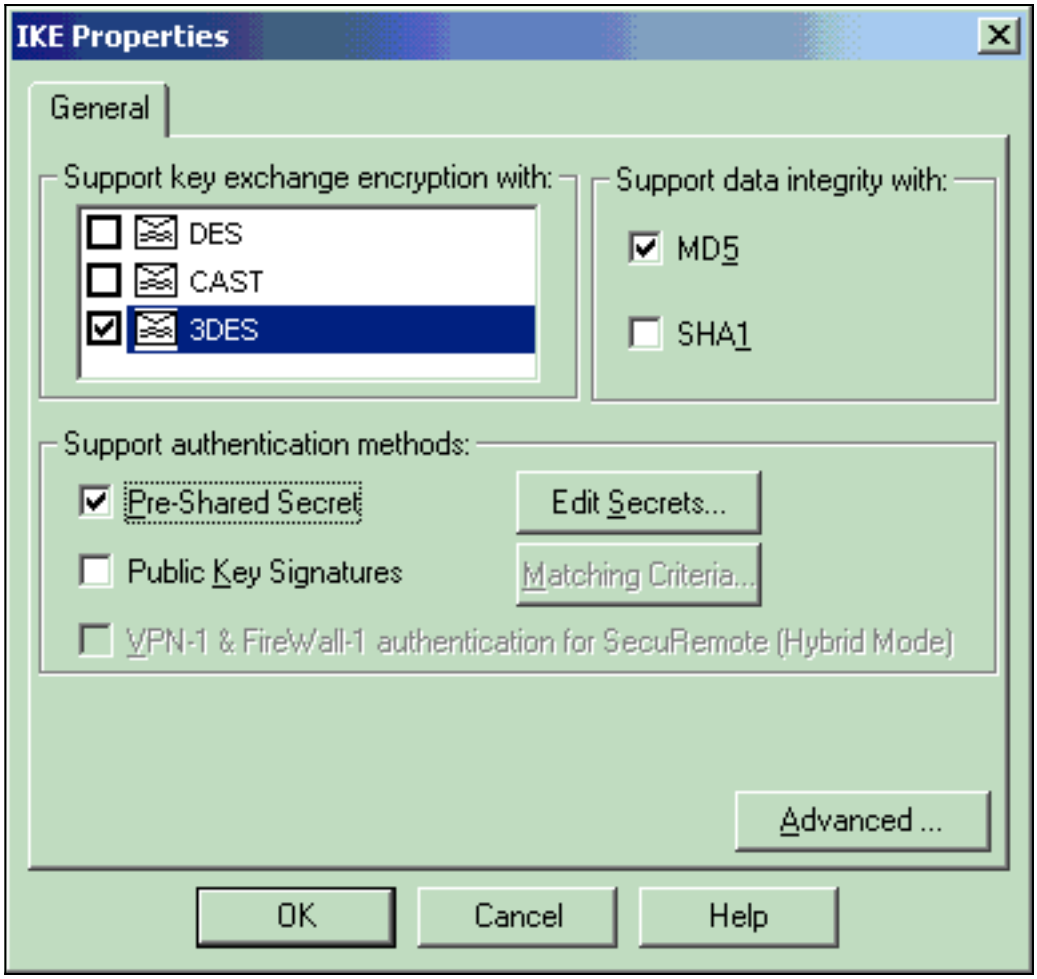
10. [Manage] > [Network objects] > [Edit] を選択して、PIXの[Workstation Properties]ウィンドウを開きます。ウィンドウの左側の選択肢から**[Topology]**を選択し、VPNドメインを手動で定義します。この設定では、PIX内部ネットワーク（PIXの内部ネットワーク）がVPNドメインとして定義されています。



11. ウィンドウの左側**の選択肢**から[VPN]を選択し、暗号化方式として[IKE]を選択します。[**Edit**]をクリックしてIKEプロパティを設定します。

