Configurazione di un tunnel IPsec - Cisco VPN 5000 Concentrator su firewall Checkpoint 4.1

Sommario

Introduzione
Prerequisiti
Requisiti
Componenti usati
Convenzioni
Configurazione
Esempio di rete
Configurazioni
Firewall checkpoint 4.1
Verifica
Risoluzione dei problemi
Comandi per la risoluzione dei problemi di VPN 5000 Concentrator
Riepilogo della rete
Debug del firewall di Checkpoint 4.1
Output di esempio del comando debug
Informazioni correlate

Introduzione

In questo documento viene illustrato come formare un tunnel IPsec con chiavi già condivise per collegarsi a due reti private. Si unisce a una rete privata all'interno di Cisco VPN 5000 Concentrator (192.168.1.x) e a una rete privata all'interno del firewall di Checkpoint 4.1 (10.32.50.x). Si presume che il traffico tra l'interno del concentratore VPN e il checkpoint e diretto a Internet (rappresentato in questo documento dalle reti 172.18.124.x) scorra prima di avviare 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:

- Cisco VPN 5000 Concentrator
- Cisco VPN 5000 Concentrator software versione 5.2.19.0001
- 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

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

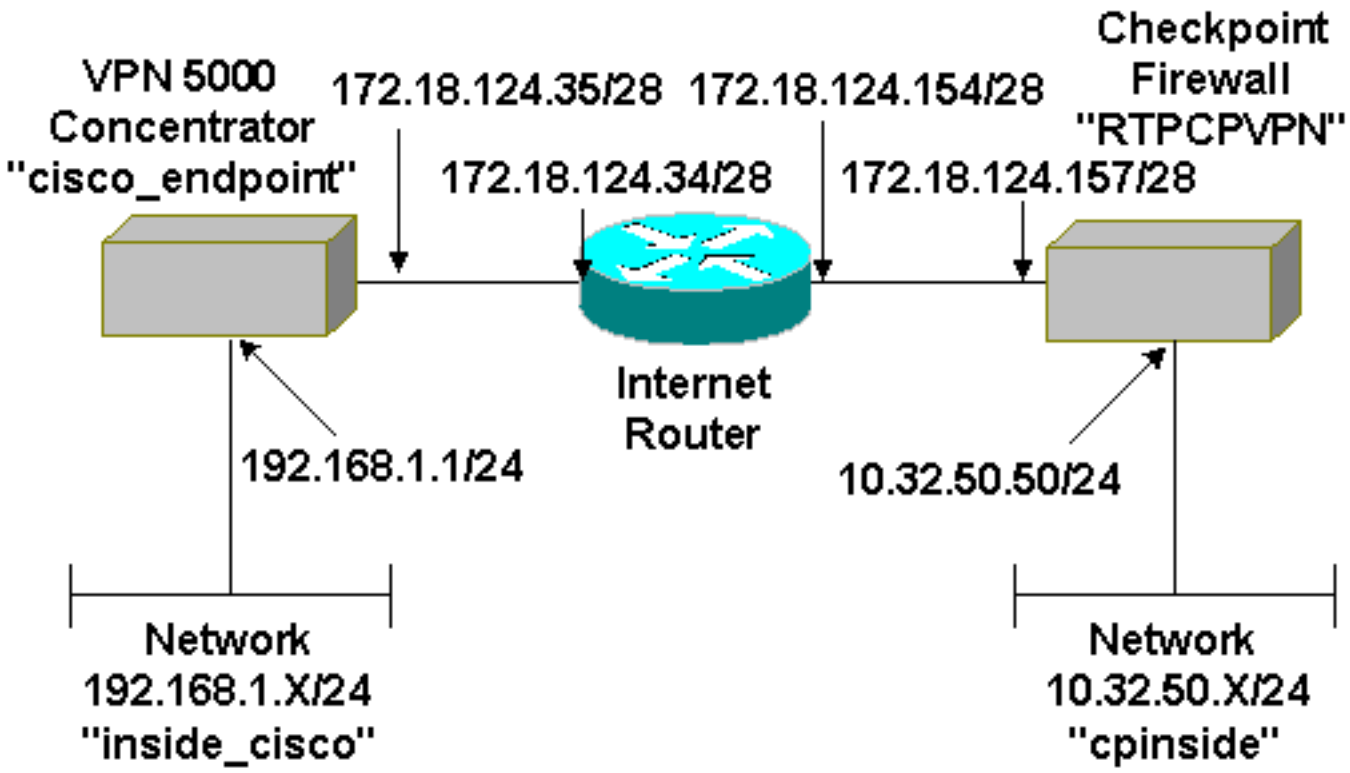
Configurazione

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 questa impostazione di rete:



Configurazioni

Nel documento viene usata questa configurazione.

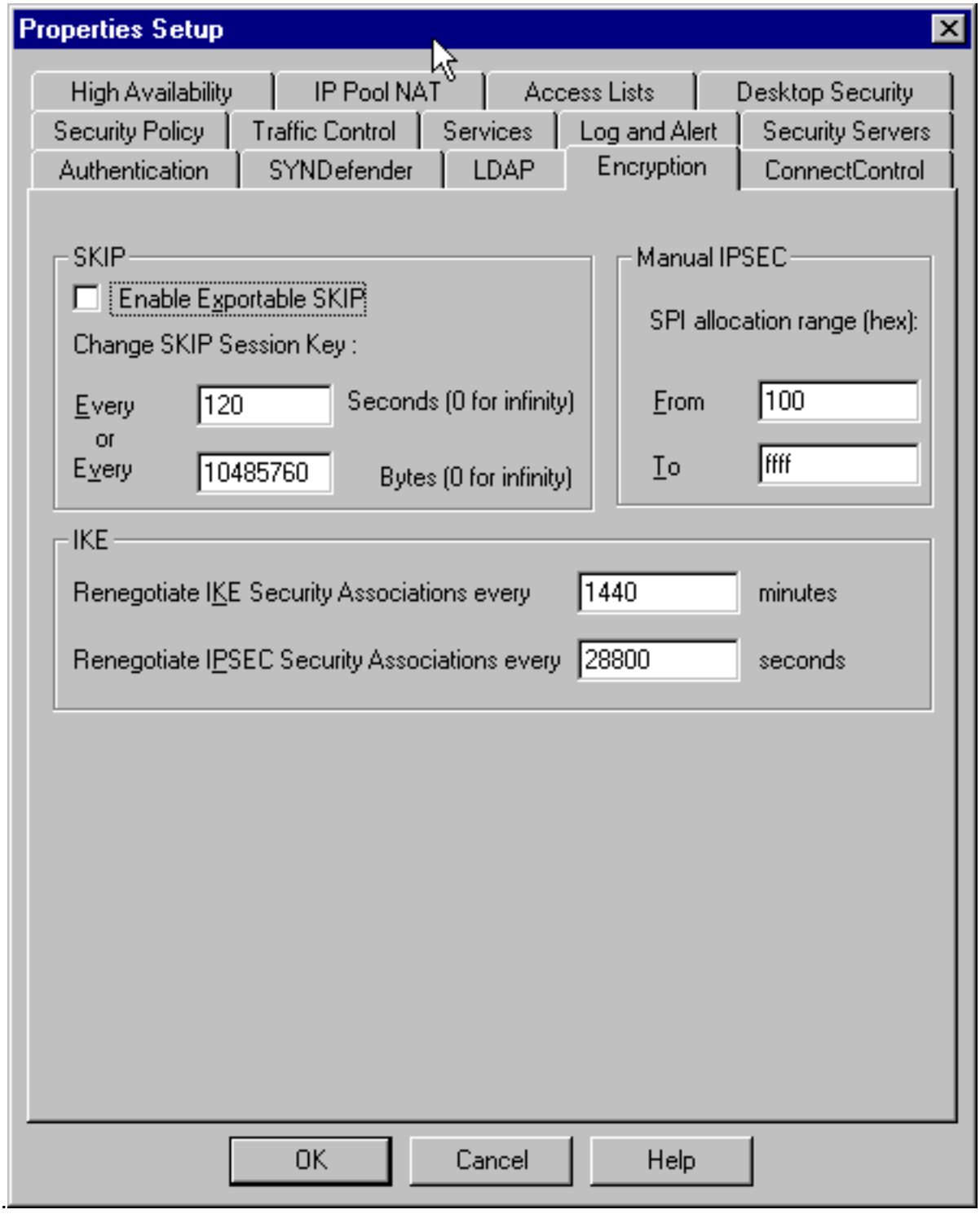
Cisco VPN 5000 Concentrator

```
[ IP Ethernet 0:0 ]
Mode                    = Routed
SubnetMask              = 255.255.255.0
IPAddress               = 192.168.1.1

[ General ]
EthernetAddress         = 00:00:a5:e9:c8:00
DeviceType              = VPN 5002/8 Concentrator
ConfiguredOn            = Timeserver not configured
ConfiguredFrom          = Command Line, from Console
DeviceName              = "cisco_endpoint"
IPSecGateway            = 172.18.124.34

[ IKE Policy ]
Protection              = SHA_DES_G2

[ Tunnel Partner VPN 1 ]
KeyLifeSecs             = 28800
LocalAccess             = "192.168.1.0/24"
Peer                    = "10.32.50.0/24"
BindTo                  = "ethernet 1:0"
SharedKey               = "ciscorules"
KeyManage               = Auto
Transform               = esp(sha,des)
Partner                 = 172.18.124.157
Mode                    = Main

[ IP VPN 1 ]
Numbered                = Off
Mode                    = Routed

[ IP Ethernet 1:0 ]
IPAddress               = 172.18.124.35
SubnetMask              = 255.255.255.240
Mode                    = Routed

[ IP Static ]
10.32.50.0 255.255.255.0 VPN 1 1

Configuration size is 1131 out of 65500 bytes.
```

