Configurazione di un tunnel IPSec tra un concentratore Cisco VPN 3000 e un firewall Checkpoint NG

Sommario

[Introduzione](#)
[Prerequisiti](#)
[Requisiti](#)
[Componenti usati](#)
[Convenzioni](#)
[Esempio di rete](#)
[Configurazioni](#)
[Configurazione di VPN 3000 Concentrator](#)
[Configurazione del checkpoint NG](#)
[Verifica](#)
[Verifica della comunicazione di rete](#)
[Visualizza stato tunnel su Checkpoint NG](#)
[Visualizza stato tunnel su VPN Concentrator](#)
[Risoluzione dei problemi](#)
[Riepilogo della rete](#)
[Debug del checkpoint NG](#)
[Debug per VPN Concentrator](#)
[Informazioni correlate](#)

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 del Cisco VPN 3000 Concentrator e la rete privata 10.32.x.x all'interno del firewall Checkpoint Next Generation (NG).

Prerequisiti

Requisiti

- Il traffico tra il concentratore VPN e l'interno del checkpoint NG e verso Internet, rappresentato qui dalle reti 172.18.124.x, deve passare prima di iniziare 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 viene effettuato tra peer IPSec.Nella fase 1 di IKE, i peer IPSec negoziano il criterio SA (Security Association) IKE stabilito. Dopo l'autenticazione dei peer, viene creato un tunnel sicuro con Internet Security Association and Key Management Protocol (ISAKMP).Nella fase 2 di IKE, i peer IPSec utilizzano il tunnel autenticato e sicuro per negoziare le trasformazioni della SA 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 alla scadenza della relativa durata.

Componenti usati

Questa configurazione è stata sviluppata e testata con le seguenti versioni software e hardware:

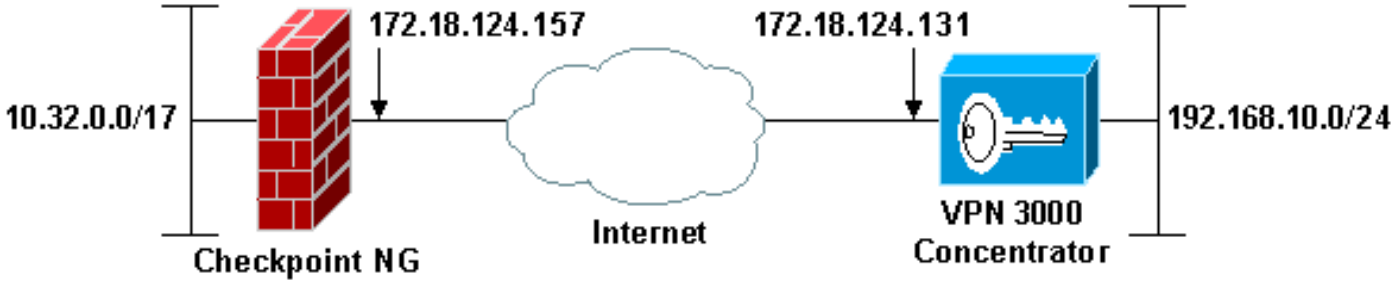
- VPN serie 3000 Concentrator 3.5.2
- Firewall NG checkpoint

Convenzioni

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

Esempio di rete

Nel documento viene usata questa impostazione di rete:



Nota: lo schema di indirizzi IP utilizzato in questa configurazione non è legalmente instradabile su Internet. Si tratta degli indirizzi RFC 1918 utilizzati in un ambiente lab.

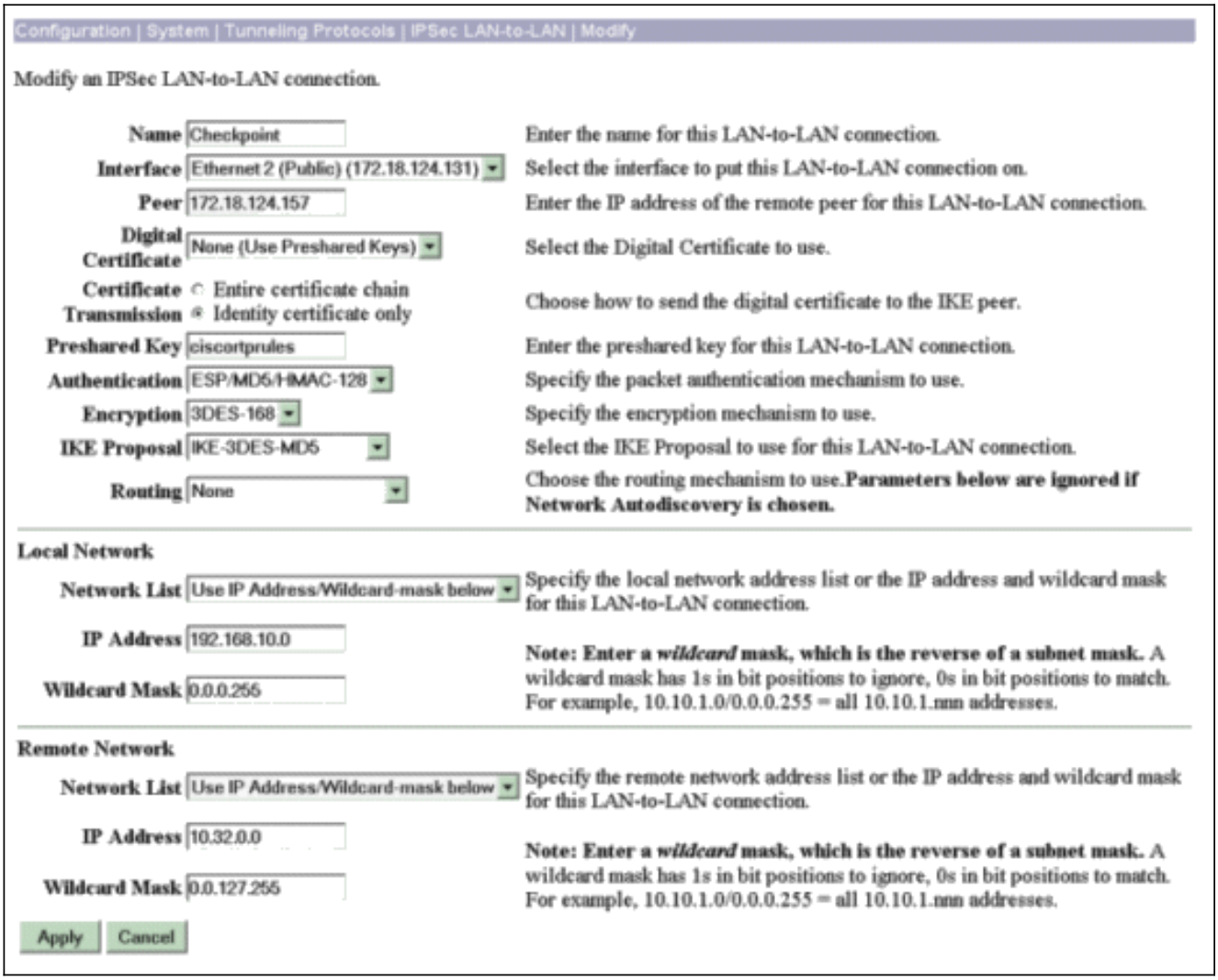
Configurazioni

Configurazione di VPN 3000 Concentrator

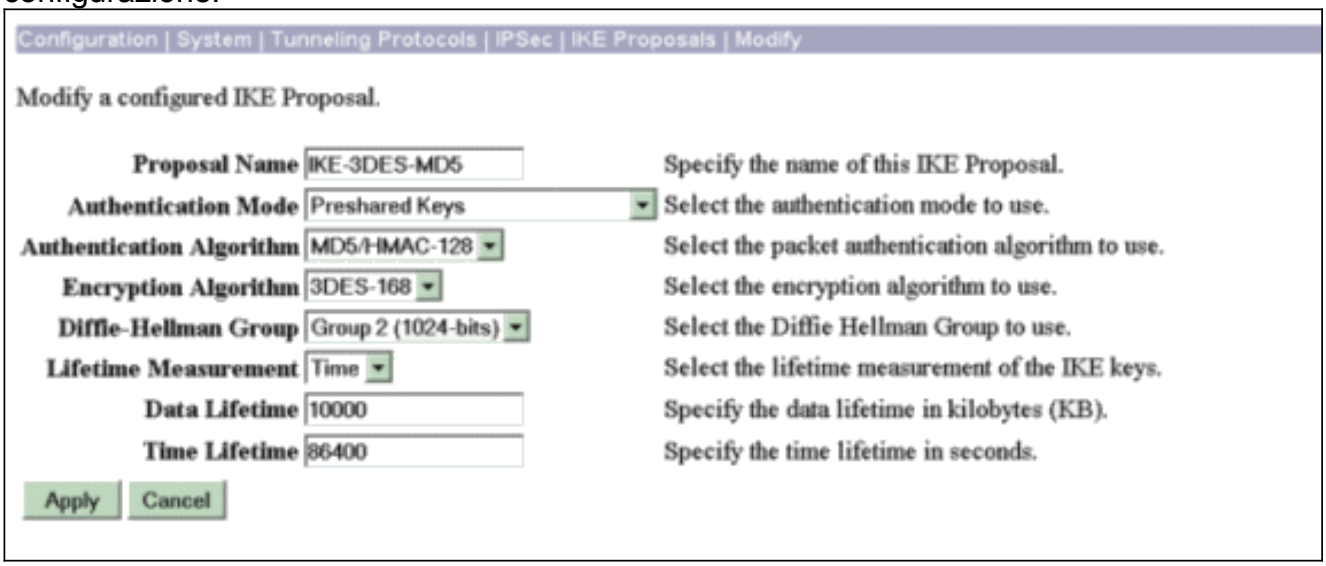
Completare questa procedura per configurare il concentratore VPN 3000:

1. Per configurare la sessione da LAN a LAN, selezionare **Configurazione > Sistema > Protocolli di tunneling > IPSec** da LAN a LAN. Impostare le opzioni per gli algoritmi di autenticazione e IKE, la chiave già condivisa, l'indirizzo IP peer e i parametri di rete locale e remota. Fare clic su **Apply** (Applica).In questa configurazione, l'autenticazione è stata impostata come ESP-MD5-HMAC e la crittografia è stata impostata come

3DES.



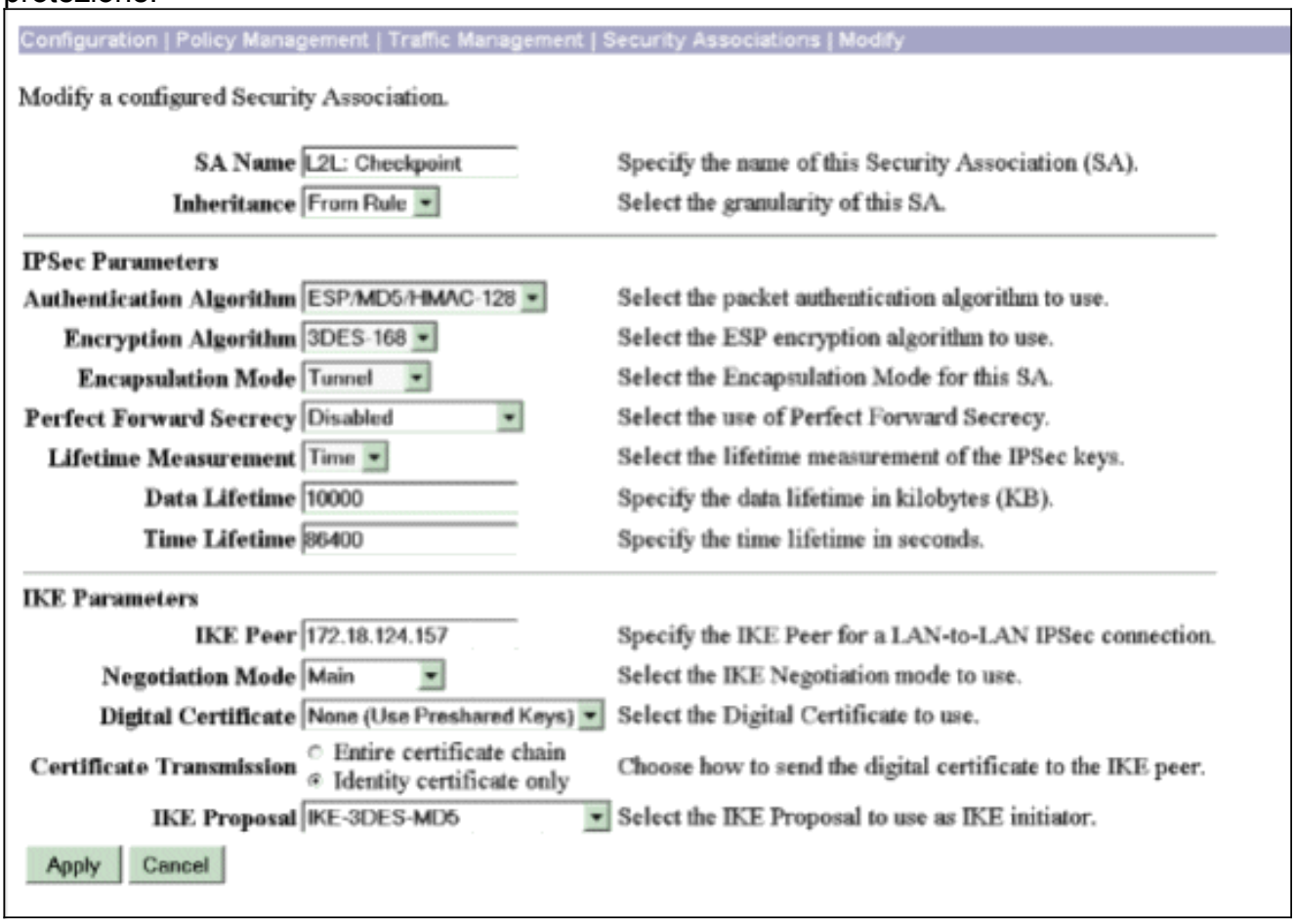
2. Selezionare **Configurazione > Sistema > Protocolli di tunneling > IPSec > Proposte IKE** e impostare i parametri richiesti.Selezionare la proposta IKE IKE-3DES-MD5 e verificare i parametri selezionati per la proposta. Per configurare la sessione da LAN a LAN, fare clic su **Apply** (Applica).Questi sono i parametri per questa configurazione:



3. Selezionare **Configurazione > Gestione delle policy > Gestione del traffico > Associazioni di sicurezza**, selezionare l'associazione di protezione IPSec creata per la sessione e verificare i parametri dell'associazione di protezione IPSec scelti per la sessione da LAN a LAN.In questa configurazione il nome della sessione LAN-LAN era "Checkpoint", quindi

l'associazione di protezione IPSec è stata creata automaticamente come "L2L: Checkpoint."