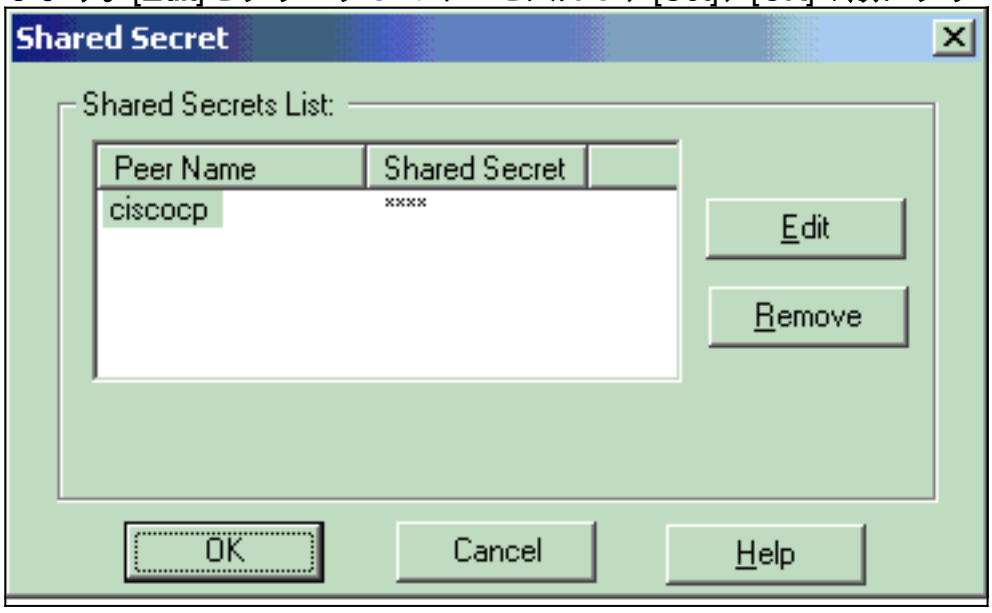


12. 次のようにIKEプロパティを設定します。3DES暗号化のオプション**を選択し**て、IKEプロパティがisakmp policy # encryption 3desコマンドと互換性**を持つようにします**。IKEプロパティが**crypto isakmp policy # hash md5**コマンドと互換性を持つように、MD5のオ**プショ**

