Configurazione di un tunnel IPSec tra un firewall Cisco Secure PIX e un firewall Checkpoint NG

Sommario

Introduzione

In questo documento viene illustrato come configurare un tunnel IPsec con chiavi già condivise per la comunicazione tra due reti private. Nell'esempio, le reti in comunicazione sono la rete privata 192.168.10.x all'interno di Cisco Secure PIX Firewall e la rete privata 10.32.x.x all'interno di CheckpointTM Next Generation (NG) Firewall.

Prerequisiti

Requisiti

Prima di provare questa configurazione, accertarsi di soddisfare i seguenti requisiti:

- Il traffico tra il PIX e l'interno del checkpointTM NG e verso Internet (rappresentato qui dalle reti 172.18.124.x) deve scorrere prima di avviare questa configurazione.
- Gli utenti devono avere familiarità con la negoziazione IPSec. Questo processo può essere suddiviso in cinque fasi, incluse due fasi IKE (Internet Key Exchange).Un tunnel IPsec viene avviato da traffico interessante. Il traffico è considerato interessante quando avviene tra peer IPsec.Nella fase 1 di IKE, i peer IPsec negoziano il criterio di associazione di sicurezza (SA)

IKE stabilito. Dopo l'autenticazione dei peer, viene creato un tunnel protetto utilizzando Internet Security Association and Key Management Protocol (ISAKMP).In IKE fase 2, i peer IPsec utilizzano il tunnel autenticato e sicuro per negoziare le trasformazioni di associazione di sicurezza IPsec. La negoziazione del criterio condiviso determina la modalità di definizione del tunnel IPSec.Il tunnel IPSec viene creato e i dati vengono trasferiti tra i peer IPSec in base ai parametri IPSec configurati nei set di trasformazioni IPSec.Il tunnel IPsec termina quando le associazioni di protezione IPsec vengono eliminate o quando scade la loro durata.

Componenti usati

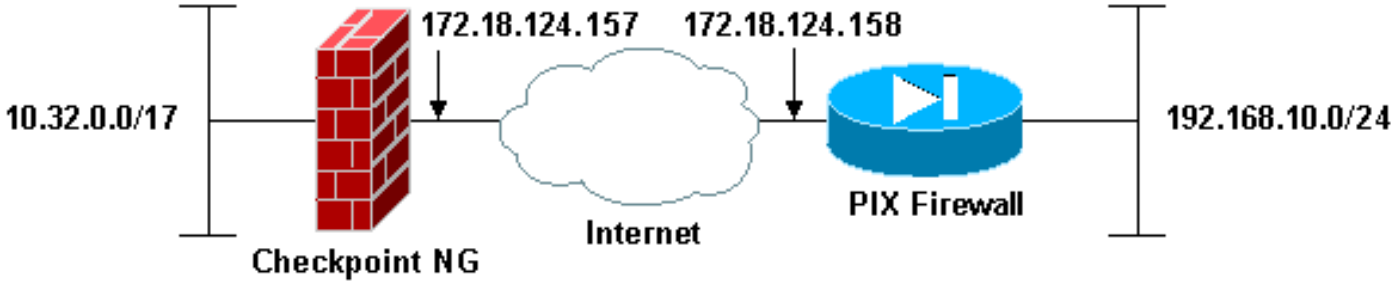
Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Software PIX versione 6.2.1
- CheckpointTM NG Firewall

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Esempio di rete

Nel documento viene usata questa impostazione di rete:



Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Configurazione del PIX

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

Configurazione PIX

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

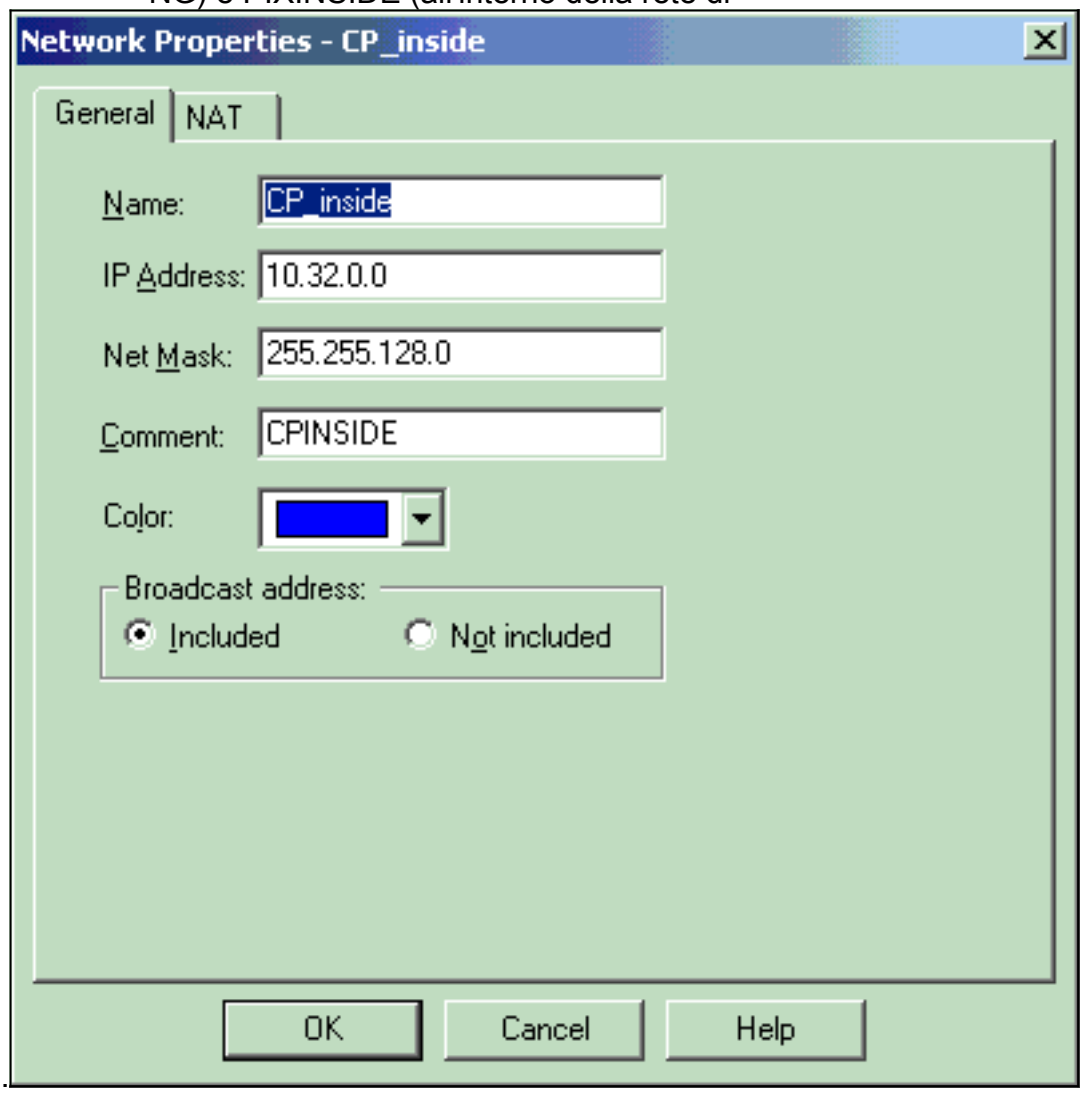
```
hostname PIXRTPVPN
domain-name cisco.com
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol ils 389
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
fixup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

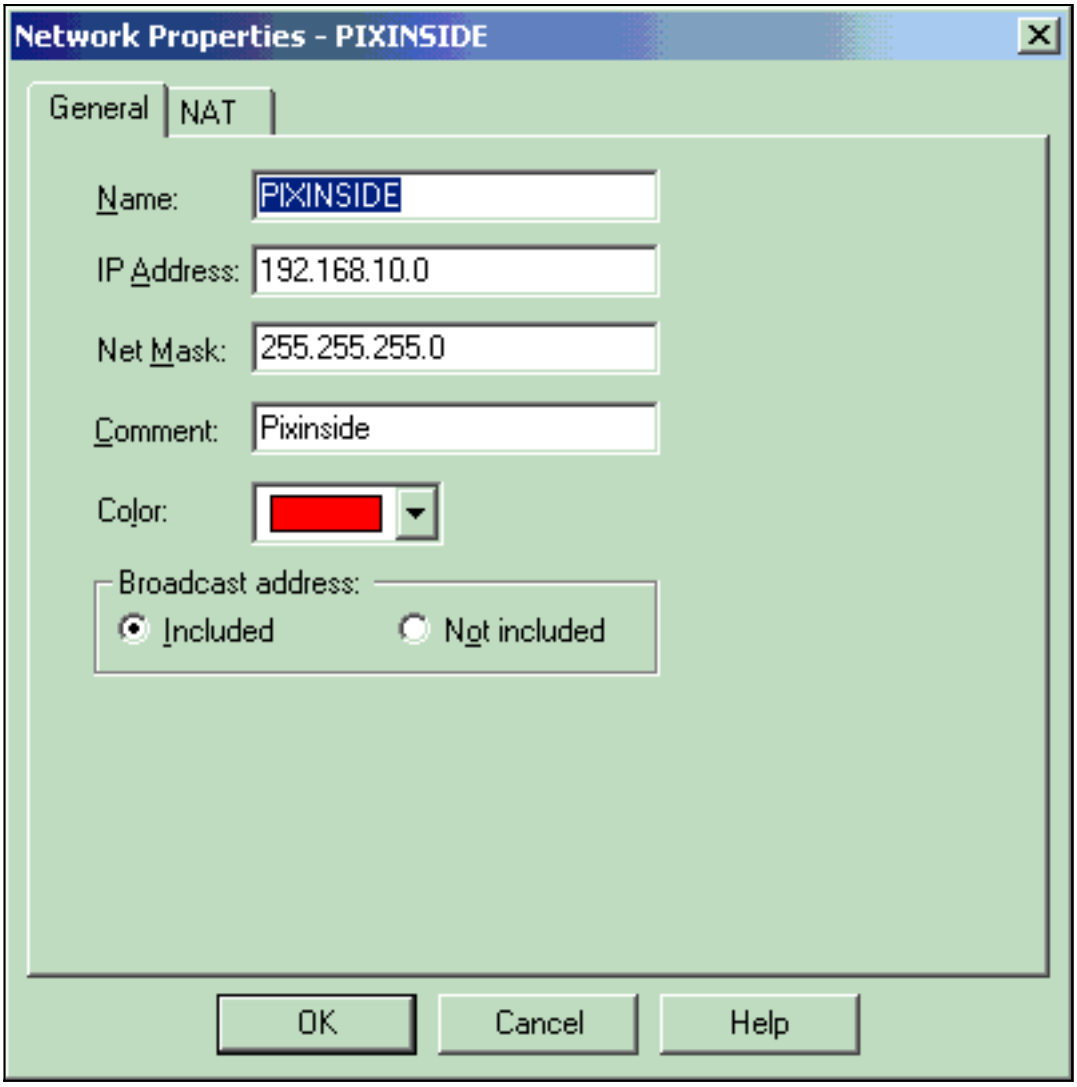
```
authentication. isakmp key ******** address
172.18.124.157 netmask 255.255.255.255
!--- Defines ISAKMP policy. isakmp policy 1
authentication pre-share
isakmp policy 1 encryption 3des
isakmp policy 1 hash md5
isakmp policy 1 group 2
isakmp policy 1 lifetime 86400
telnet timeout 5
ssh timeout 5
terminal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

