

# Configurazione di un tunnel IPSec tra un'istanza di Checkpoint e un router

## Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Esempio di rete](#)

[Convenzioni](#)

[Configurazione di Cisco 1751 VPN Router](#)

[Configurazione del checkpoint NG](#)

[Verifica](#)

[Verifica del router Cisco](#)

[Verifica NG checkpoint](#)

[Risoluzione dei problemi](#)

[Cisco Router](#)

[Informazioni correlate](#)

## Introduzione

In questo documento viene illustrato come formare un tunnel IPSec con chiavi già condivise per collegarsi a due reti private:

- La rete privata 172.16.15.x all'interno del router.
- La rete privata 192.168.10.x all'interno di <sup>Checkpoint™</sup> Next Generation (NG).

## Prerequisiti

### Requisiti

Le procedure descritte nel presente documento si basano su queste ipotesi.

- Il criterio di base <sup>Checkpoint™</sup> NG è impostato.
- Vengono configurate tutte le impostazioni di accesso, NAT (Network Address Translation) e routing.
- Il traffico tra il router e l'interno del <sup>checkpoint™</sup> NG e i flussi Internet.

## Componenti usati

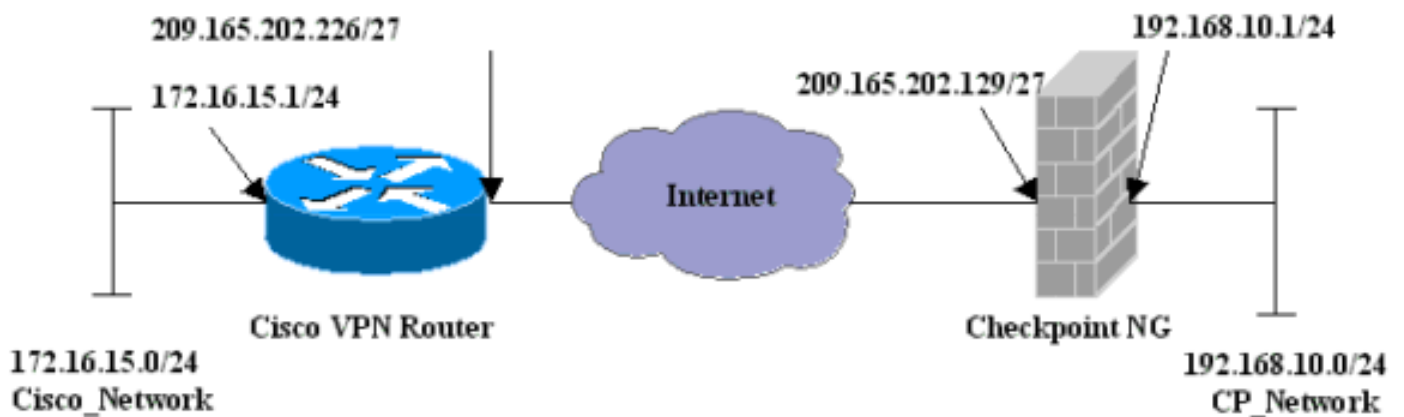
Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco 1751 Router
- Software Cisco IOS® (C1700-K9O3SY7-M), versione 12.2(8)T4, RELEASE SOFTWARE (fc1)
- Checkpoint™ NG Build 50027

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 di Cisco 1751 VPN Router

### Cisco VPN 1751 Router

```
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
hostname svl-6
memory-size iomem 15
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip subnet-zero
no ip domain-lookup
ip audit notify log
ip audit po max-events 100
!--- Internet Key Exchange (IKE) configuration. crypto
isakmp policy 1
  encr 3des
```

```

hash md5
authentication pre-share
group 2
lifetime 1800
!--- IPsec configuration. crypto isakmp key aptrules
address 209.165.202.129
!
crypto ipsec transform-set aptset esp-3des esp-md5-hmac
!
crypto map aptmap 1 ipsec-isakmp
  set peer 209.165.202.129
  set transform-set aptset
  match address 110
!
interface Ethernet0/0
  ip address 209.165.202.226 255.255.255.224
  ip nat outside
  half-duplex
  crypto map aptmap
!
interface FastEthernet0/0
  ip address 172.16.15.1 255.255.255.0
  ip nat inside
  speed auto
!--- NAT configuration. ip nat inside source route-map
nonat interface Ethernet0/0 overload
ip classless
ip route 0.0.0.0 0.0.0.0 209.165.202.225
no ip http server
ip pim bidir-enable
!--- Encryption match address access list. access-list
110 permit ip 172.16.15.0 0.0.0.255 192.168.10.0
0.0.0.255
!--- NAT access list. access-list 120 deny ip
172.16.15.0 0.0.0.255 192.168.10.0 0.0.0.255
access-list 120 permit ip 172.16.15.0 0.0.0.255 any
route-map nonat permit 10
  match ip address 120
line con 0
  exec-timeout 0 0
line aux 0
line vty 0 4
  password cisco
  login
end

