Configurazione di un tunnel IPSec - Cisco Secure PIX Firewall per il firewall Checkpoint 4.1

Sommario

Introduzione

In questa configurazione di esempio viene illustrato come formare un tunnel IPSec con chiavi già condivise per il collegamento a due reti private. Nell'esempio, le reti unite sono la rete privata 192.168.1.X all'interno di Cisco Secure Pix Firewall (PIX) e la rete privata 10.32.50.X all'interno del checkpoint. Si presume che il traffico tra il PIX e l'interno del firewall di checkpoint 4.1 e Internet (rappresentato qui dalle reti 172.18.124.X) scorra prima di iniziare questa configurazione.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

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

- Software PIX versione 5.3.1
- Firewall checkpoint 4.1

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.

Convenzioni

Fare riferimento a Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.

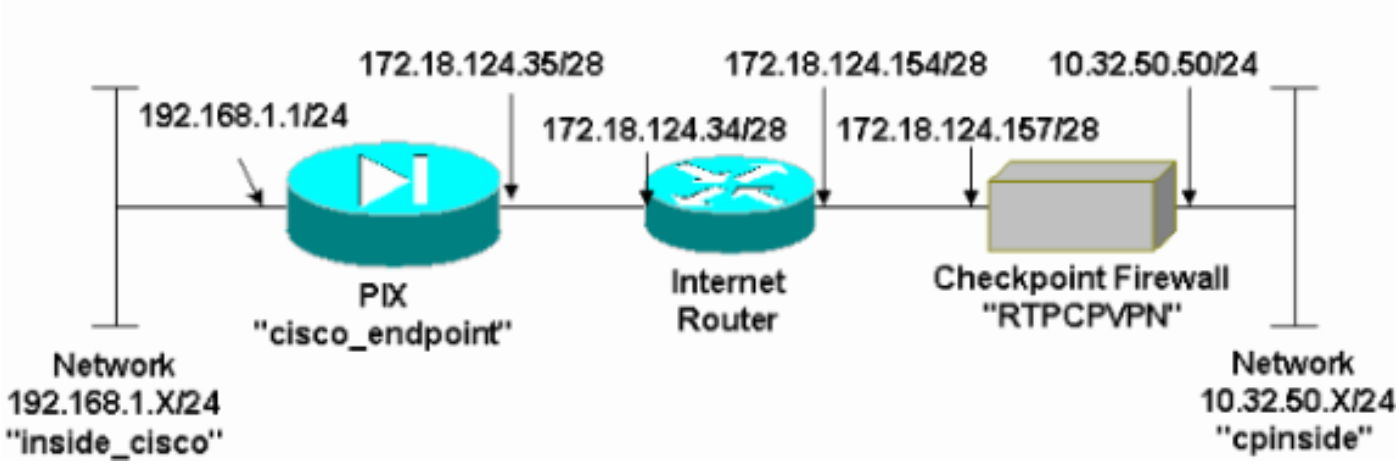
Configurazione

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

Nota: per ulteriori informazioni sui comandi menzionati in questo documento, usare lo strumento di ricerca dei comandi (solo utenti registrati).

Esempio di rete

Nel documento viene usata l'impostazione di rete mostrata nel diagramma:



Configurazioni

Nel documento vengono usate le configurazioni mostrate in questa sezione.

Configurazione PIX

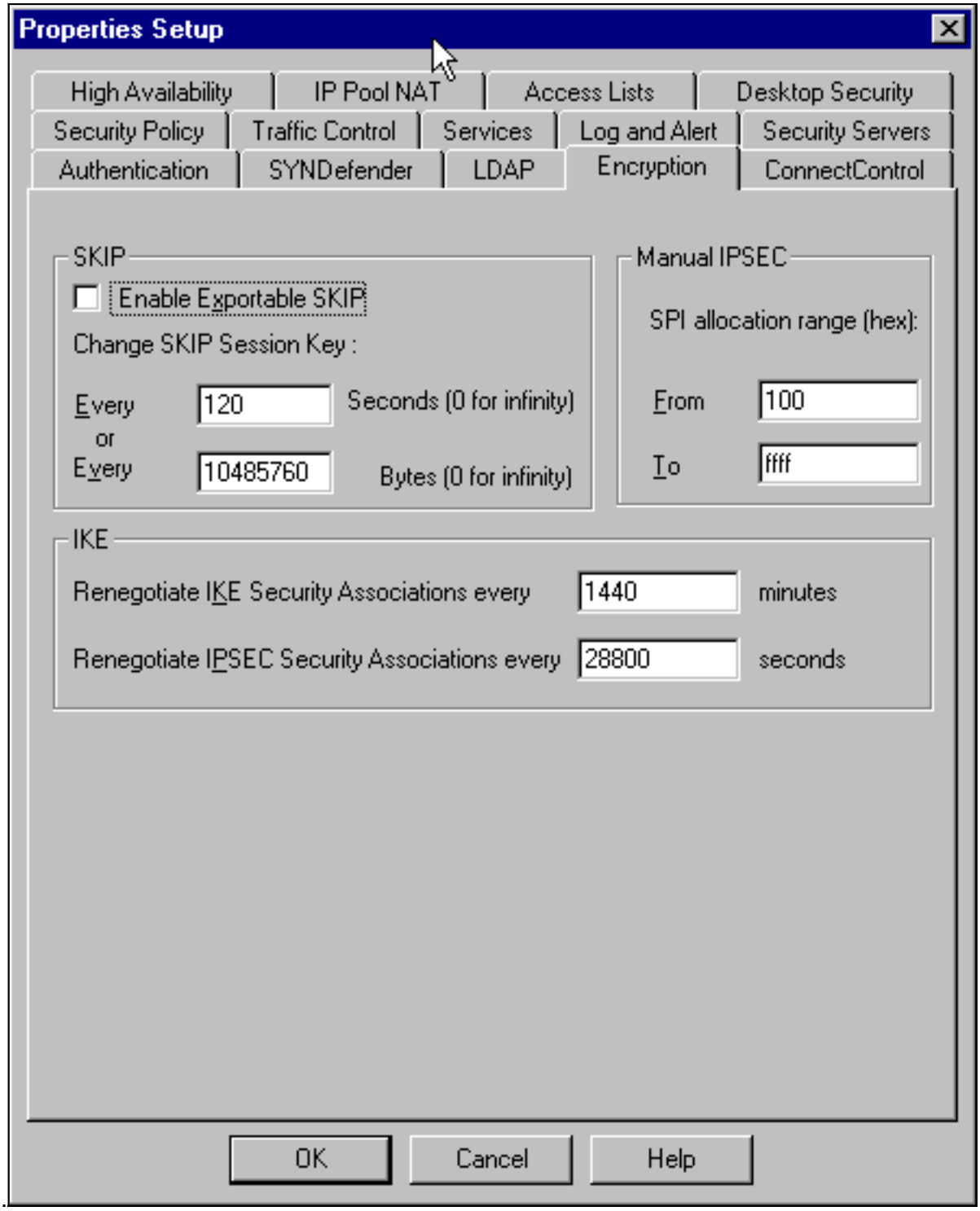
```
PIX Version 5.3(1)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname cisco_endpoint
fixup protocol ftp 21
fixup protocol http 80
```

```
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
names
access-list 115 permit ip 192.168.1.0 255.255.255.0
10.32.50.0 255.255.255.0
access-list 115 deny ip 192.168.1.0 255.255.255.0 any
pager lines 24
logging on
no logging timestamp
no logging standby
no logging console
logging monitor debugging
no logging buffered
logging trap debugging
no logging history
logging facility 20
logging queue 512
interface ethernet0 auto
interface ethernet1 auto
mtu outside 1500
mtu inside 1500
ip address outside 172.18.124.35 255.255.255.240
ip address inside 192.168.1.1 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
no failover
failover timeout 0:00:00
failover poll 15
failover ip address outside 0.0.0.0
failover ip address inside 0.0.0.0
arp timeout 14400
global (outside) 1 172.18.124.36
nat (inside) 0 access-list 115
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
route outside 0.0.0.0 0.0.0.0 172.18.124.34 1
timeout xlate 3:00:00g SA 0x80bd6a10, conn_id = 0
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
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
!--- IPSec configuration sysopt connection permit-ipsec
no sysopt route dnat
crypto ipsec transform-set myset esp-des esp-sha-hmac
crypto map rtpmap 10 ipsec-isakmp
crypto map rtpmap 10 match address 115
crypto map rtpmap 10 set peer 172.18.124.157
crypto map rtpmap 10 set transform-set myset
crypto map rtpmap 10 set security-association lifetime
seconds
3600 kilobytes 4608000
crypto map rtpmap interface outside
!--- IKE configuration isakmp enable outside
isakmp key ******** address 172.18.124.157 netmask
255.255.255.240
```

```
isakmp identity address
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption des
isakmp policy 10 hash sha
isakmp policy 10 group 1
isakmp policy 10 lifetime 86400
telnet timeout 5
ssh timeout 5
terminal width 80
Cryptochecksum:dc43c44e4513d3633a3fc7b1c3802c79
: end
[OK]
```