Configurazione del checkpoint NG

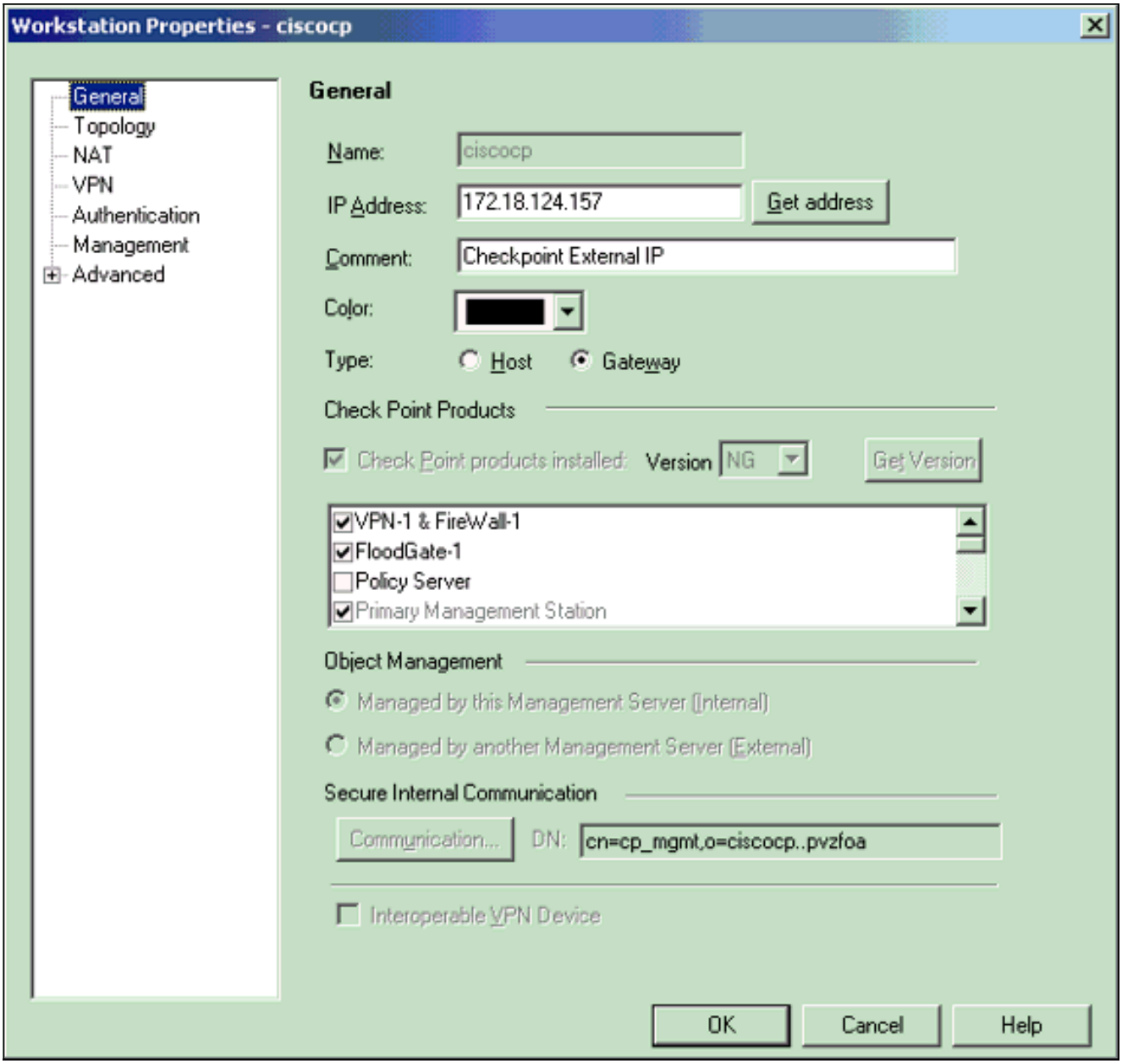
Gli oggetti e le regole di rete vengono definiti nel CheckpointTM NG per definire i criteri relativi alla configurazione VPN da configurare. Questo criterio viene quindi installato utilizzando CheckpointTM NG Policy Editor per completare il lato CheckpointTM NG della configurazione.

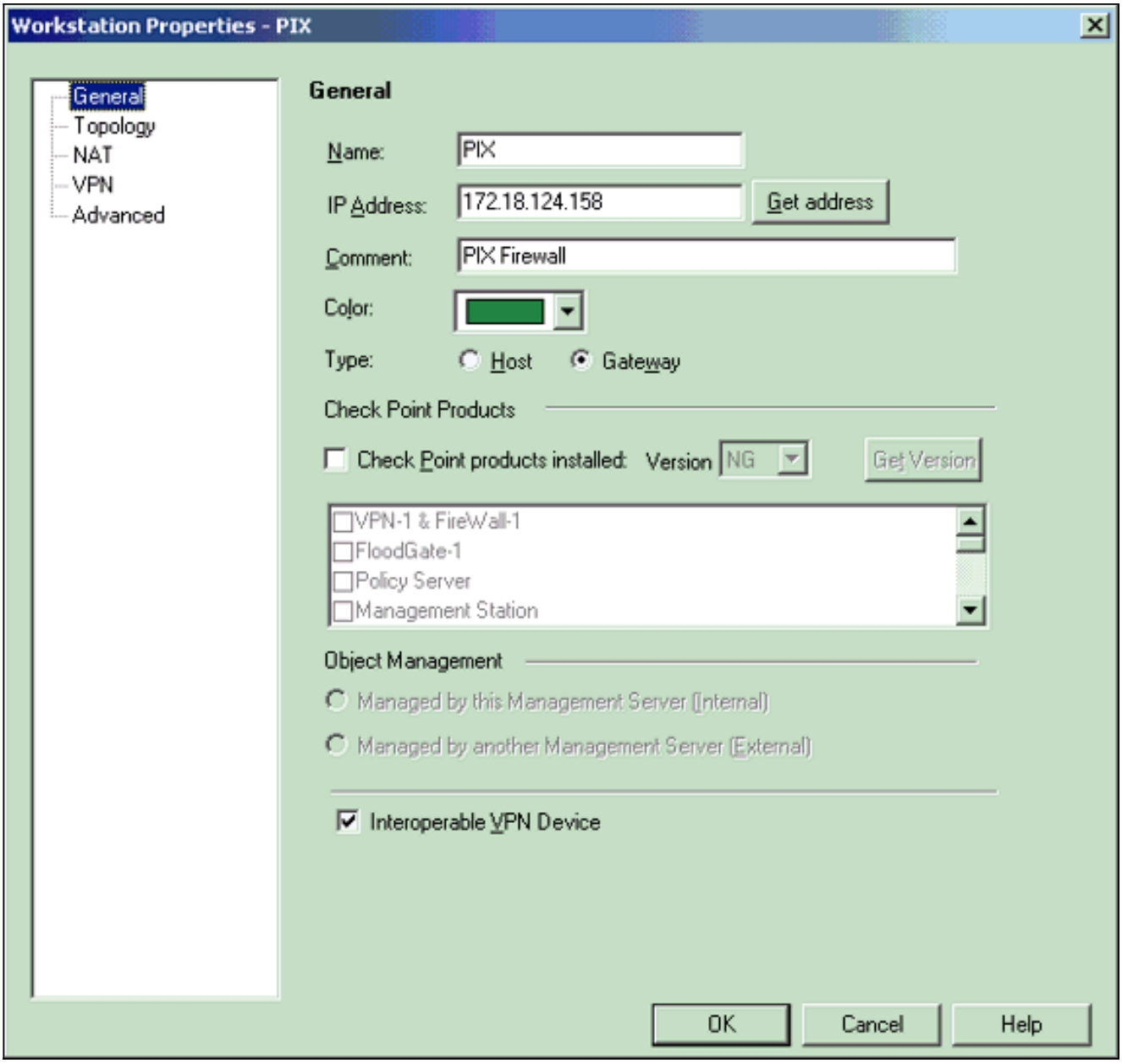
1. Creare i due oggetti di rete per la rete del checkpoint e la rete del firewall PIX che crittografano il traffico interessante.A tale scopo, selezionare **Gestisci > Oggetti di rete**, quindi selezionare **Nuovo > Rete**. Immettere le informazioni di rete appropriate, quindi fare clic su **OK**.Questi esempi mostrano un set di oggetti di rete chiamati CP_Inside (all'interno della rete di CheckpointTM NG) e PIXINSIDE (all'interno della rete di PIX).



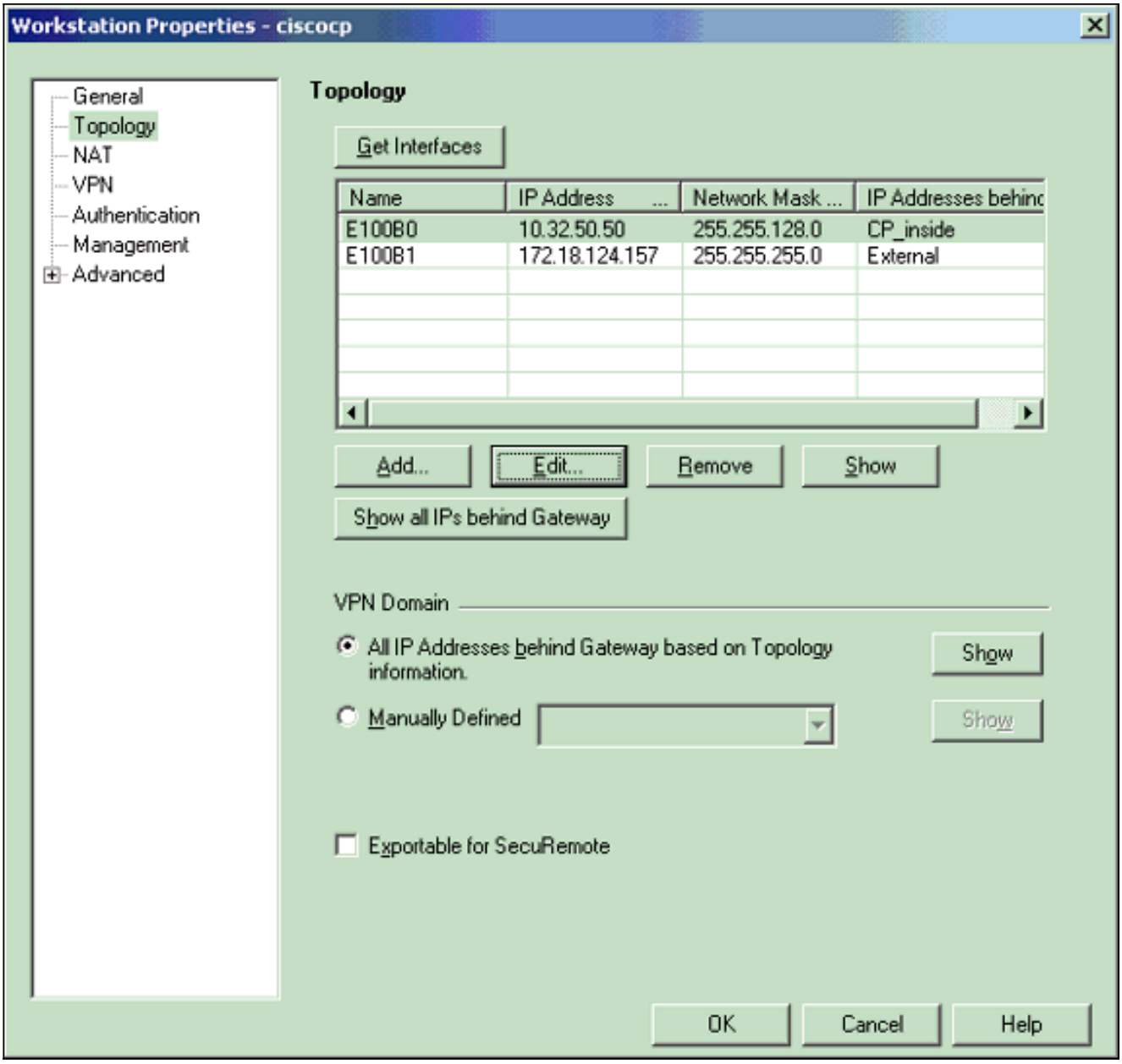


2. Create gli oggetti della stazione di lavoro per CheckpointTM NG e PIX. A tale scopo, selezionare **Gestisci > Oggetti di rete > Nuovo > Workstation**.Èpossibile utilizzare l'oggetto stazione di lavoro CheckpointTM NG creato durante l'impostazione iniziale di CheckpointTM NG. Selezionare le opzioni per impostare la workstation come Gateway e Dispositivo VPN interoperabile e quindi fare clic su **OK**.Questi esempi mostrano una serie di oggetti chiamati ciscocp (**CheckpointTM** NG) e PIX (PIX Firewall).