```

## Configurazione del checkpoint NG

Checkpoint<sup>TM</sup> NG è una configurazione orientata agli oggetti. Gli oggetti e le regole di rete vengono definiti per creare il criterio relativo alla configurazione VPN da configurare. Questo criterio viene quindi installato utilizzando Checkpoint<sup>TM</sup> NG Policy Editor per completare il lato Checkpoint<sup>TM</sup> NG della configurazione VPN.

1. Creare la subnet di rete Cisco e la subnet di rete Checkpoint<sup>TM</sup> NG come oggetti di rete. Questo è ciò che è criptato. Per creare gli oggetti, selezionare **Gestisci > Oggetti di rete**, quindi selezionare **Nuovo > Rete**. Immettere le informazioni di rete appropriate, quindi fare clic su **OK**. In questi esempi viene illustrata una serie di oggetti denominati CP\_Network e

Network Properties - CP\_Network

General NAT

Name: CP\_Network

IP Address: 192.168.10.0

Net Mask: 255.255.255.0

Comment:

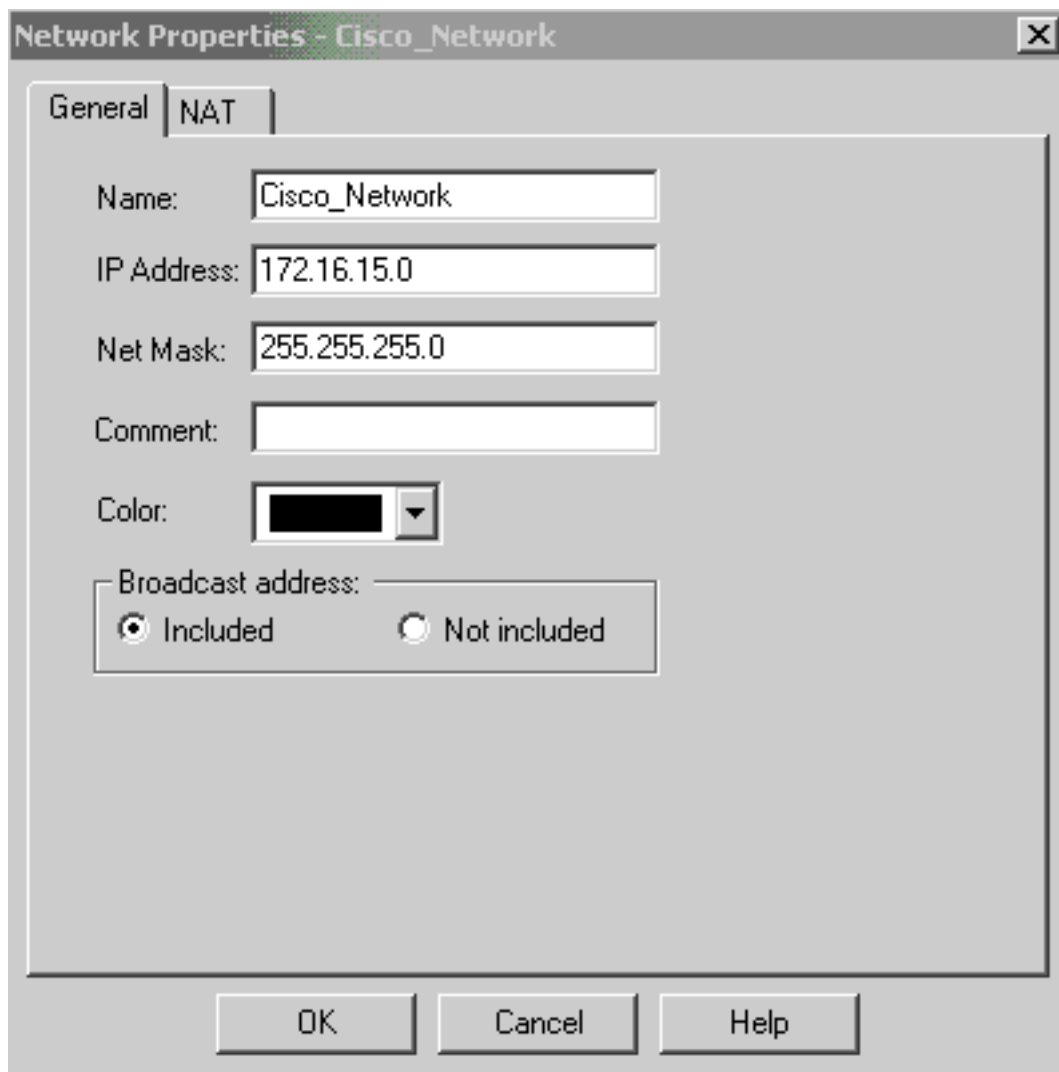
Color:

Broadcast address:

Included  Not included

OK Cancel Help

Cisco\_Network.



2. Create gli oggetti Cisco\_Router e Checkpoint\_NG come oggetti workstation. Questi sono i dispositivi VPN. Per creare gli oggetti, selezionare **Gestisci > Oggetti di rete**, quindi selezionare **Nuovo > Workstation**. 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**. In questi esempi viene illustrata una serie di oggetti denominati chef e Cisco\_Router.

## General

Topology

NAT

VPN

Authentication

Management

+ Advanced

## General

Name: chef

IP Address: 209.165.202.129

Get address

Comment: CP\_Server

Color: Type:  Host  Gateway

Check Point Products

 Check Point products installed: Version NG 

- 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)

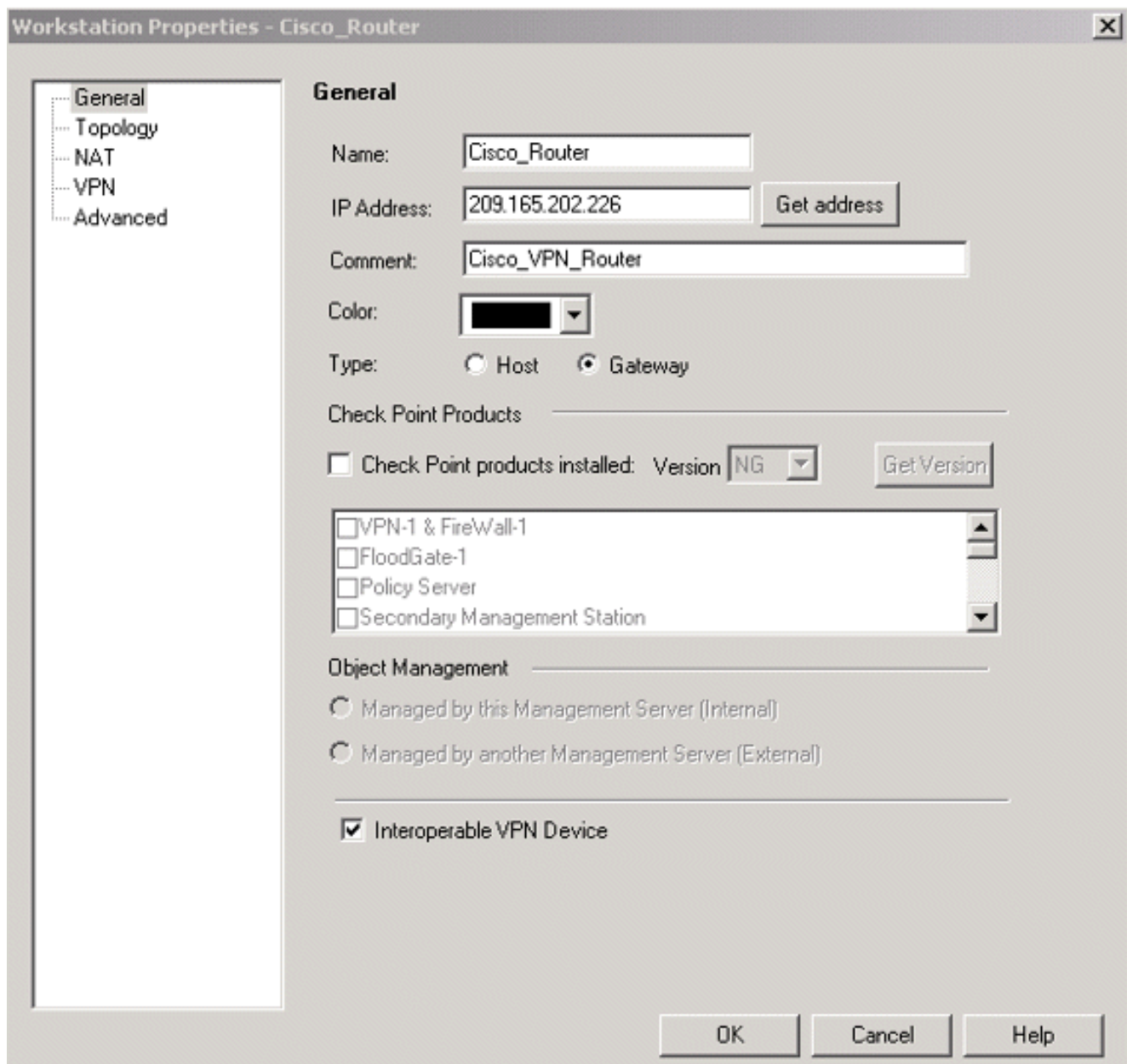
Secure Internal Communication

 DN: cn=cp\_mgmt,o=chef.6h9tua Interoperable VPN Device

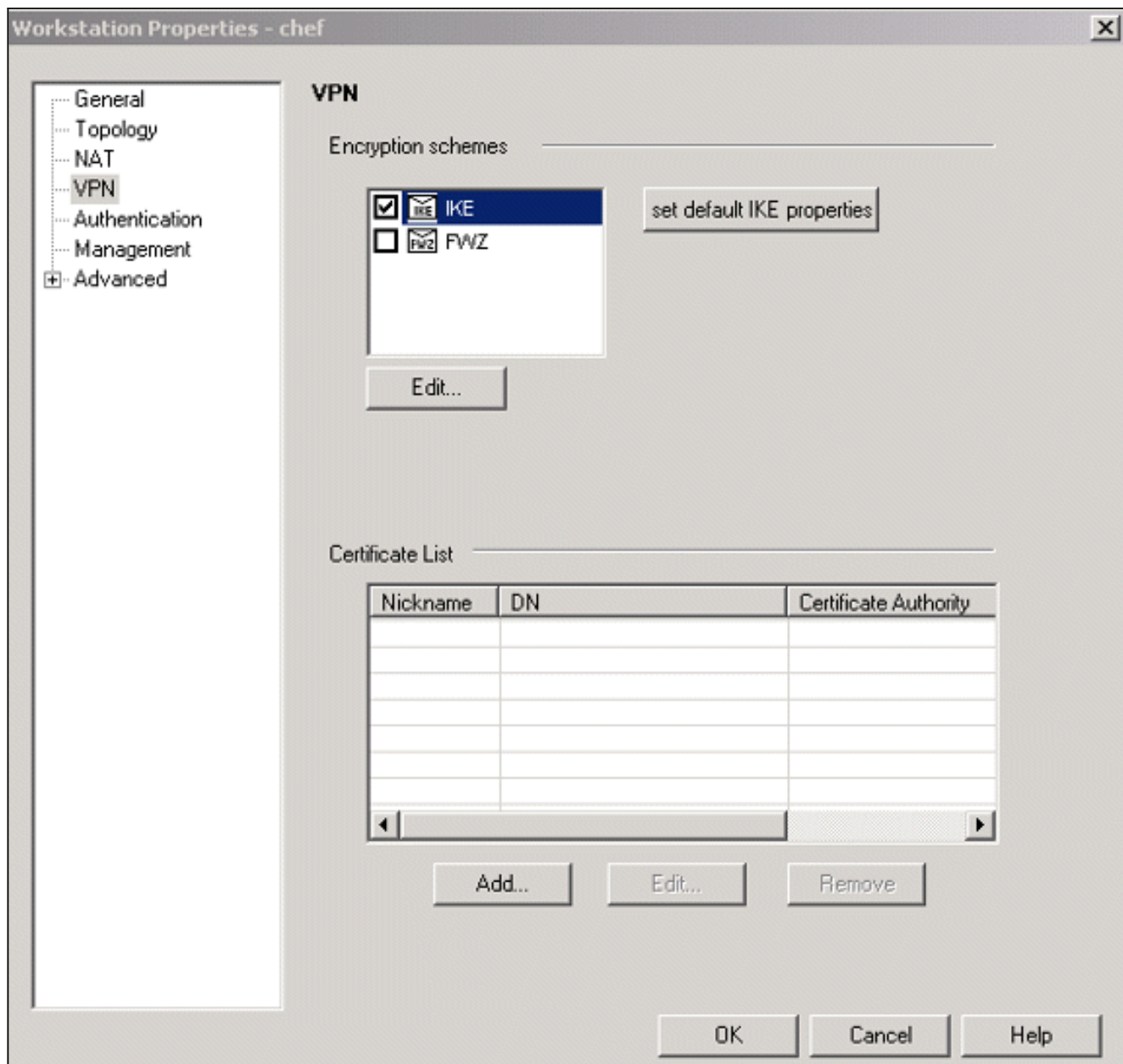