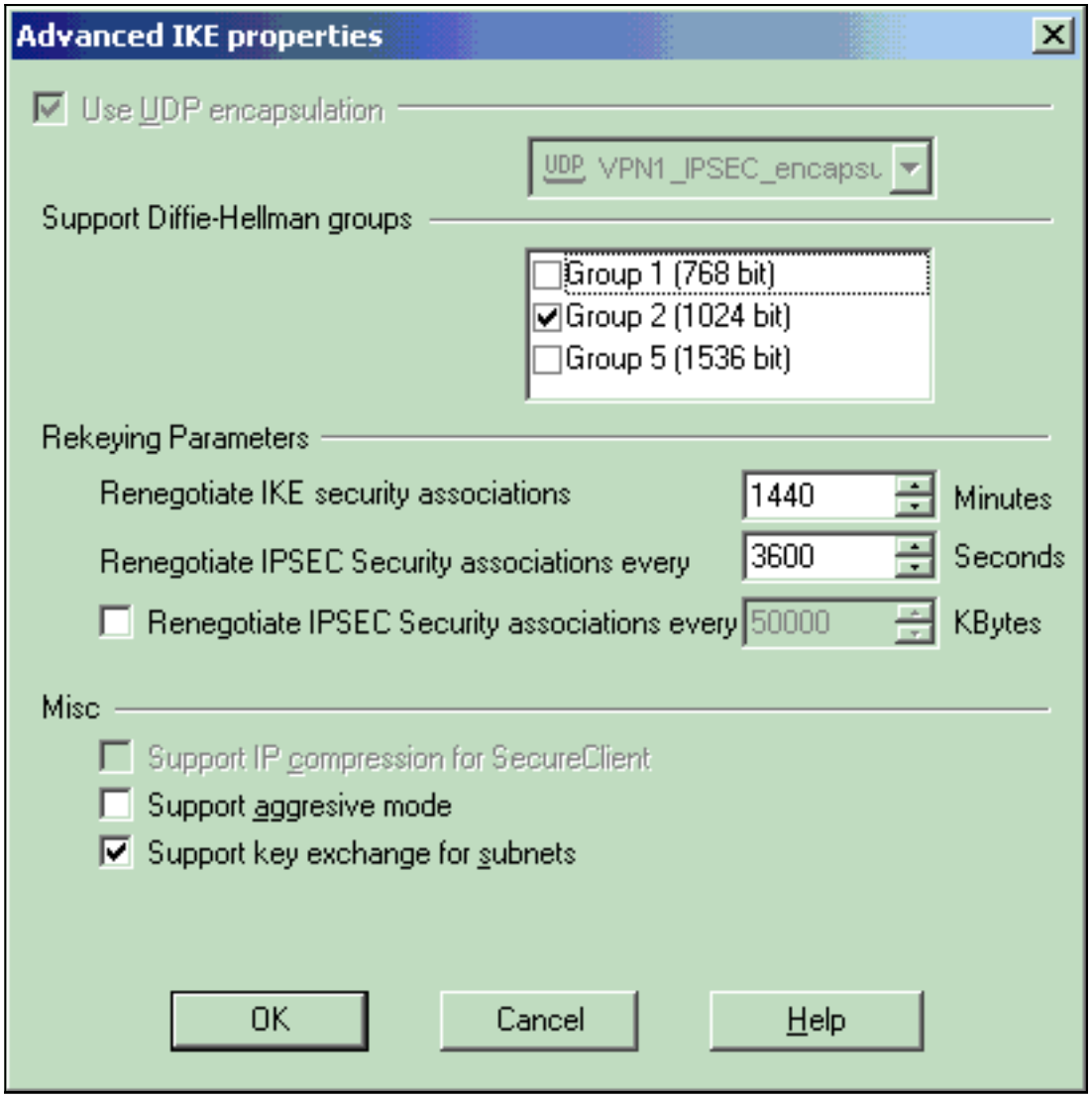


ンを選択します。

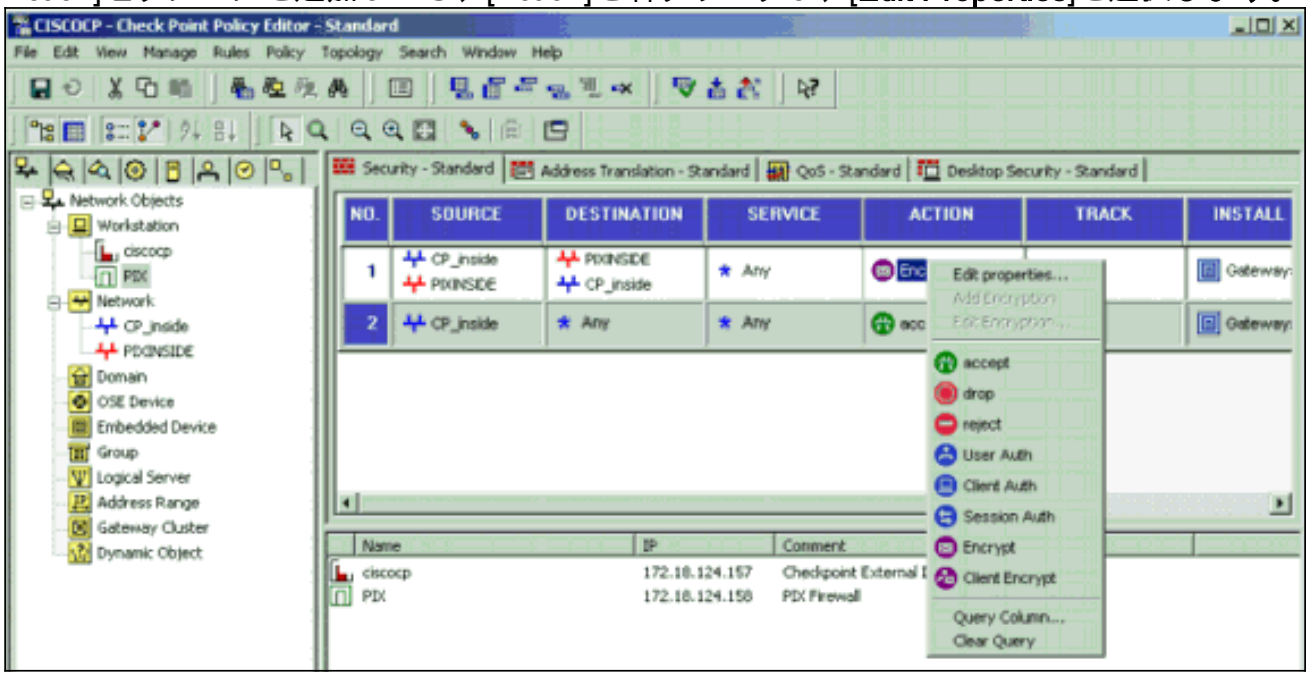
13. Pre-Shared Secretsの認証オプションを選択し、Edit Secretsをクリックして、事前共有キーをPIXコマンド**isakmp key *address address* netmask *netmaskと互換性があるように設定します。*[Edit]をクリックしてキーを入力し、[Set]、[OK]の順にクリックします。**