Di seguito sono riportati i parametri per questa associazione di protezione:

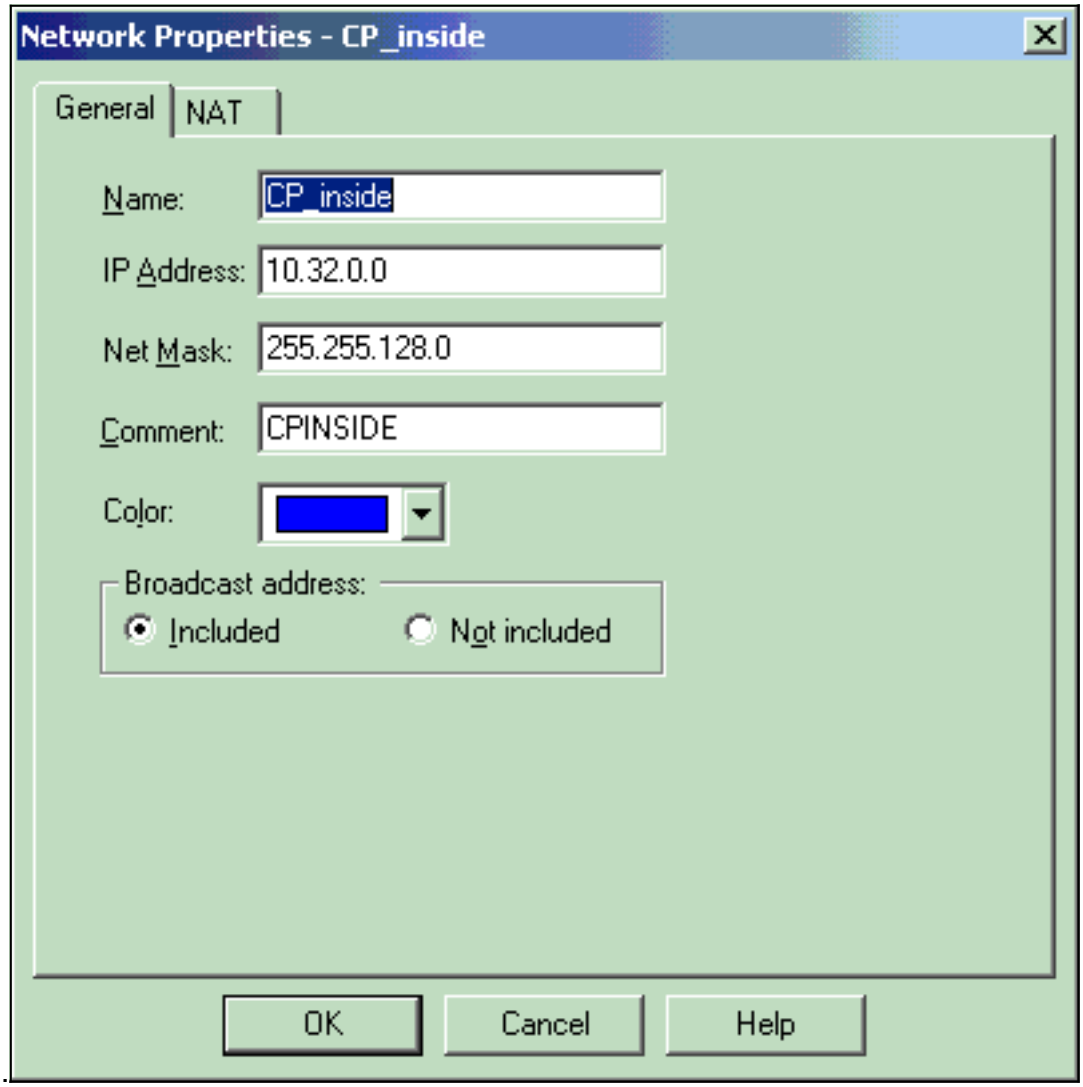


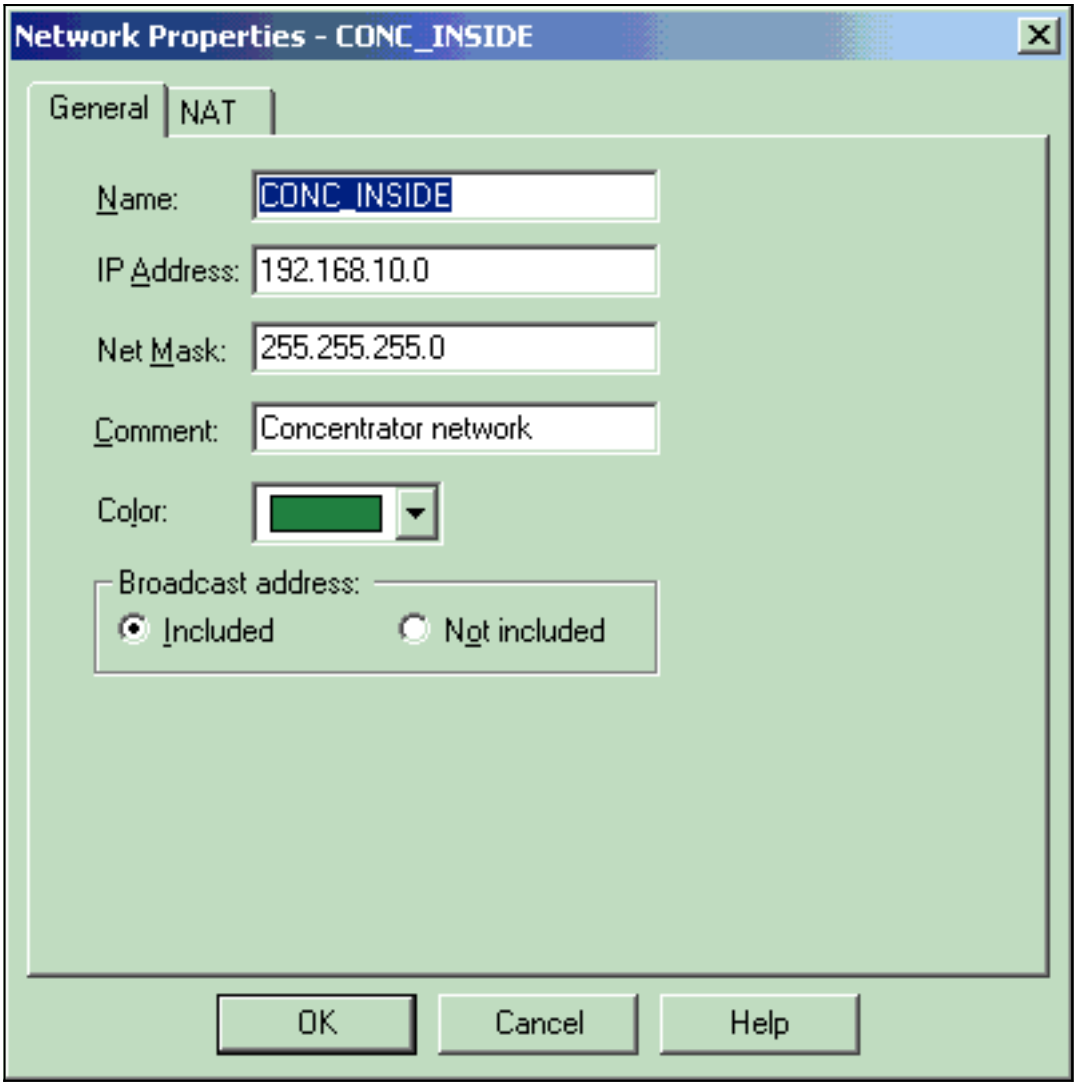
Configurazione del checkpoint NG

Gli oggetti e le regole di rete vengono definiti nel file NG del checkpoint per creare il criterio relativo alla configurazione VPN da configurare. Questo criterio viene quindi installato con l'Editor criteri NG checkpoint per completare il lato NG checkpoint della configurazione.

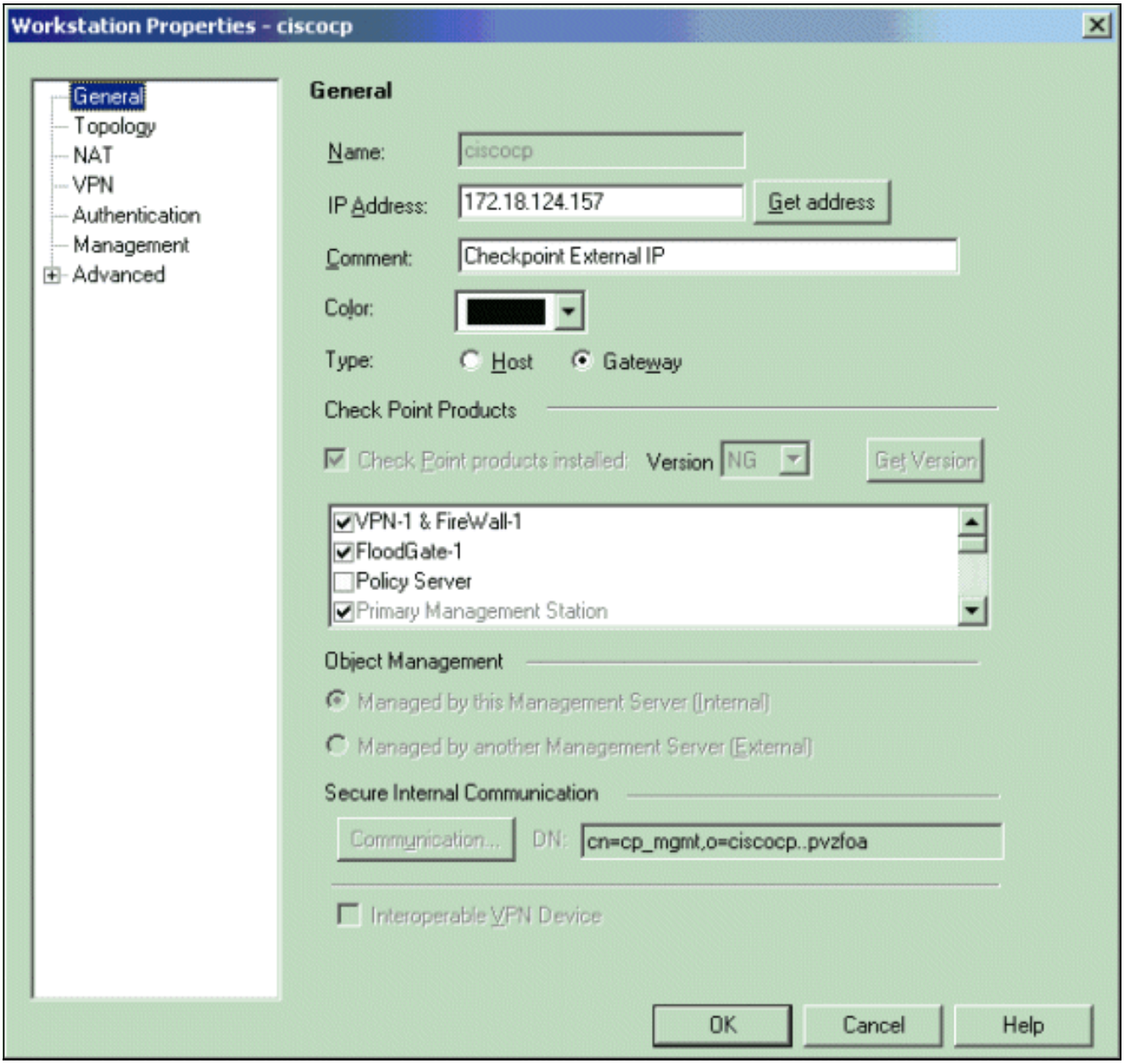
1. Creare i due oggetti di rete per la rete Checkpoint NG e la rete VPN Concentrator che crittograferanno il traffico interessante.per creare gli oggetti, selezionare **Gestisci > Oggetti di rete**, quindi selezionare **Nuovo > Rete**. Immettere le informazioni di rete appropriate, quindi

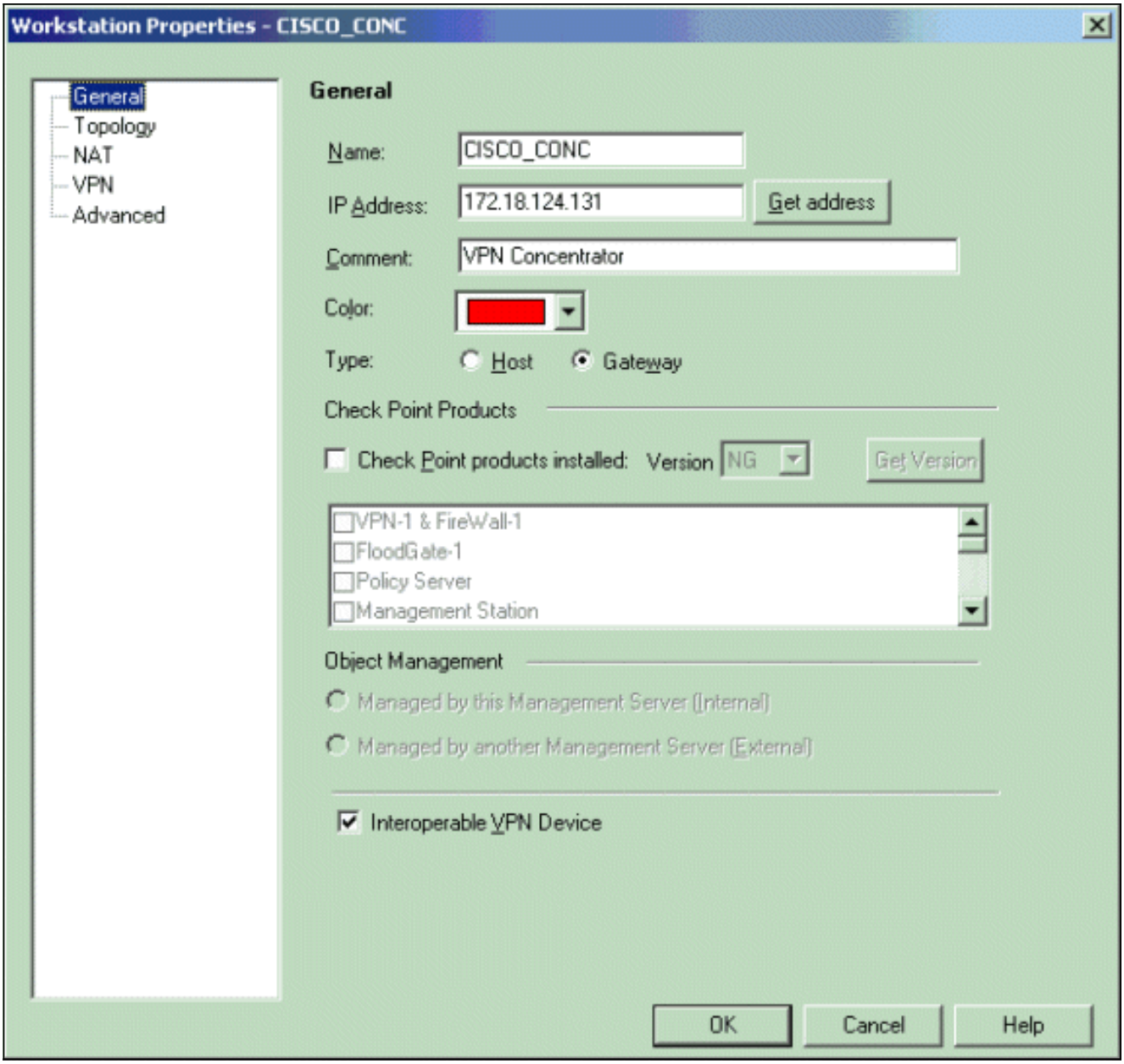
fare clic su OK.Questi esempi mostrano la configurazione di oggetti di rete chiamati CP_inside (la rete interna del Checkpoint NG) e CONC_INSIDE (la rete interna del Concentrator VPN).



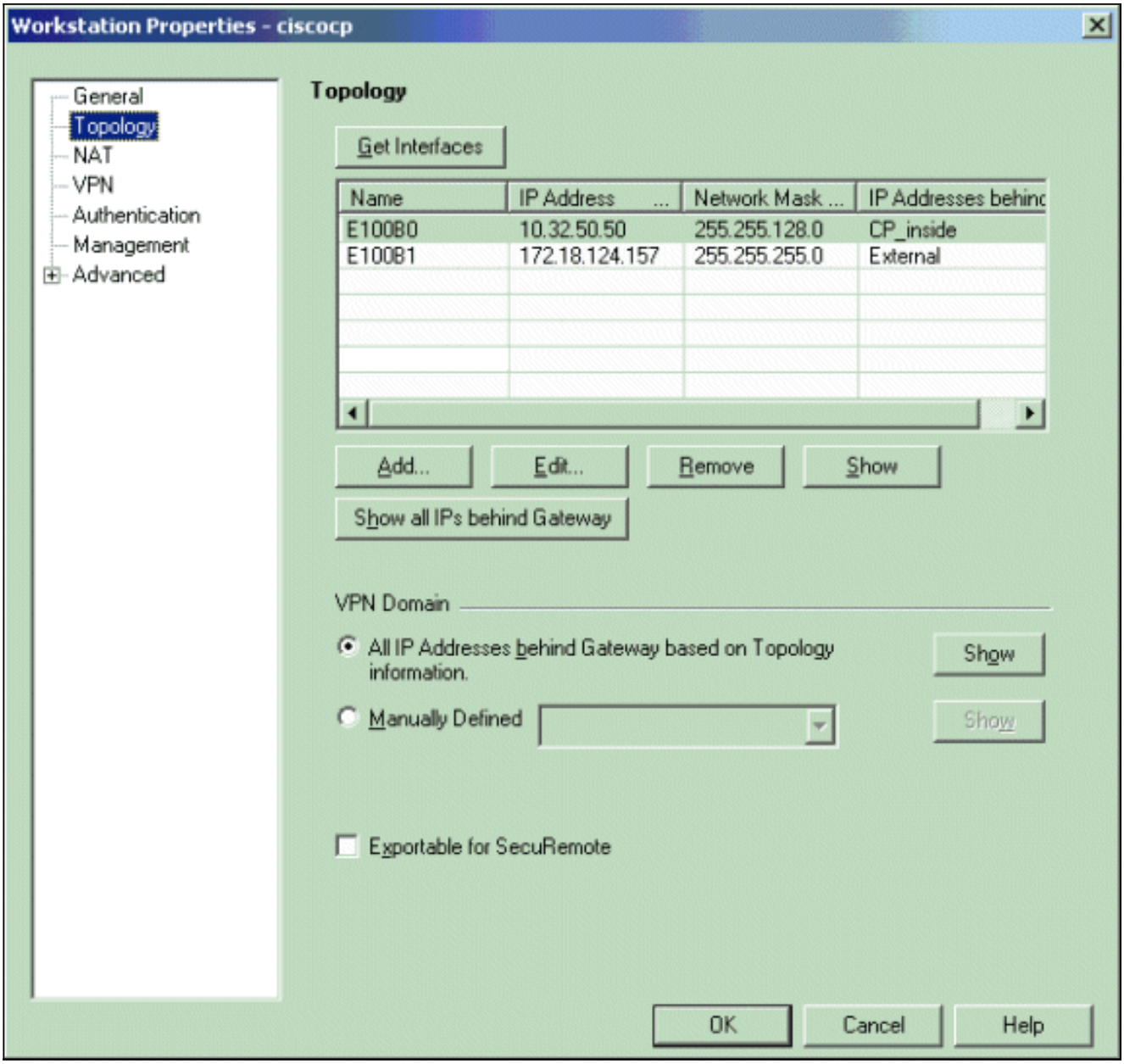


2. Selezionare **Gestisci > Oggetti di rete** e **Nuovo > Workstation** per creare oggetti workstation per i dispositivi VPN, Checkpoint NG e VPN Concentrator.**Nota:** è possibile utilizzare l'oggetto stazione di lavoro Checkpoint NG creato durante l'impostazione iniziale di Checkpoint NG. Selezionare le opzioni per impostare la workstation come Gateway e Dispositivo VPN interoperabile, quindi fare clic su **OK**.Gli esempi mostrano la configurazione di oggetti chiamati ciscop (Checkpoint NG) e CISCO_CONC (VPN 3000 Concentrator):