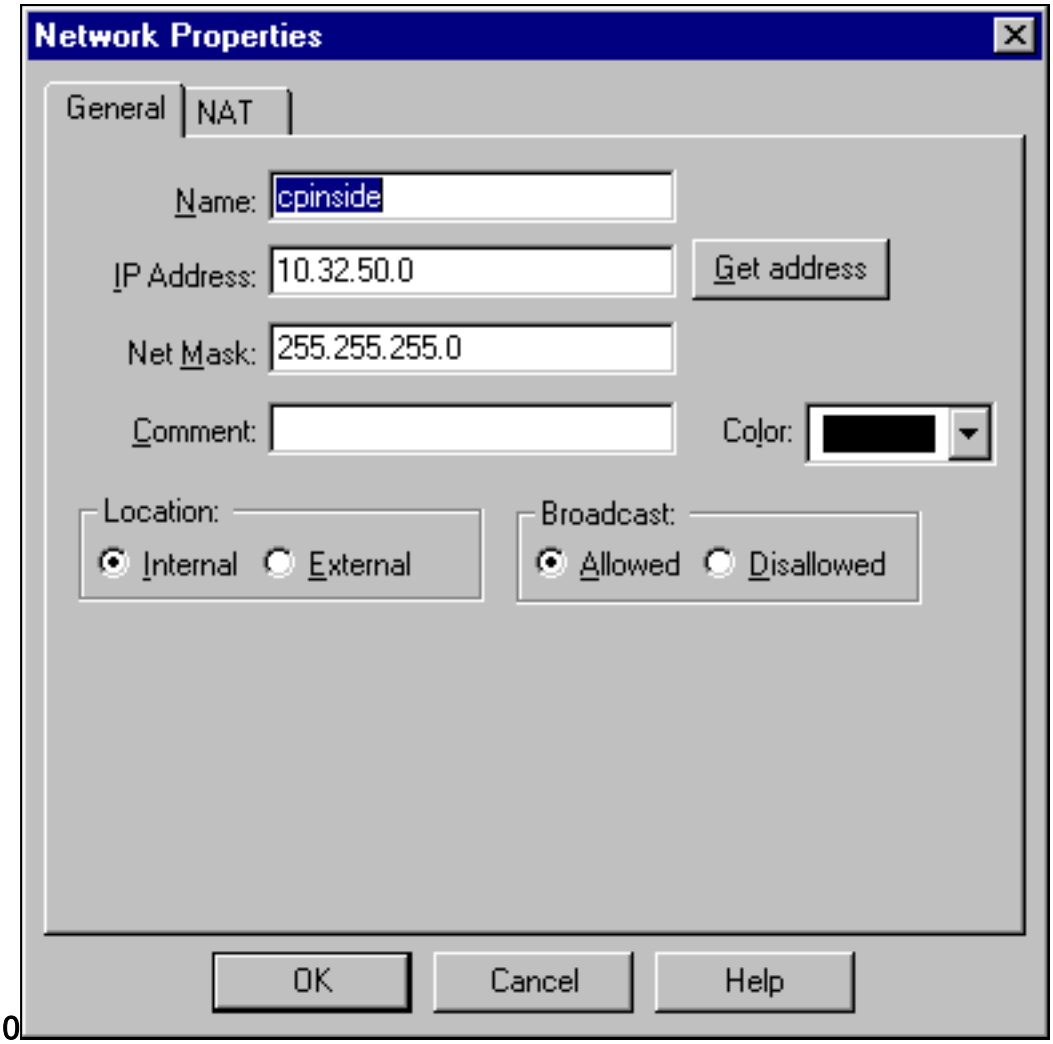
Checkpoint Firewall

1. Poiché la durata predefinita di IKE e IPSec varia a seconda del fornitore, selezionare **Proprietà > Crittografia** per impostare la durata del checkpoint in modo che corrisponda a quella predefinita di PIX.La durata IKE predefinita PIX è 86400 secondi (=1440 minuti), modificabile con questo comando: **durata criterio isakmp 86400**La durata IKE PIX può essere configurata tra 60 e 86400 secondi.La durata IPSec predefinita PIX è di 2800 secondi, modificabile con questo comando: **secondi durata associazione di protezione ipsec crypto #**È possibile configurare una durata IPSec PIX compresa tra 120 e 86400



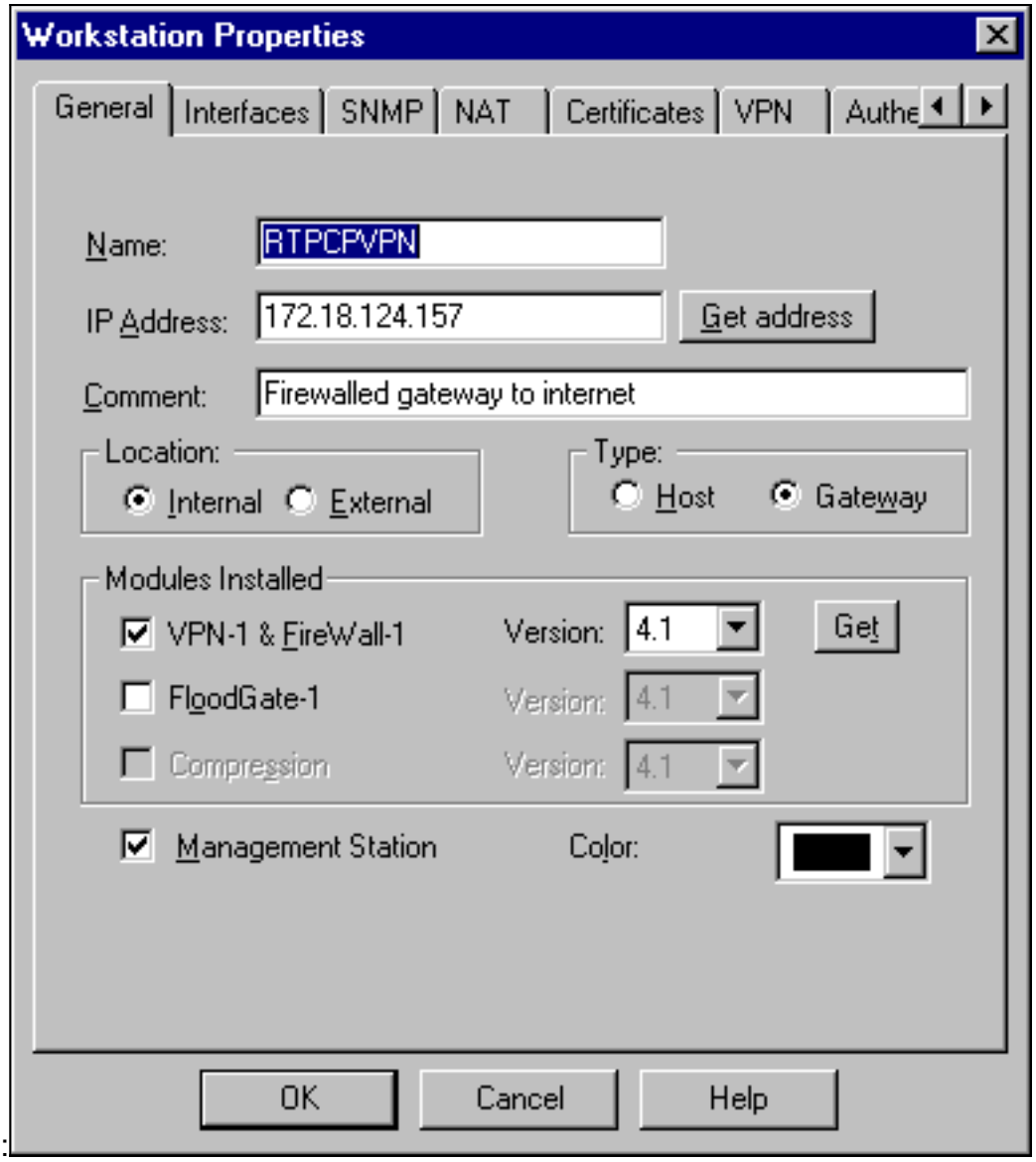
secondi.