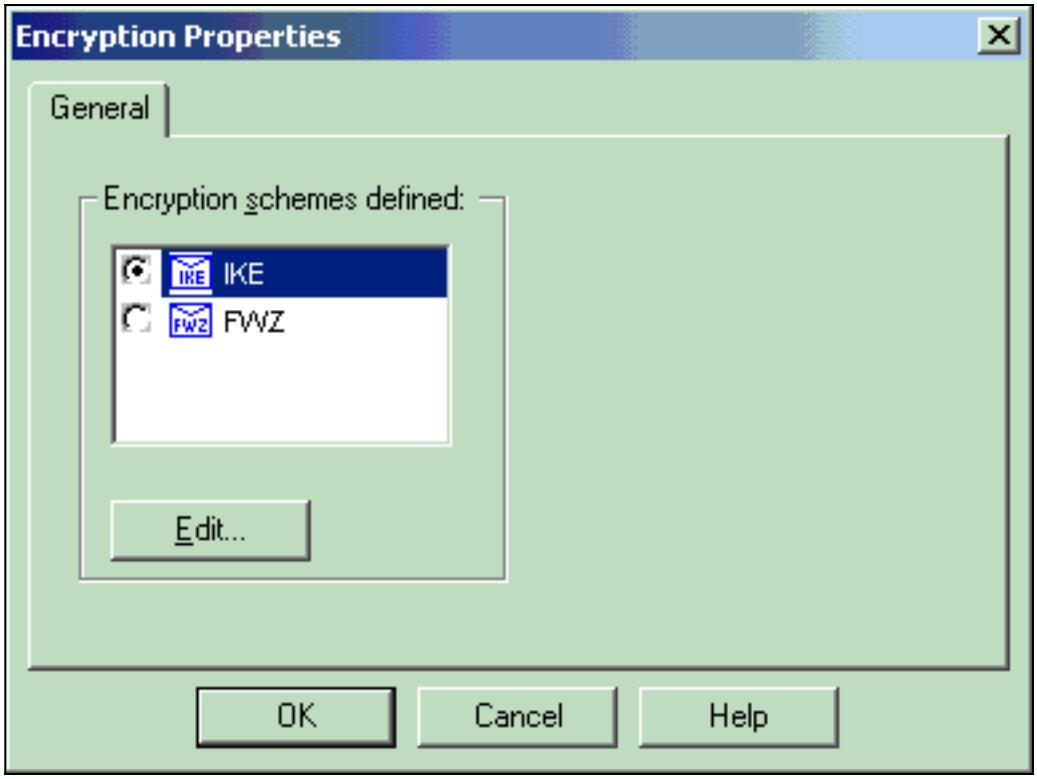
14. IKEプロパティウィンドウで、**[Advanced...]をクリックして**、これらの設定を変更します。IKEプロパティに適したDiffie-Hellmanグループを選択します。「アグレッシブモードをサポート」**のオプションを選択解除します。**[サブネットのキー交換をサポート**する]オプションを選択します。**完了したら、**[OK]、[OK]**の順にクリックします。



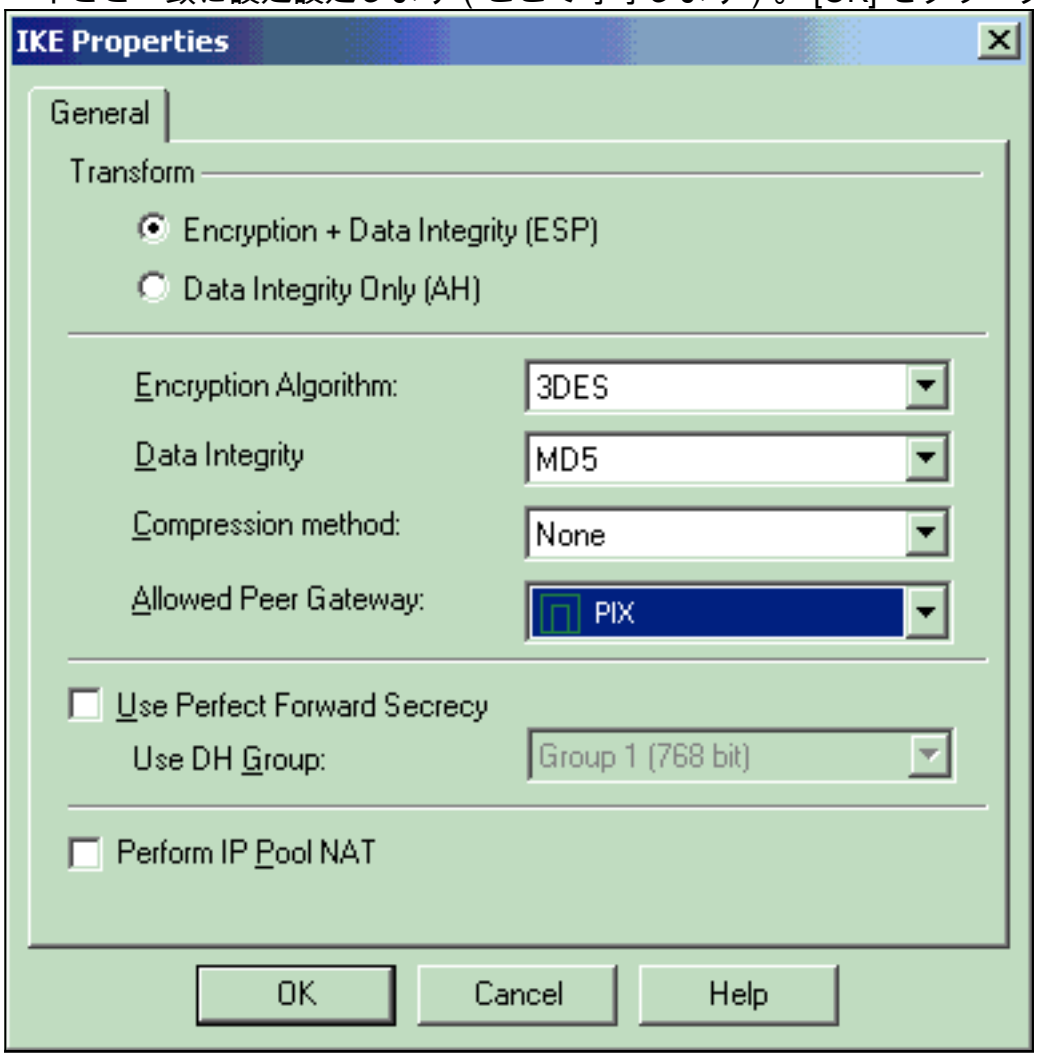
15. [Rules] > [Add Rules] > [Top] を選択して、ポリシーの暗号化ルールを設定します。Policy Editorウィンドウで、送信元と宛先の両方のカラムにCP_inside(Checkpoint ™ NGの内部ネットワーク)とPIXINSIDE（PIXの内部ネットワーク）のソースを持つルールを挿入します。Service = **Any**、**Action = Encrypt**、**Track = Logの値を設定します**。ルールの[Encrypt Action]セクションを追加したら、[Action]を右クリックし、[**Edit Properties**]を選択**します**。