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

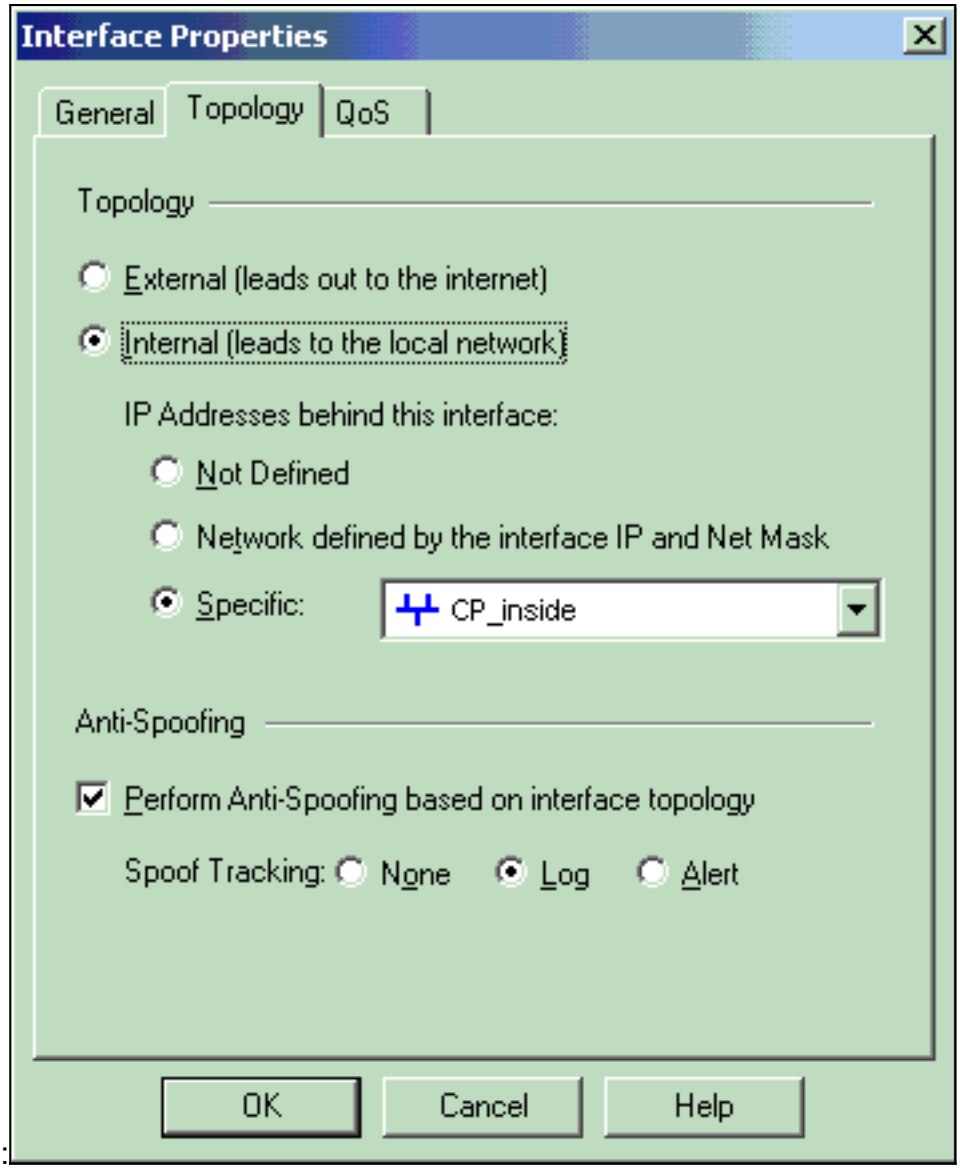


3. Selezionare **Gestisci > Oggetti di rete > Modifica** per aprire la finestra Proprietà stazione di lavoro relativa alla stazione di lavoro NG checkpoint (ciscocp in questo esempio). Selezionare **Topologia** dalle opzioni sul lato sinistro della finestra, quindi selezionare la rete da crittografare. Per impostare le proprietà dell'interfaccia, fare clic su **Edit** (Modifica).In questo esempio, CP_inside è la rete interna del checkpoint
NG.

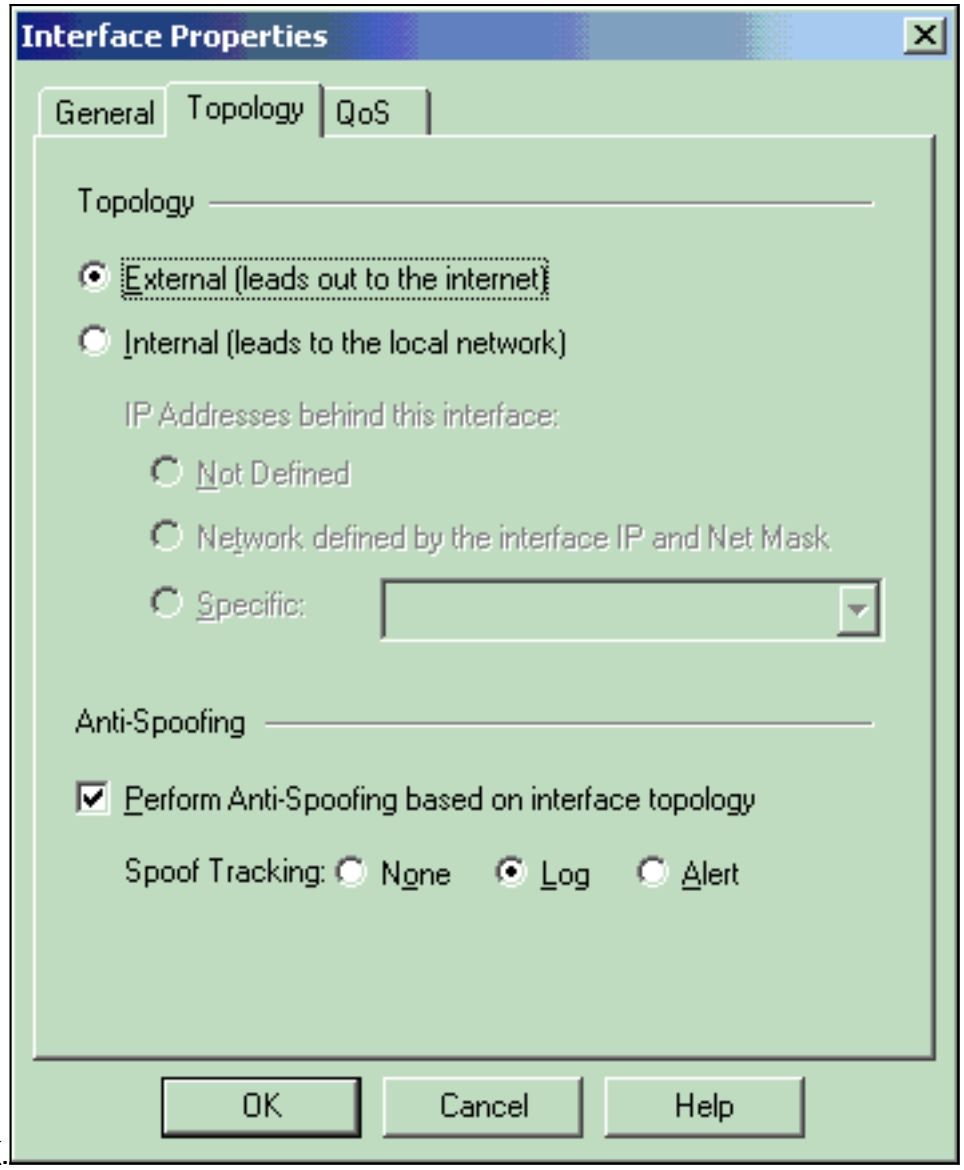


4. Nella finestra Proprietà interfaccia, selezionare l'opzione per designare la workstation come interna, quindi specificare l'indirizzo IP appropriato. Fare clic su **OK**.Le selezioni della topologia mostrate designano la workstation come interna e specificano gli indirizzi IP dietro

l'interfaccia CP_inside:

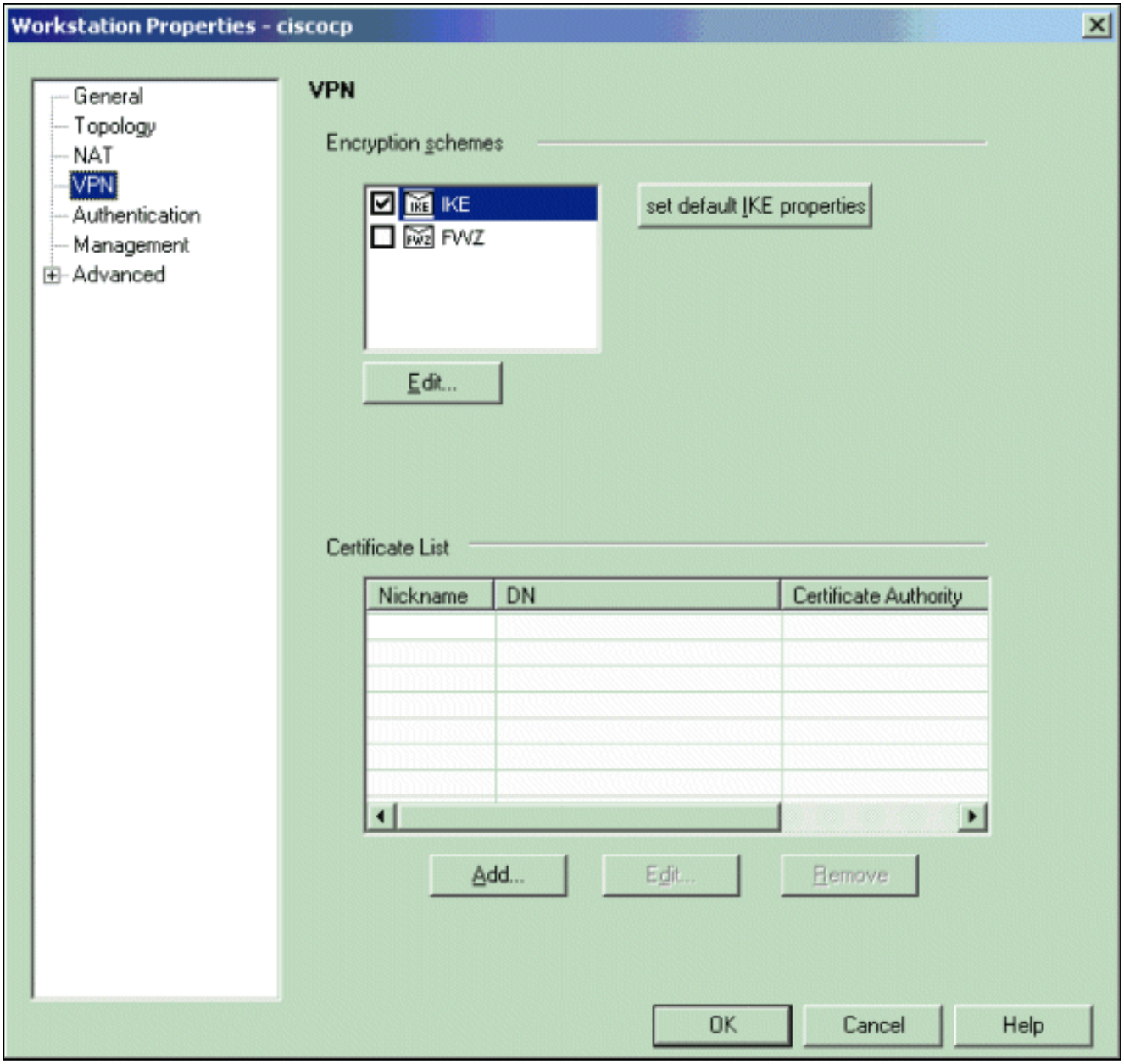


5. Dalla finestra Proprietà workstation, selezionare l'interfaccia esterna sul Checkpoint NG che conduce a Internet, quindi fare clic su **Modifica** per impostare le proprietà dell'interfaccia. Selezionare l'opzione per designare la topologia come esterna, quindi fare clic su



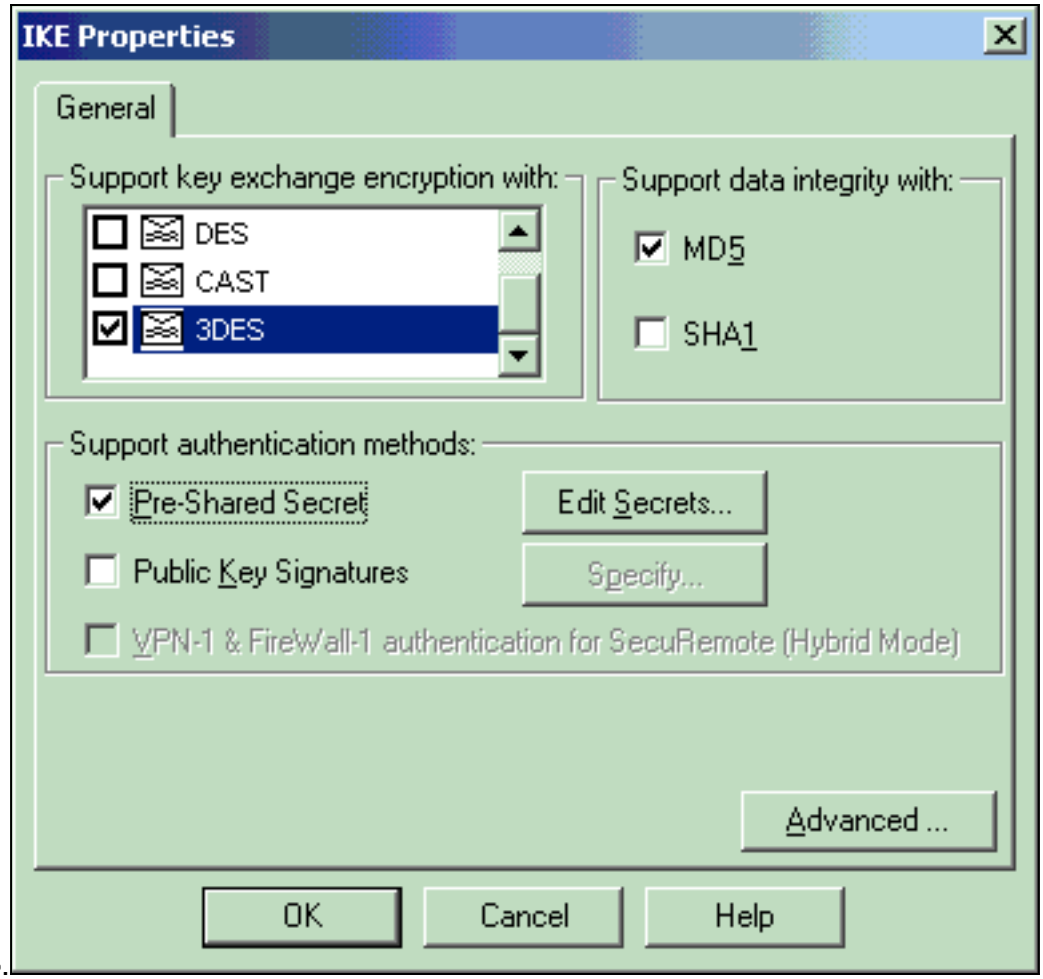
OK.