Firewall checkpoint 4.1

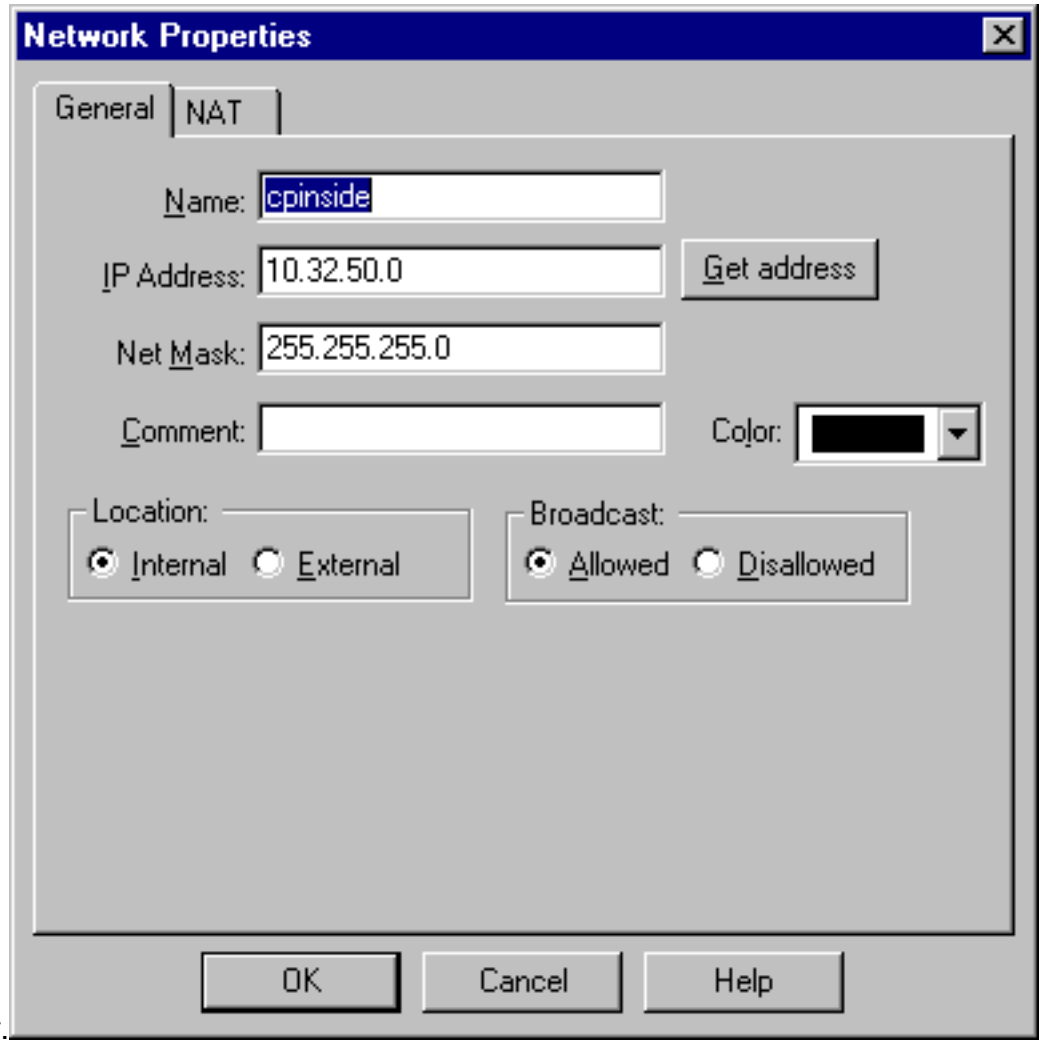
Completare la procedura seguente per configurare il firewall di Checkpoint 4.1.

1. Selezionare **Proprietà > Crittografia** per impostare la durata di IPSec del checkpoint in modo che corrisponda al comando **KeyLifeSecs = 28800** VPN Concentrator.**Nota:** lasciare invariata la durata predefinita di Scambio chiave Internet (IKE) del punto di



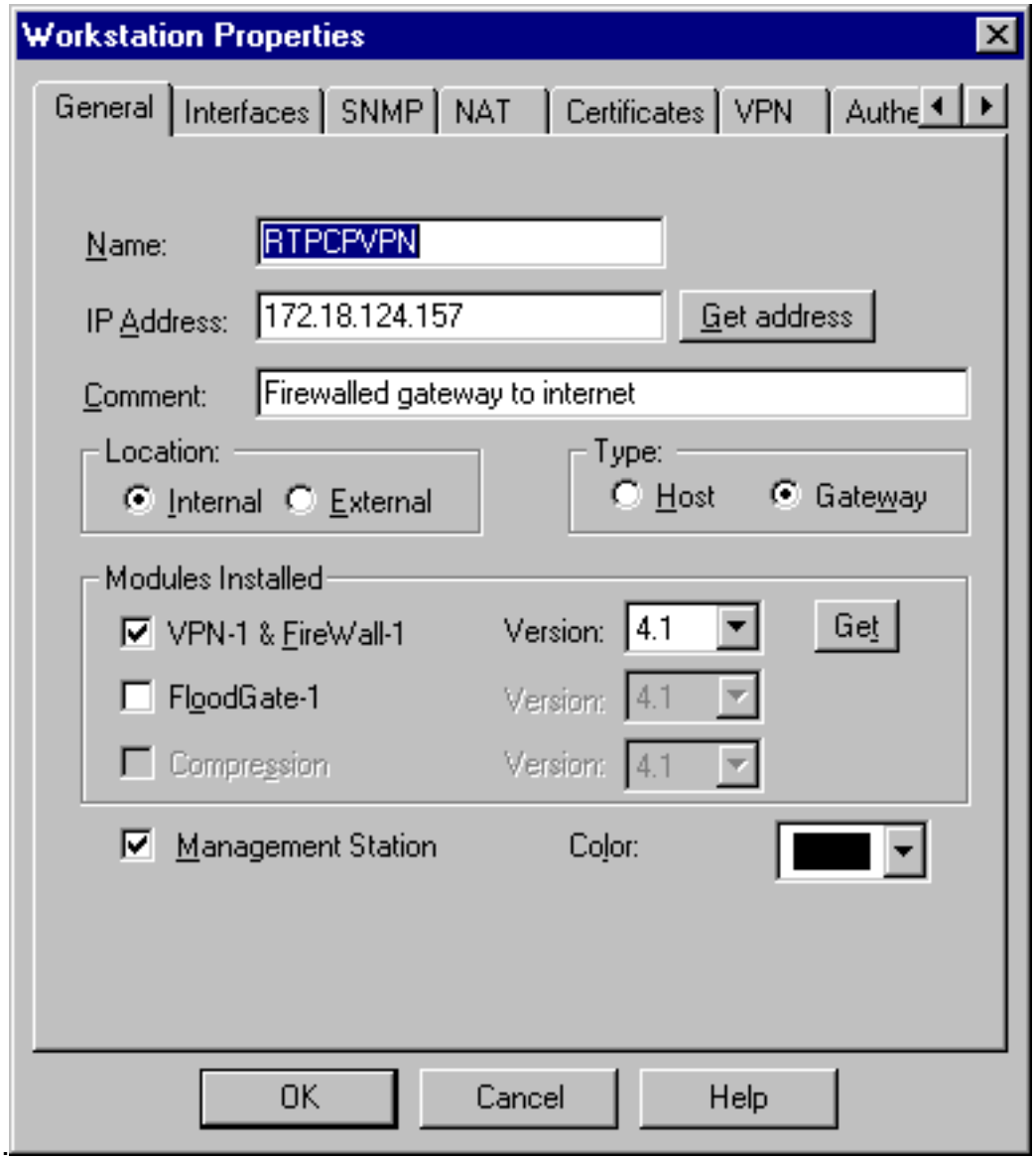
controllo.