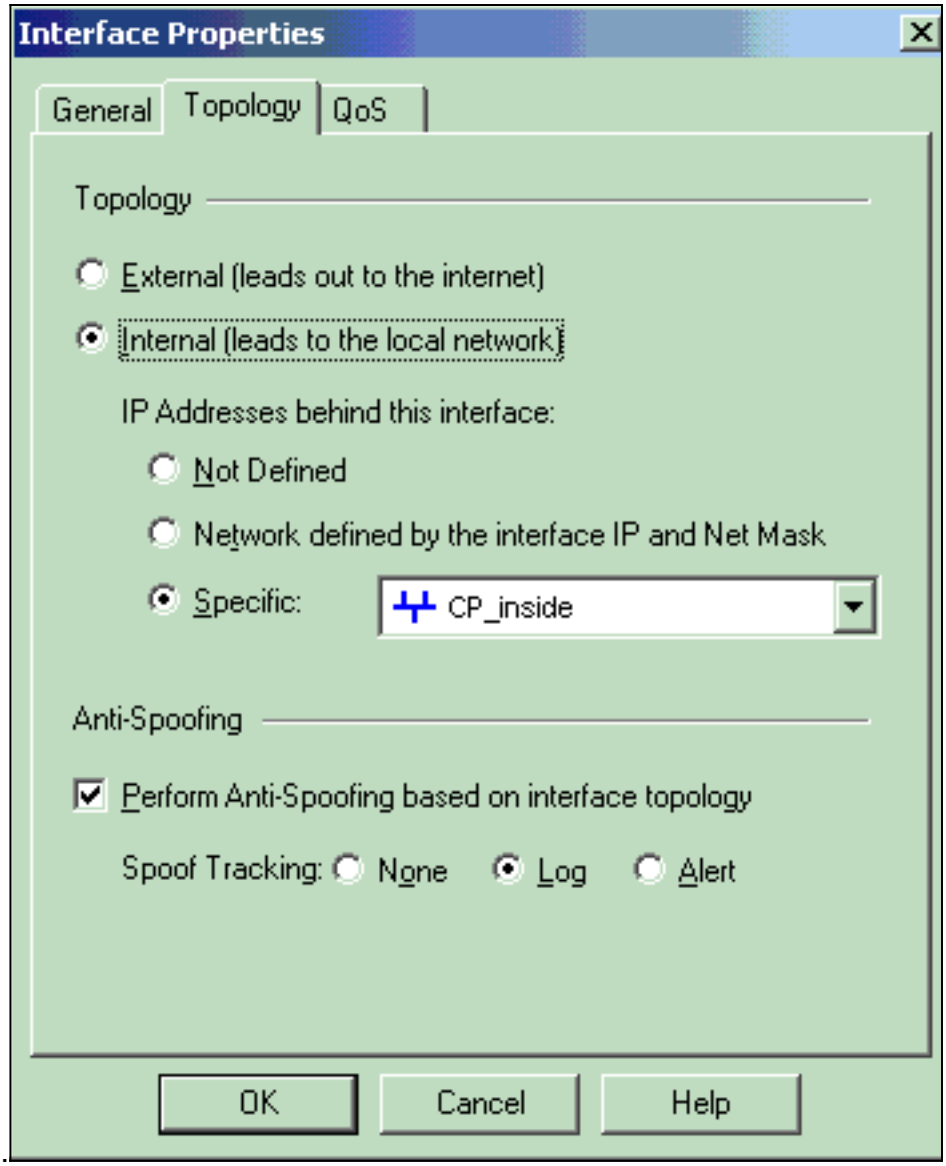

Workstation Properties - ciscocp
General
Topology
NAT
VPN
Authentication
Management
Advanced
General
Name:
ciscocp
IP Address:
172.18.124.157
Get address
Comment:
Checkpoint External IP
Color:
Type:
Host
Gateway
Check Point Products
Check Point products installed:
Version
NG
Get Version
VPN-1 & FireWall-1
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. Selezionare **Gestisci > Oggetti di rete > Modifica** per aprire la finestra Proprietà stazione di lavoro per la stazione di lavoro CheckpointTM NG (ciscocp in questo esempio).Selezionare **Topologia** dalle opzioni sul lato sinistro della finestra, quindi selezionare la rete da crittografare. Fare clic su **Modifica** per impostare le proprietà dell'interfaccia.

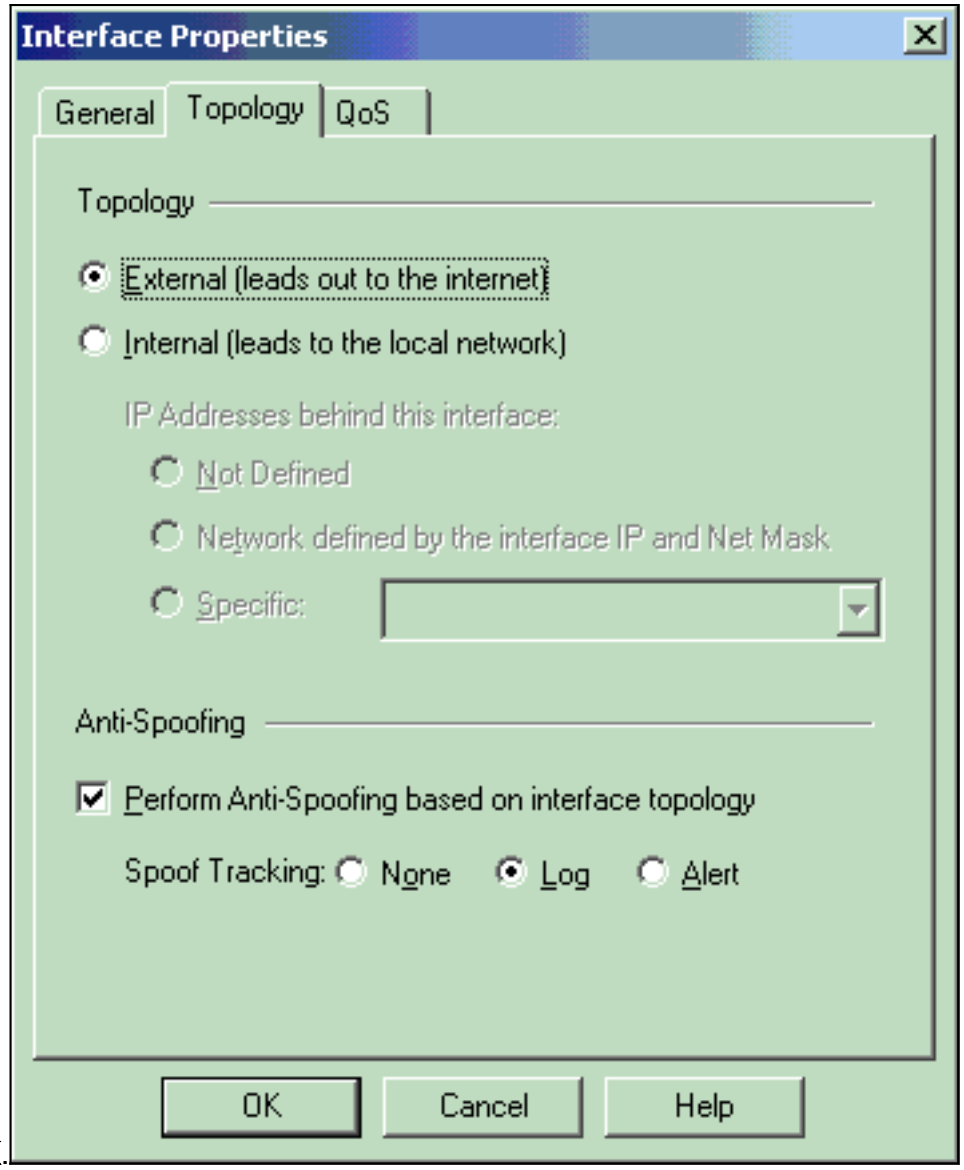


4. Selezionare l'opzione per designare la workstation come interna, quindi specificare l'indirizzo IP appropriato. Fare clic su **OK**.In questa configurazione, CP_inside è la rete interna del checkpointTM NG. Le selezioni di topologia mostrate di seguito designano la workstation come interna e specificano l'indirizzo



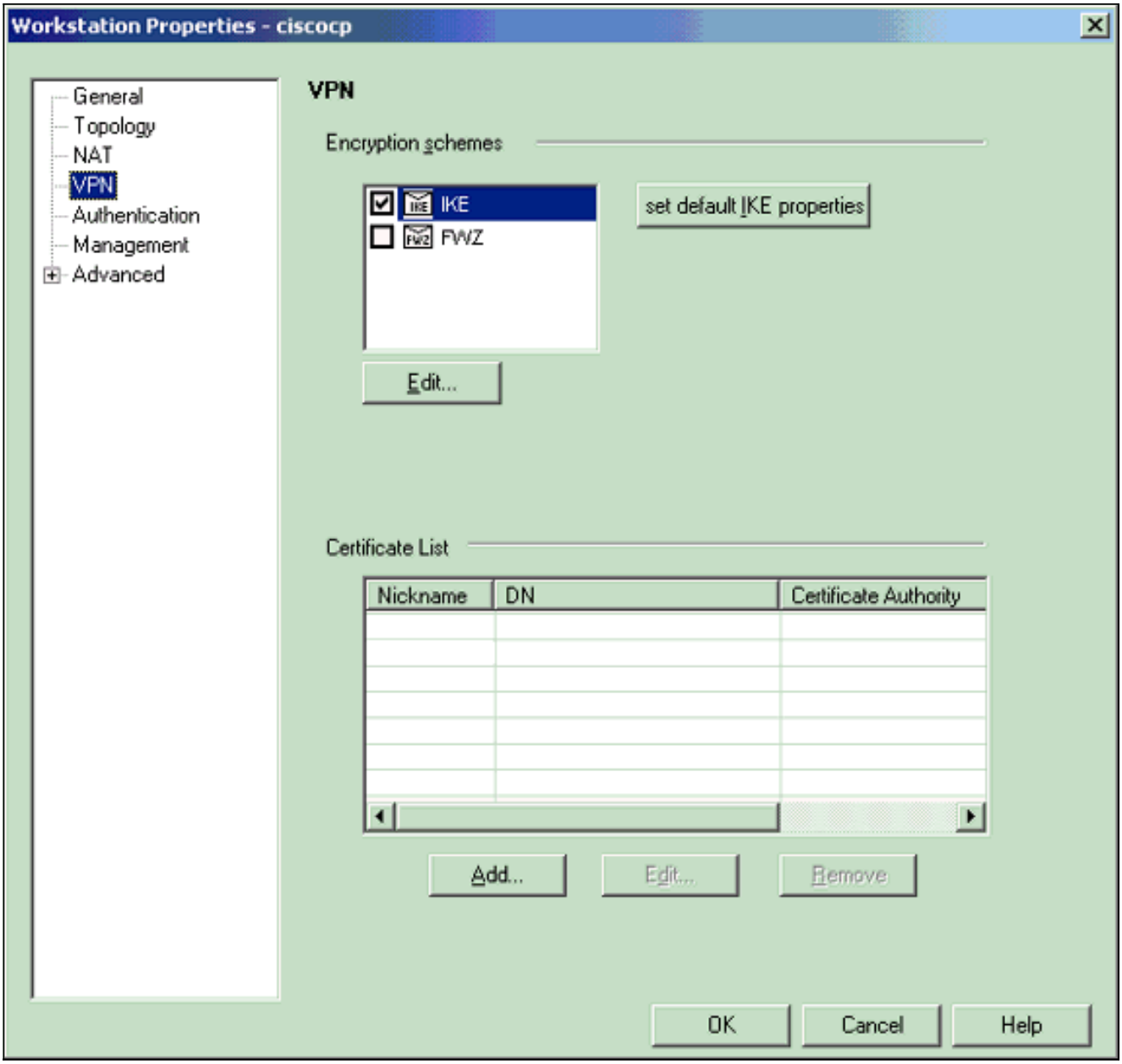
CP_inside.