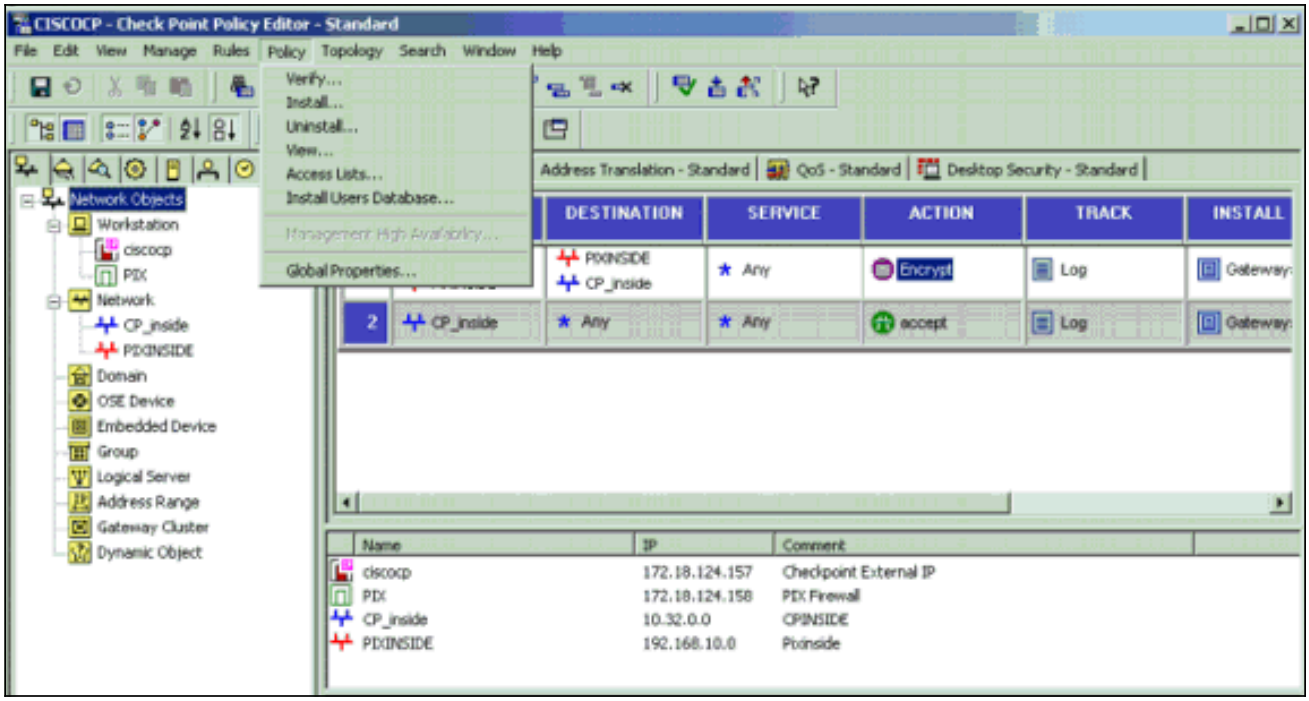
16. [IKE] が選択され、強調表示された状態で、[Edit] をクリックします。