OK

Cancel

Help

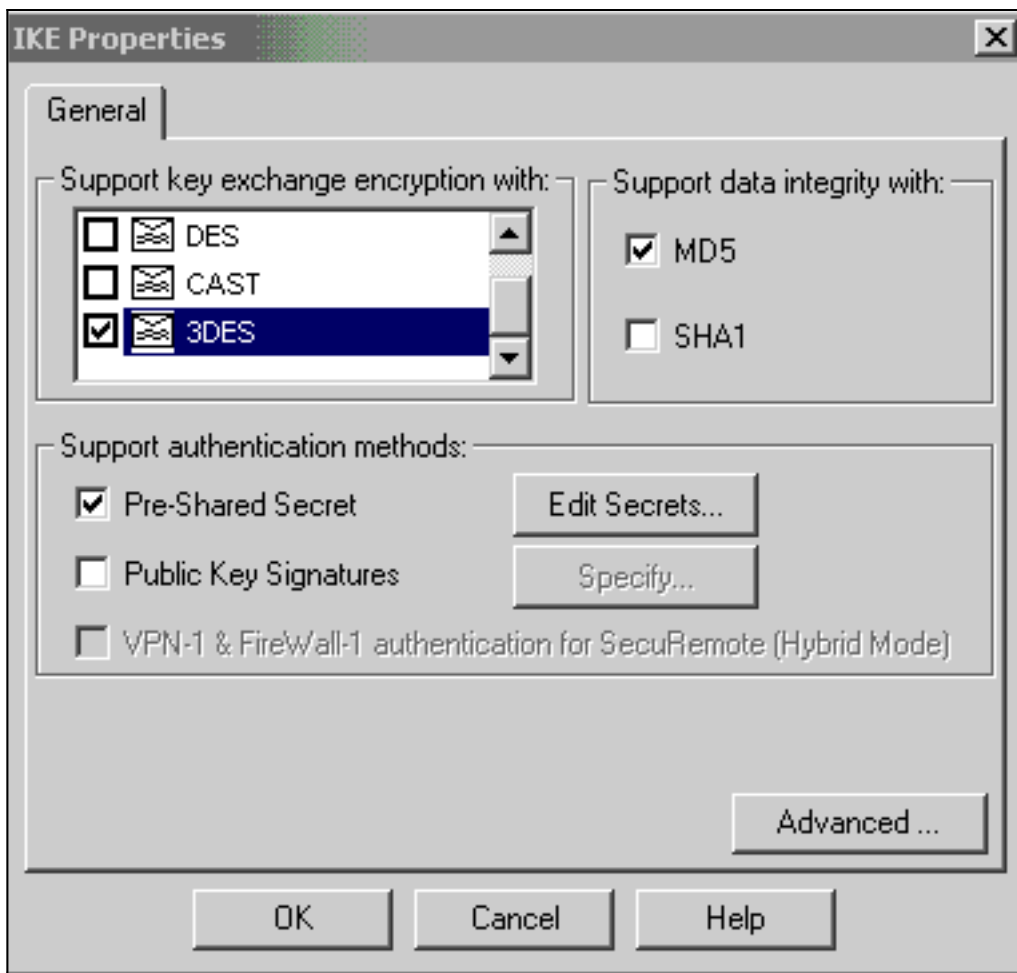


3. Configurare IKE nella scheda VPN, quindi fare clic su **Modifica**.



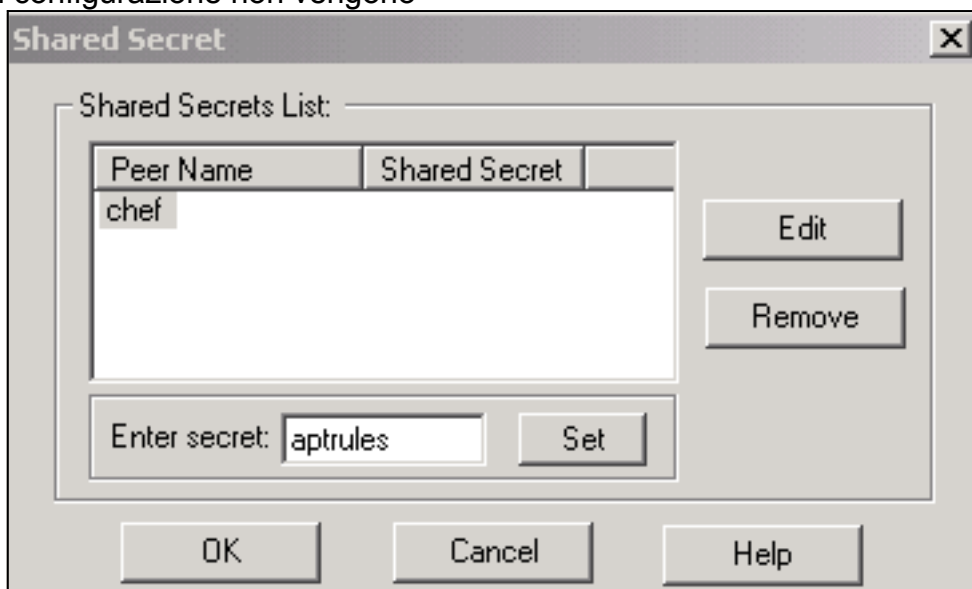
4. Configurare il criterio di scambio chiavi e fare clic su **Modifica**





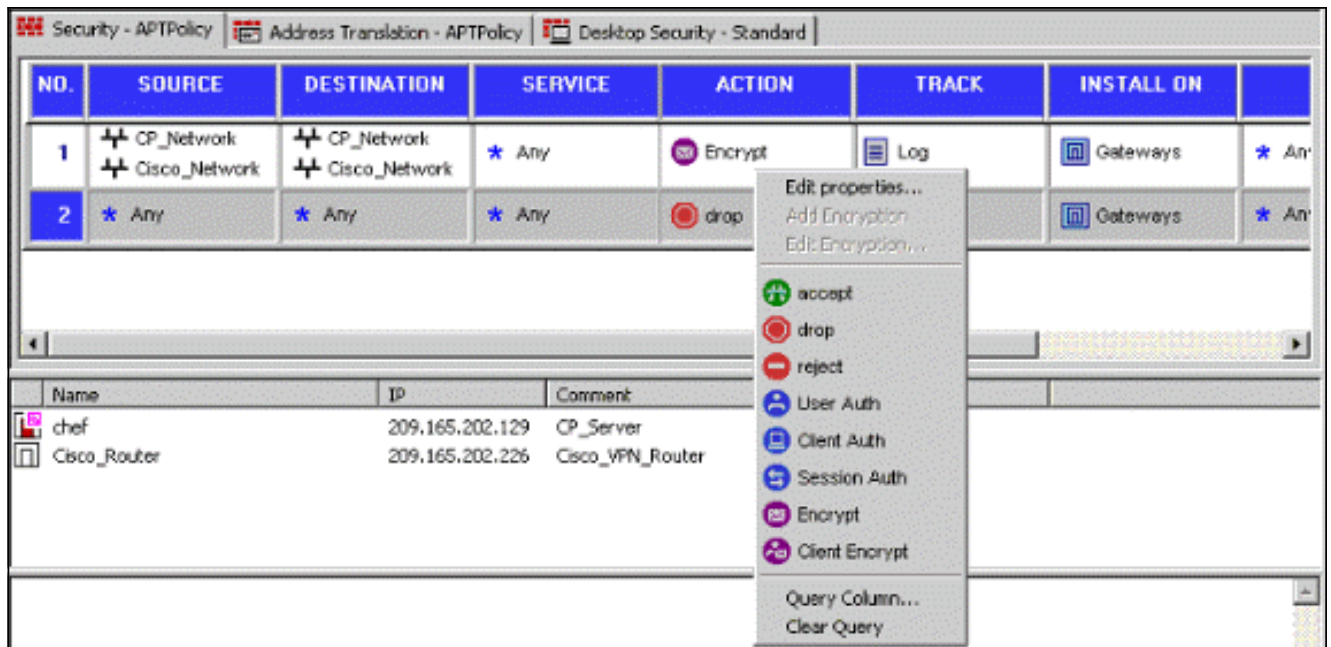
segreti.