5. Nella finestra Proprietà workstation, selezionare l'interfaccia esterna sul CheckpointTM NG che conduce a Internet, quindi fare clic su **Modifica** per impostare le proprietà dell'interfaccia. Selezionare l'opzione per designare la topologia come esterna, quindi fare clic su

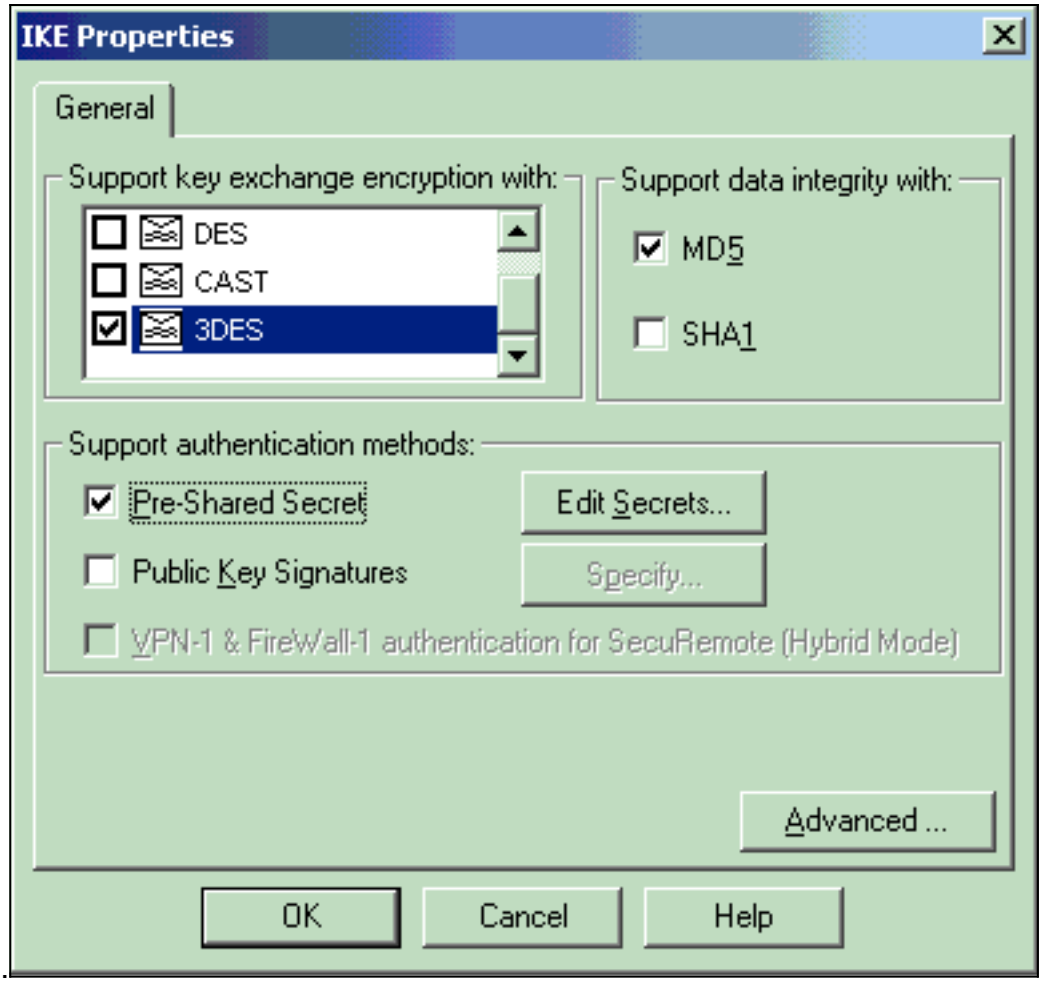


OK.

6. Dalla finestra Workstation Properties sul CheckpointTM NG, selezionare **VPN** dalle opzioni sul lato sinistro della finestra, quindi selezionare i parametri IKE per gli algoritmi di crittografia e autenticazione. Fare clic su **Modifica** per configurare le proprietà IKE.

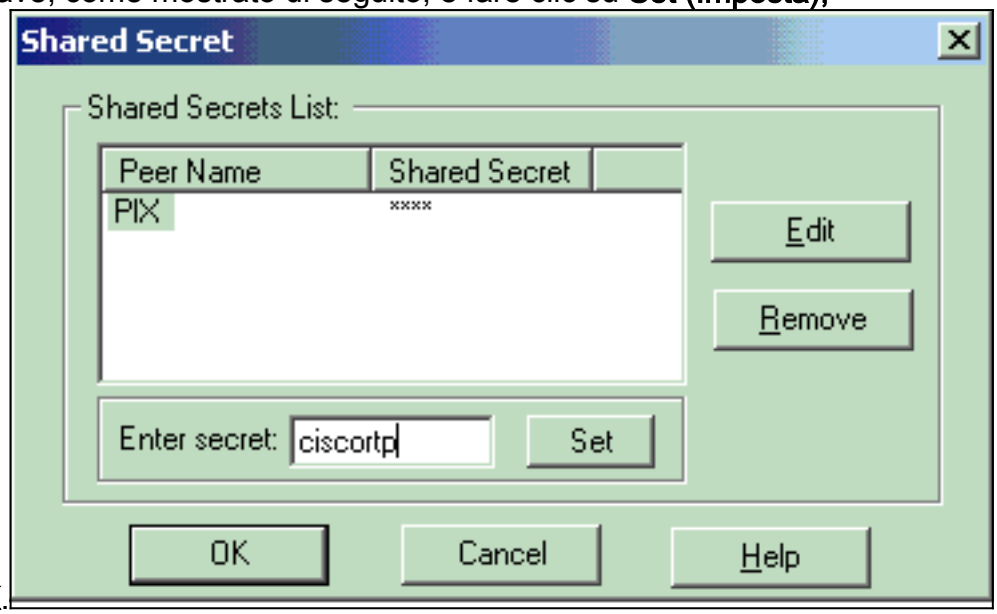


7. Configurare le proprietà IKE:Selezionare l'opzione per la crittografia **3DES** in modo che le proprietà IKE siano compatibili con il comando **isakmp policy # encryption 3des**.Selezionare l'opzione **MD5** in modo che le proprietà IKE siano compatibili con il comando **crypto isakmp**



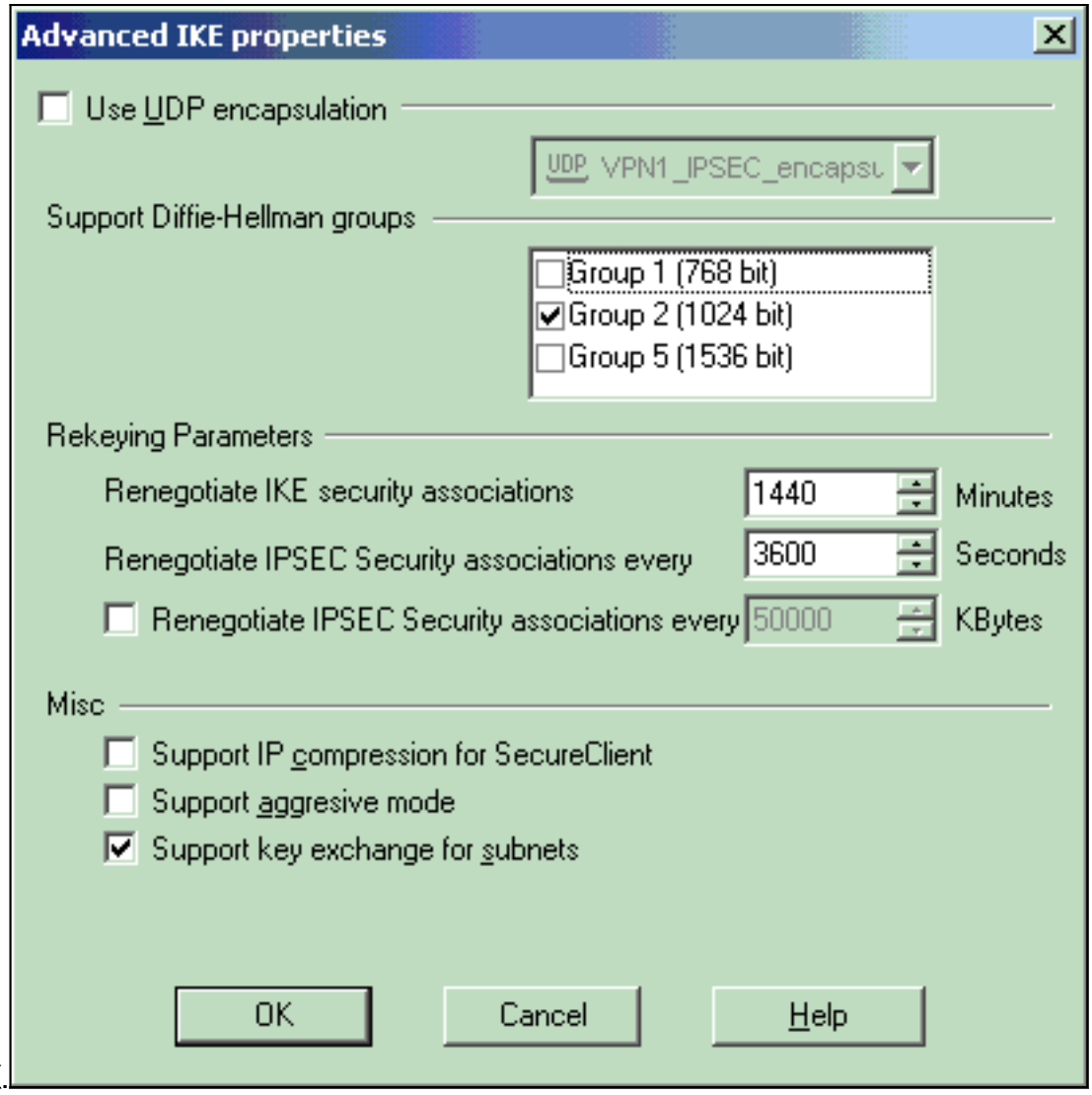
policy # hash md5.