2. Selezionare **Gestisci > Oggetti di rete > Nuovo (o Modifica) > Rete** per configurare l'oggetto per la rete interna ("cpinside") dietro il checkpoint.Questo deve corrispondere alla rete di destinazione (seconda) in questo comando PIX: **access-list 115 allow ip 192.168.1.0 255.255.255.0 10.32.50.0**



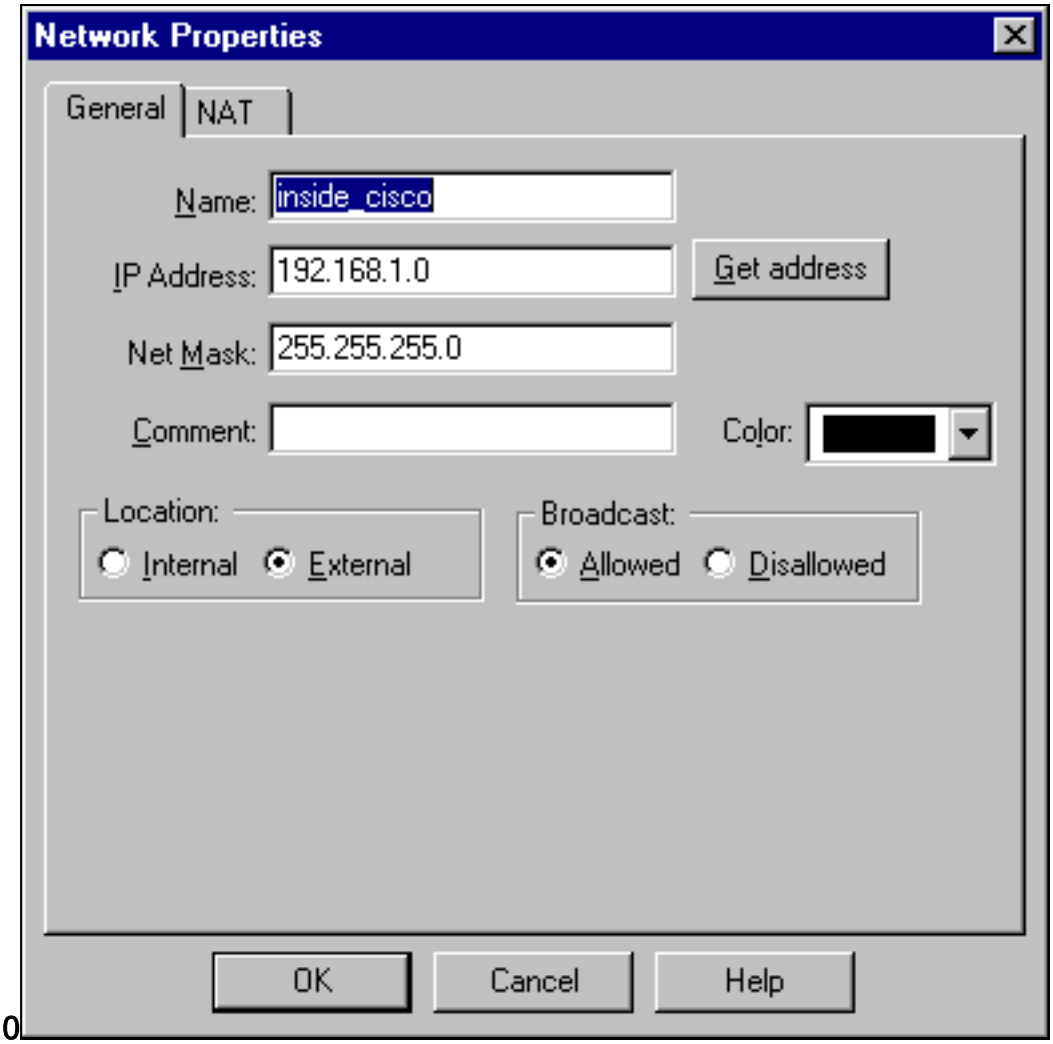
255.255.255.0

3. Selezionare **Gestisci > Oggetti di rete > Modifica** per modificare l'oggetto per l'endpoint gateway ("RTPCPVPN" Checkpoint) a cui punta il PIX in questo comando: **nome mappa crittografica # set peer indirizzo_ip**In Posizione selezionare **Interno**. Per Tipo, selezionare **Gateway**. In Moduli installati, selezionare la casella di controllo **VPN-1 e FireWall-1** e selezionare anche la casella di controllo **Stazione di**



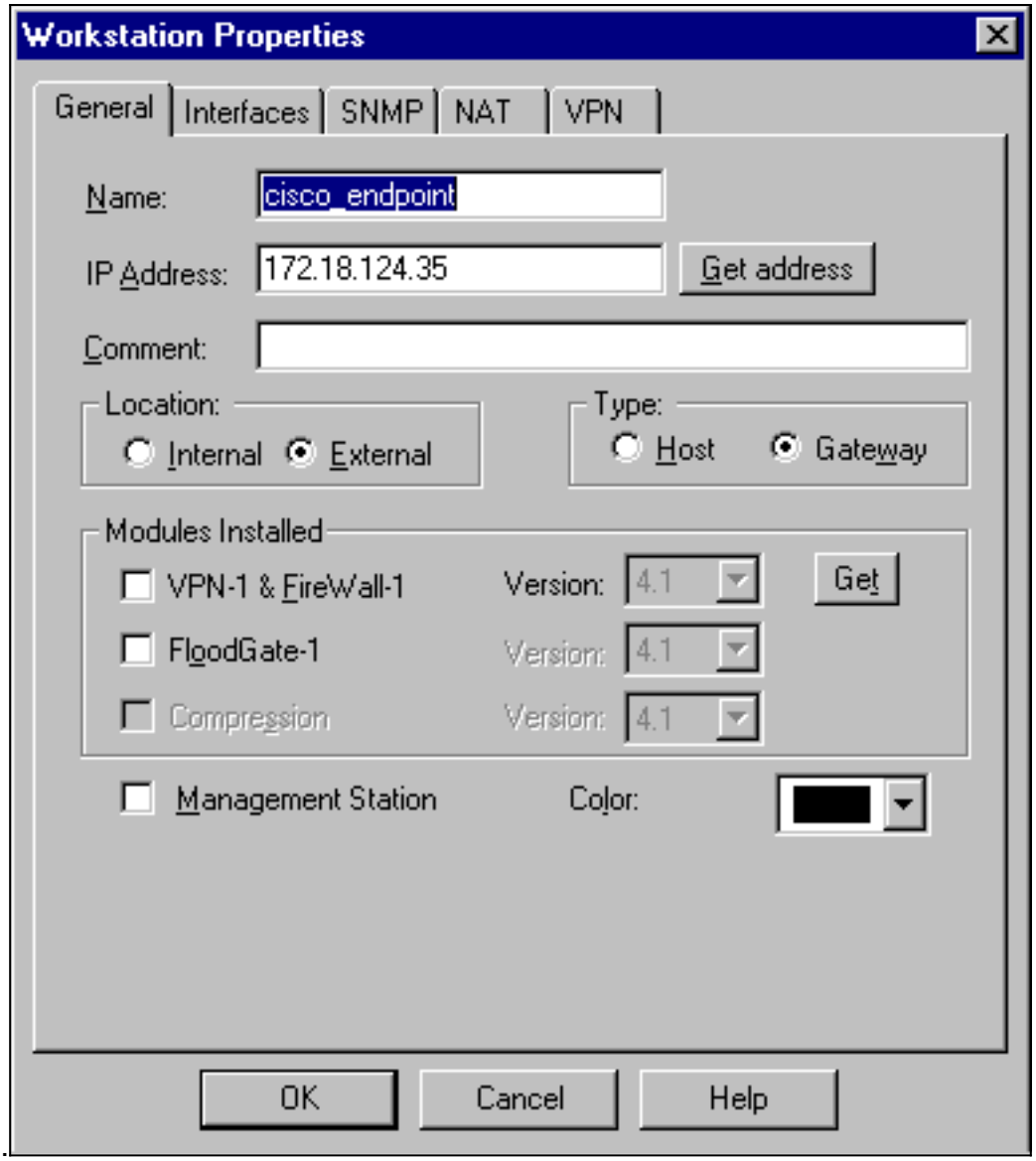
gestione:

4. Selezionare **Gestisci > Oggetti di rete > Nuovo > Rete** per configurare l'oggetto per la rete esterna ("inside_cisco") dietro il PIX.Questo deve corrispondere alla (prima) rete di origine in questo comando PIX: **access-list 115 allow ip 192.168.1.0 255.255.255.0 10.32.50.0**