2. Selezionare **Gestisci > Oggetti di rete > Nuovo (o Modifica) > Rete** per configurare l'oggetto per la rete interna ("cpinside") dietro il checkpoint. In questo caso, il comando deve essere **Peer = "10.32.50.0/24"** VPN



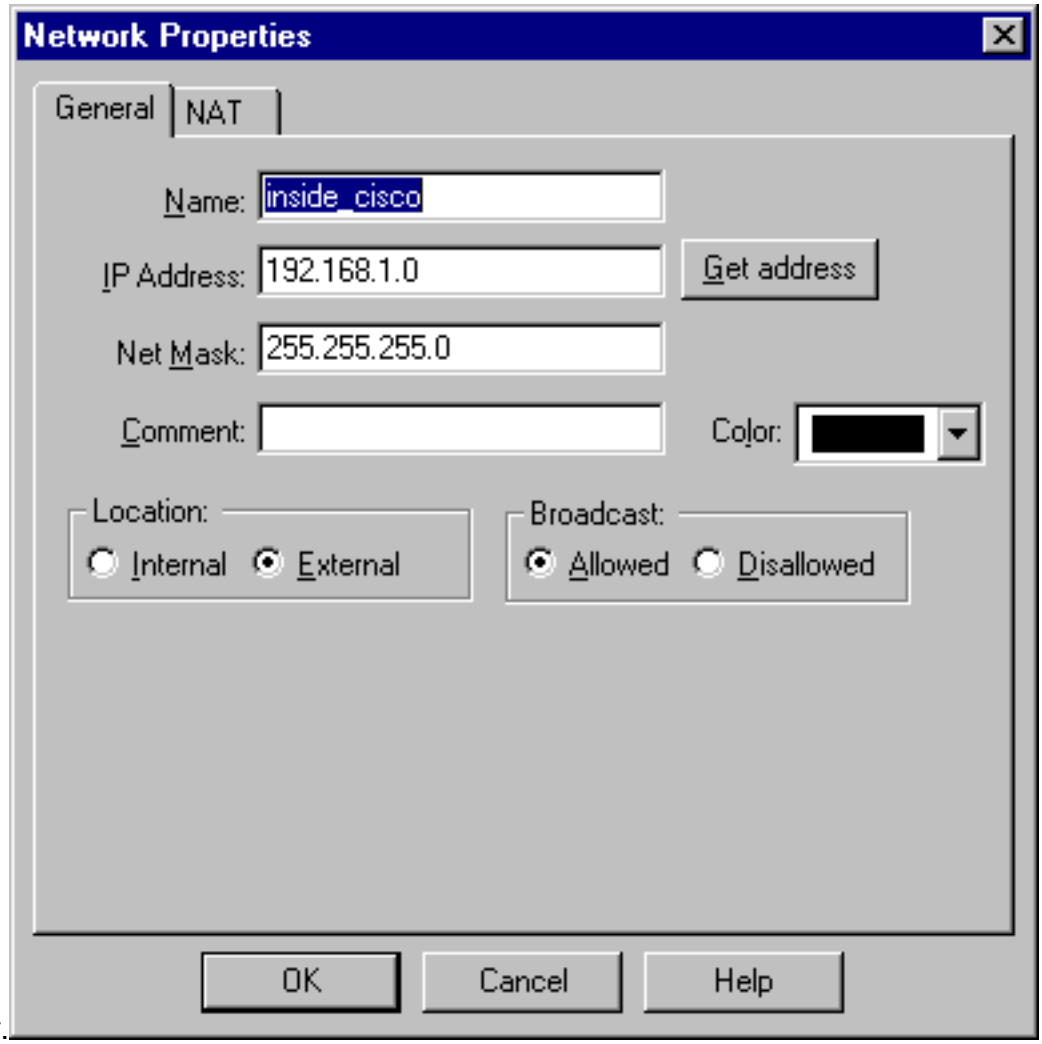
Concentrator.

3. Selezionare **Gestisci > Oggetti di rete > Modifica** per modificare l'oggetto per l'endpoint gateway (checkpoint "RTPCPVPN") a cui punta il concentratore VPN nel comando **Partner = <ip>**.Selezionare **Interno** in Posizione.Selezionare **Gateway** per Type (Tipo di gateway).Controllare **VPN-1 e FireWall-1** e la **stazione di gestione** sotto Moduli



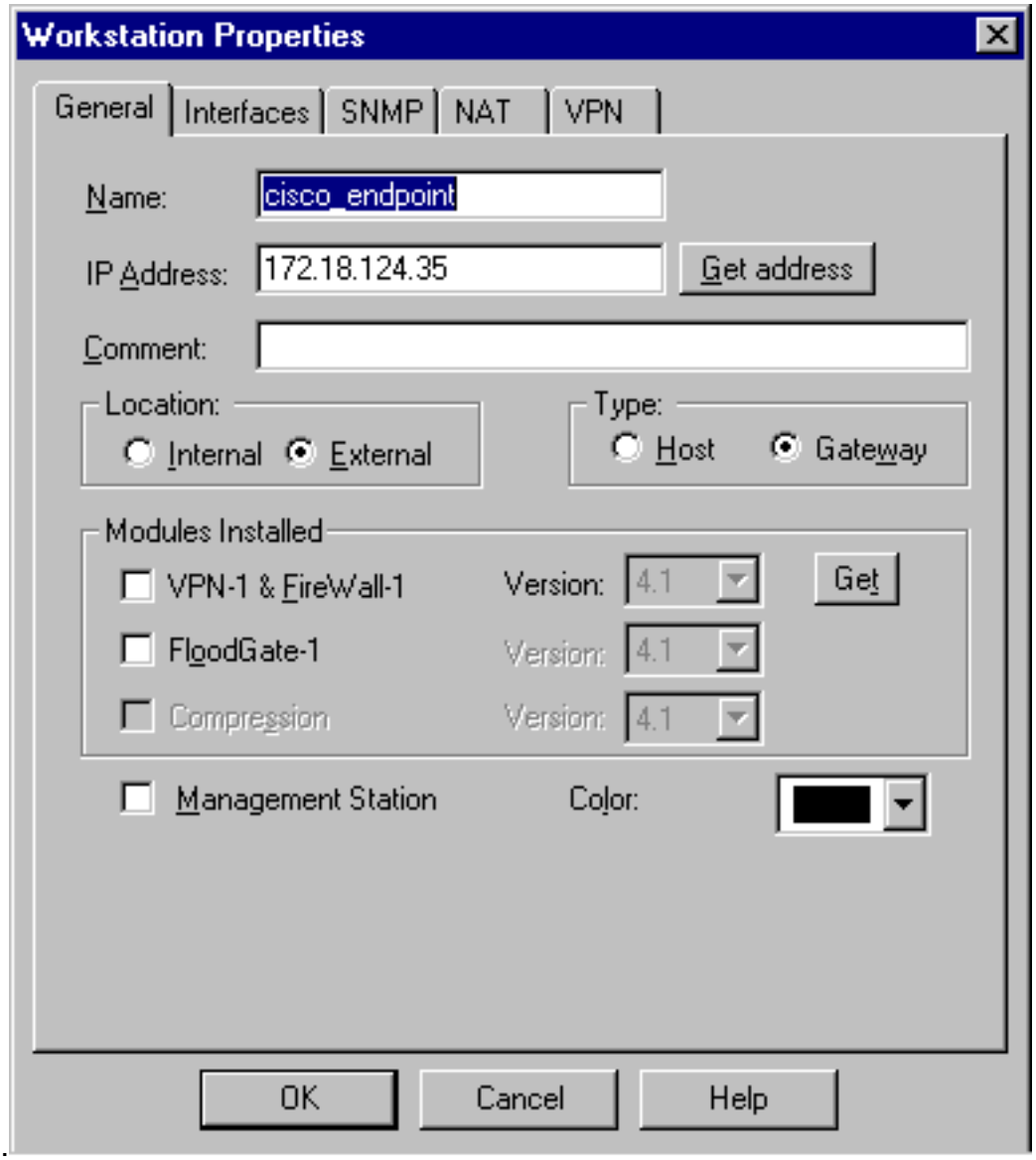
installati.