8. Selezionare l'opzione di autenticazione per Segreti già condivisi, quindi fare clic su Modifica segreti per impostare la chiave già condivisa come compatibile con il comando PIX **isakmp chiave *chiave* indirizzo *netmask netmask*** . Fare clic su **Edit** (Modifica) per immettere la chiave, come mostrato di seguito, e fare clic su **Set (Imposta),**



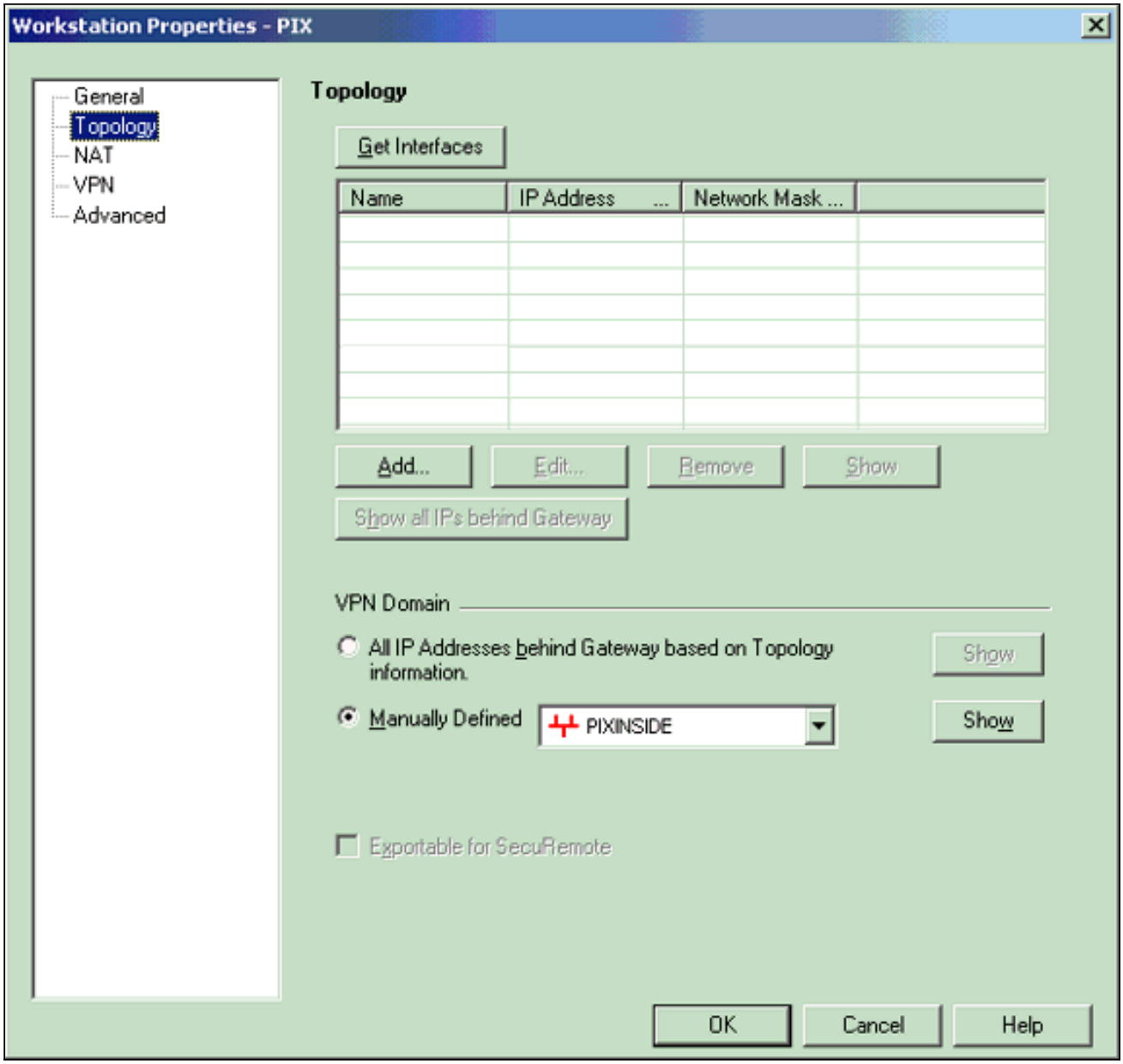
OK.

9. Dalla finestra delle proprietà di IKE, fare clic su **Avanzate...** e modificare le seguenti impostazioni:Deselezionare l'opzione **Supporto modalità aggressiva**.Selezionare l'opzione **Supporta scambio chiave per le subnet**.Al termine, fare clic su

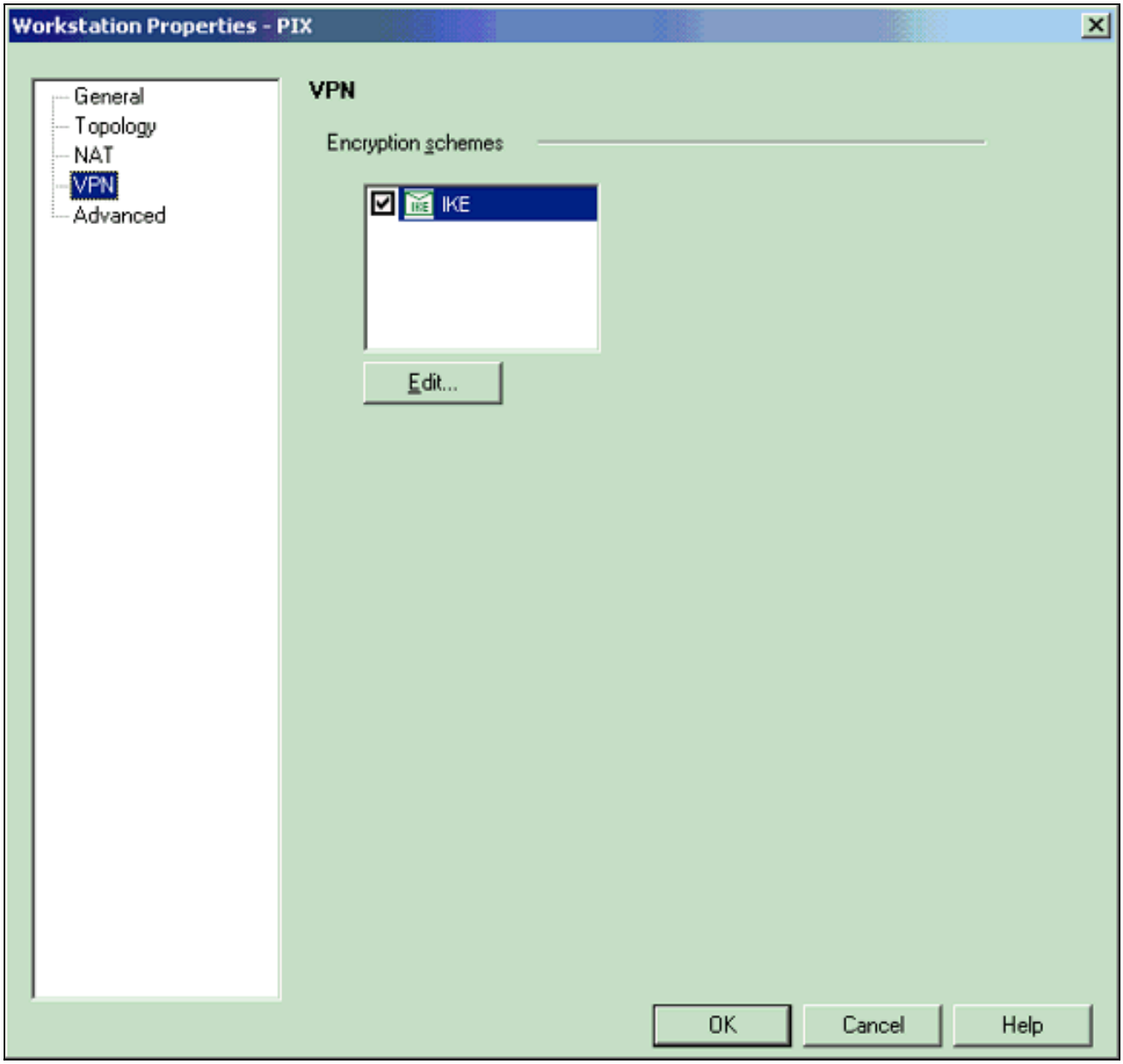


OK.

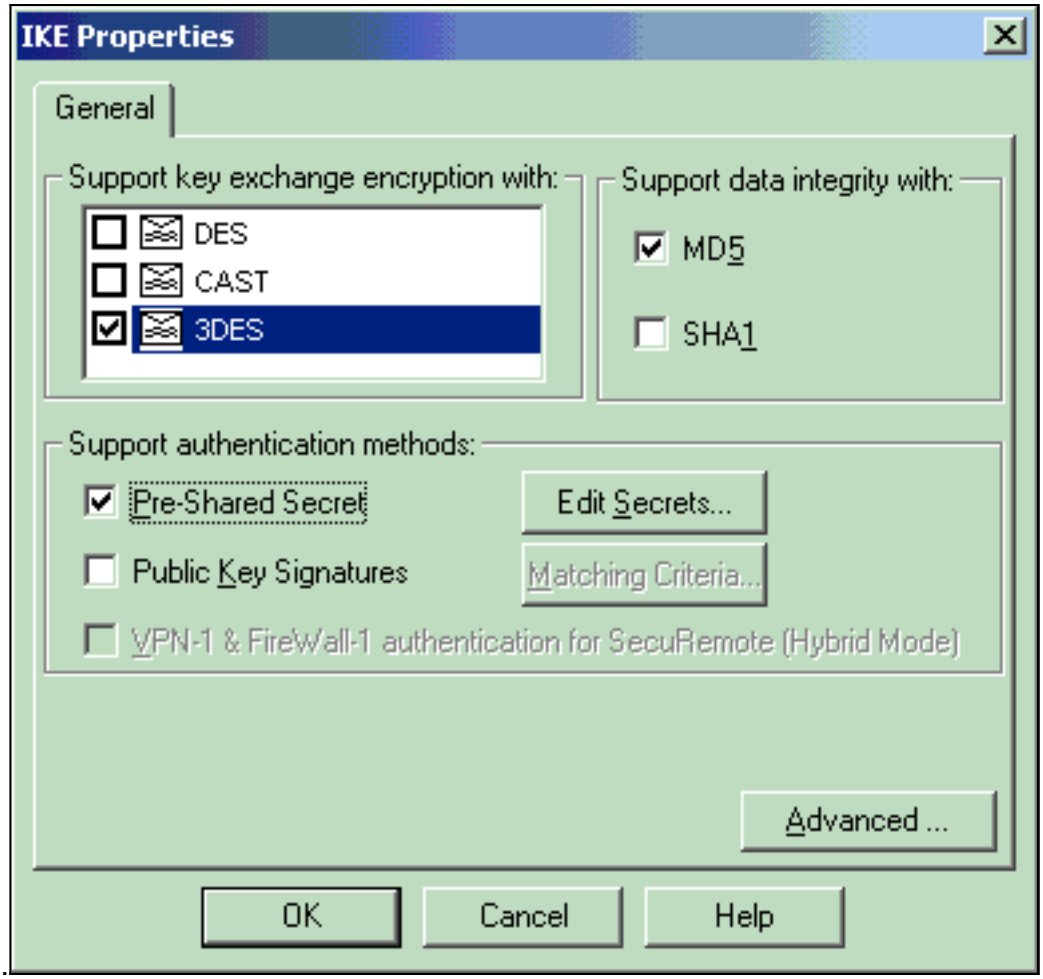
10. Selezionare **Gestisci > Oggetti di rete > Modifica** per aprire la finestra Proprietà stazione di lavoro per il PIX. Selezionare **Topologia** dalle opzioni sul lato sinistro della finestra per definire manualmente il dominio VPN.In questa configurazione, PIXINSIDE (all'interno della rete PIX) è definito come dominio
VPN.