6. Dalla finestra Proprietà stazione di lavoro sul Checkpoint NG, selezionare **VPN** dalle opzioni sul lato sinistro della finestra, quindi selezionare i parametri IKE per gli algoritmi di crittografia e autenticazione. Per configurare le proprietà IKE, fare clic su **Edit** (Modifica).

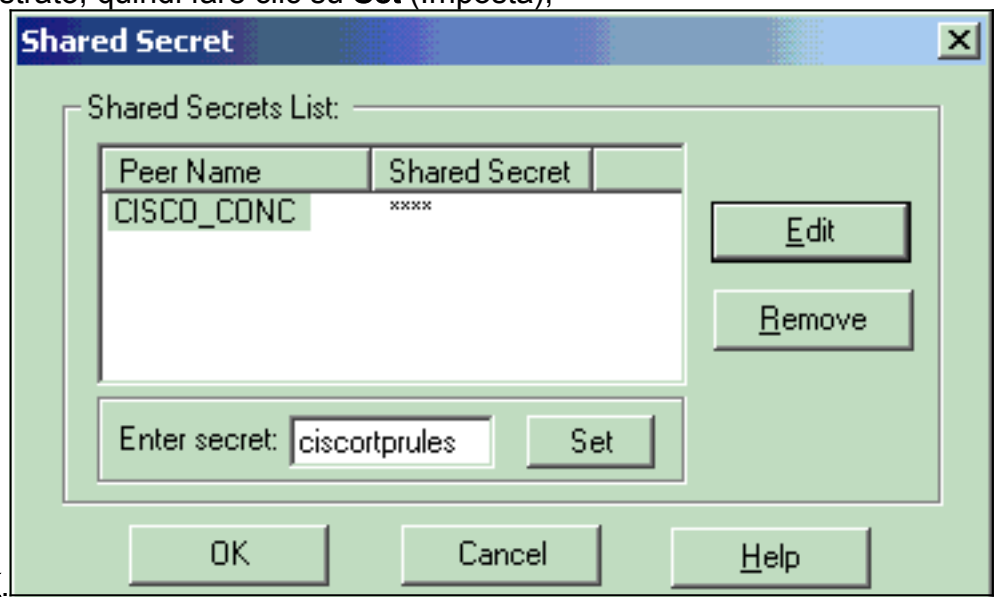


7. Impostare le proprietà IKE in modo che corrispondano alle proprietà nel concentratore VPN.In questo esempio, selezionare l'opzione di crittografia per **3DES** e l'opzione di hashing

per **MD5**.

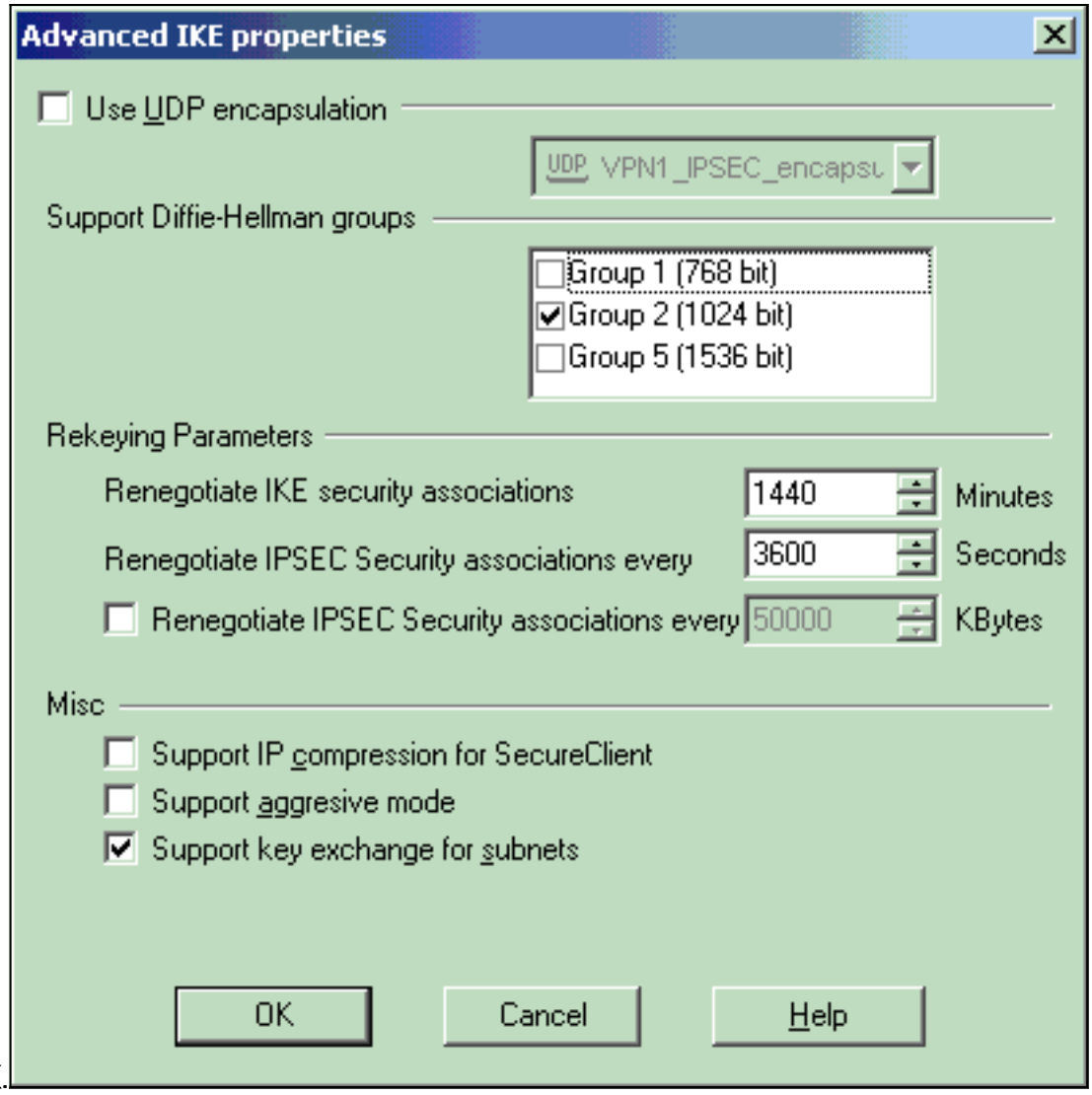


8. Selezionare l'opzione di autenticazione per **Segreti già condivisi**, quindi fare clic su **Modifica segreti** per impostare la chiave già condivisa in modo che sia compatibile con la chiave già condivisa nel concentratore VPN. Fare clic su **Edit** (Modifica) per immettere la chiave come mostrato, quindi fare clic su **Set** (Imposta),



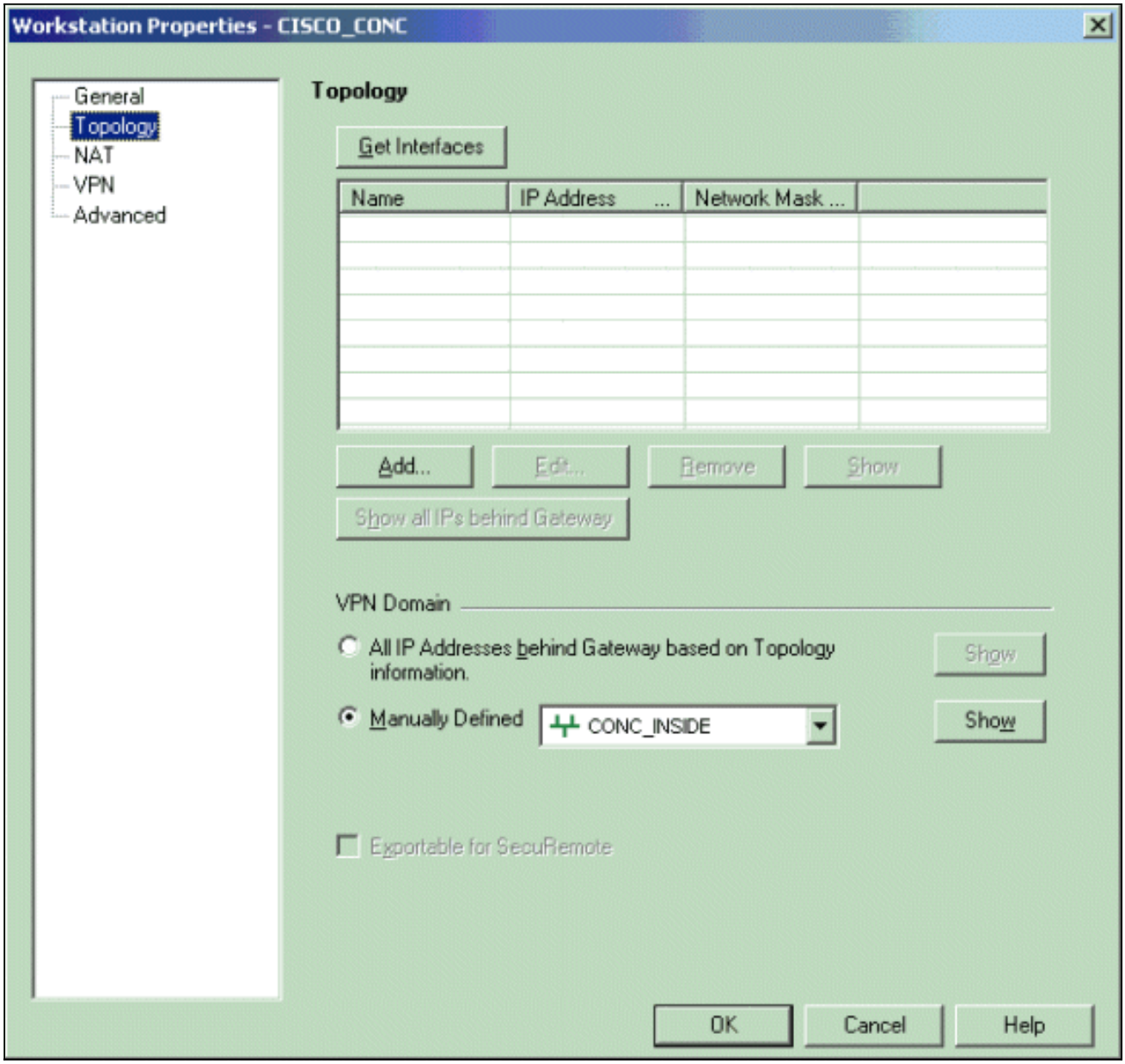
OK.

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**,

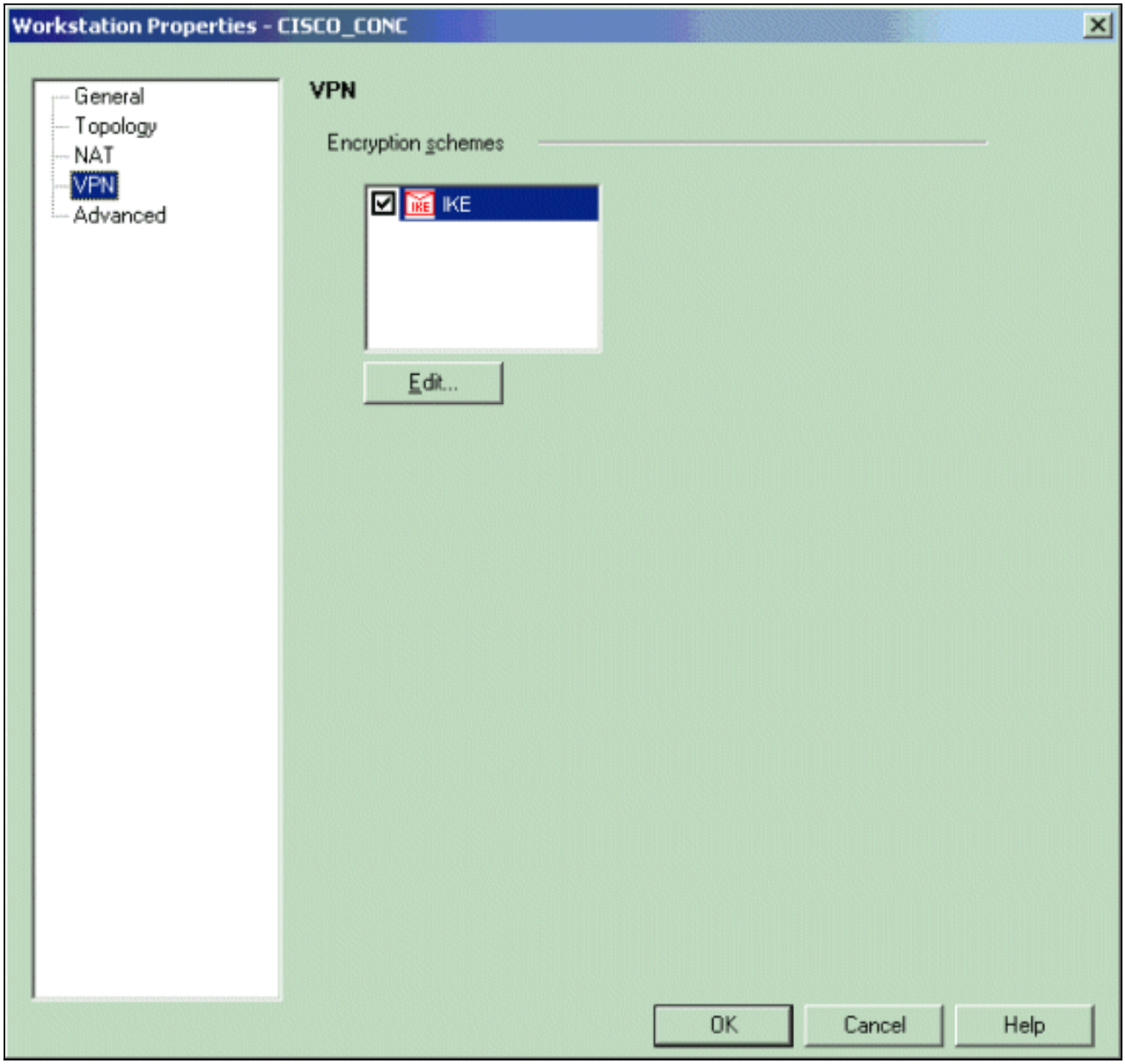


OK.

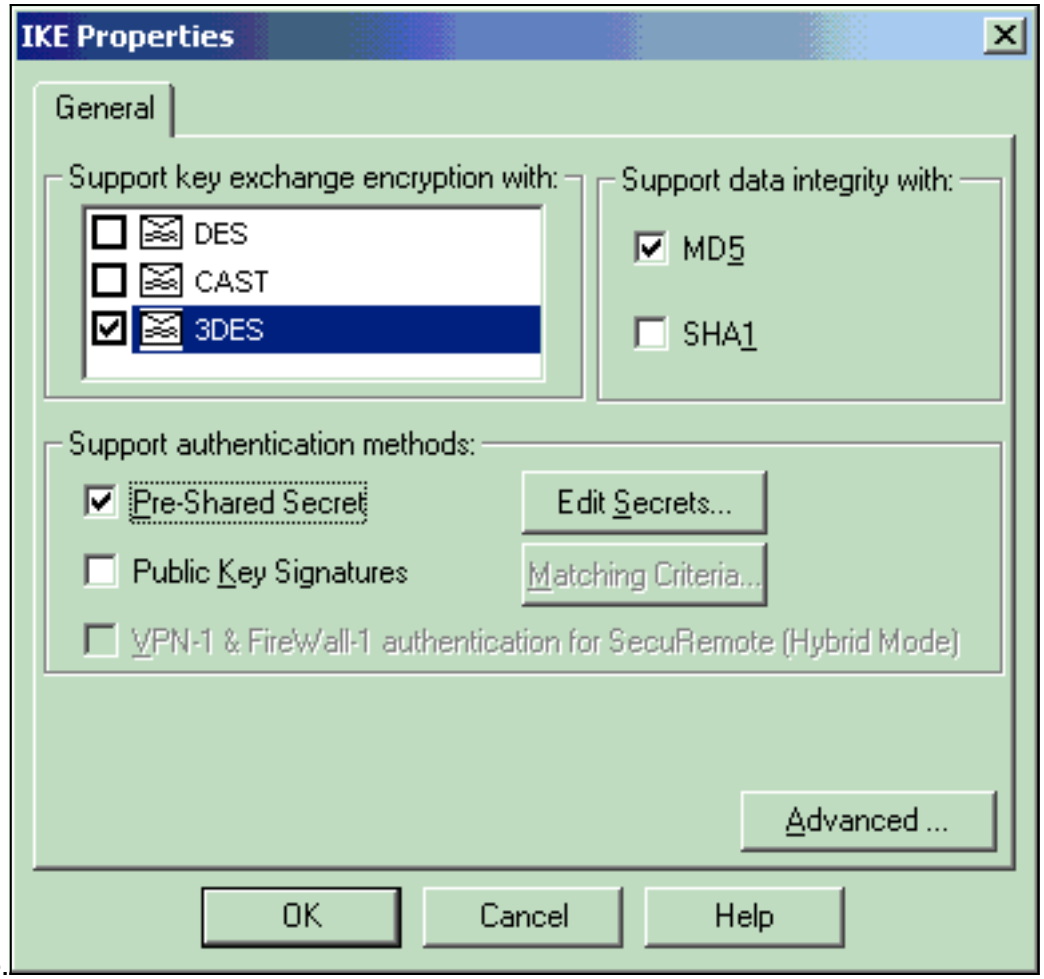
10. Selezionare **Gestisci > Oggetti di rete > Modifica** per aprire la finestra Proprietà workstation per VPN Concentrator. Selezionare **Topologia** dalle opzioni sul lato sinistro della finestra per definire manualmente il dominio VPN.Nell'esempio, CONC_INSIDE (la rete interna di VPN Concentrator) è definito come dominio
VPN.