4. Selezionare **Gestisci > Oggetti di rete > Nuovo (o Modifica) > Rete** per configurare l'oggetto per la rete esterna ("inside_cisco") dietro al concentratore VPN.In questo caso, si deve accettare il comando **LocalAccess = <192.168.1.0/24>** VPN

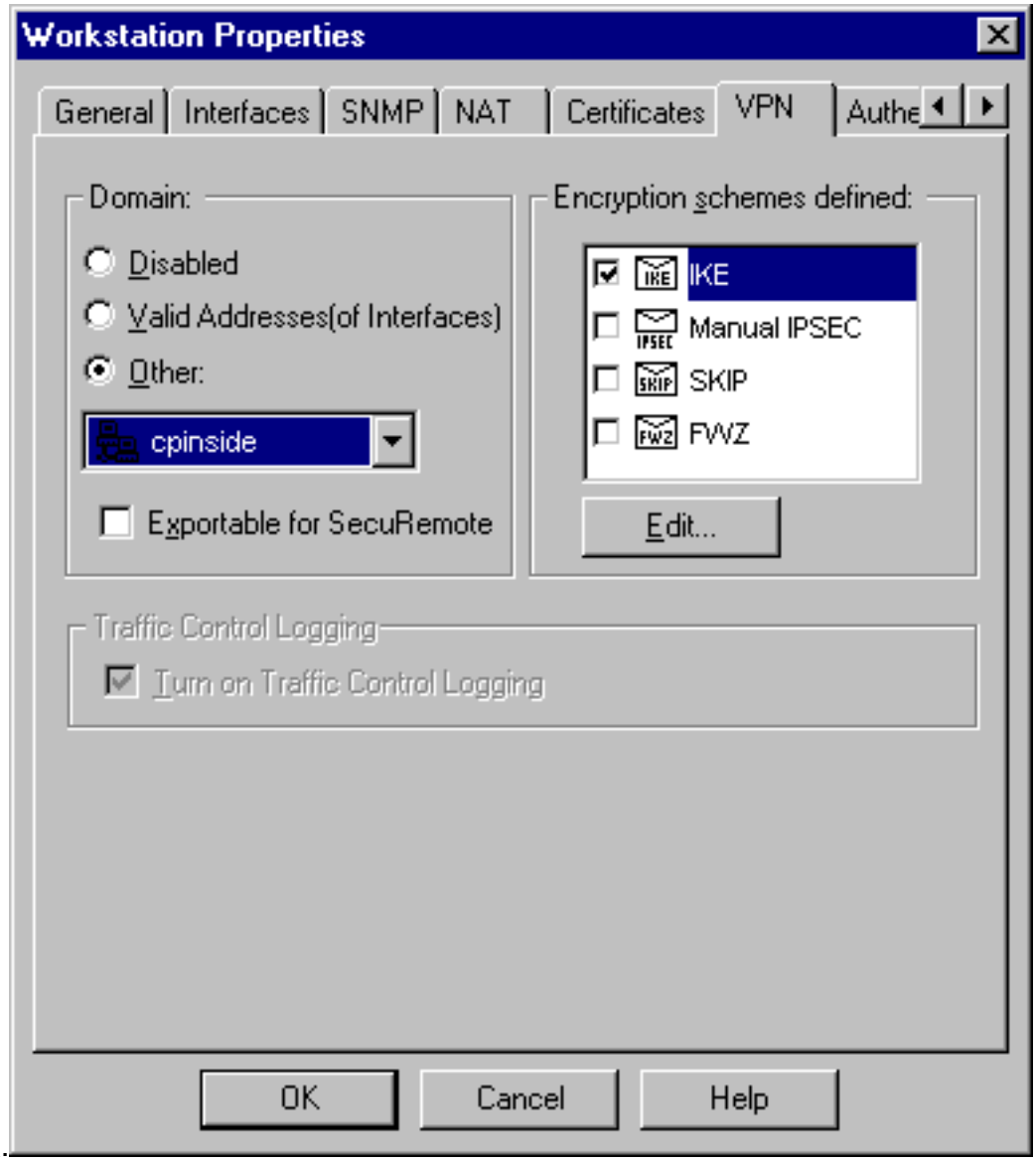


Concentrator.

5. Selezionare **Gestisci > Oggetti di rete > Nuovo > Workstation** per aggiungere un oggetto per il gateway VPN Concentrator esterno ("cisco_endpoint").Questa è l'interfaccia "esterna" del concentratore VPN con connettività al checkpoint (in questo documento, 172.18.124.35 è l'indirizzo IP nel comando **IPAddress = <ip>**).Selezionare **Esterno** in Posizione. Selezionare **Gateway** per Type (Tipo di gateway).**Nota:** non selezionare VPN-1/FireWall-

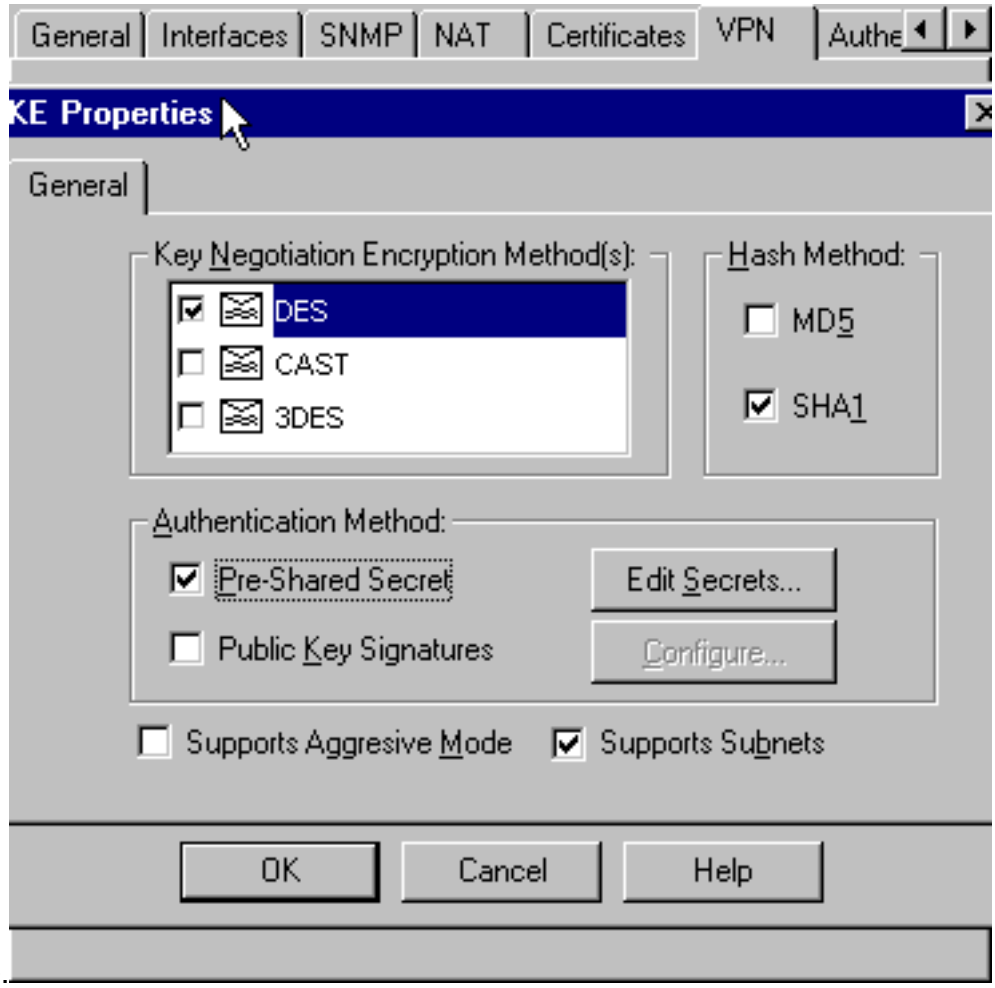
1. 