11. Selezionare **VPN** dalle opzioni sul lato sinistro della finestra, quindi selezionare IKE come schema di crittografia. Fare clic su **Modifica** per configurare le proprietà IKE.

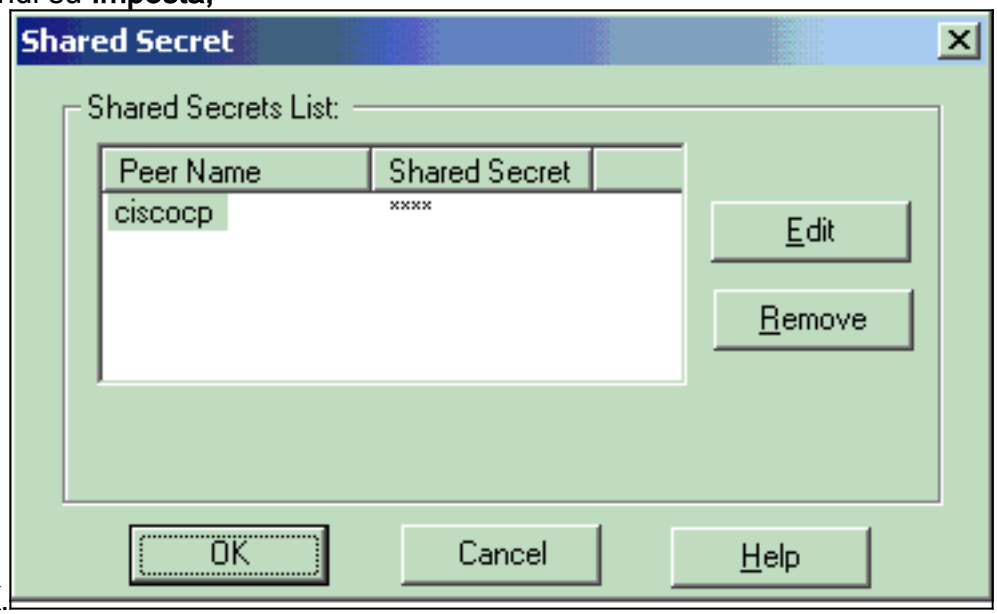


12. Configurare le proprietà IKE come illustrato di seguito:Selezionare l'opzione per la crittografia **3DES** in modo che le proprietà IKE siano compatibili con il comando **isakmp policy # encryption 3des**.Selezionare l'opzione **MD5** in modo che le proprietà IKE siano compatibili con il comando **crypto isakmp policy # hash**



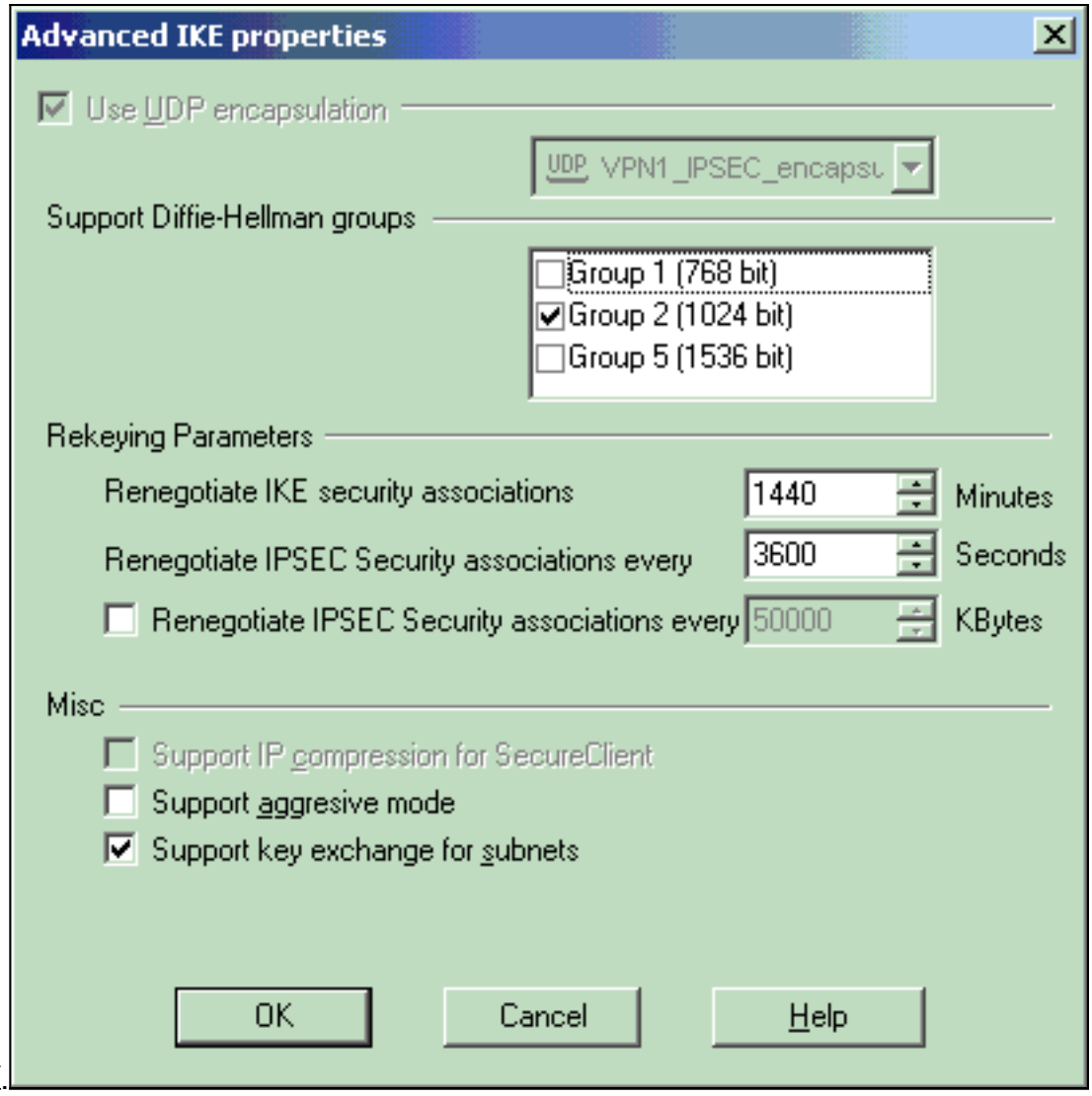
md5.

13. Selezionare l'opzione di autenticazione per Segreti già condivisi, quindi fare clic su Modifica segreti per impostare la chiave già condivisa come compatibile con il comando PIX **isakmp key** ***key*** **address** ***address*** **netmask** ***netmask*** . Fare clic su **Modifica** per immettere la chiave, quindi su **Imposta,**



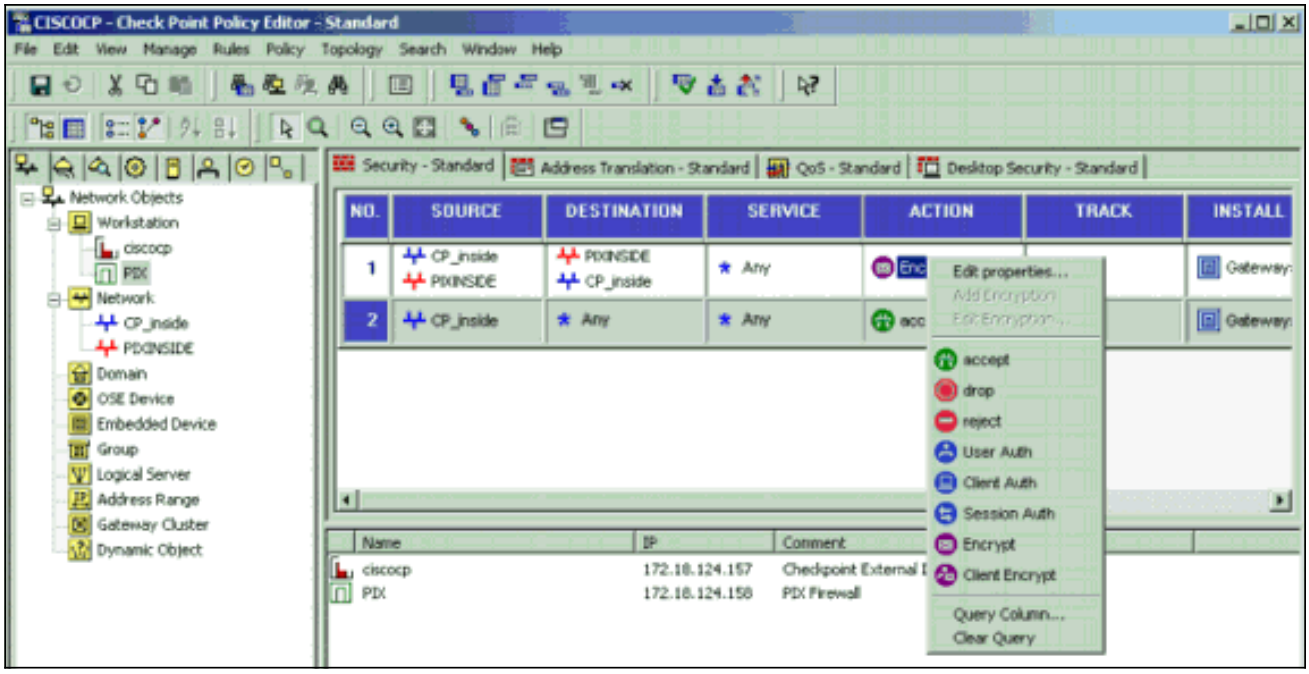
OK.

14. Nella finestra delle proprietà di IKE fare clic su **Avanzate** e modificare le impostazioni.Selezionare il gruppo Diffie-Hellman appropriato per le proprietà IKE.Deselezionare l'opzione **Supporto modalità aggressiva**.Selezionare l'opzione **Supporta scambio chiave per le subnet**.Al termine, fare clic su **OK,**

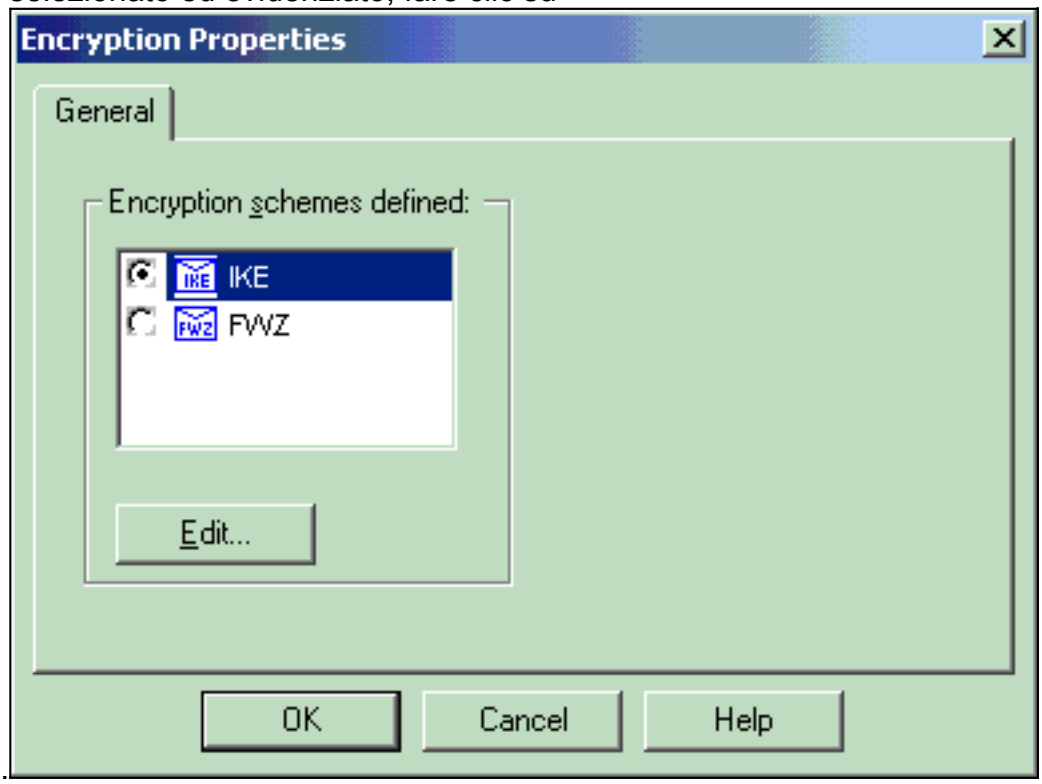


OK.