11. Selezionare **VPN** dalle opzioni sul lato sinistro della finestra, quindi selezionare **IKE** come schema di crittografia. Per configurare le proprietà IKE, fare clic su **Edit** (Modifica).

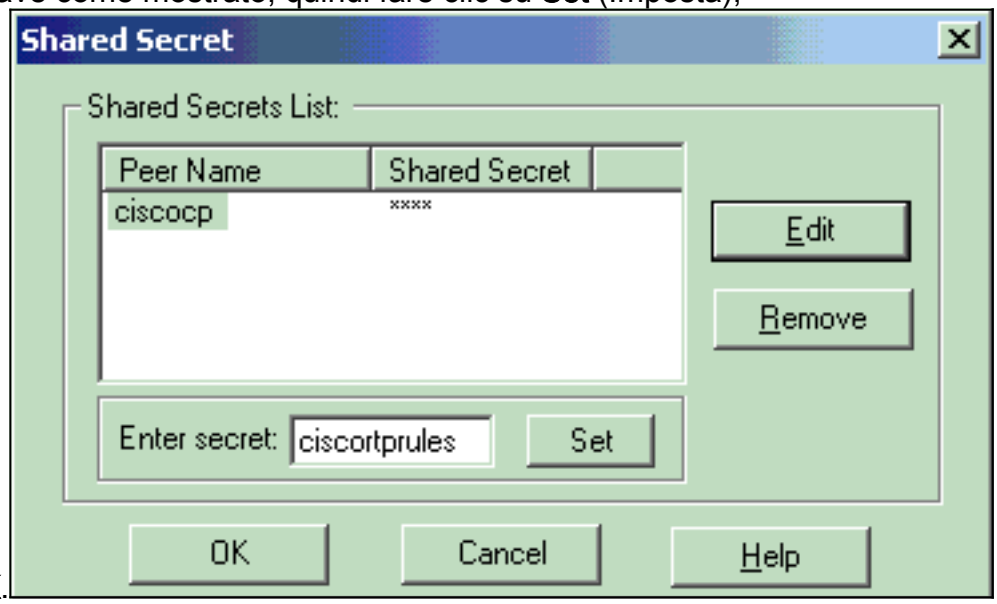


12. Impostare le proprietà IKE in modo che riflettano la configurazione corrente nel concentratore VPN.In questo esempio, impostare l'opzione di crittografia per **3DES** e l'opzione di hashing per



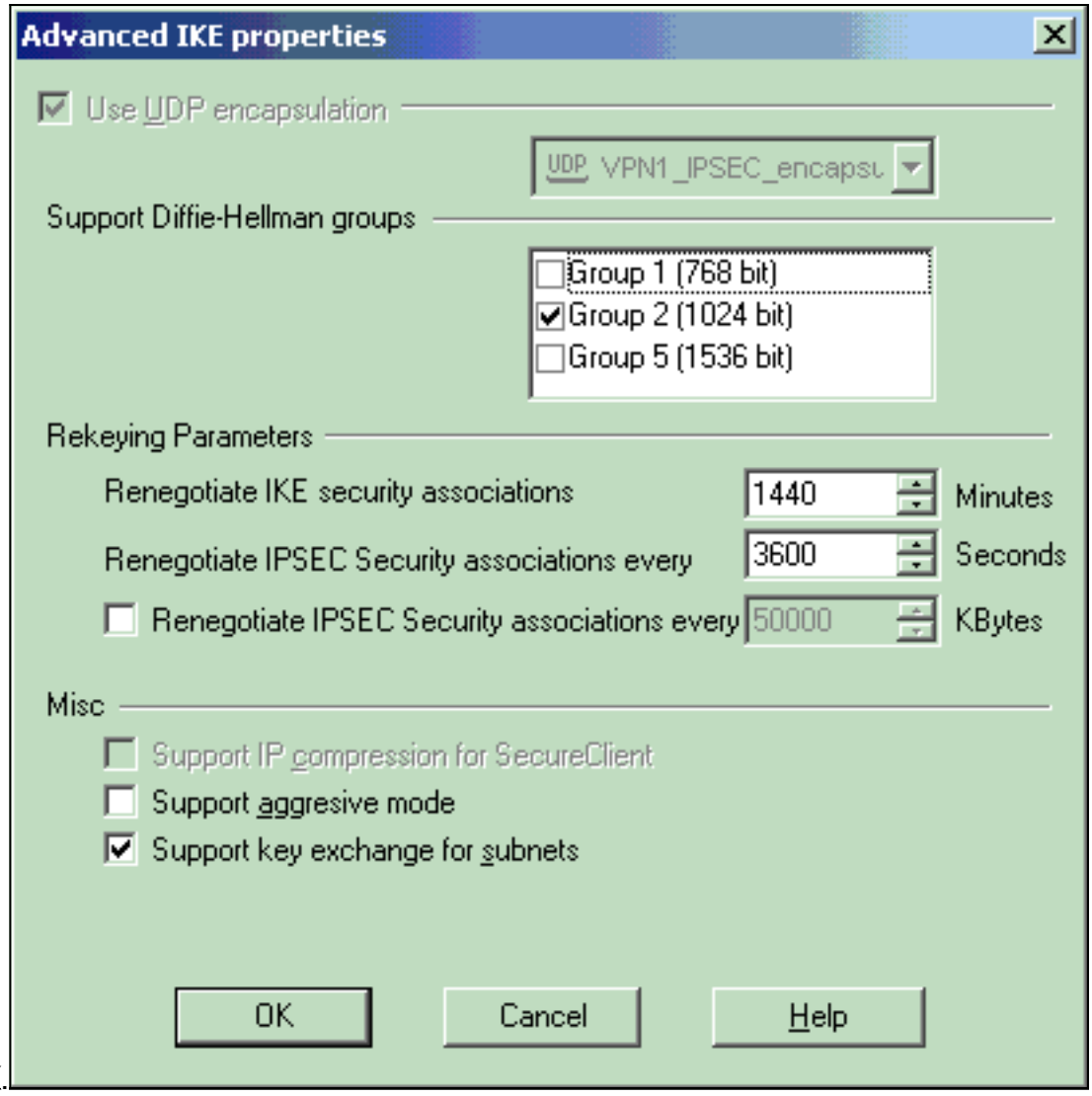
MD5.

13. Selezionare l'opzione di autenticazione per **Segreti già condivisi**, quindi fare clic su **Modifica segreti** per impostare la chiave già condivisa. Fare clic su **Edit** (Modifica) per immettere la chiave come mostrato, quindi fare clic su **Set** (Imposta),



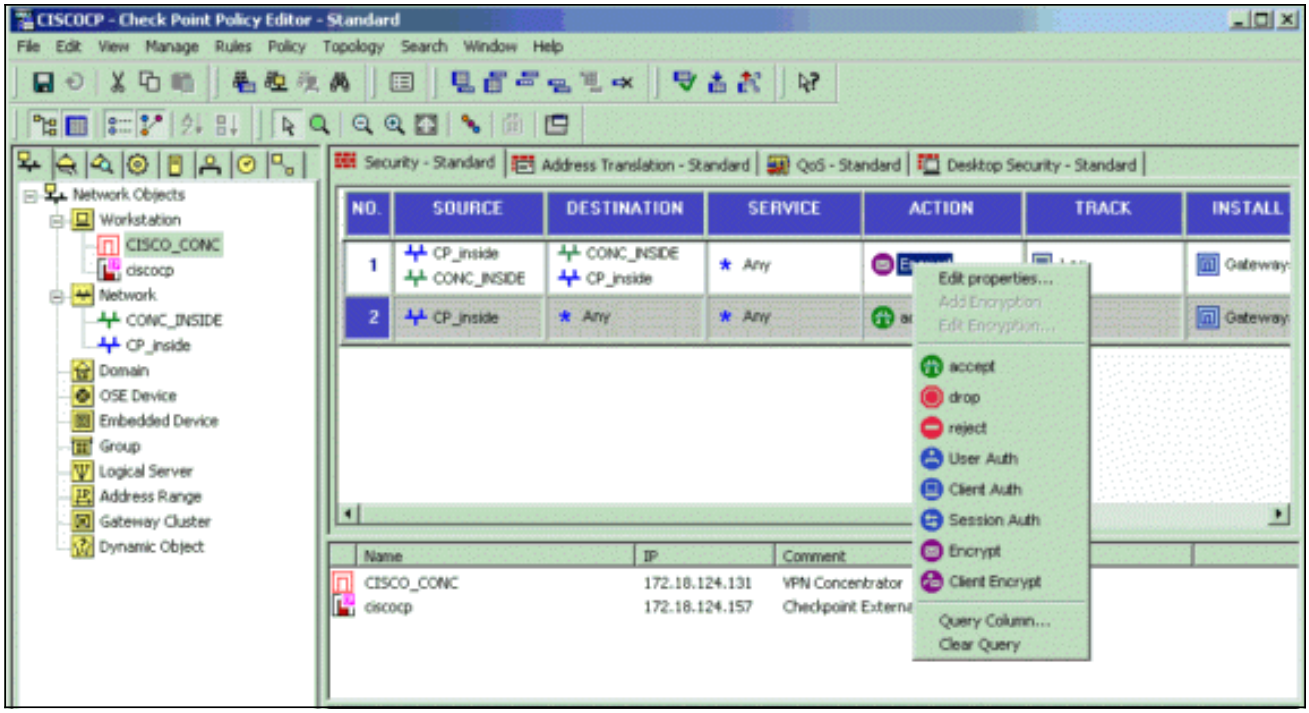
OK.

14. Dalla finestra delle proprietà di IKE, fare clic su **Avanzate...** e modificare le seguenti 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**,

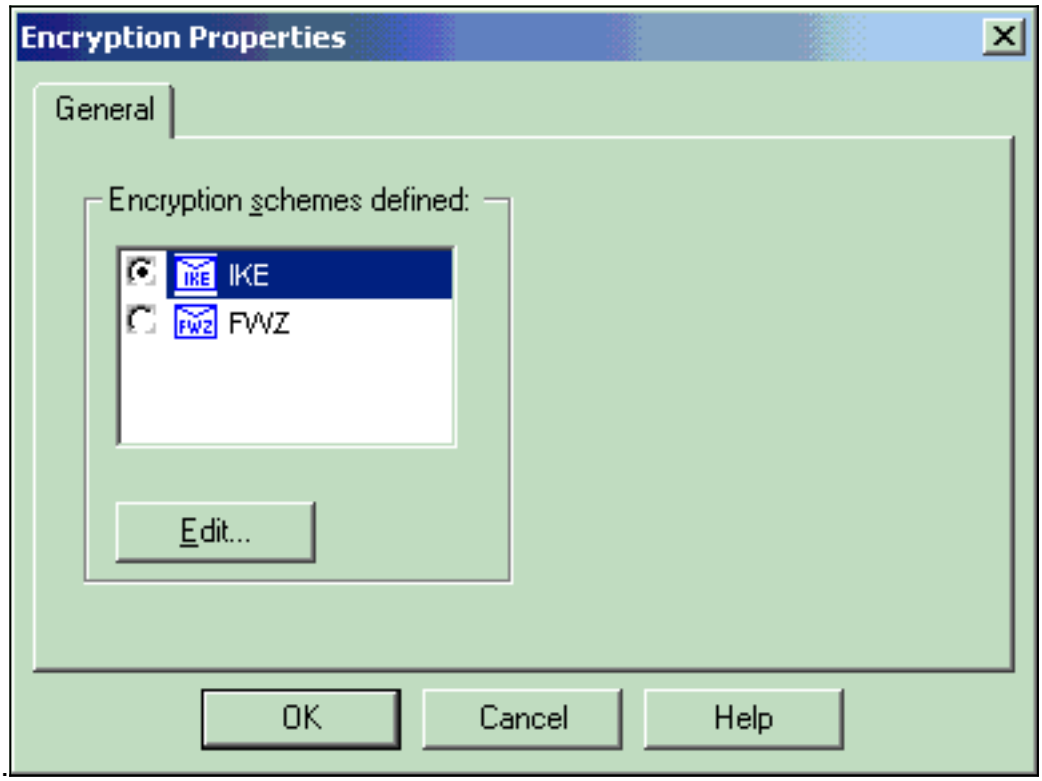


OK.

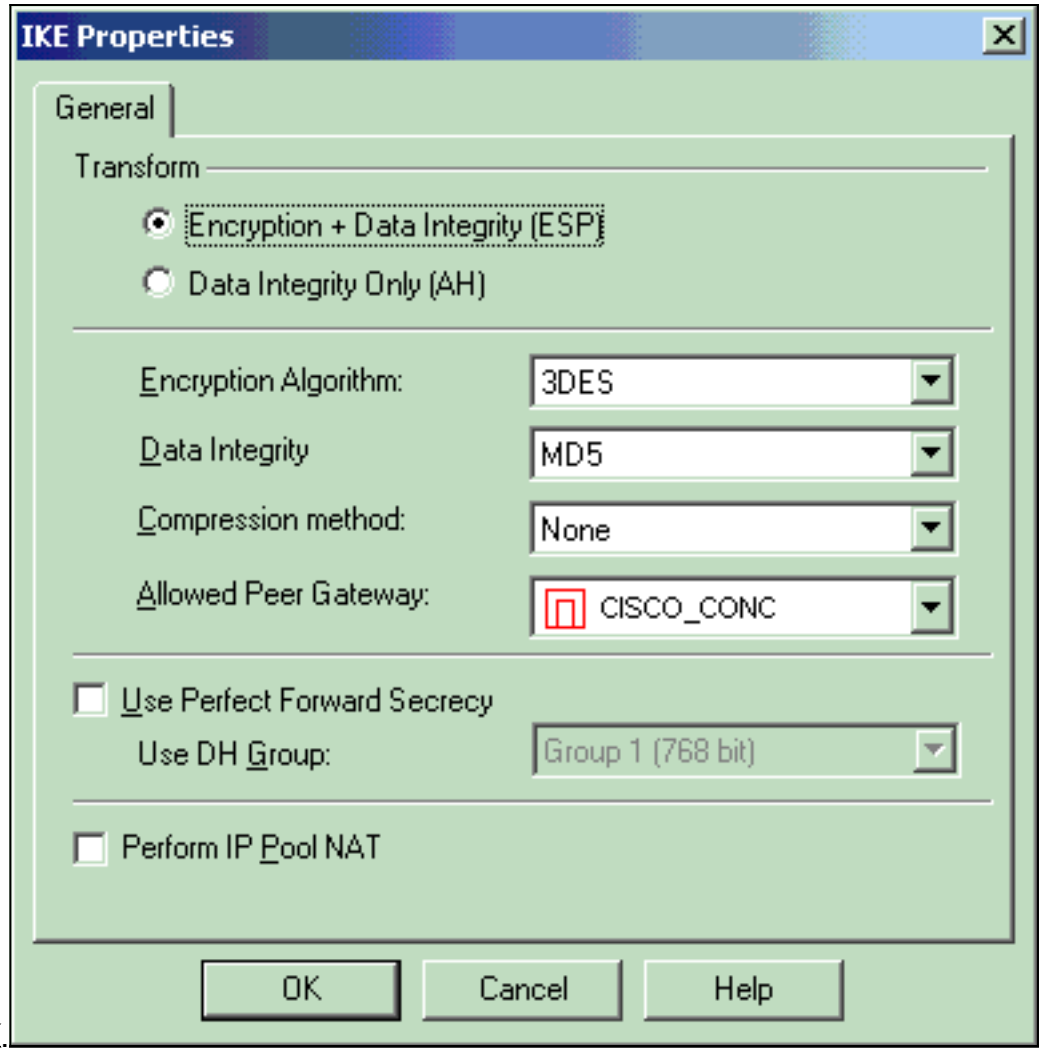
15. Per configurare le regole di crittografia per il criterio, selezionare **Regole > Aggiungi regole > In alto**. Nella finestra Editor dei criteri, inserire una regola con origine CP_inside (all'interno della rete del checkpoint NG) e destinazione CONC_INSIDE (all'interno della rete del concentratore VPN). 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. Selezionare **IKE** e fare clic su **Modifica**.