6. Selezionare **Gestisci > Oggetti di rete > Modifica** per modificare la scheda VPN dell'endpoint del gateway del checkpoint (chiamata "RTPCPVPN"). 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



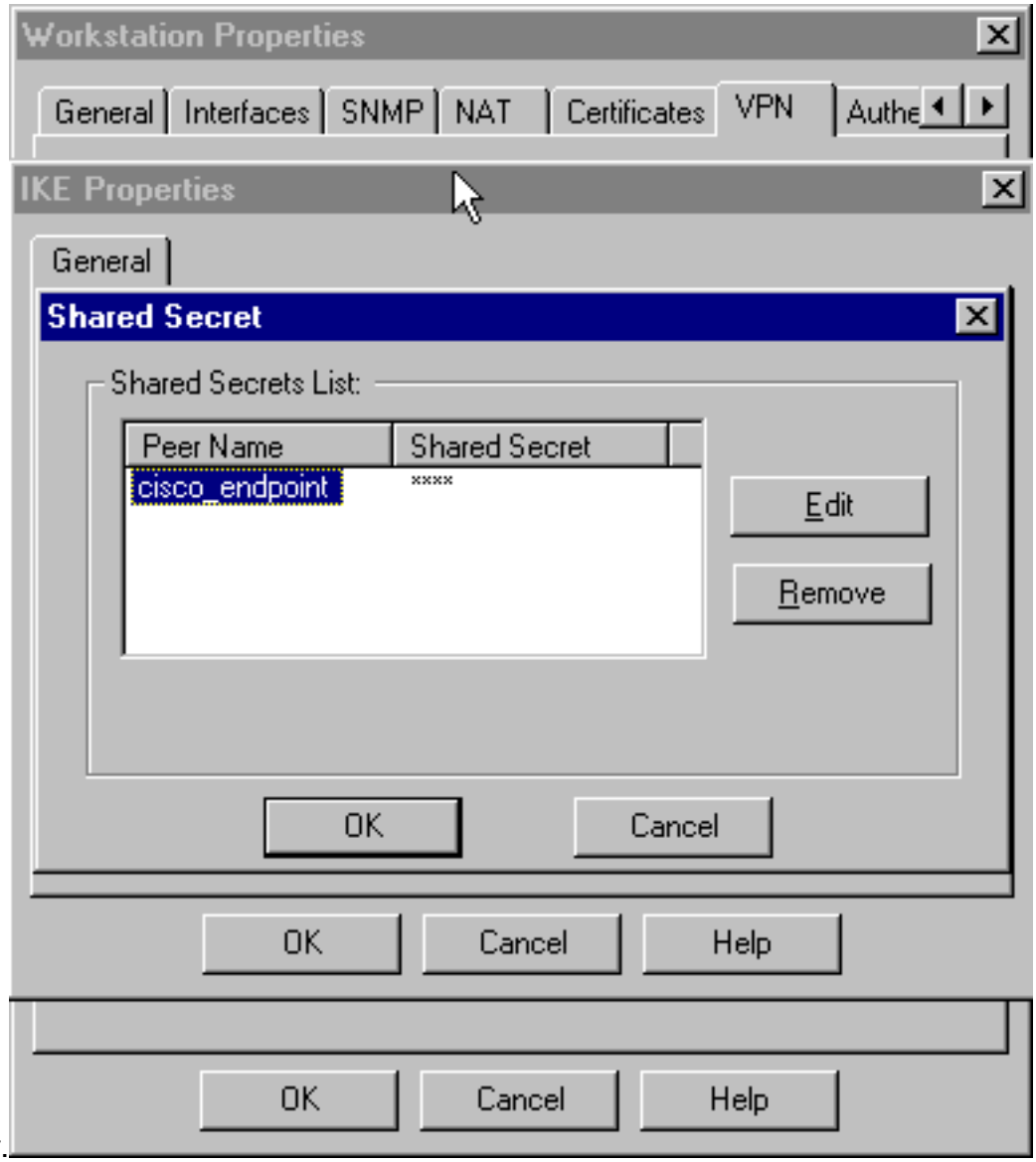
Modifica.

7. Modificare le proprietà IKE in crittografia **DES** e hashing **SHA1** per accettare il comando **SHA_DES_G2** VPN Concentrator.**Nota:** la sigla "G2" si riferisce al gruppo Diffie-Hellman 1 o 2. Durante il test è stato rilevato che il checkpoint accetta "G2" o "G1".Cambia le impostazioni:Deselezionare **Modalità aggressiva**.Selezionare **Supporta le subnet**.Selezionare **Segreto precondiviso** in Metodo di



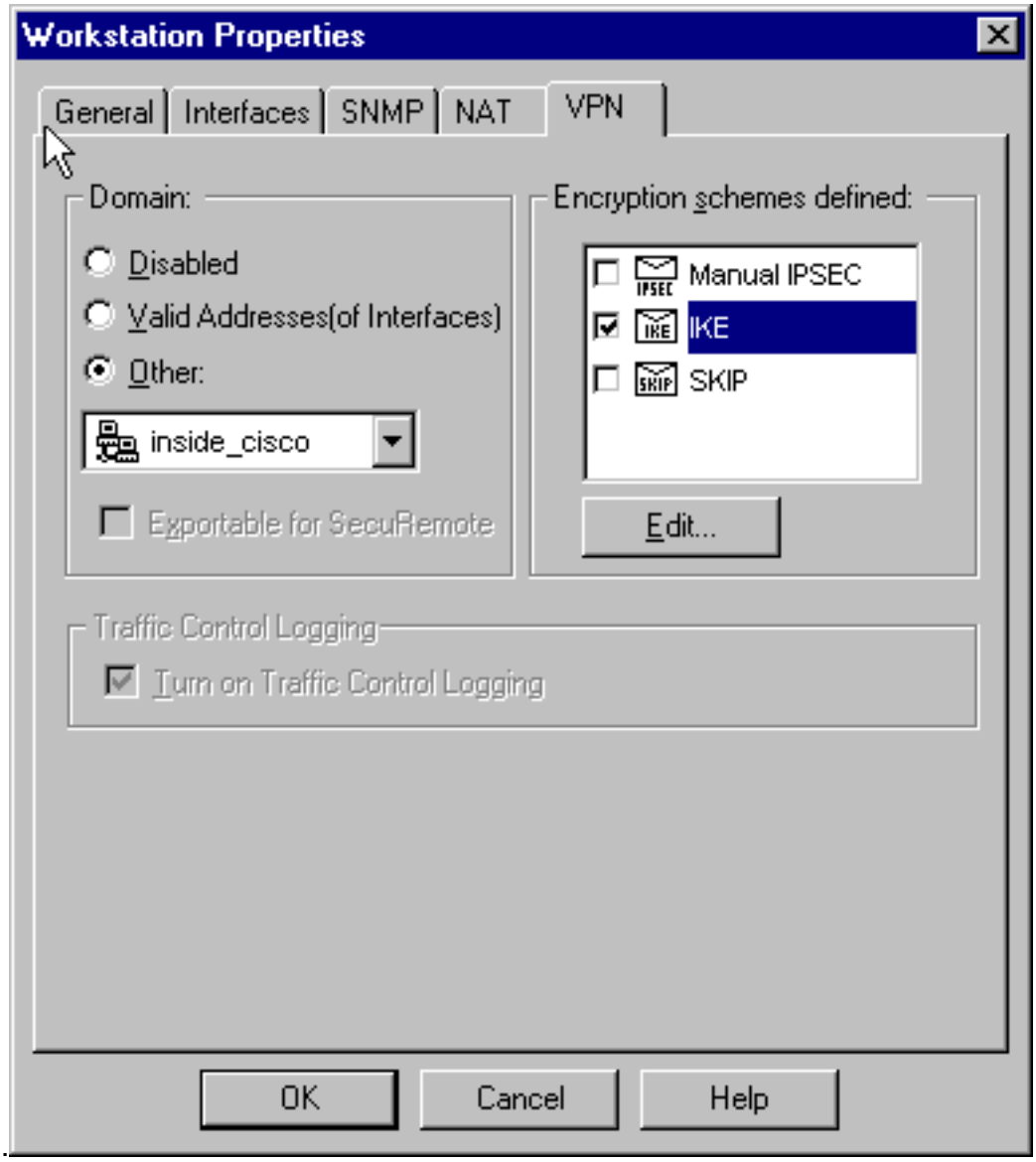
autenticazione.