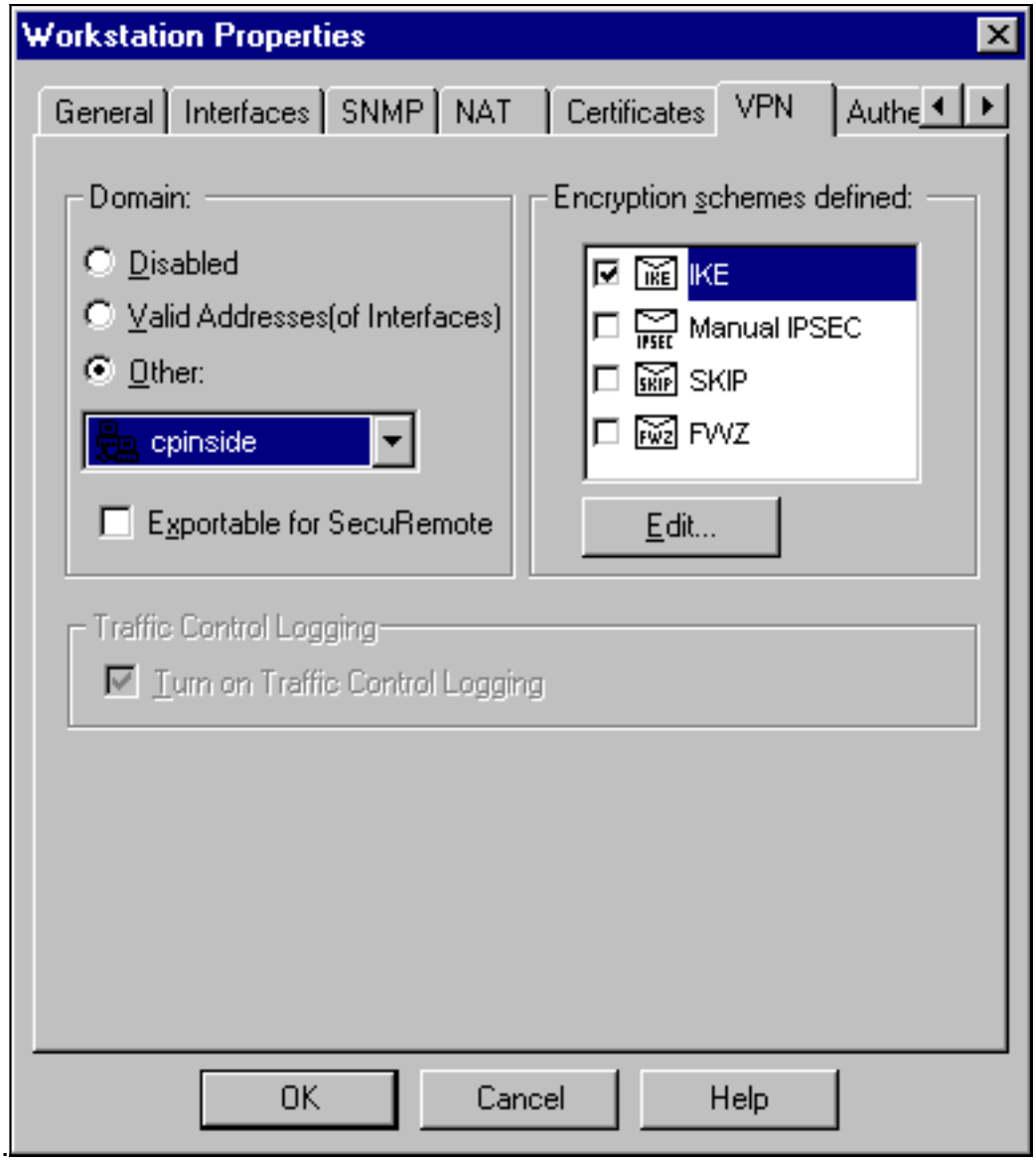


255.255.255.0

5. Selezionare **Gestisci > Oggetti di rete > Nuovo > Workstation** per aggiungere un oggetto per il gateway PIX esterno ("cisco_endpoint"). Questa è l'interfaccia PIX a cui viene applicato il comando: **interfaccia *nome* mappa crittografica esterna**In Posizione selezionare **Esterna**. Per Tipo, selezionare **Gateway**.**Nota:** non selezionare la casella di controllo VPN-1/FireWall-

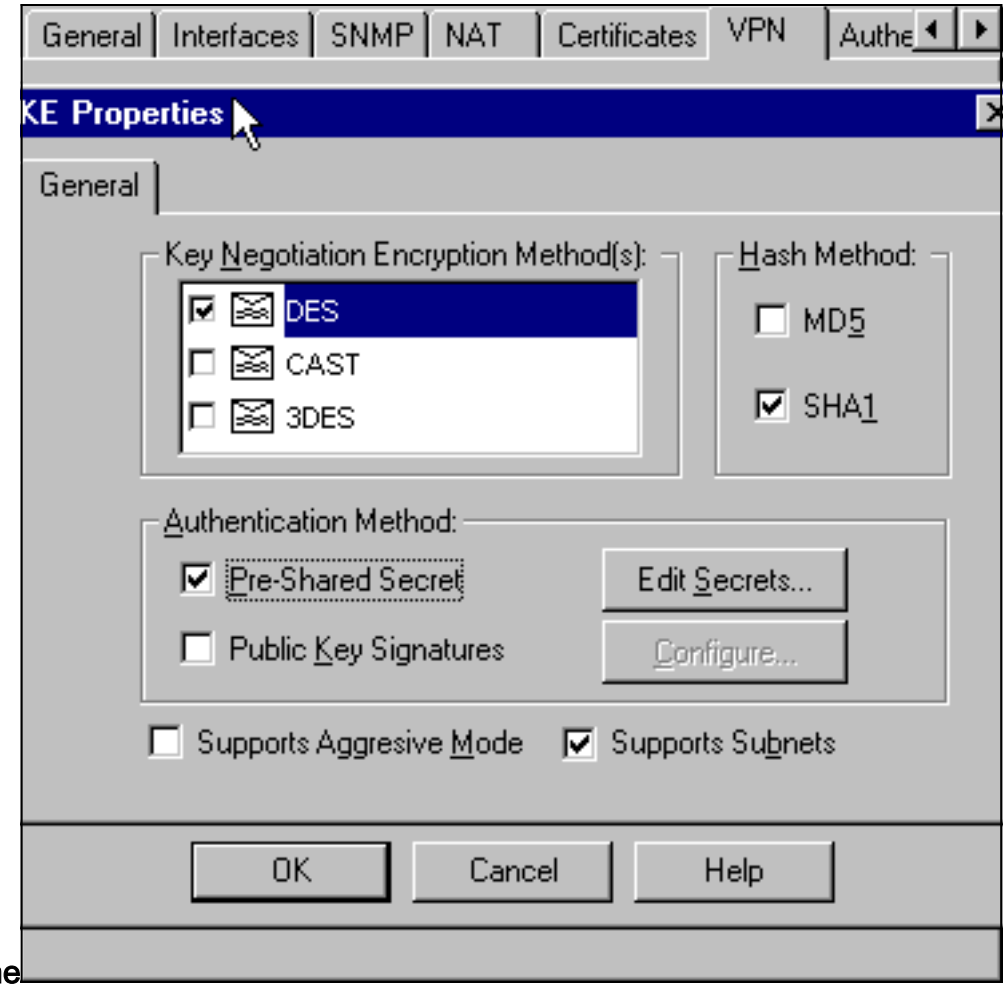
1. 

6. Selezionare **Gestisci > Oggetti di rete > Modifica** per modificare l'endpoint del gateway del checkpoint (denominato "RTPCPVPN") nella scheda VPN. In Dominio selezionare **Altro**, quindi selezionare dall'elenco a discesa l'interno della rete del checkpoint (denominata "cpinside"). In Definizione schemi di crittografia selezionare **IKE**, quindi fare clic su