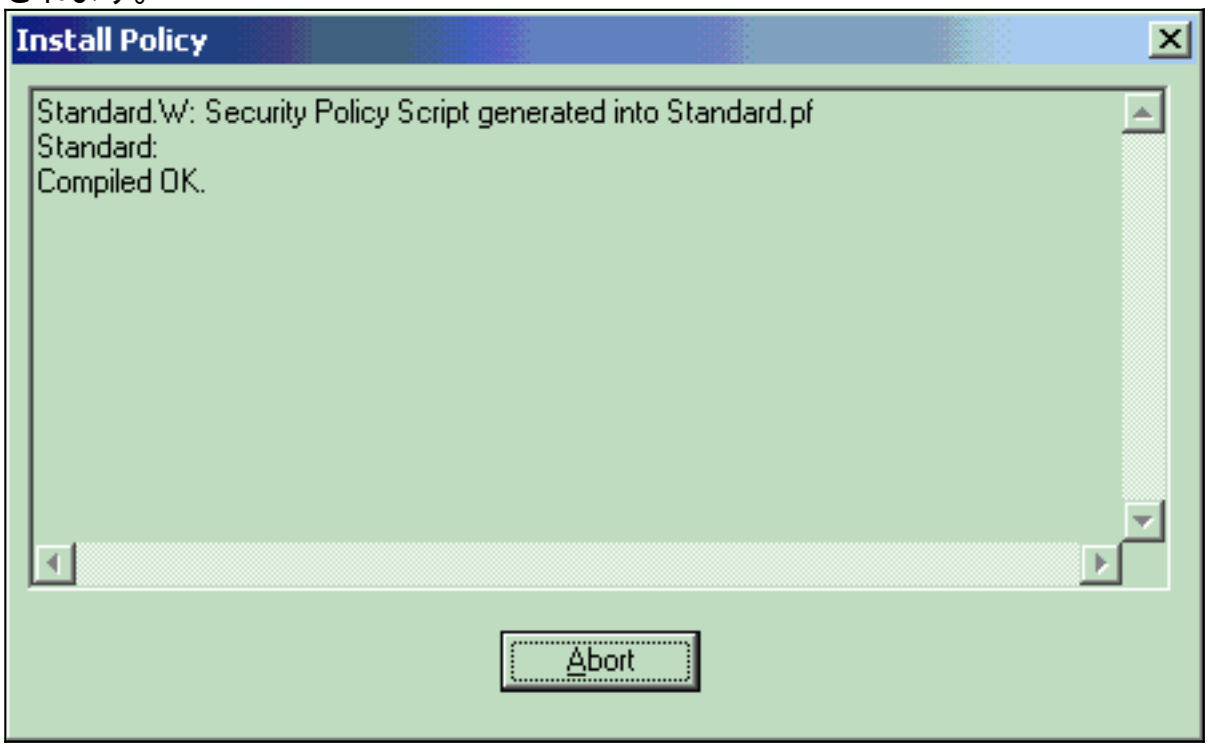
17. [IKE Properties]ウィンドウで、**crypto ipsec transform-set rtptac esp-3des esp-md5-hmacコマンドのPIX IPSecトランスフォームと一致するようにプロパティを変更します。** Transformオプションを**Encryption + Data Integrity(ESP)に設定**し、Encryption Algorithmを**3DES**に設定し、Data Integrityを**MD5**に設定し、Allowed Peer Gatewayを外部PIXゲートウェイととと一致に設定設定します（ここで呼呼します）。 [OK] をクリックします。



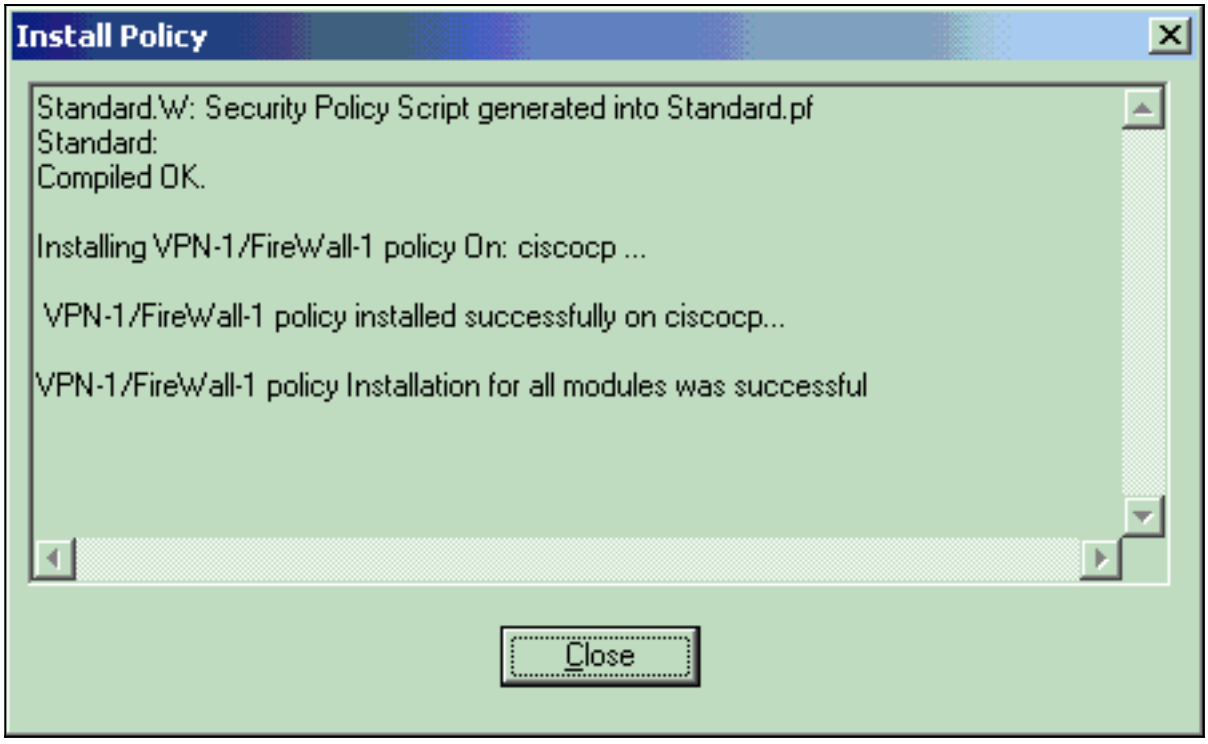
18. CheckpointTM NGを設定した後、ポリシーを保存し、**[Policy] > [Install]を選択して有効にします。**