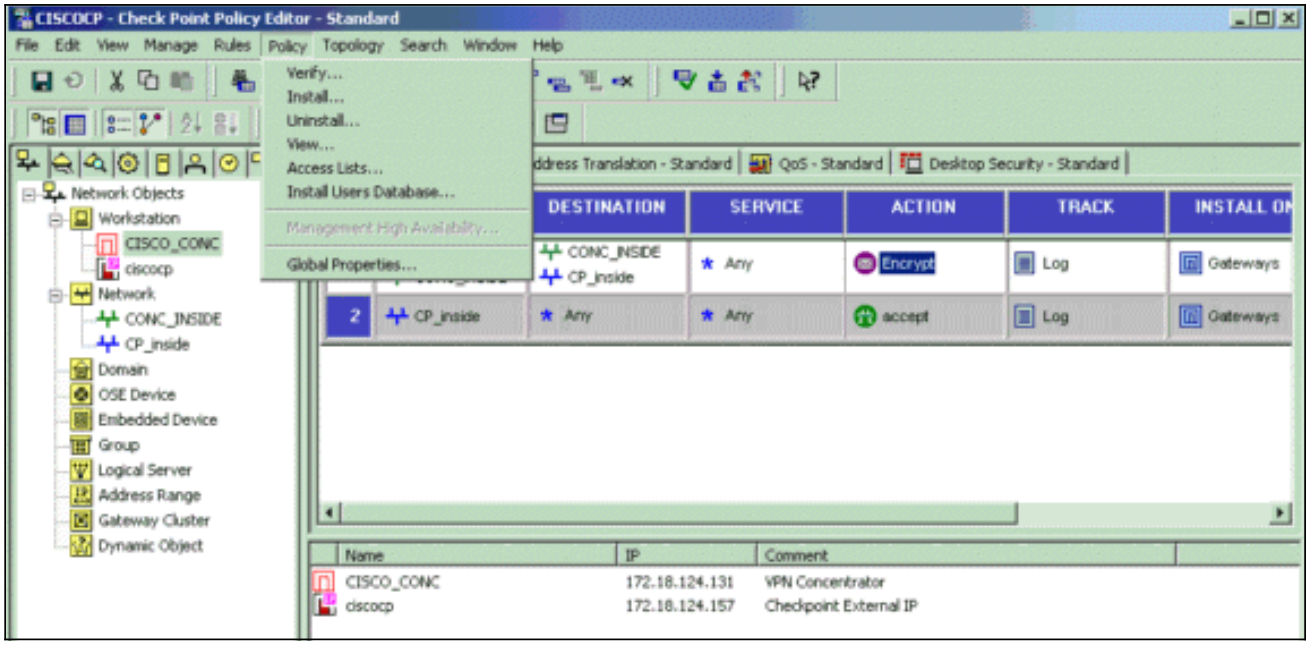


17. Nella finestra Proprietà IKE modificare le proprietà per accettare la trasformazione Concentrator VPN.Impostare l'opzione Trasforma su **Crittografia + integrità dei dati (ESP)**.Impostare l'algoritmo di crittografia su **3DES**.Impostare l'integrità dei dati su **MD5**.Impostare il gateway peer consentito in modo che corrisponda al concentratore VPN (CISCO_CONC).Al termine, fare clic su

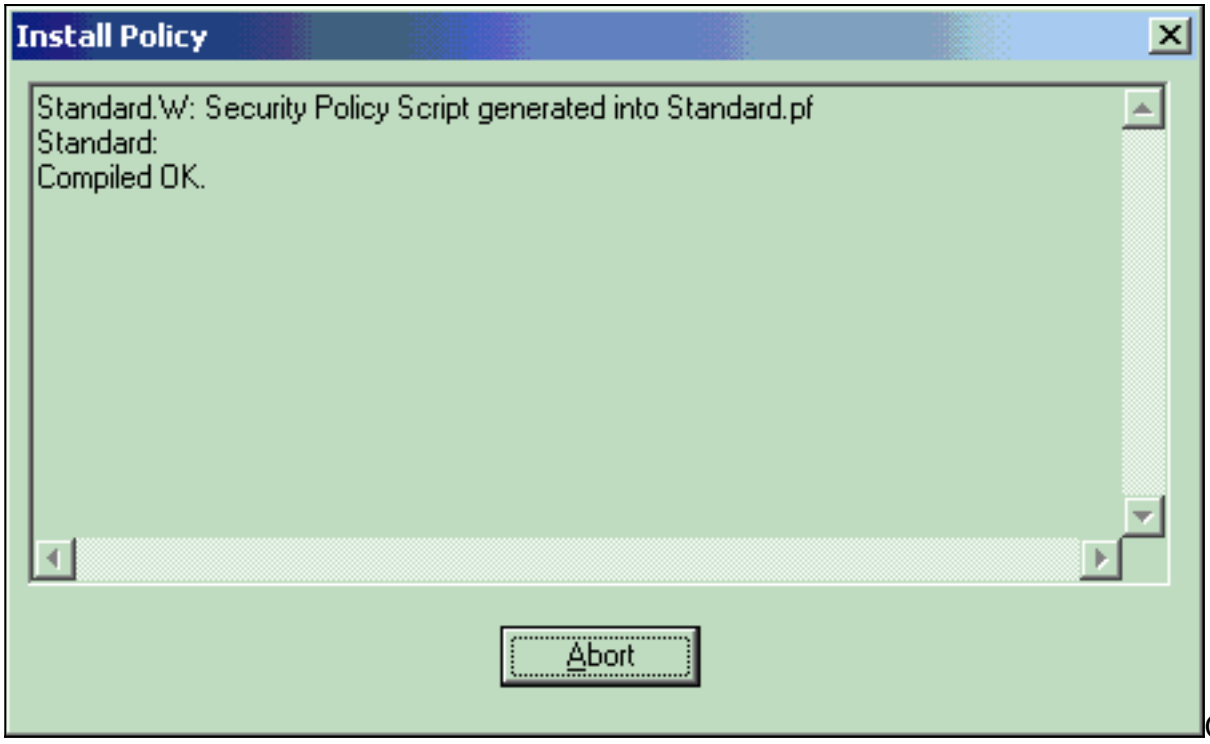


OK.

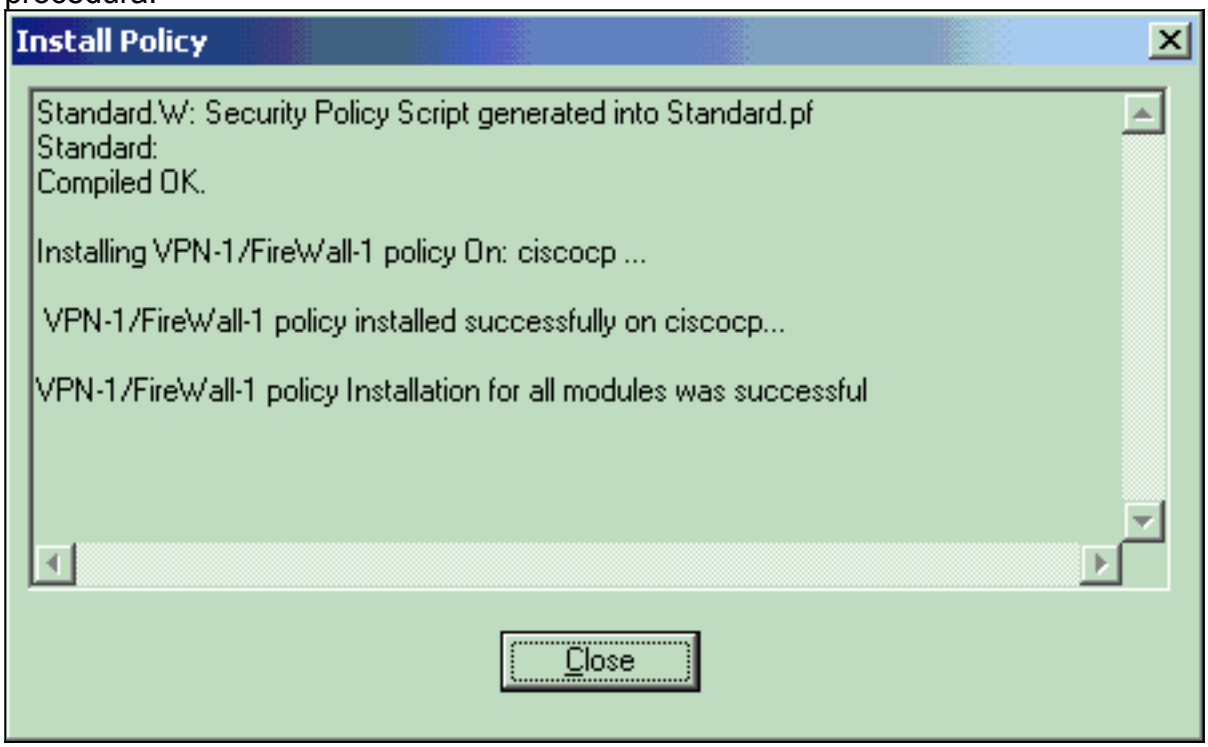
18. Dopo aver configurato Checkpoint NG, salvare il criterio e selezionare **Criterio > Installa** per abilitarlo.



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 del criterio è stata completata, fare clic su **Chiudi** per completare la procedura.

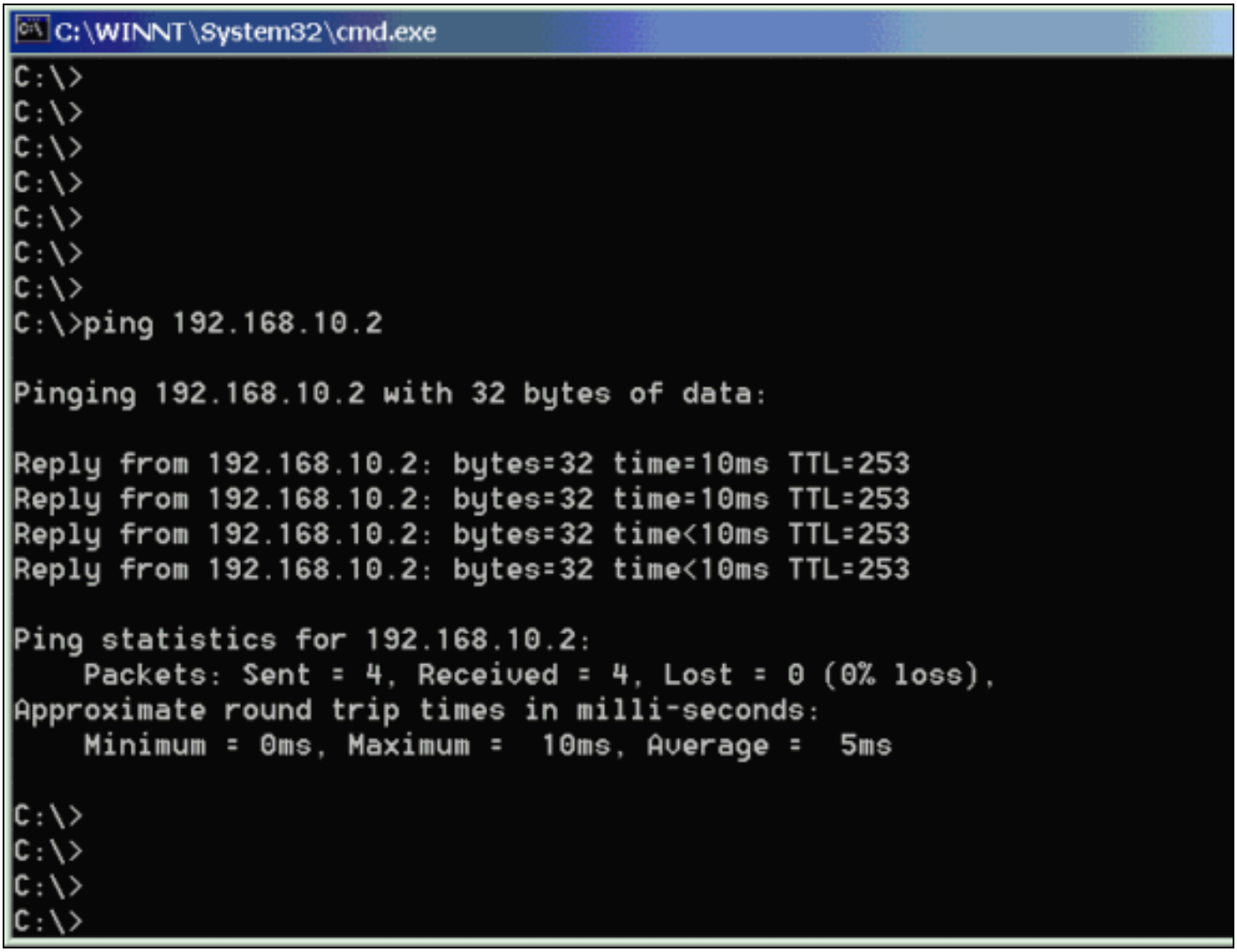


Verifica

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

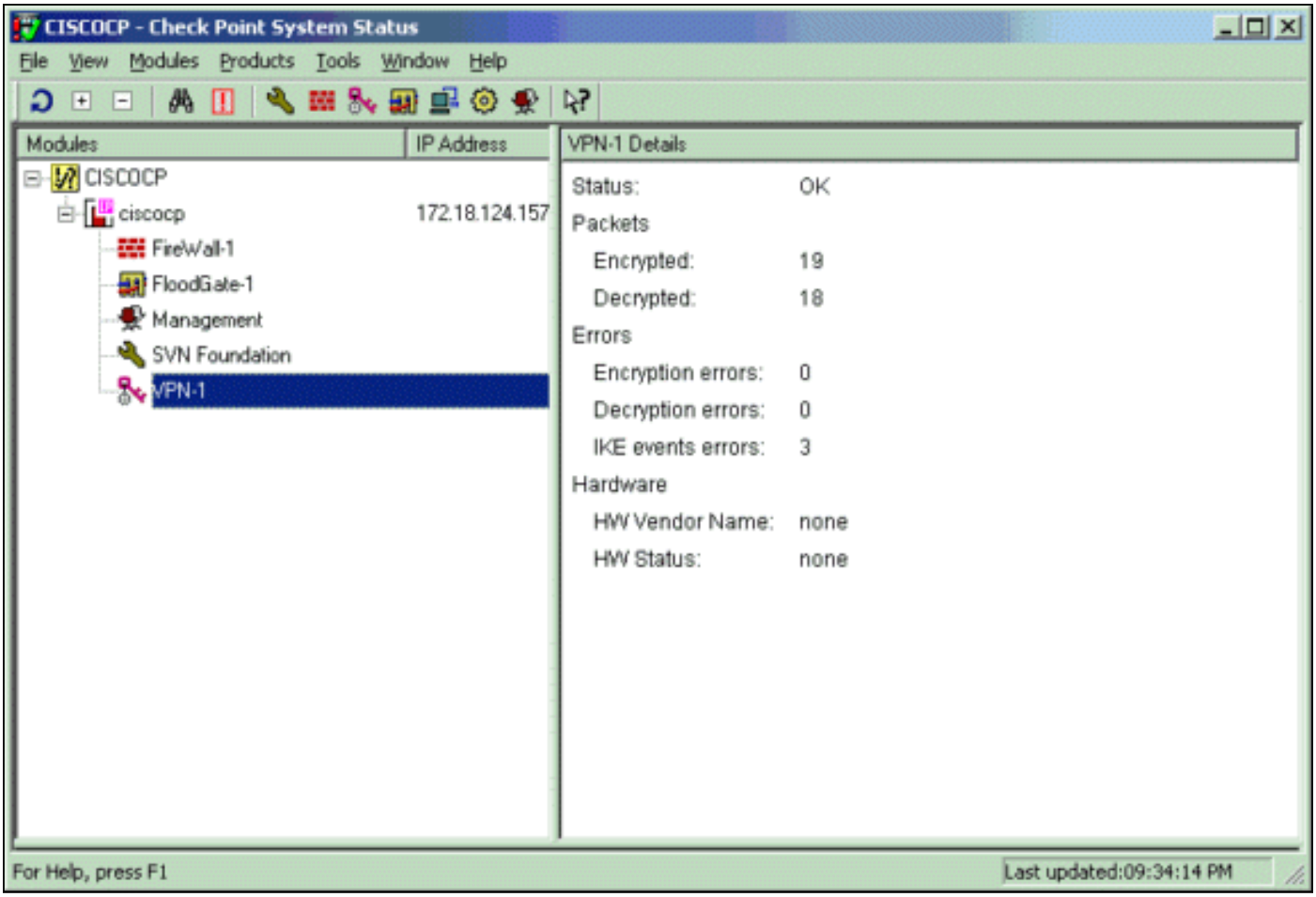
Verifica della comunicazione di rete

Per verificare la comunicazione tra le due reti private, è possibile avviare un ping tra una delle reti private e l'altra. In questa configurazione, è stato inviato un ping dal lato Checkpoint NG (10.32.50.51) alla rete VPN Concentrator (192.168.10.2).