8. Fare clic su **Edit Secrets** (Modifica segreti) per impostare la chiave già condivisa in modo che accetti il comando **SharedKey = <key>** VPN



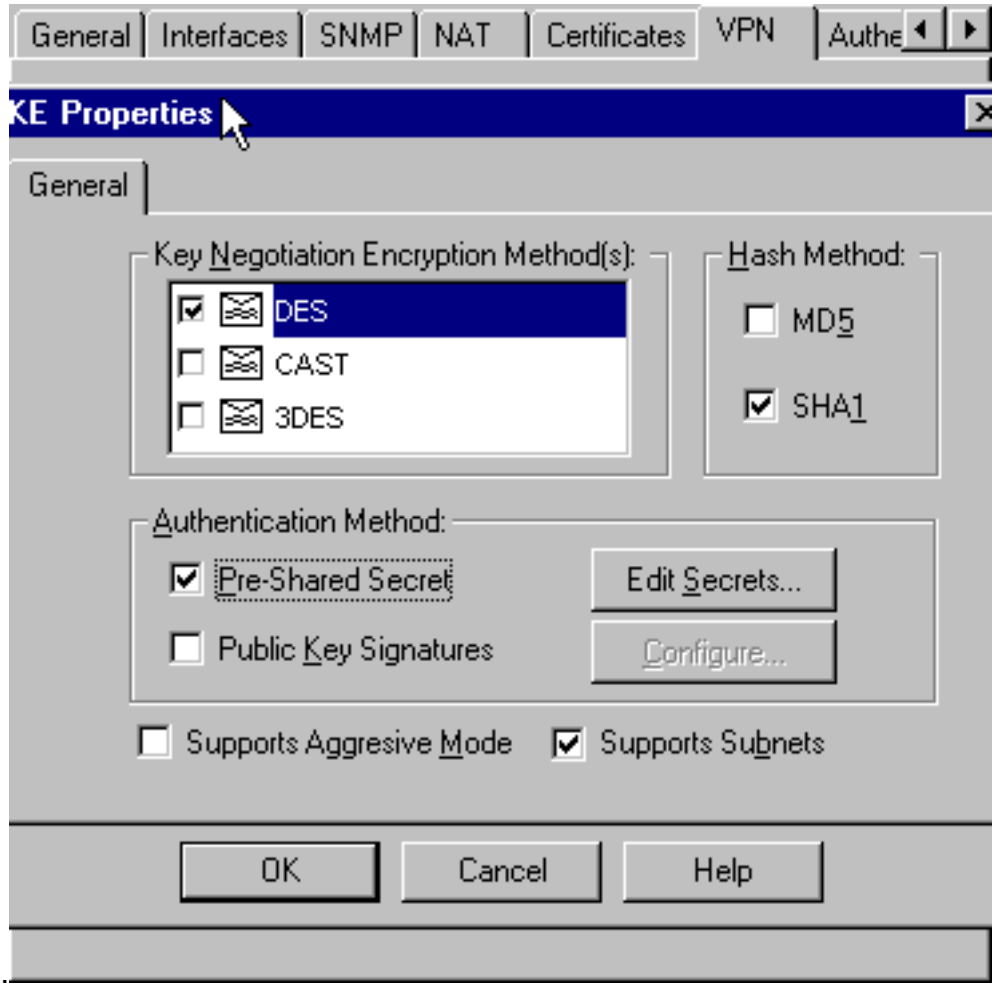
Concentrator.

9. Selezionare **Gestisci > Oggetti di rete > Modifica** per modificare la scheda VPN "cisco_endpoint". In Dominio selezionare **Altro**, quindi selezionare l'interno della rete VPN Concentrator (denominata "inside_cisco"). In Definizione schemi di crittografia selezionare **IKE**, quindi fare clic su



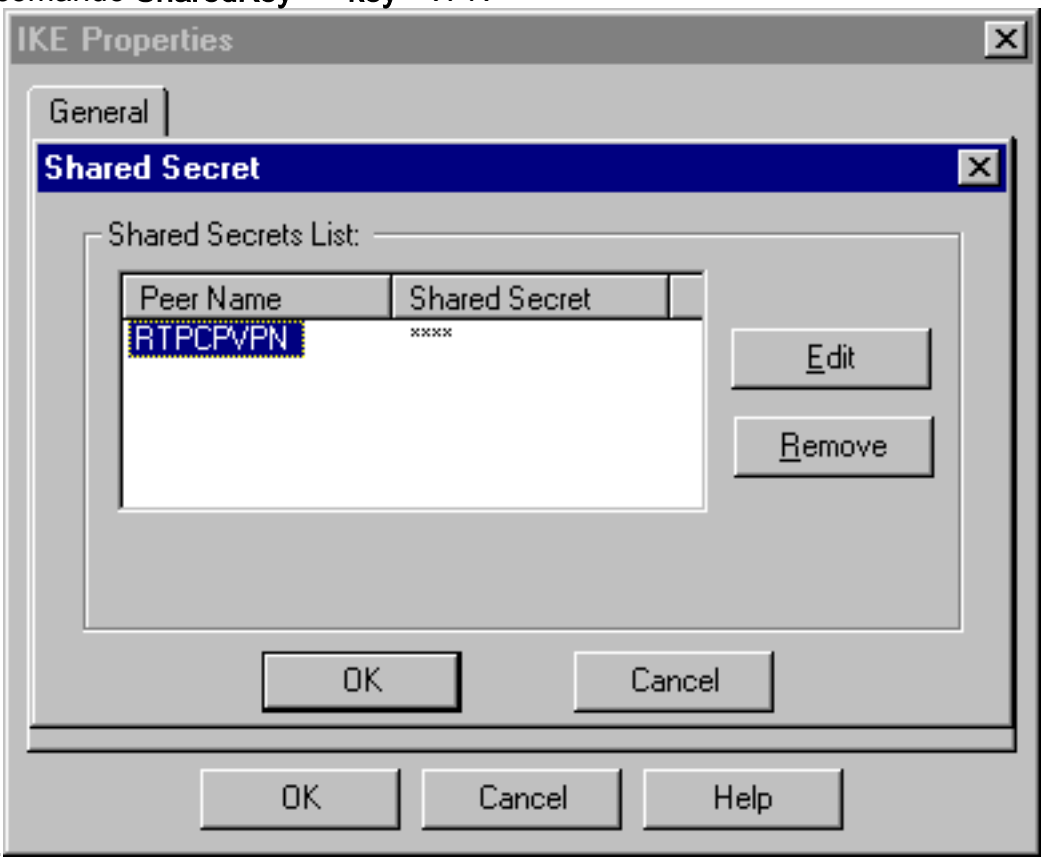
Modifica.

10. Modificare le proprietà IKE in crittografia **DES** e hashing **SHA1** per accettare il comando **SHA_DES_G2** VPN Concentrator.**Nota:** la sigla "G2" si riferisce al gruppo Diffie-Hellman 1 o 2. Durante il test, è stato rilevato che il checkpoint accetta "G2" o "G1".Cambia le impostazioni:Deselezionare **Modalità aggressiva**.Selezionare **Supporta le subnet**.Selezionare **Segreto precondiviso** in Metodo di



autenticazione.

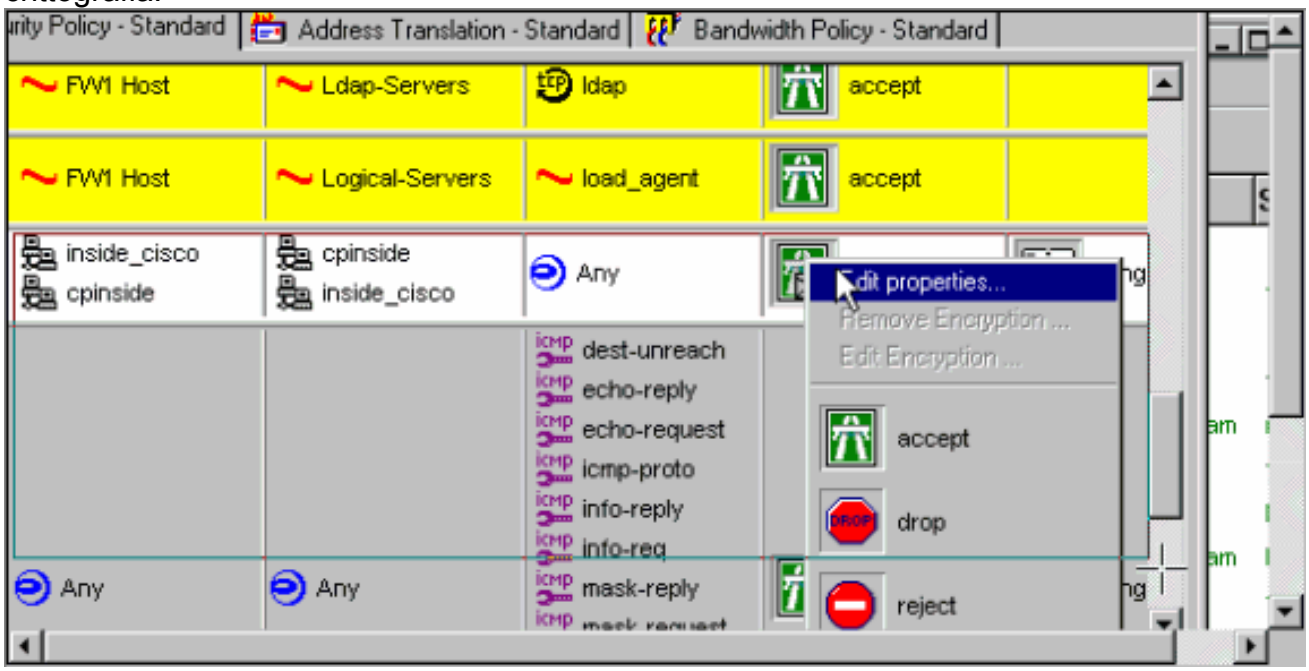
11. Fare clic su **Edit Secrets** (Modifica segreti) per impostare la chiave già condivisa in modo che accetti il comando **SharedKey = <key>** VPN