ポリシーがコンパイルされるときには、インストレーション ウィンドウに進捗状態が表示されます。



インストールウィンドウに、ポリシーのインストールが完了したことが示された場合。**[閉じる]をクリック**して、手順を終了します。



確認

PIX 設定の検証

ここでは、設定が正常に機能しているかどうかを確認します。

アウトプット インタープリタ ツール（登録ユーザ専用）（OIT）は、特定の show コマンドをサポートします。OIT を使用して、show コマンドの出力の分析を表示します。

2つのプライベートネットワーク間の通信をテストするために、プライベートネットワークの1つから他のプライベートネットワークへのpingを開始します。この設定では、pingがPIX側(192.168.10.2)から CheckpointTM NG内部ネットワーク(10.32.50.51)に送信されました。

- **show crypto isakmp sa：現在ピアにあるすべての IKE SA を表示します。**

```
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
```

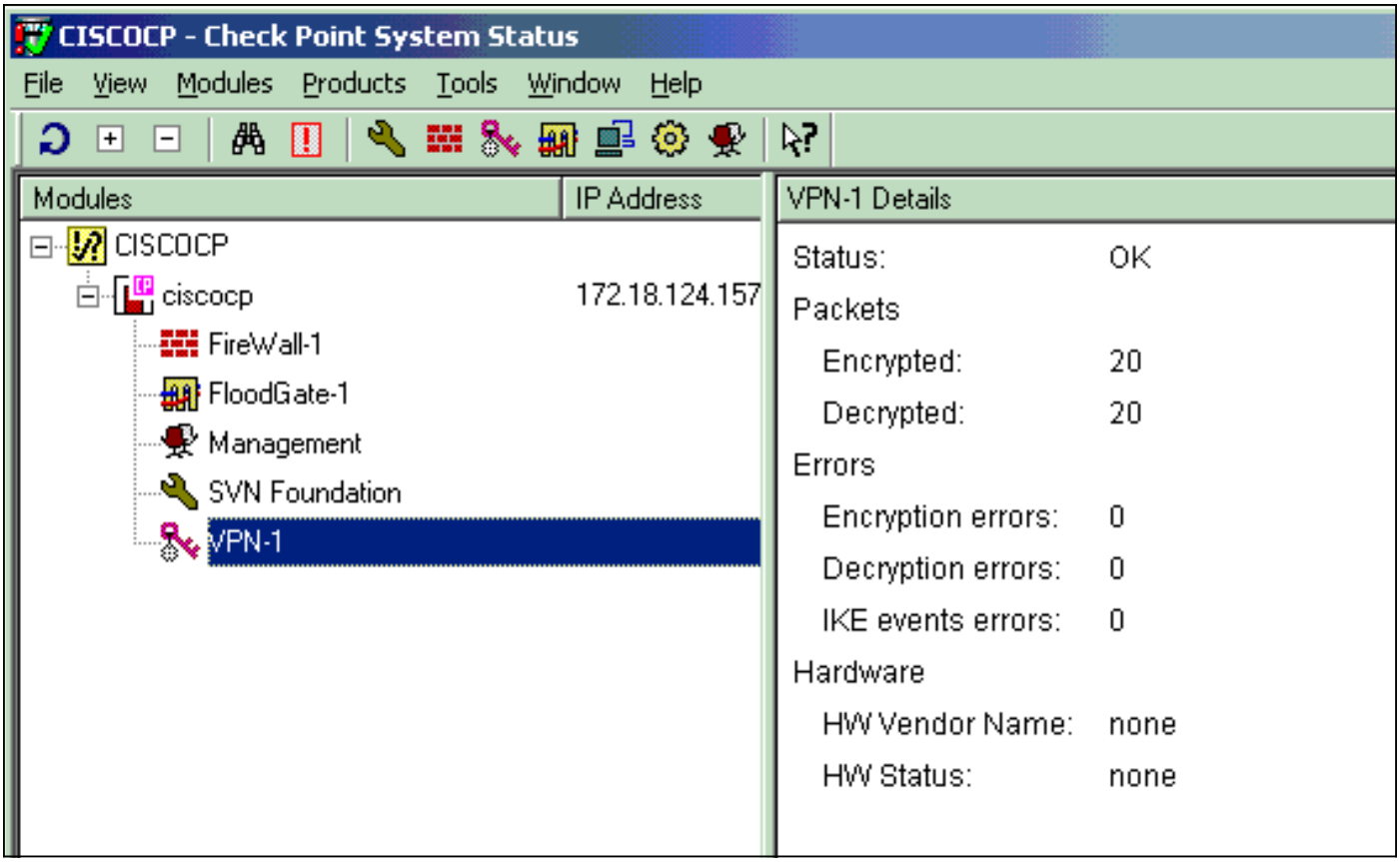
- **show crypto ipsec sa**：現在の SA で使用されている設定を表示します。

```
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:
```