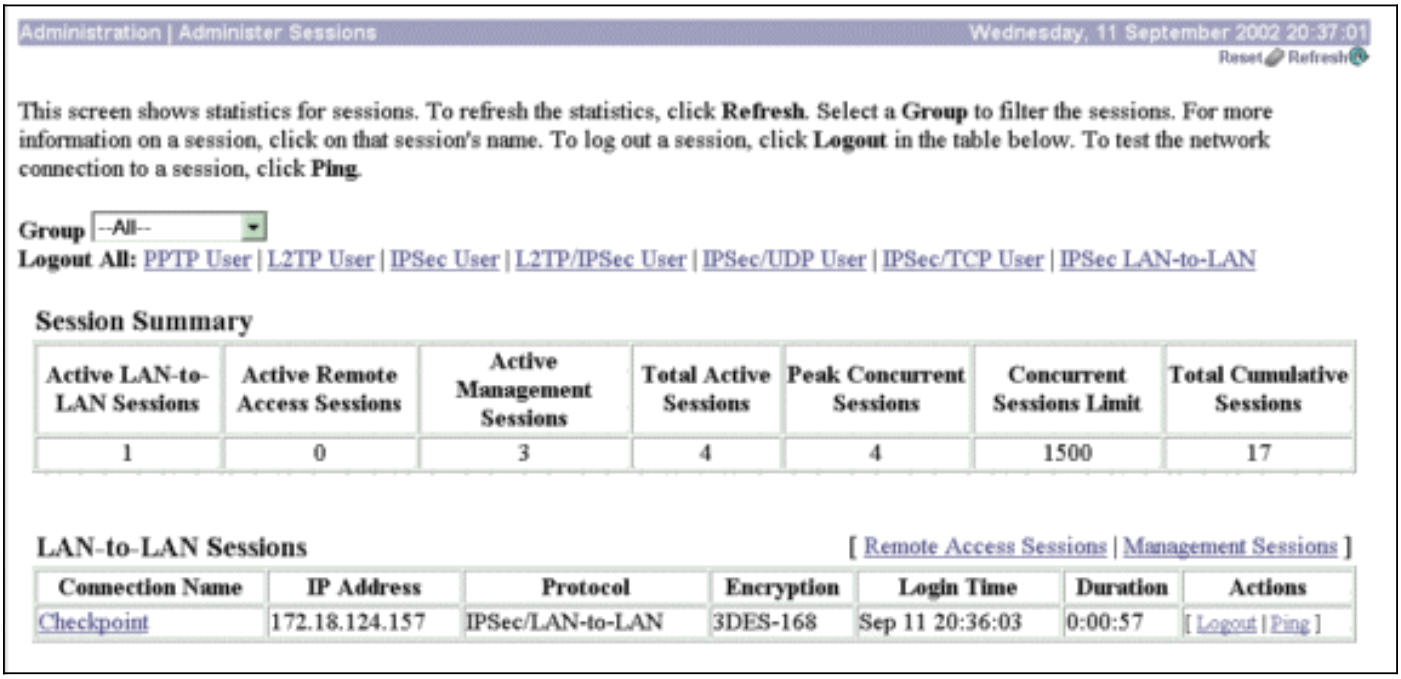
Visualizza stato tunnel su Checkpoint NG

Per visualizzare lo stato del tunnel, accedere all'Editor dei criteri e selezionare **Finestra > Stato del sistema**.

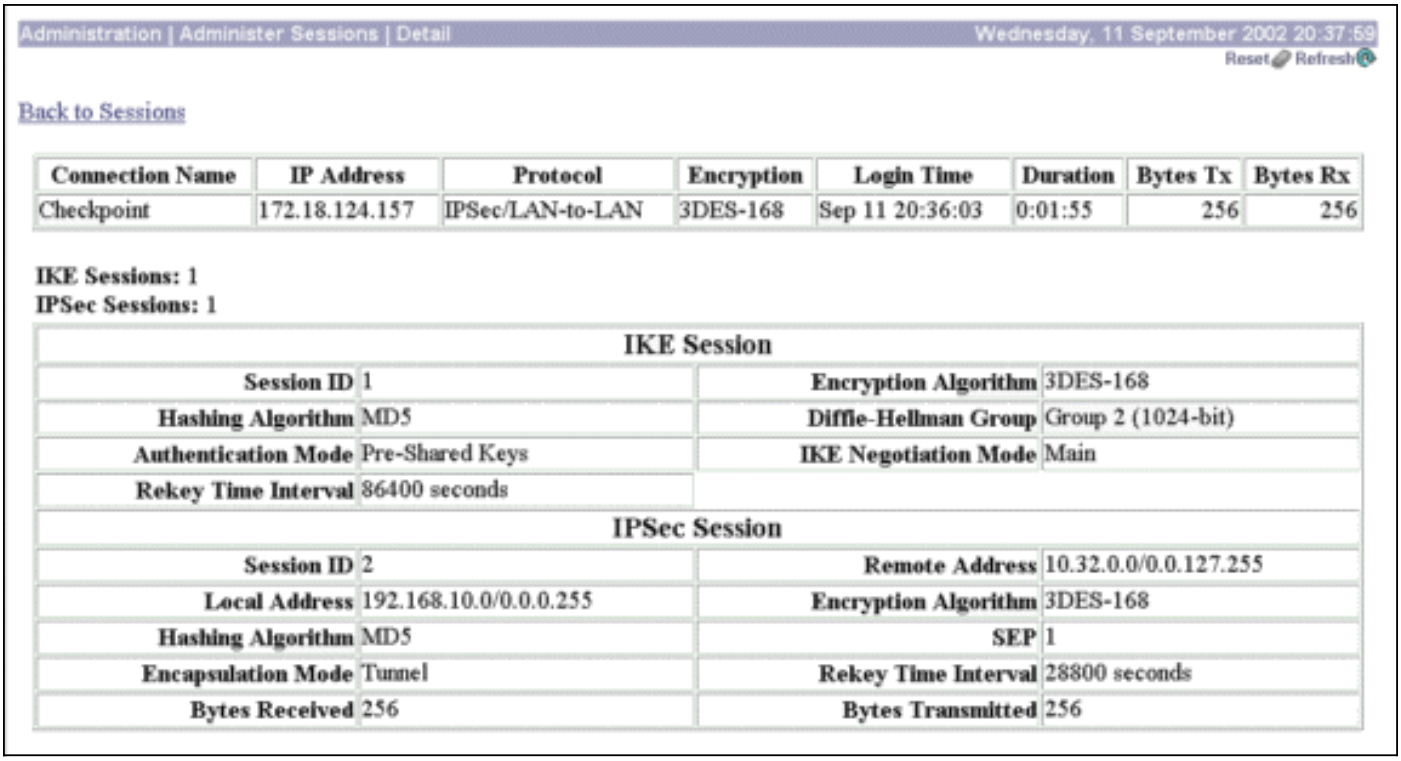


Visualizza stato tunnel su VPN Concentrator

Per verificare lo stato del tunnel sul concentratore VPN, selezionare **Amministrazione > Amministra sessioni**.



In Sessioni da LAN a LAN selezionare il nome della connessione per il checkpoint per visualizzare i dettagli sulle associazioni di protezione create e il numero di pacchetti trasmessi/ricevuti.



Administration | Administer Sessions | Detail — Wednesday, 11 September 2002 20:37:59

Reset Refresh

Back to Sessions

Connection Name	IP Address	Protocol	Encryption	Login Time	Duration	Bytes Tx	Bytes Rx
Checkpoint	172.18.124.157	IPSec/LAN-to-LAN	3DES-168	Sep 11 20:36:03	0:01:55	256	256

IKE Sessions: 1
IPSec Sessions: 1

IKE Session			
Session ID	1	**Encryption Algorithm**	3DES-168
Hashing Algorithm	MD5	**Diffie-Hellman Group**	Group 2 (1024-bit)
Authentication Mode	Pre-Shared Keys	**IKE Negotiation Mode**	Main
Rekey Time Interval	86400 seconds		
IPSec Session			
Session ID	2	**Remote Address**	10.32.0.0/0.0.127.255
Local Address	192.168.10.0/0.0.0.255	**Encryption Algorithm**	3DES-168
Hashing Algorithm	MD5	**SEP**	1
Encapsulation Mode	Tunnel	**Rekey Time Interval**	28800 seconds
Bytes Received	256	**Bytes Transmitted**	256

Risoluzione dei problemi

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

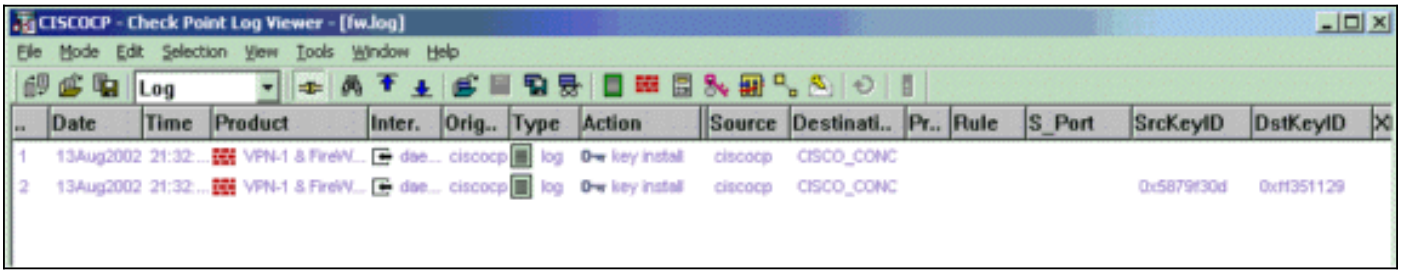
Nota: il traffico non deve essere indirizzato attraverso il tunnel IPSec utilizzando l'indirizzo IP pubblico (interfaccia esterna) di VPN Concentrator. In caso contrario, il tunnel non funzionerà. Pertanto, l'indirizzo IP utilizzato per il ping deve essere diverso da quello configurato sull'interfaccia esterna.

Riepilogo della rete

Quando più reti adiacenti all'interno vengono configurate nel dominio di crittografia sul punto di controllo, il dispositivo può riepilogare automaticamente le reti 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 riepilogare queste reti in 10.0.0.0 /23.

Debug del checkpoint NG

Per visualizzare i log, selezionare **Finestra > Visualizzatore log**.