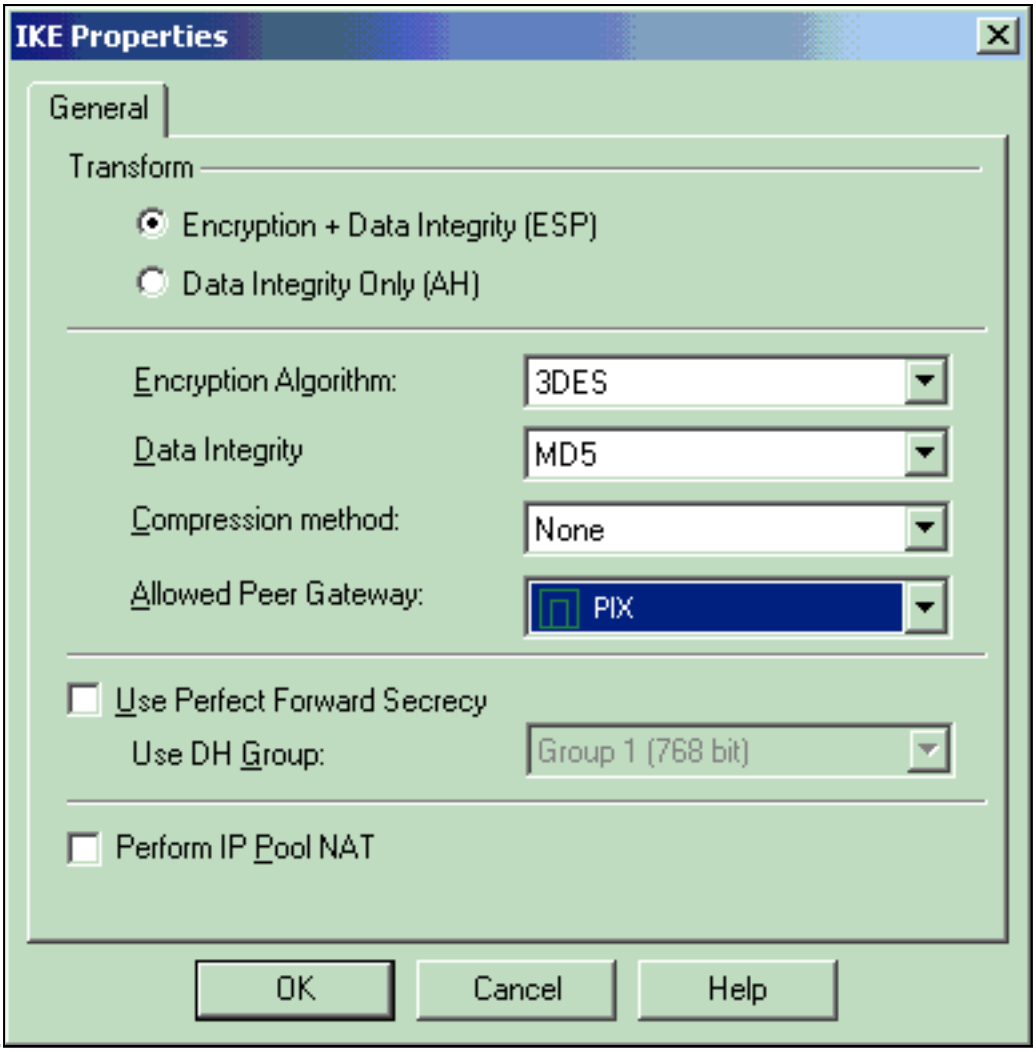
15. Selezionare **Regole > Aggiungi regole > In alto** per configurare le regole di crittografia per il criterio.Nella finestra Editor dei criteri, inserire una regola con un'origine CP_inside (all'interno della rete del checkpoint ™ NG) e PIXINSIDE (all'interno della rete del PIX) sia sulle colonne di origine che di destinazione. Impostare i valori per **Service = Any**, **Action = Encrypt** e **Track = Log**. Dopo aver aggiunto la sezione Azione crittografia della regola, fare clic con il pulsante destro del mouse su **Azione**, quindi selezionare **Modifica proprietà**.



16. Con IKE selezionato ed evidenziato, fare clic su **Modifica**.

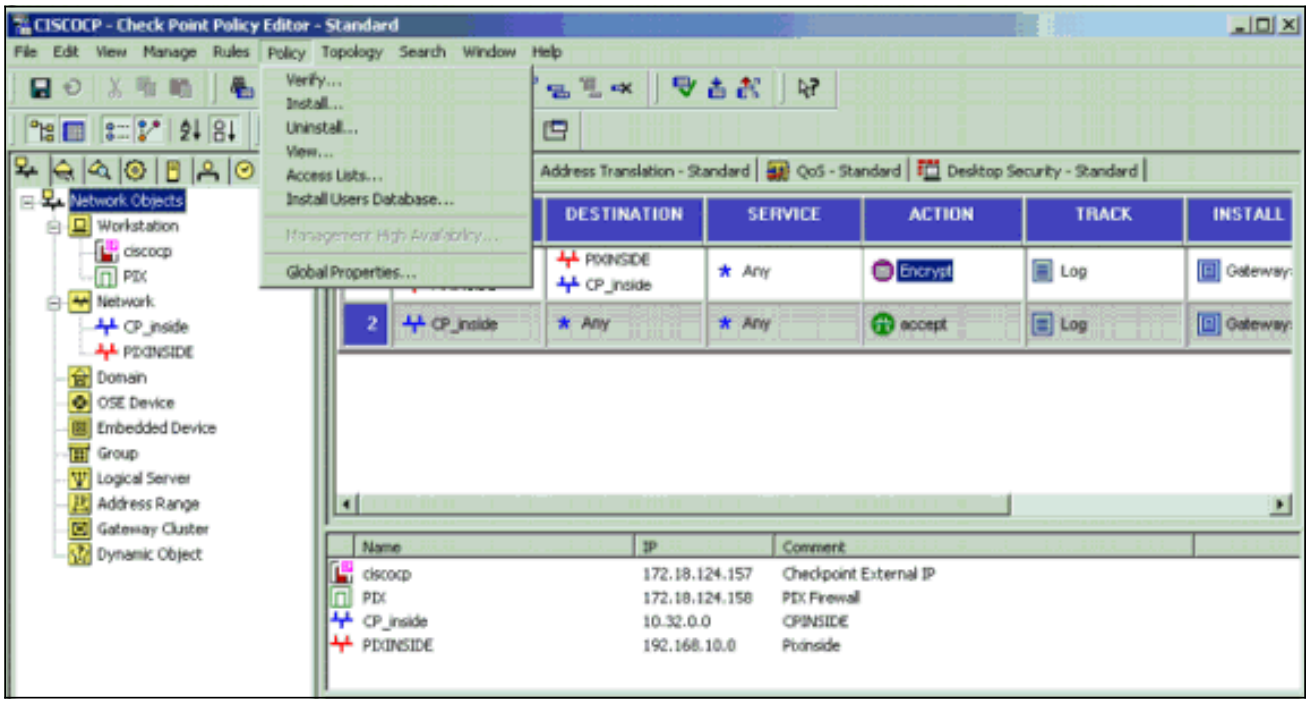


17. Nella finestra Proprietà IKE modificare le proprietà in modo che corrispondano alle trasformazioni IPSec PIX nel comando **crypto ipsec transform-set rtptac esp-3des esp-md5-hmac**.Impostare l'opzione Transform su **Encryption + Data Integrity (ESP)**, impostare Encryption Algorithm su **3DES**, impostare Data Integrity su **MD5** e impostare Allowed Peer Gateway in modo che corrisponda al gateway PIX esterno (qui denominato PIX). Fare clic

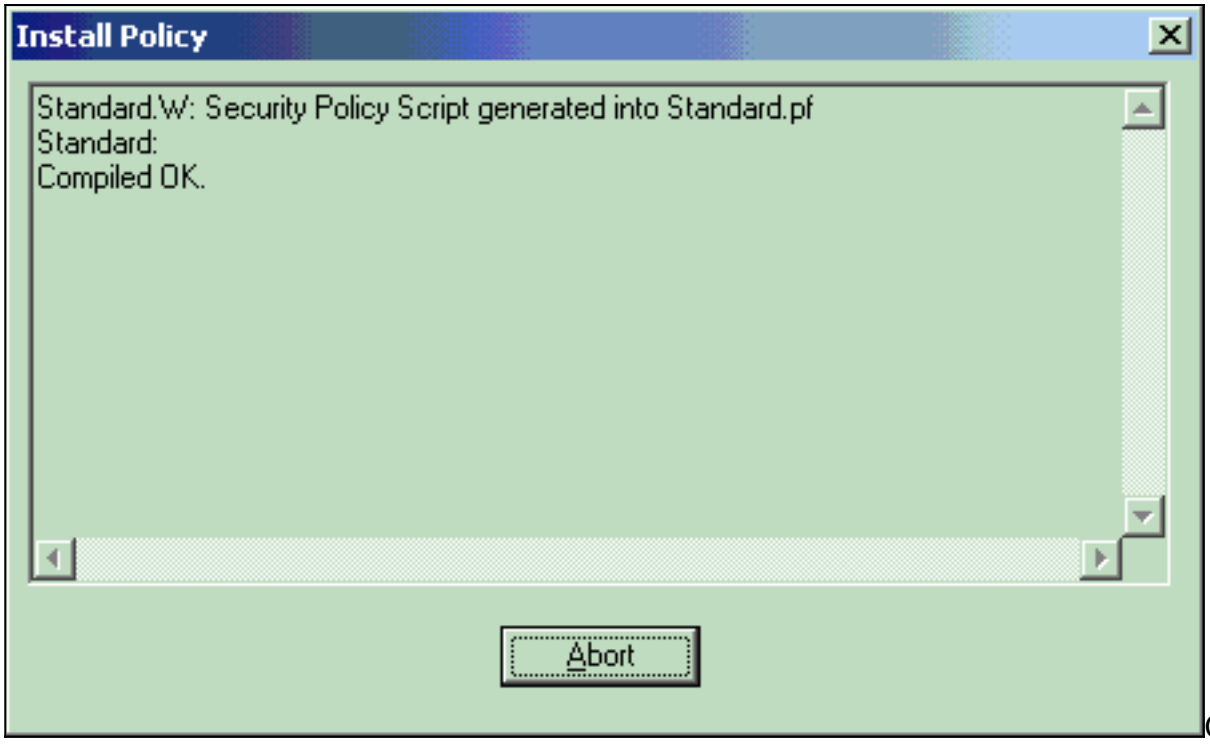


su **OK**.