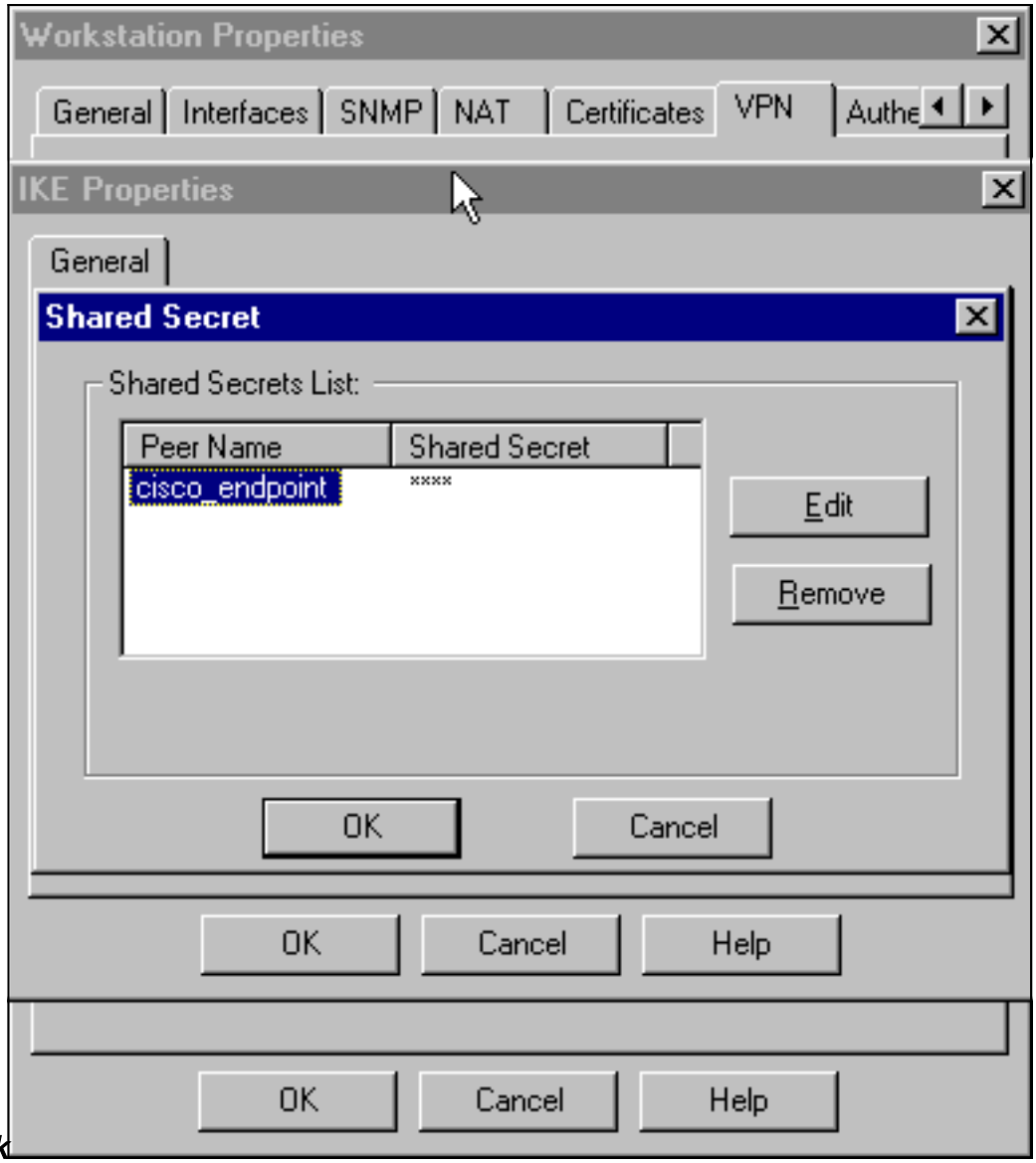
Modifica.

7. Modificare le proprietà IKE per la crittografia DES in modo che corrispondano a questo comando:**crittografia n. criteri isakmp**
8. Modificare le proprietà IKE in hashing SHA1 per accettare questo comando:**isakmp criteri # hash sha**Cambia le impostazioni:Deselezionare **Modalità aggressiva**.Selezionare la casella di controllo **Supporta subnet**.In Metodo di autenticazione selezionare la casella di controllo **Segreto precondiviso**. L'operazione accetta il comando:**criterio isakmp # autenticazione pre-**



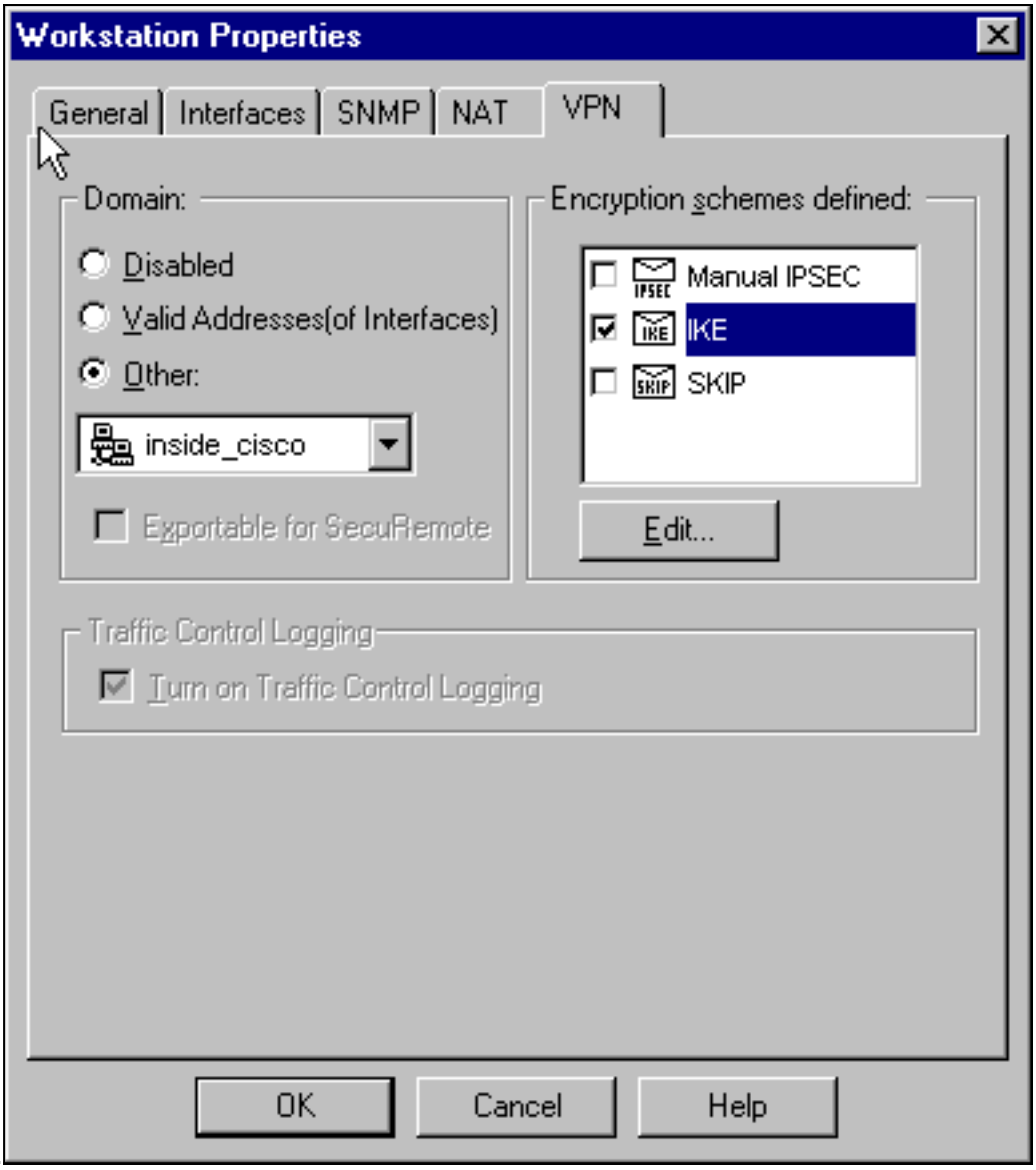
condivisione

9. Fare clic su **Edit Secrets** (Modifica segreti) per impostare la chiave già condivisa in modo che concordi con il comando PIX:**isakmp** ***chiave*** **indirizzo** ***indirizzo*** **netmask**