Debug per VPN Concentrator

Per abilitare i debug su VPN Concentrator, selezionare **Configurazione > Sistema > Eventi > Classi**. Abilitare AUTH, AUTHDBG, IKE, IKEDBG, IPSEC e IPSECDBG per la gravità in modo che vengano registrati come 1 - 13. Per visualizzare i debug, selezionare **Monitoraggio > Registro eventi filtrabile**.

```
1 09/11/2002 20:36:03.610 SEV=8 IKEDBG/0 RPT=506 172.18.124.157
RECEIVED Message (msgid=0) with payloads :
HDR + SA (1) + VENDOR (13) + NONE (0) ... total length : 128

3 09/11/2002 20:36:03.610 SEV=9 IKEDBG/0 RPT=507 172.18.124.157
processing SA payload

4 09/11/2002 20:36:03.610 SEV=8 IKEDBG/0 RPT=508
Proposal # 1, Transform # 1, Type ISAKMP, Id IKE
Parsing received transform:
Phase 1 failure against global IKE proposal # 1:
Mismatched attr types for class Auth Method:
Rcv'd: Preshared Key
Cfg'd: XAUTH with Preshared Key (Initiator authenticated)

10 09/11/2002 20:36:03.610 SEV=8 IKEDBG/0 RPT=509
Phase 1 failure against global IKE proposal # 2:
Mismatched attr types for class DH Group:
Rcv'd: Oakley Group 2
Cfg'd: Oakley Group 1

13 09/11/2002 20:36:03.610 SEV=7 IKEDBG/0 RPT=510 172.18.124.157
Oakley proposal is acceptable

14 09/11/2002 20:36:03.610 SEV=9 IKEDBG/47 RPT=9 172.18.124.157
processing VID payload

15 09/11/2002 20:36:03.610 SEV=9 IKEDBG/0 RPT=511 172.18.124.157
processing IKE SA

16 09/11/2002 20:36:03.610 SEV=8 IKEDBG/0 RPT=512
Proposal # 1, Transform # 1, Type ISAKMP, Id IKE
Parsing received transform:
Phase 1 failure against global IKE proposal # 1:
Mismatched attr types for class Auth Method:
Rcv'd: Preshared Key
Cfg'd: XAUTH with Preshared Key (Initiator authenticated)

22 09/11/2002 20:36:03.610 SEV=8 IKEDBG/0 RPT=513
Phase 1 failure against global IKE proposal # 2:
Mismatched attr types for class DH Group:
Rcv'd: Oakley Group 2
Cfg'd: Oakley Group 1

25 09/11/2002 20:36:03.610 SEV=7 IKEDBG/28 RPT=9 172.18.124.157
IKE SA Proposal # 1, Transform # 1 acceptable
Matches global IKE entry # 3

26 09/11/2002 20:36:03.610 SEV=9 IKEDBG/0 RPT=514 172.18.124.157
constructing ISA_SA for isakmp

27 09/11/2002 20:36:03.610 SEV=8 IKEDBG/0 RPT=515 172.18.124.157
SENDING Message (msgid=0) with payloads :
HDR + SA (1) + NONE (0) ... total length : 84

29 09/11/2002 20:36:03.630 SEV=8 IKEDBG/0 RPT=516 172.18.124.157
```

```
RECEIVED Message (msgid=0) with payloads :
HDR + KE (4) + NONCE (10) + NONE (0) ... total length : 184

31 09/11/2002 20:36:03.630 SEV=8 IKEDBG/0 RPT=517 172.18.124.157
RECEIVED Message (msgid=0) with payloads :
HDR + KE (4) + NONCE (10) + NONE (0) ... total length : 184

33 09/11/2002 20:36:03.630 SEV=9 IKEDBG/0 RPT=518 172.18.124.157
processing ke payload

34 09/11/2002 20:36:03.630 SEV=9 IKEDBG/0 RPT=519 172.18.124.157
processing ISA_KE

35 09/11/2002 20:36:03.630 SEV=9 IKEDBG/1 RPT=91 172.18.124.157
processing nonce payload

36 09/11/2002 20:36:03.660 SEV=9 IKEDBG/0 RPT=520 172.18.124.157
constructing ke payload

37 09/11/2002 20:36:03.660 SEV=9 IKEDBG/1 RPT=92 172.18.124.157
constructing nonce payload

38 09/11/2002 20:36:03.660 SEV=9 IKEDBG/46 RPT=37 172.18.124.157
constructing Cisco Unity VID payload

39 09/11/2002 20:36:03.660 SEV=9 IKEDBG/46 RPT=38 172.18.124.157
constructing xauth V6 VID payload

40 09/11/2002 20:36:03.660 SEV=9 IKEDBG/48 RPT=19 172.18.124.157
Send IOS VID

41 09/11/2002 20:36:03.660 SEV=9 IKEDBG/38 RPT=10 172.18.124.157
Constructing VPN 3000 spoofing IOS Vendor ID payload (version: 1.0.0,
capabilities: 20000001)

43 09/11/2002 20:36:03.660 SEV=9 IKEDBG/46 RPT=39 172.18.124.157
constructing VID payload

44 09/11/2002 20:36:03.660 SEV=9 IKEDBG/48 RPT=20 172.18.124.157
Send Altiga GW VID

45 09/11/2002 20:36:03.660 SEV=9 IKEDBG/0 RPT=521 172.18.124.157
Generating keys for Responder...

46 09/11/2002 20:36:03.670 SEV=8 IKEDBG/0 RPT=522 172.18.124.157
SENDING Message (msgid=0) with payloads :
HDR + KE (4) + NONCE (10) ... total length : 256

48 09/11/2002 20:36:03.690 SEV=8 IKEDBG/0 RPT=523 172.18.124.157
RECEIVED Message (msgid=0) with payloads :
HDR + ID (5) + HASH (8) + NONE (0) ... total length : 60

50 09/11/2002 20:36:03.690 SEV=9 IKEDBG/1 RPT=93 172.18.124.157
Group [172.18.124.157]
Processing ID

51 09/11/2002 20:36:03.690 SEV=9 IKEDBG/0 RPT=524 172.18.124.157
Group [172.18.124.157]
processing hash

52 09/11/2002 20:36:03.690 SEV=9 IKEDBG/0 RPT=525 172.18.124.157
Group [172.18.124.157]
computing hash
```

```
53 09/11/2002 20:36:03.690 SEV=9 IKEDBG/23 RPT=10 172.18.124.157
Group [172.18.124.157]
Starting group lookup for peer 172.18.124.157

54 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/1 RPT=10
AUTH_Open() returns 9

55 09/11/2002 20:36:03.690 SEV=7 AUTH/12 RPT=10
Authentication session opened: handle = 9

56 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/3 RPT=10
AUTH_PutAttrTable(9, 748174)

57 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/6 RPT=10
AUTH_GroupAuthenticate(9, 2f1b19c, 49c648)

58 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/59 RPT=10
AUTH_BindServer(51a6b48, 0, 0)

59 09/11/2002 20:36:03.690 SEV=9 AUTHDBG/69 RPT=10
Auth Server e054d4 has been bound to ACB 51a6b48, sessions = 1

60 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/65 RPT=10
AUTH_CreateTimer(51a6b48, 0, 0)

61 09/11/2002 20:36:03.690 SEV=9 AUTHDBG/72 RPT=10
Reply timer created: handle = 4B0018

62 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/61 RPT=10
AUTH_BuildMsg(51a6b48, 0, 0)

63 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/64 RPT=10
AUTH_StartTimer(51a6b48, 0, 0)

64 09/11/2002 20:36:03.690 SEV=9 AUTHDBG/73 RPT=10
Reply timer started: handle = 4B0018, timestamp = 1163319,
timeout = 30000

65 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/62 RPT=10
AUTH_SndRequest(51a6b48, 0, 0)

66 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/50 RPT=19
IntDB_Decode(3825300, 156)

67 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/47 RPT=19
IntDB_Xmt(51a6b48)

68 09/11/2002 20:36:03.690 SEV=9 AUTHDBG/71 RPT=10
xmit_cnt = 1

69 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/47 RPT=20
IntDB_Xmt(51a6b48)

70 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/49 RPT=10
IntDB_Match(51a6b48, 3eb7ab0)

71 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/63 RPT=10
AUTH_RcvReply(51a6b48, 0, 0)

72 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/50 RPT=20
IntDB_Decode(3eb7ab0, 298)

73 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/48 RPT=10
IntDB_Rcv(51a6b48)
```

```
74 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/66 RPT=10
AUTH_DeleteTimer(51a6b48, 0, 0)

75 09/11/2002 20:36:03.790 SEV=9 AUTHDBG/74 RPT=10
Reply timer stopped: handle = 4B0018, timestamp = 1163329

76 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/58 RPT=10
AUTH_Callback(51a6b48, 0, 0)

77 09/11/2002 20:36:03.790 SEV=6 AUTH/41 RPT=10 172.18.124.157
Authentication successful: handle = 9, server = Internal,
group = 172.18.124.157

78 09/11/2002 20:36:03.790 SEV=7 IKEDBG/0 RPT=526 172.18.124.157
Group [172.18.124.157]
Found Phase 1 Group (172.18.124.157)

79 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/4 RPT=10
AUTH_GetAttrTable(9, 748420)

80 09/11/2002 20:36:03.790 SEV=7 IKEDBG/14 RPT=10 172.18.124.157
Group [172.18.124.157]
Authentication configured for Internal

81 09/11/2002 20:36:03.790 SEV=9 IKEDBG/19 RPT=19 172.18.124.157
Group [172.18.124.157]
IKEGetUserAttributes: IP Compression = disabled

82 09/11/2002 20:36:03.790 SEV=9 IKEDBG/19 RPT=20 172.18.124.157
Group [172.18.124.157]
IKEGetUserAttributes: Split Tunneling Policy = Disabled

83 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/2 RPT=10
AUTH_Close(9)

84 09/11/2002 20:36:03.790 SEV=9 IKEDBG/1 RPT=94 172.18.124.157
Group [172.18.124.157]
constructing ID

85 09/11/2002 20:36:03.790 SEV=9 IKEDBG/0 RPT=527
Group [172.18.124.157]
construct hash payload

86 09/11/2002 20:36:03.790 SEV=9 IKEDBG/0 RPT=528 172.18.124.157
Group [172.18.124.157]
computing hash

87 09/11/2002 20:36:03.790 SEV=9 IKEDBG/46 RPT=40 172.18.124.157
Group [172.18.124.157]
constructing dpd vid payload

88 09/11/2002 20:36:03.790 SEV=8 IKEDBG/0 RPT=529 172.18.124.157
SENDING Message (msgid=0) with payloads :
HDR + ID (5) + HASH (8) ... total length : 80

90 09/11/2002 20:36:03.790 SEV=4 IKE/119 RPT=10 172.18.124.157
Group [172.18.124.157]
PHASE 1 COMPLETED

91 09/11/2002 20:36:03.790 SEV=6 IKE/121 RPT=10 172.18.124.157
Keep-alive type for this connection: None

92 09/11/2002 20:36:03.790 SEV=6 IKE/122 RPT=10 172.18.124.157
```

```
Keep-alives configured on but peer does not
support keep-alives (type = None)

93 09/11/2002 20:36:03.790 SEV=7 IKEDBG/0 RPT=530 172.18.124.157
Group [172.18.124.157]
Starting phase 1 rekey timer: 64800000 (ms)

94 09/11/2002 20:36:03.790 SEV=4 AUTH/22 RPT=16
User 172.18.124.157 connected

95 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/60 RPT=10
AUTH_UnbindServer(51a6b48, 0, 0)

96 09/11/2002 20:36:03.790 SEV=9 AUTHDBG/70 RPT=10
Auth Server e054d4 has been unbound from ACB 51a6b48, sessions = 0

97 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/10 RPT=10
AUTH_Int_FreeAuthCB(51a6b48)

98 09/11/2002 20:36:03.790 SEV=7 AUTH/13 RPT=10
Authentication session closed: handle = 9

99 09/11/2002 20:36:03.790 SEV=8 IKEDBG/0 RPT=531 172.18.124.157
RECEIVED Message (msgid=54796f76) with payloads :
HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0)
... total length : 156

102 09/11/2002 20:36:03.790 SEV=9 IKEDBG/0 RPT=532 172.18.124.157
Group [172.18.124.157]
processing hash

103 09/11/2002 20:36:03.790 SEV=9 IKEDBG/0 RPT=533 172.18.124.157
Group [172.18.124.157]
processing SA payload

104 09/11/2002 20:36:03.790 SEV=9 IKEDBG/1 RPT=95 172.18.124.157
Group [172.18.124.157]
processing nonce payload

105 09/11/2002 20:36:03.790 SEV=9 IKEDBG/1 RPT=96 172.18.124.157
Group [172.18.124.157]
Processing ID

106 09/11/2002 20:36:03.790 SEV=5 IKE/35 RPT=6 172.18.124.157
Group [172.18.124.157]
Received remote IP Proxy Subnet data in ID Payload:
Address 10.32.0.0, Mask 255.255.128.0, Protocol 0, Port 0

109 09/11/2002 20:36:03.790 SEV=9 IKEDBG/1 RPT=97 172.18.124.157
Group [172.18.124.157]
Processing ID

110 09/11/2002 20:36:03.790 SEV=5 IKE/34 RPT=6 172.18.124.157
Group [172.18.124.157]
Received local IP Proxy Subnet data in ID Payload:
Address 192.168.10.0, Mask 255.255.255.0, Protocol 0, Port 0

113 09/11/2002 20:36:03.790 SEV=8 IKEDBG/0 RPT=534
QM IsRekeyed old sa not found by addr

114 09/11/2002 20:36:03.790 SEV=5 IKE/66 RPT=8 172.18.124.157
Group [172.18.124.157]
IKE Remote Peer configured for SA: L2L: Checkpoint
```

```
115 09/11/2002 20:36:03.790 SEV=9 IKEDBG/0 RPT=535 172.18.124.157
Group [172.18.124.157]
processing IPSEC SA

116 09/11/2002 20:36:03.790 SEV=7 IKEDBG/27 RPT=8 172.18.124.157
Group [172.18.124.157]
IPSec SA Proposal # 1, Transform # 1 acceptable

117 09/11/2002 20:36:03.790 SEV=7 IKEDBG/0 RPT=536 172.18.124.157
Group [172.18.124.157]
IKE: requesting SPI!

118 09/11/2002 20:36:03.790 SEV=9 IPSECDBG/6 RPT=39
IPSEC key message parse - msgtype 6, len 200, vers 1, pid 00000000,
seq 10, err 0, type 2, mode 0, state 32, label 0, pad 0,
spi 00000000, encrKeyLen 0, hashKeyLen 0, ivlen 0, alg 0, hmacAlg 0,
lifetype 0, lifetime1 17248580, lifetime2 0, dsId 300

122 09/11/2002 20:36:03.790 SEV=9 IPSECDBG/1 RPT=139
Processing KEY_GETSPI msg!

123 09/11/2002 20:36:03.790 SEV=7 IPSECDBG/13 RPT=10
Reserved SPI 305440147

124 09/11/2002 20:36:03.790 SEV=8 IKEDBG/6 RPT=10
IKE got SPI from key engine: SPI = 0x1234a593

125 09/11/2002 20:36:03.790 SEV=9 IKEDBG/0 RPT=537 172.18.124.157
Group [172.18.124.157]
oakley constucting quick mode

126 09/11/2002 20:36:03.800 SEV=9 IKEDBG/0 RPT=538 172.18.124.157
Group [172.18.124.157]
constructing blank hash

127 09/11/2002 20:36:03.800 SEV=9 IKEDBG/0 RPT=539 172.18.124.157
Group [172.18.124.157]
constructing ISA_SA for ipsec

128 09/11/2002 20:36:03.800 SEV=9 IKEDBG/1 RPT=98 172.18.124.157
Group [172.18.124.157]
constructing ipsec nonce payload

129 09/11/2002 20:36:03.800 SEV=9 IKEDBG/1 RPT=99 172.18.124.157
Group [172.18.124.157]
constructing proxy ID

130 09/11/2002 20:36:03.800 SEV=7 IKEDBG/0 RPT=540 172.18.124.157
Group [172.18.124.157]
Transmitting Proxy Id:
Remote subnet: 10.32.0.0 Mask 255.255.128.0 Protocol 0 Port 0
Local subnet: 192.168.10.0 mask 255.255.255.0 Protocol 0 Port 0

134 09/11/2002 20:36:03.800 SEV=9 IKEDBG/0 RPT=541 172.18.124.157
Group [172.18.124.157]
constructing qm hash

135 09/11/2002 20:36:03.800 SEV=8 IKEDBG/0 RPT=542 172.18.124.157
SENDING Message (msgid=54796f76) with payloads :
HDR + HASH (8) + SA (1) ... total length : 152

137 09/11/2002 20:36:03.800 SEV=8 IKEDBG/0 RPT=543 172.18.124.157
RECEIVED Message (msgid=54796f76) with payloads :
HDR + HASH (8) + NONE (0) ... total length : 48
```

```
139 09/11/2002 20:36:03.800 SEV=9 IKEDBG/0 RPT=544 172.18.124.157
Group [172.18.124.157]
processing hash

140 09/11/2002 20:36:03.800 SEV=9 IKEDBG/0 RPT=545 172.18.124.157
Group [172.18.124.157]
loading all IPSEC SAs

141 09/11/2002 20:36:03.800 SEV=9 IKEDBG/1 RPT=100 172.18.124.157
Group [172.18.124.157]
Generating Quick Mode Key!

142 09/11/2002 20:36:03.800 SEV=9 IKEDBG/1 RPT=101 172.18.124.157
Group [172.18.124.157]
Generating Quick Mode Key!

143 09/11/2002 20:36:03.800 SEV=7 IKEDBG/0 RPT=546 172.18.124.157
Group [172.18.124.157]
Loading subnet:
Dst: 192.168.10.0 mask: 255.255.255.0
Src: 10.32.0.0 mask: 255.255.128.0

146 09/11/2002 20:36:03.800 SEV=4 IKE/49 RPT=7 172.18.124.157
Group [172.18.124.157]
Security negotiation complete for LAN-to-LAN Group (172.18.124.157)
Responder, Inbound SPI = 0x1234a593, Outbound SPI = 0x0df37959

149 09/11/2002 20:36:03.800 SEV=9 IPSECDBG/6 RPT=40
IPSEC key message parse - msgtype 1, len 606, vers 1, pid 00000000,
seq 0, err 0, type 2, mode 1, state 64, label 0, pad 0,
spi 0df37959, encrKeyLen 24, hashKeyLen 16, ivlen 8, alg 2, hmacAlg 3,
lifetype 0, lifetime1 17248580, lifetime2 0, dsId 0

153 09/11/2002 20:36:03.800 SEV=9 IPSECDBG/1 RPT=140
Processing KEY_ADD msg!

154 09/11/2002 20:36:03.800 SEV=9 IPSECDBG/1 RPT=141
key_msghdr2secassoc(): Enter

155 09/11/2002 20:36:03.800 SEV=7 IPSECDBG/1 RPT=142
No USER filter configured

156 09/11/2002 20:36:03.800 SEV=9 IPSECDBG/1 RPT=143
KeyProcessAdd: Enter

157 09/11/2002 20:36:03.800 SEV=8 IPSECDBG/1 RPT=144
KeyProcessAdd: Adding outbound SA

158 09/11/2002 20:36:03.800 SEV=8 IPSECDBG/1 RPT=145
KeyProcessAdd: src 192.168.10.0 mask 0.0.0.255,
dst 10.32.0.0 mask 0.0.127.255

159 09/11/2002 20:36:03.810 SEV=8 IPSECDBG/1 RPT=146
KeyProcessAdd: FilterIpsecAddIkeSa success

160 09/11/2002 20:36:03.810 SEV=9 IPSECDBG/6 RPT=41
IPSEC key message parse - msgtype 3, len 327, vers 1, pid 00000000,
seq 0, err 0, type 2, mode 1, state 32, label 0, pad 0,
spi 1234a593, encrKeyLen 24, hashKeyLen 16, ivlen 8, alg 2, hmacAlg 3,
lifetype 0, lifetime1 17248580, lifetime2 0, dsId 0

164 09/11/2002 20:36:03.810 SEV=9 IPSECDBG/1 RPT=147
Processing KEY_UPDATE msg!
```

```
165 09/11/2002 20:36:03.810 SEV=9 IPSECDBG/1 RPT=148
Update inbound SA addresses

166 09/11/2002 20:36:03.810 SEV=9 IPSECDBG/1 RPT=149
key_msghdr2secassoc(): Enter

167 09/11/2002 20:36:03.810 SEV=7 IPSECDBG/1 RPT=150
No USER filter configured

168 09/11/2002 20:36:03.810 SEV=9 IPSECDBG/1 RPT=151
KeyProcessUpdate: Enter

169 09/11/2002 20:36:03.810 SEV=8 IPSECDBG/1 RPT=152
KeyProcessUpdate: success

170 09/11/2002 20:36:03.810 SEV=8 IKEDBG/7 RPT=7
IKE got a KEY_ADD msg for SA: SPI = 0x0df37959

171 09/11/2002 20:36:03.810 SEV=8 IKEDBG/0 RPT=547
pitcher: rcv KEY_UPDATE, spi 0x1234a593

172 09/11/2002 20:36:03.810 SEV=4 IKE/120 RPT=7 172.18.124.157
Group [172.18.124.157]
PHASE 2 COMPLETED (msgid=54796f76)
```

Informazioni correlate

- Cisco VPN serie 3000 Concentrator Support Page
- Cisco VPN serie 3000 Client Support Page
- Pagina di supporto per IPSec
- Supporto tecnico – Cisco Systems