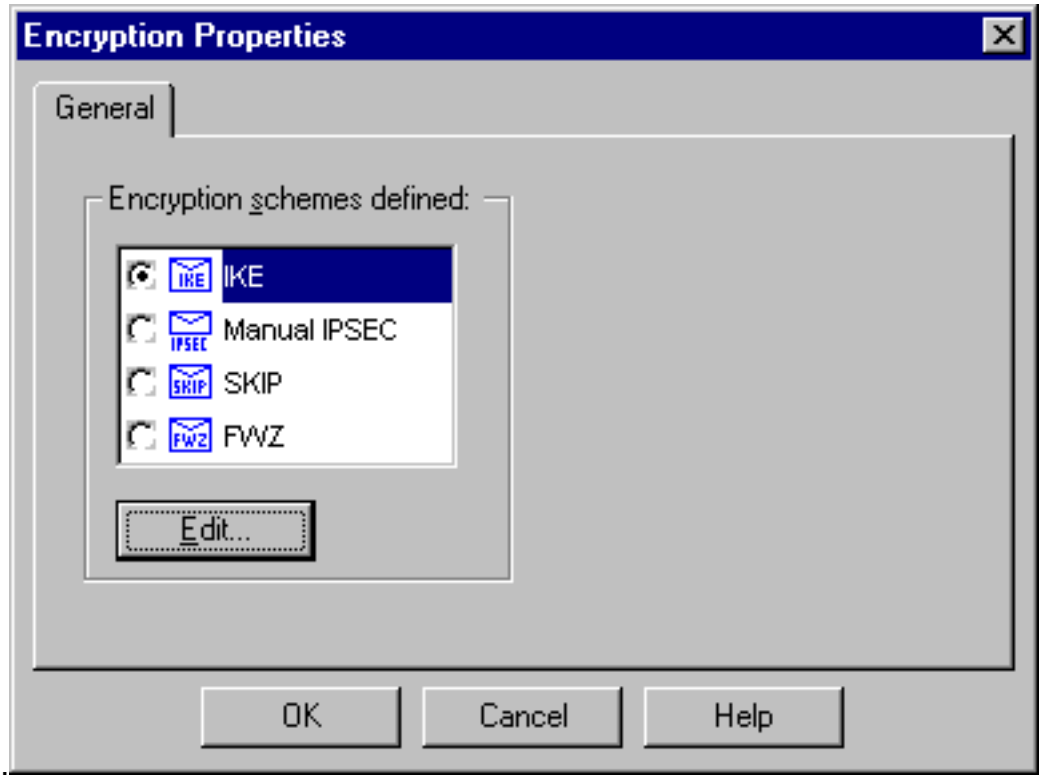
Concentrator.

12. 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**.

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

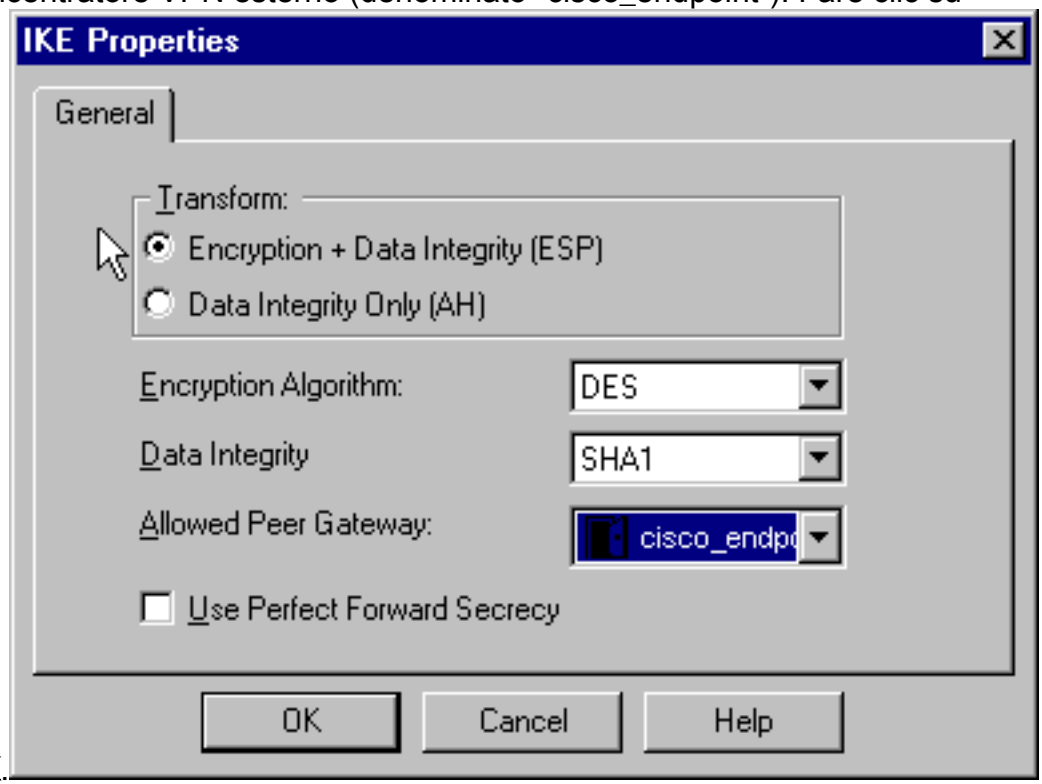


14. Selezionare **IKE**, quindi fare clic su



Modifica.

15. Nella finestra Proprietà IKE modificare queste proprietà in modo che corrispondano al comando **Transform = esp(sha,des)** VPN Concentrator.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 del concentratore VPN esterno (denominato "cisco_endpoint"). Fare clic su



OK.

16. Dopo aver configurato il checkpoint, selezionare **Criterio > Installa** nel menu del checkpoint per rendere effettive le modifiche.

Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

Risoluzione dei problemi

Comandi per la risoluzione dei problemi di VPN 5000 Concentrator

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**.

- **vpn trace dump all**: visualizza le informazioni su tutte le connessioni VPN corrispondenti, incluse le informazioni sull'ora, il numero VPN, l'indirizzo IP reale del peer, gli script eseguiti e, in caso di errore, la routine e il numero di riga del codice software in cui si è verificato l'errore.
- **show system log buffer**: visualizza il contenuto del log buffer interno.
- **show vpn statistics**: visualizza queste informazioni per utenti, partner e il totale di entrambi. Per i modelli modulari, il display include una sezione per ogni slot del modulo. Fare riferimento alla sezione Output di esempio del comando debug.)`Attivo corrente (Current Active)` - Connessioni attive correnti.`In Negot` - Connessioni attualmente in fase di negoziazione.`Acqua alta (High Water)` - Numero massimo di connessioni attive simultanee dall'ultimo riavvio.`Totale parziale`: il numero totale di connessioni riuscite dall'ultimo riavvio.`Tunnel OK`: il numero di tunnel per i quali non si sono verificati errori.`Tunnel Starts`: il numero di avvii del tunnel.`Errore tunnel`: il numero di tunnel con errori.
- **show vpn statistics verbose**: visualizza le statistiche di negoziazione ISAKMP e molte altre statistiche di connessione attive.