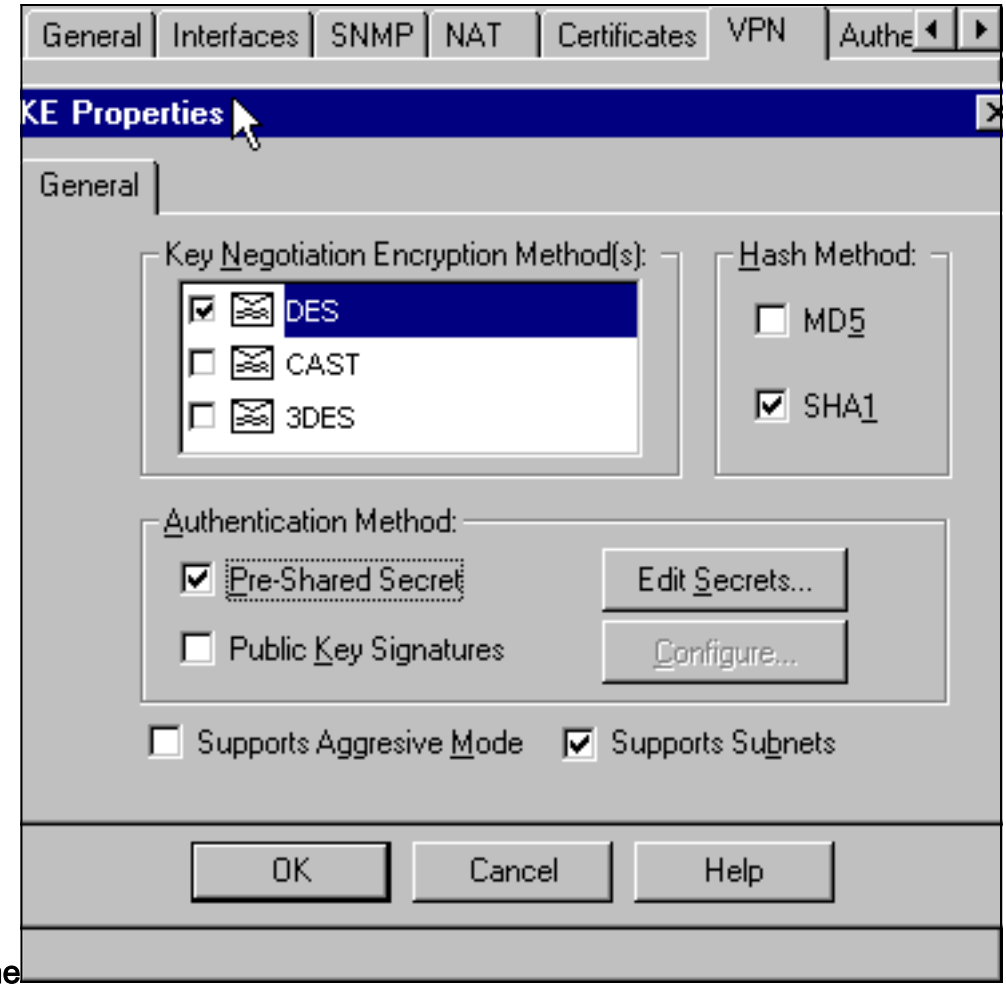
netmask

10. Selezionare **Gestisci > Oggetti di rete > Modifica** per modificare la scheda VPN "cisco_endpoint". In Dominio, selezionare **Altro**, quindi selezionare l'interno della rete PIX (chiamata "inside_cisco"). In Definizione schemi di crittografia selezionare **IKE** e quindi fare



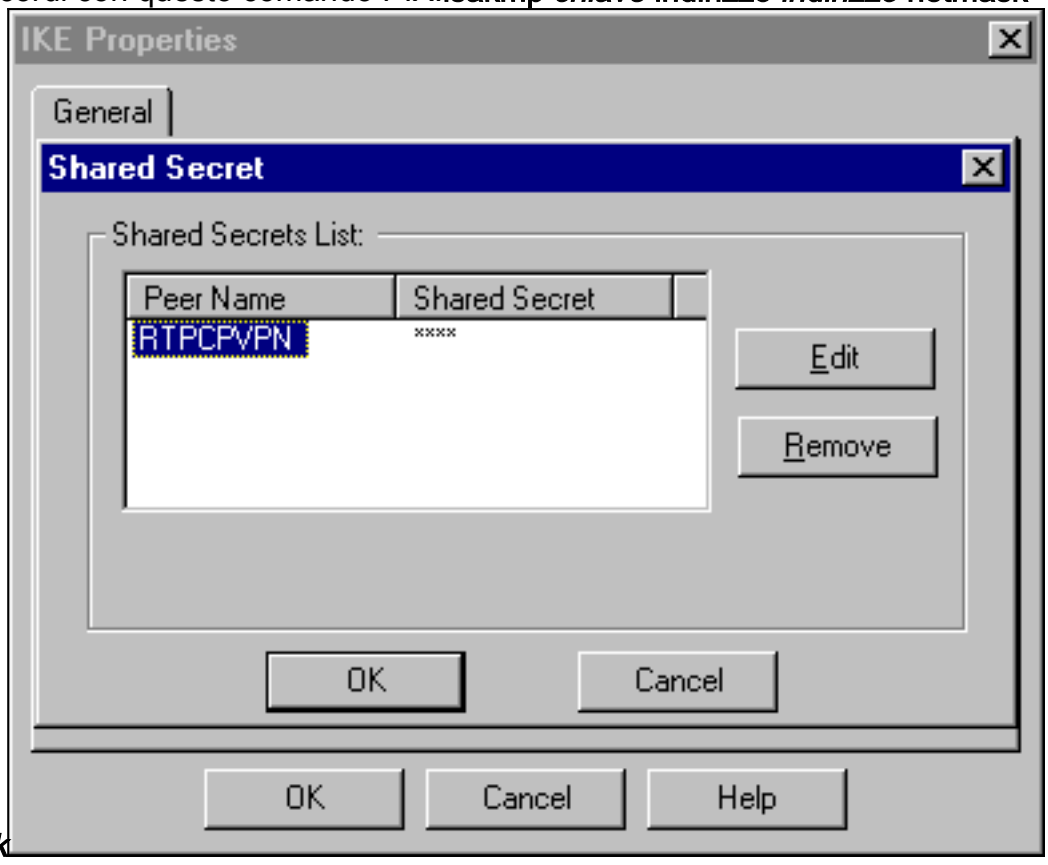
clic su **Modifica**.

11. Modificare le proprietà IKE della crittografia DES per accettare questo comando:**crittografia n. criteri isakmp**
12. Modificare le proprietà IKE in hashing SHA1 per accettare questo comando:**crypto isakmp policy # hash sha**Cambia le impostazioni:Deselezionare **Modalità aggressiva**.Selezionare la casella di controllo **Supporta subnet**.In Metodo di autenticazione selezionare la casella di controllo **Segreto precondiviso**. L'azione concorda con questo comando:**criterio isakmp # autenticazione pre-**



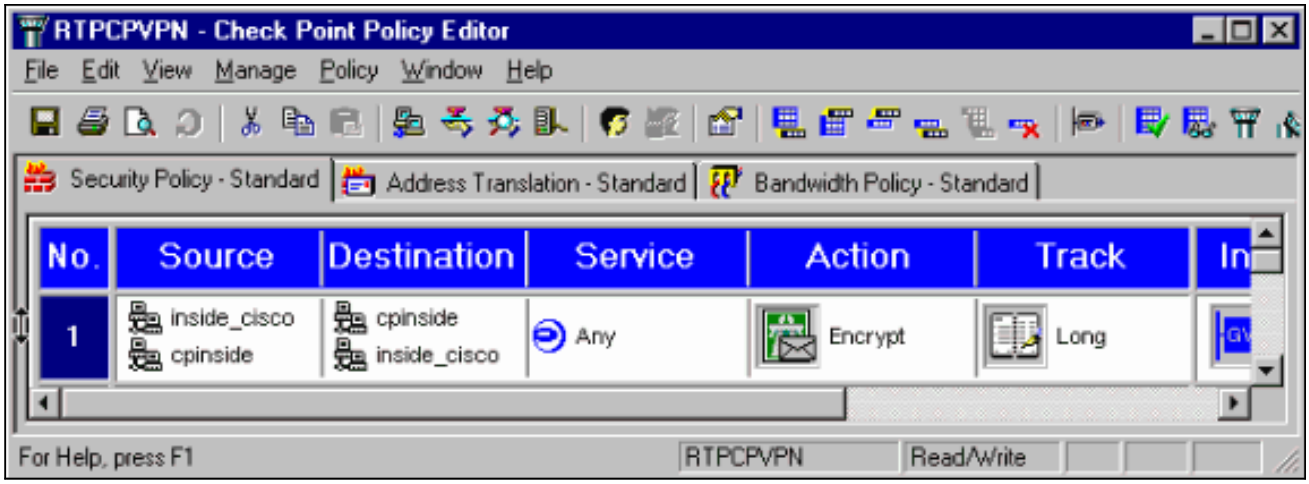
condivisione

13. Fare clic su **Edit Secrets** (Modifica segreti) per impostare la chiave già condivisa in modo che concordi con questo comando PIX:**isakmp** ***chiave*** **indirizzo** ***indirizzo*** **netmask**