チェックポイントNGのトンネルステータスの表示

Policy Editorに移動し、Window > System Statusの順に選択してトンネルのステータスを表示します。



トラブルシュート

PIX設定のトラブルシューティング

アウトプット インタープリタ ツール（登録ユーザ専用）（OIT）は、特定の show コマンドをサポートします。OIT を使用して、show コマンドの出力の分析を表示します。

注：debug コマンドを使用する前に、**『debug コマンドの重要な情報』**を参照してください。

次のコマンドを使用して、PIX Firewallのデバッグを有効にします。

- **debug crypto engine：暗号化と復号化を行う暗号化エンジンに関するデバッグ メッセージを表示します。**
- **debug crypto isakmp**：IKE イベントに関するメッセージを表示します。

```
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
```

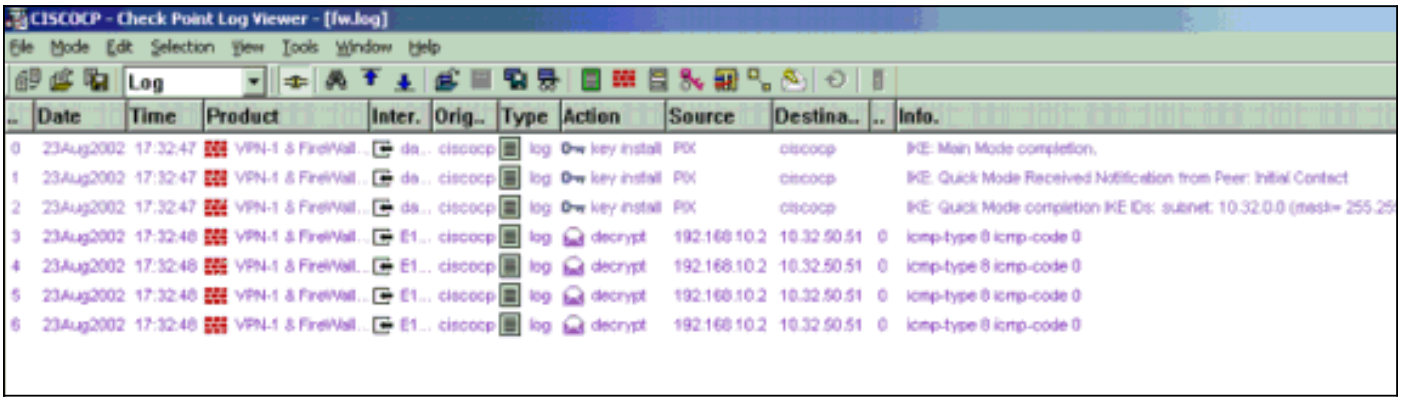
```
lifetime of 4608000 kilobytesIPSEC(key_engine): got a queue event...
IPSEC(initialize_sas): ,
(key eng. msg.) dest= 172.18.124.158, src= 172.18.124.157,
dest_proxy= 192.168.10.0/255.255.255.0/0/0 (type=4),
src_proxy= 10.32.0.0/255.255.128.0/0/0 (type=4),
protocol= ESP, transform= esp-3des esp-md5-hmac ,
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
```

ネットワーク集約

暗号化ドメイン内の Checkpoint で複数の隣接する内部ネットワークが設定されている場合、このデバイスによってそれらのネットワークが特定のトラフィックに関して自動的に集約されることがあります。PIXの暗号アクセスコントロールリスト(ACL)が一致するように設定されていない場合、トンネルは失敗する可能性があります。たとえば、10.0.0.0 /24と10.0.1.0 /24の内部ネットワークがトンネルに含まれるように設定されている場合、それらを10.0.0.0 /23に集約できます。

チェックポイントNGログの表示

[Window] > [Log Viewer]を選択して、ログを表示します。



関連情報

- Cisco PIX Firewall ソフトウェア
- Cisco Secure PIX ファイアウォール コマンド リファレンス
- セキュリティ製品に関する Field Notice (PIX を含む)
- Requests for Comments (RFCs)
- テクニカル サポートとドキュメント – Cisco Systems