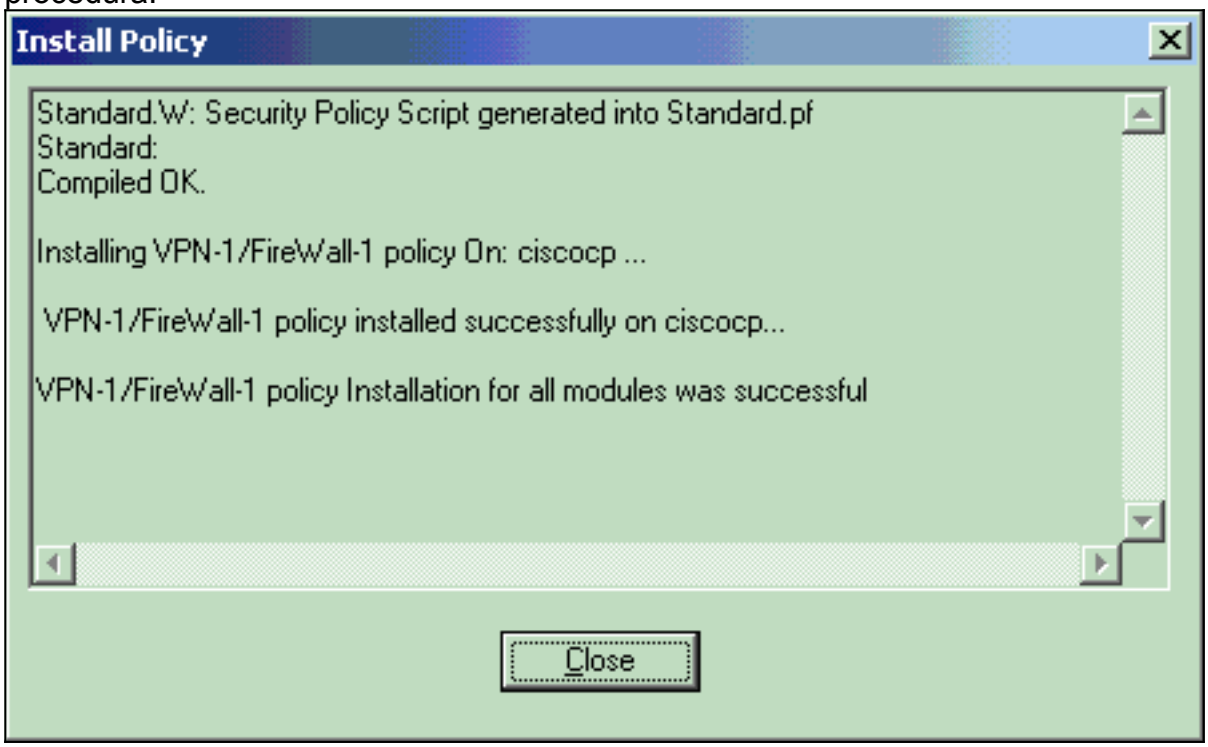
18. Dopo aver configurato il file CheckpointTM NG, salvare il criterio e selezionare **Criterio > Installa** per attivarlo.



Durante la compilazione del criterio, nella finestra di installazione vengono visualizzate note sullo stato di avanzamento.



Quando la finestra di installazione indica che l'installazione dei criteri è stata completata. Fare clic su **Chiudi** per completare la procedura.



Verifica

Verifica della configurazione PIX

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

Lo strumento Output Interpreter (solo utenti registrati) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

Eseguire il ping tra una delle reti private e l'altra per verificare la comunicazione tra le due reti private. In questa configurazione, è stato inviato un ping dal lato PIX (192.168.10.2) alla rete interna di CheckpointTM NG (10.32.50.51).

- **show crypto isakmp sa**: visualizza tutte le SA IKE correnti in un peer.

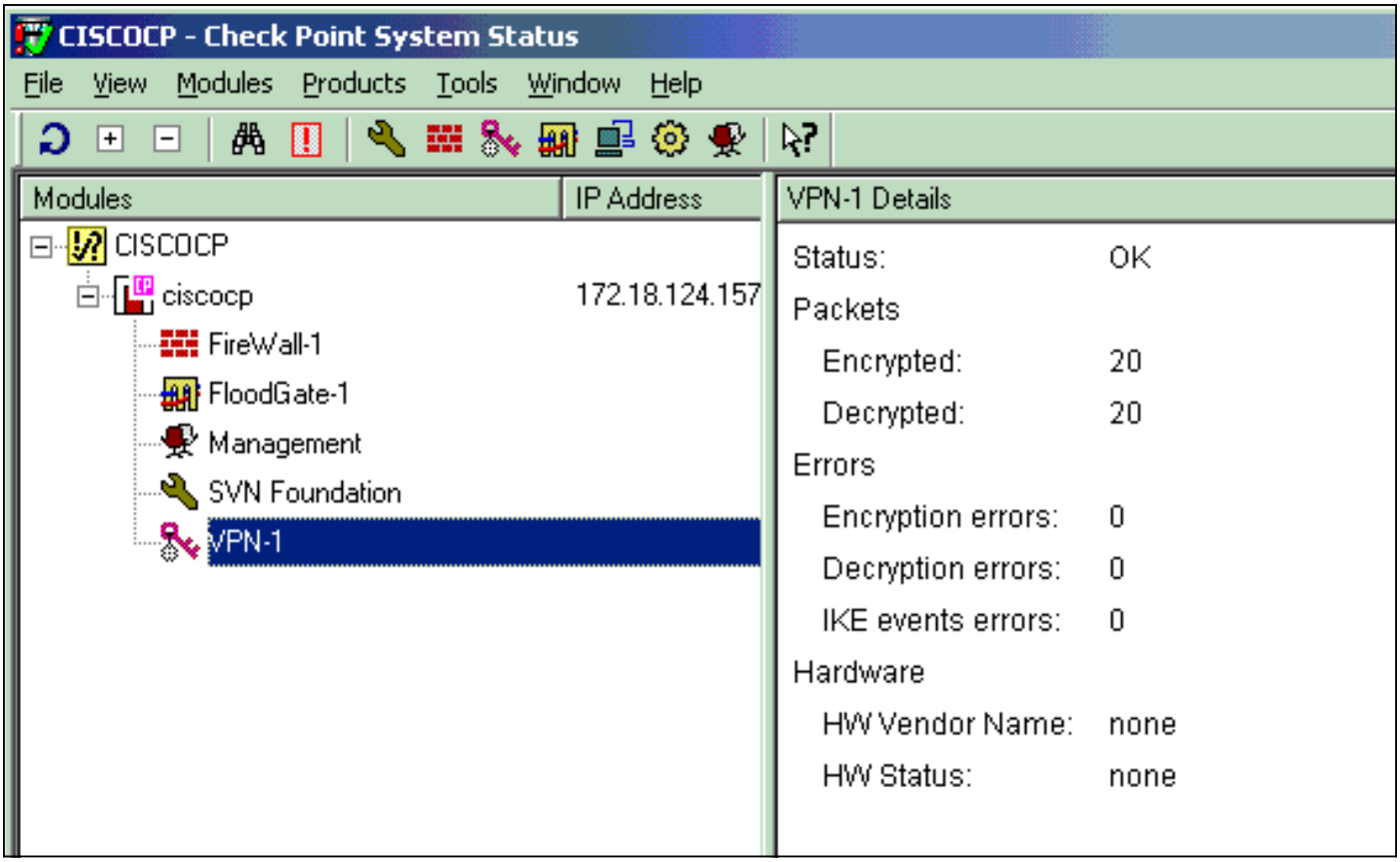
```
show crypto isakmp sa
Total    : 1
Embryonic : 0
             dst                     src                   state     pending   created
  172.18.124.157   172.18.124.158   QM_IDLE         0          1
```

- **show crypto ipsec sa**: visualizza le impostazioni utilizzate dalle associazioni di protezione correnti.

```
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:
```

Visualizza stato tunnel su checkpoint NG

Andare all'Editor criteri e selezionare **Finestra > Stato sistema** per visualizzare lo stato del tunnel.



Risoluzione dei problemi

Risoluzione dei problemi relativi alla configurazione PIX

Lo strumento Output Interpreter (solo utenti registrati) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

Nota: consultare le informazioni importanti sui comandi di debug prima di usare i comandi di **debug**.

Utilizzare questi comandi per abilitare i debug sul firewall PIX.

- **debug crypto engine**: visualizza i messaggi di debug sui motori di crittografia, che eseguono la crittografia e la decrittografia.
- **debug crypto isakmp**: visualizza i messaggi sugli eventi IKE.

```
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
```

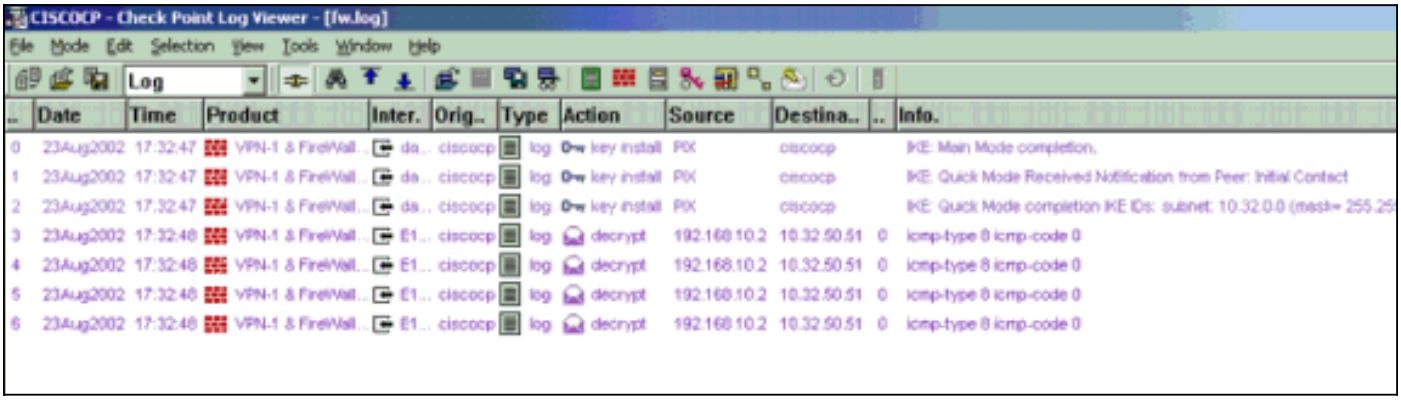
```
lifetime of 28800 seconds
lifetime of 4608000 kilobytesIPSEC(key_engine): got a queue event...
IPSEC(initialize_sas): ,
(key eng. msg.) dest= 172.18.124.158, src= 172.18.124.157,
dest_proxy= 192.168.10.0/255.255.255.0/0/0 (type=4),
src_proxy= 10.32.0.0/255.255.128.0/0/0 (type=4),
protocol= ESP, transform= 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
```

Riepilogo della rete

Quando più reti interne adiacenti sono configurate nel dominio di crittografia sul checkpoint, il dispositivo potrebbe riepilogarle automaticamente in relazione al traffico interessante. Se l'elenco di controllo di accesso (ACL) crittografico sul PIX non è configurato per corrispondere, è probabile che il tunnel abbia esito negativo. Ad esempio, se le reti interne 10.0.0.0 /24 e 10.0.1.0 /24 sono configurate per essere incluse nel tunnel, è possibile riepilogarle in 10.0.0.0 /23.

Visualizza registri Checkpoint NG

Selezionare **Finestra > Visualizzatore log** per visualizzare i log.



Informazioni correlate

- Software Cisco PIX Firewall
- Riferimenti per i comandi di Cisco Secure PIX Firewall
- Avvisi sui prodotti per la sicurezza (inclusi PIX)
- RFC (Requests for Comments)
- Documentazione e supporto tecnico – Cisco Systems