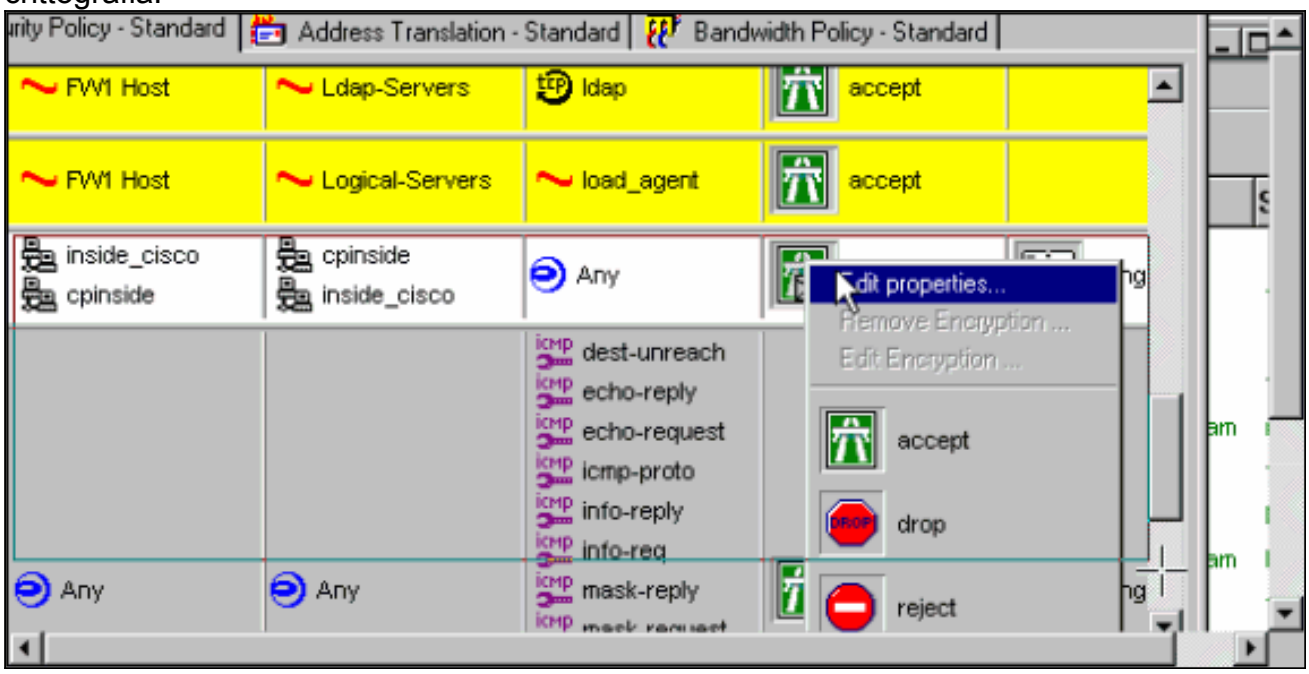


netmask

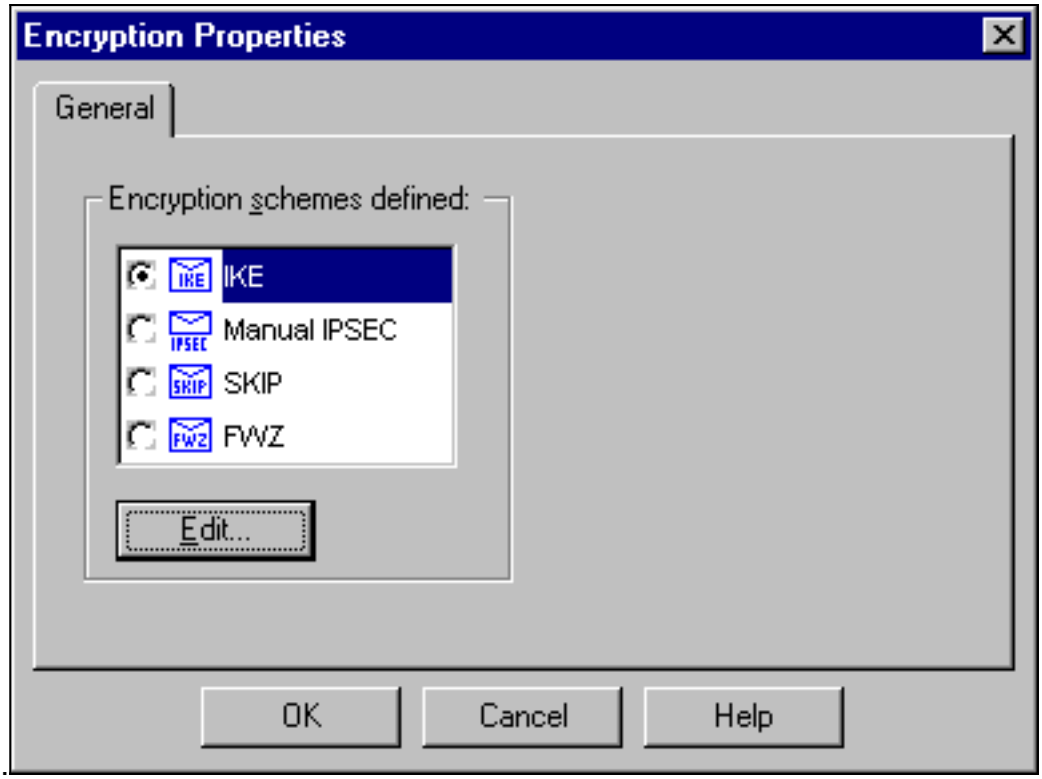
14. Nella finestra Editor dei criteri inserire una regola con Origine e Destinazione come "inside_cisco" e "cpinside" (bidirezionale). Set **Service=Any**, **Action=Encrypt** e **Track=Long**.



15. Sotto l'intestazione Azione, fare clic sull'icona **Encrypt** verde e selezionare **Modifica proprietà** per configurare i criteri di crittografia.

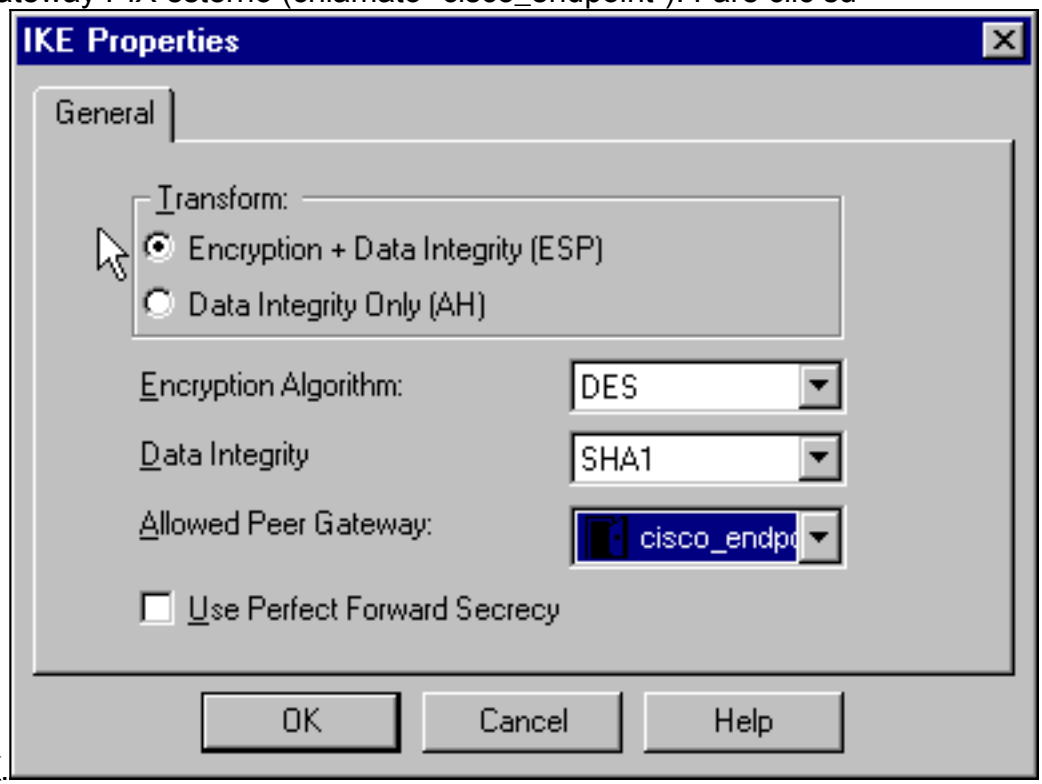


16. Selezionare **IKE**, quindi fare clic su



Modifica.

17. Nella schermata Proprietà IKE, modificare queste proprietà per accettare le trasformazioni IPSec PIX in questo comando:**crypto ipsec transform-set myset esp-des esp-sha-hmac**In Trasforma, selezionare **Crittografia + integrità dei dati (ESP)**. L'algoritmo di crittografia deve essere **DES**, l'integrità dei dati deve essere **SHA1** e il gateway peer consentito deve essere il gateway PIX esterno (chiamato "cisco_endpoint"). Fare clic su



OK.

18. Una volta configurato il checkpoint, selezionare **Policy > Install** (Installa) nel menu Checkpoint per rendere effettive le modifiche.