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 VPN Concentrator non è configurato per la corrispondenza, è probabile che il tunnel non riesca. 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.

Debug del firewall di Checkpoint 4.1

Si tratta di un'installazione di Microsoft Windows NT. Poiché il rilevamento è stato impostato per `Long` nella finestra Editor dei criteri (come illustrato nel passaggio 12), il traffico negato dovrebbe essere visualizzato in rosso nel Visualizzatore log. Per ottenere un debug più dettagliato, procedere come segue:

```
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
```

Utilizzare i seguenti comandi per cancellare le associazioni di sicurezza (SA) sul checkpoint:

```
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
```

Rispondi **sì** al `messaggio. .`

Output di esempio del comando debug

```
cisco_endpoint#vpn trac dump all
         4 seconds -- stepmngr trace enabled --
   new script: lan-lan primary initiator for <no id> (start)
manage @ 38 seconds :: lan-lan-VPN0:1:[172.18.124.157] (start)
         38 seconds doing l2lp_init, (0 @ 0)
         38 seconds doing l2lp_do_negotiation, (0 @ 0)
   new script: ISAKMP secondary Main for lan-lan-VPN0:1:[172.18.124.157] (start)
         38 seconds doing isa_i_main_init, (0 @ 0)
manage @ 38 seconds :: lan-lan-VPN0:1:[172.18.124.157] (done)
manage @ 38 seconds :: lan-lan-VPN0:1:[172.18.124.157] (start)
         38 seconds doing isa_i_main_process_pkt_2, (0 @ 0)
manage @ 38 seconds :: lan-lan-VPN0:1:[172.18.124.157] (done)
manage @ 38 seconds :: lan-lan-VPN0:1:[172.18.124.157] (start)
         38 seconds doing isa_i_main_process_pkt_4, (0 @ 0)
manage @ 38 seconds :: lan-lan-VPN0:1:[172.18.124.157] (done)
manage @ 39 seconds :: lan-lan-VPN0:1:[172.18.124.157] (start)
         39 seconds doing isa_i_main_process_pkt_6, (0 @ 0)
         39 seconds doing isa_i_main_last_op, (0 @ 0)
   end script: ISAKMP secondary Main for lan-lan-VPN0:1:[172.18.124.157], (0 @ 0)
   next script: lan-lan primary initiator for lan-lan-VPN0:1:[172.18.124.157], (0 @ 0)
         39 seconds doing l2lp_phase_1_done, (0 @ 0)
         39 seconds doing l2lp_start_phase_2, (0 @ 0)
   new script: phase 2 initiator for lan-lan-VPN0:1:[172.18.124.157] (start)
         39 seconds doing iph2_init, (0 @ 0)
         39 seconds doing iph2_build_pkt_1, (0 @ 0)
         39 seconds doing iph2_send_pkt_1, (0 @ 0)
manage @ 39 seconds :: lan-lan-VPN0:1:[172.18.124.157] (done)
manage @ 39 seconds :: lan-lan-VPN0:1:[172.18.124.157] (start)
         39 seconds doing iph2_pkt_2_wait, (0 @ 0)
         39 seconds doing ihp2_process_pkt_2, (0 @ 0)
         39 seconds doing iph2_build_pkt_3, (0 @ 0)
         39 seconds doing iph2_config_SAs, (0 @ 0)
         39 seconds doing iph2_send_pkt_3, (0 @ 0)
         39 seconds doing iph2_last_op, (0 @ 0)
   end script: phase 2 initiator for lan-lan-VPN0:1:[172.18.124.157], (0 @ 0)
   next script: lan-lan primary initiator for lan-lan-VPN0:1:[172.18.124.157], (0 @ 0)
         39 seconds doing l2lp_open_tunnel, (0 @ 0)
         39 seconds doing l2lp_start_i_maint, (0 @ 0)
   new script: initiator maintenance for lan-lan-VPN0:1:[172.18.124.157] (start)
         39 seconds doing imnt_init, (0 @ 0)
manage @ 39 seconds :: lan-lan-VPN0:1:[172.18.124.157] (done)


cisco_endpoint#show vpn stat

          Current  In       High     Running  Tunnel   Tunnel   Tunnel
          Active   Negot    Water    Total    Starts   OK       Error
          ---------------------------------------------------------------
Users     0        0        0        0        0        0        0
Partners  1        0        1        1        1        0        0
Total     1        0        1        1        1        0        0

IOP slot 1:
```

```
          Current  In       High     Running  Tunnel   Tunnel   Tunnel
          Active   Negot    Water    Total    Starts   OK       Error
          -----------------------------------------------------------
Users     0        0        0        0        0        0        0
Partners  0        0        0        0        0        0        0
Total     0        0        0        0        0        0        0

cisco_endpoint#show vpn stat verb

          Current  In       High     Running  Tunnel   Tunnel   Tunnel
          Active   Negot    Water    Total    Starts   OK       Error
          -----------------------------------------------------------
Users     0        0        0        0        0        0        0
Partners  1        0        1        1        1        0        0
Total     1        0        1        1        1        0        0

Stats             VPN0:1
Wrapped              13
Unwrapped             9
BadEncap              0
BadAuth               0
BadEncrypt            0
rx IP                 9
rx IPX                0
rx Other              0
tx IP                13
tx IPX                0
tx Other              0
IKE rekey             0

Input VPN pkts dropped due to no SA: 0

Input VPN pkts dropped due to no free queue entries: 0

ISAKMP Negotiation stats
Admin packets in        4
Fastswitch packets in   0
No cookie found         0
Can't insert cookie     0
Inserted cookie(L)      1
Inserted cookie(R)      0
Cookie not inserted(L)  0
Cookie not inserted(R)  0
Cookie conn changed     0
Cookie already inserted  0
Deleted cookie(L)       0
Deleted cookie(R)       0
Cookie not deleted(L)   0
Cookie not deleted(R)   0
Forwarded to RP         0
Forwarded to IOP        0
Bad UDP checksum        0
Not fastswitched        0
Bad Initiator cookie    0
Bad Responder cookie    0
Has Responder cookie    0
No Responder cookie     0
No SA                   0
Bad find conn           0
Admin queue full        0
Priority queue full     0
Bad IKE packet          0
No memory               0
```

```
Bad Admin Put           0
IKE pkt dropped         0
No UDP PBuf             0
No Manager              0
Mgr w/ no cookie        0
Cookie Scavenge Add     1
Cookie Scavenge Rem     0
Cookie Scavenged        0
Cookie has mgr err      0
New conn limited        0

IOP slot 1:

          Current  In       High     Running  Tunnel   Tunnel   Tunnel
          Active   Negot    Water    Total    Starts   OK       Error
          -----------------------------------------------------------
Users     0        0        0        0        0        0        0
Partners  0        0        0        0        0        0        0
Total     0        0        0        0        0        0        0

Stats
Wrapped
Unwrapped
BadEncap
BadAuth
BadEncrypt
rx IP
rx IPX
rx Other
tx IP
tx IPX
tx Other
IKE rekey

Input VPN pkts dropped due to no SA: 0

Input VPN pkts dropped due to no free queue entries: 0

ISAKMP Negotiation stats
Admin packets in        0
Fastswitch packets in   3
No cookie found         0
Can't insert cookie     0
Inserted cookie(L)      0
Inserted cookie(R)      1
Cookie not inserted(L)  0
Cookie not inserted(R)  0
Cookie conn changed     0
Cookie already inserted  0
Deleted cookie(L)       0
Deleted cookie(R)       0
Cookie not deleted(L)   0
Cookie not deleted(R)   0
Forwarded to RP         0
Forwarded to IOP        3
Bad UDP checksum        0
Not fastswitched        0
Bad Initiator cookie    0
Bad Responder cookie    0
Has Responder cookie    0
No Responder cookie     0
No SA                   0
Bad find conn           0
Admin queue full        0
```

```
Priority queue full     0
Bad IKE packet          0
No memory               0
Bad Admin Put           0
IKE pkt dropped         0
No UDP PBuf             0
No Manager              0
Mgr w/ no cookie        0
Cookie Scavenge Add     1
Cookie Scavenge Rem     0
Cookie Scavenged        0
Cookie has mgr err      0
New conn limited        0
```

Informazioni correlate

- Cisco VPN serie 5000 concentrator: annuncio di fine vendita
- Negoziazione IPSec/protocolli IKE
- Documentazione e supporto tecnico – Cisco Systems