Comandi debug, show e clear

Le informazioni contenute in questa sezione permettono di verificare che la configurazione

funzioni correttamente.

Alcuni comandi **show sono supportati dallo** strumento Output Interpreter (solo utenti registrati); lo strumento permette di visualizzare un'analisi dell'output del comando **show.**

Prima di usare il comando **debug**, consultare le informazioni importanti sui comandi di debug.

Cisco PIX Firewall

- **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.
- **debug crypto ipsec**: visualizza gli eventi IPSec.
- **show crypto isakmp sa**: visualizza tutte le associazioni di sicurezza IKE (SA) correnti in un peer.
- **show crypto ipsec sa**: visualizza le impostazioni utilizzate dalle associazioni di sicurezza correnti.
- **clear crypto isakmp sa**— (dalla modalità di configurazione) Cancella tutte le connessioni IKE attive.
- **clear crypto ipsec sa**: (dalla modalità di configurazione) elimina tutte le associazioni di protezione IPSec.

Checkpoint:

Poiché il rilevamento è stato impostato su Long nella finestra Editor dei criteri visualizzata al passaggio 14, il traffico negato viene visualizzato in rosso nel Visualizzatore log. Per ottenere un debug più dettagliato, immettere:

```
C:\WINNT\FW1\4.1\fwstop
C:\WINNT\FW1\4.1\fw d -d
```

e in un'altra finestra:

```
C:\WINNT\FW1\4.1\fwstart
```

Nota: si tratta di un'installazione di Microsoft Windows NT.

Èpossibile cancellare le associazioni di protezione sul checkpoint con i seguenti comandi:

```
fw tab -t IKE_SA_table -x
fw tab -t ISAKMP_ESP_table -x
fw tab -t inbound_SPI -x
fw tab -t ISAKMP_AH_table -x
```

e rispondendo **sì** al questionario. .

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Riepilogo della rete

Quando nel dominio di crittografia del checkpoint sono configurate più reti adiacenti all'interno, il dispositivo può riepilogarle automaticamente in relazione al traffico interessante. Se l'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.

Output di esempio del comando debug da PIX

```
cisco_endpoint# show debug
debug crypto ipsec 1
debug crypto isakmp 1
debug crypto engine
debug fover status
        tx      Off
        rx      Off
        open    Off
        cable   Off
        txdmp   Off
        rxdmp   Off
        ifc     Off
        rxip    Off
        txip    Off
        get     Off
        put     Off
        verify  Off
        switch  Off
        fail    Off
        fmsg    Off
cisco_endpoint# term mon
cisco_endpoint#
ISAKMP (0): beginning Quick Mode exchange,
M-ID of 2112882468:7df00724IPSEC(key_engine):
 got a queue event...
IPSEC(spi_response): getting spi 0x9d71f29c(2641490588) for SA
        from  172.18.124.157 to   172.18.124.35 for prot 3
70
crypto_isakmp_process_block: src 172.18.124.157, dest 172.18.124.35
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_IDLE
ISAKMP (0): processing SA payload. message ID = 2112882468

ISAKMP : Checking IPSec proposal 1

ISAKMP: transform 1, ESP_DES
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-SHA
ISAKMP (0): atts are acceptable.IPSEC(validate_proposal_request):
proposal part #1,
```

```
  (key eng. msg.) dest= 172.18.124.157, src= 172.18.124.35,
    dest_proxy= 10.32.50.0/255.255.255.0/0/0 (type=4),
    src_proxy= 192.168.1.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-des esp-sha-hmac ,
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4

ISAKMP (0): processing NONCE payload. message ID = 2112882468

ISAKMP (0): processing ID payload. message ID = 2112882468
ISAKMP (0): processing ID payload. message ID = 2112882468map_alloc_entry:
allocating entry 3
map_alloc_entry: allocating entry 4

ISAKMP (0): Creating IPSec SAs
        inbound SA from  172.18.124.157 to   172.18.124.35 (proxy
      10.32.50.0 to 192.168.1.0)
        has spi 2641490588 and conn_id 3 and flags 4
        lifetime of 28800 seconds
        lifetime of 4608000 kilobytes
        outbound SA from   172.18.124.35 to  172.18.124.157 (proxy
     192.168.1.0 to 10.32.50.0)
        has spi 3955804195 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= 172.18.124.35, src= 172.18.124.157,
    dest_proxy= 192.168.1.0/255.255.255.0/0/0 (type=4),
    src_proxy= 10.32.50.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-des esp-sha-hmac ,
    lifedur= 28800s and 4608000kb,
    spi= 0x9d71f29c(2641490588), conn_id= 3, keysize= 0, flags= 0x4
IPSEC(initialize_sas): ,
  (key eng. msg.) src= 172.18.124.35, dest= 172.18.124.157,
    src_proxy= 192.168.1.0/255.255.255.0/0/0 (type=4),
    dest_proxy= 10.32.50.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-des esp-sha-hmac ,
    lifedur= 28800s and 4608000kb,
    spi= 0xebc8c823(3955804195), conn_id= 4, keysize= 0, flags= 0x4

return status is IKMP_NO_ERROR2303: sa_request, (key eng. msg.)
src= 172.18.124.35, dest= 172.18.124.157,
src_proxy= 192.168.1.0/255.255.255.0/0/0 (type=4), dest_proxy=
10.32.50.0/255.255.255.0/0/0 (type=4),
protocol= ESP,
transform= esp-des esp-sha-hmac , lifedur= 28800s and 4608000kb,
spi= 0x0(0), conn_id= 0, keysize= 0,
flags= 0x4004

602301: sa created, (sa) sa_dest= 172.18.124.35, sa_prot= 50, sa_spi=
0x9d71f29c(2641490588),
sa_trans= esp-des esp-sha-hmac , sa_conn_id= 3

602301: sa created, (sa) sa_dest= 172.18.124.157, sa_prot= 50, sa_spi=
0xebc8c823(3955804195),
sa_trans= esp-des esp-sha-hmac , sa_conn_id= 4

cisco_endpoint# sho cry ips sa

interface: outside
    Crypto map tag: rtpmap, local addr. 172.18.124.35

   local  ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
```

```
current_peer: 172.18.124.157
  PERMIT, flags={origin_is_acl,}
 #pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0
 #pkts decaps: 0, #pkts decrypt: 0, #pkts verify 0
 #pkts compressed: 0, #pkts decompressed: 0
 #pkts not compressed: 0, #pkts compr. failed: 0,
 #pkts decompress failed: 0 #send errors 0, #recv errors 0

  local crypto endpt.: 172.18.124.35,
  remote crypto endpt.: 172.18.124.157
  path mtu 1500, ipsec overhead 0, media mtu 1500
  current outbound spi: 0

  inbound esp sas:

  inbound ah sas:

  inbound pcp sas:

  outbound esp sas:

  outbound ah sas:

  outbound pcp sas:

local  ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (10.32.50.0/255.255.255.0/0/0)
current_peer: 172.18.124.157
  PERMIT, flags={origin_is_acl,}
 #pkts encaps: 4, #pkts encrypt: 4, #pkts digest 4
 #pkts decaps: 4, #pkts decrypt: 4, #pkts verify 4
 #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.: 172.18.124.35, remote crypto endpt.: 172.18.124.157
  path mtu 1500, ipsec overhead 56, media mtu 1500
  current outbound spi: ebc8c823

  inbound esp sas:
   spi: 0x9d71f29c(2641490588)
     transform: esp-des esp-sha-hmac ,
     in use settings ={Tunnel, }
     slot: 0, conn id: 3, crypto map: rtpmap
     sa timing: remaining key lifetime (k/sec): (4607999/28777)
     IV size: 8 bytes
     replay detection support: Y

  inbound ah sas:

  inbound pcp sas:

  outbound esp sas:
   spi: 0xebc8c823(3955804195)
     transform: esp-des esp-sha-hmac ,
     in use settings ={Tunnel, }
     slot: 0, conn id: 4, crypto map: rtpmap
     sa timing: remaining key lifetime (k/sec): (4607999/28777)
     IV size: 8 bytes
     replay detection support: Y

  outbound ah sas:

  outbound pcp sas:
```

```
cisco_endpoint# sho cry is sa
        dst             src         state     pending    created
  172.18.124.157   172.18.124.35    QM_IDLE         0          2
```

Informazioni correlate

- Pagina di supporto PIX
- Informazioni di riferimento sui comandi PIX
- RFC (Requests for Comments)
- Configurazione di IPSec Network Security
- Configurazione del protocollo di protezione di Internet Key Exchange
- PIX 5.2: Configurazione di IPSec
- PIX 5.3: Configurazione di IPSec
- Pagina di supporto per IPSec
- Supporto tecnico – Cisco Systems