5. Impostare le chiavi già condivise da utilizzare, quindi fare clic su **OK** più volte fino a quando le finestre di configurazione non vengono

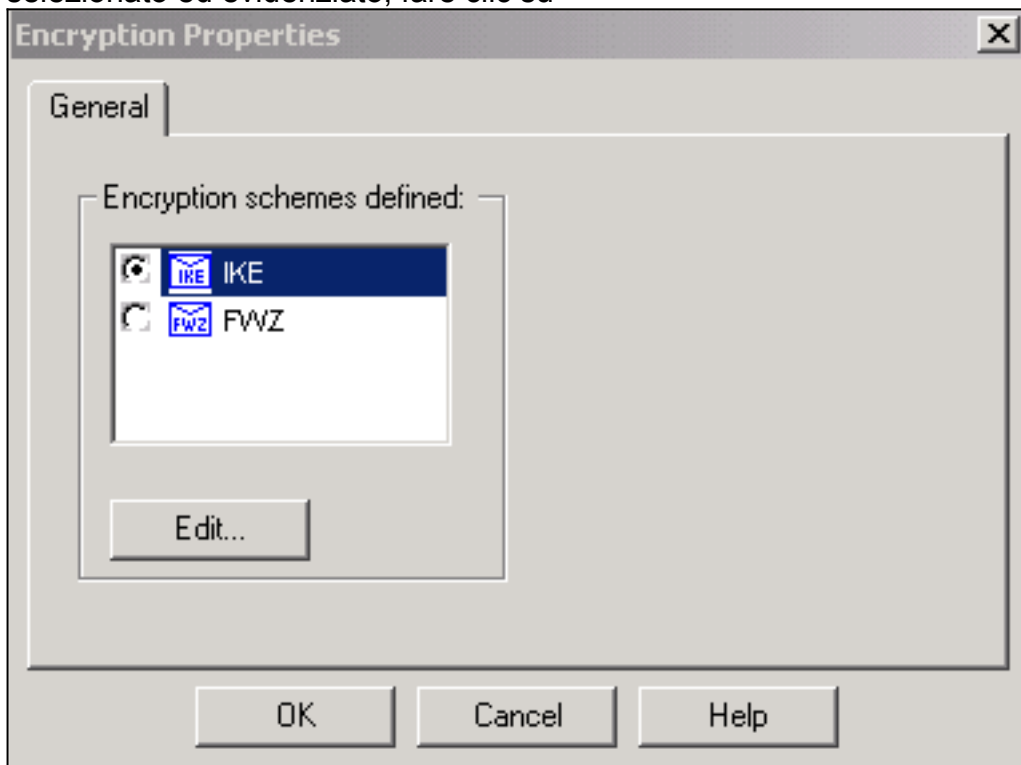


visualizzate.

6. Selezionare **Regole > Aggiungi regole > In alto** per configurare le regole di crittografia per il criterio. La regola in alto è la prima regola eseguita prima di qualsiasi altra regola che potrebbe ignorare la crittografia. Configurare l'origine e la destinazione in modo da includere CP\_Network e Cisco\_Network, come mostrato di seguito. Dopo aver aggiunto la sezione Azione crittografia della regola, fare clic con il pulsante destro del mouse su **Azione** e selezionare **Modifica proprietà**.

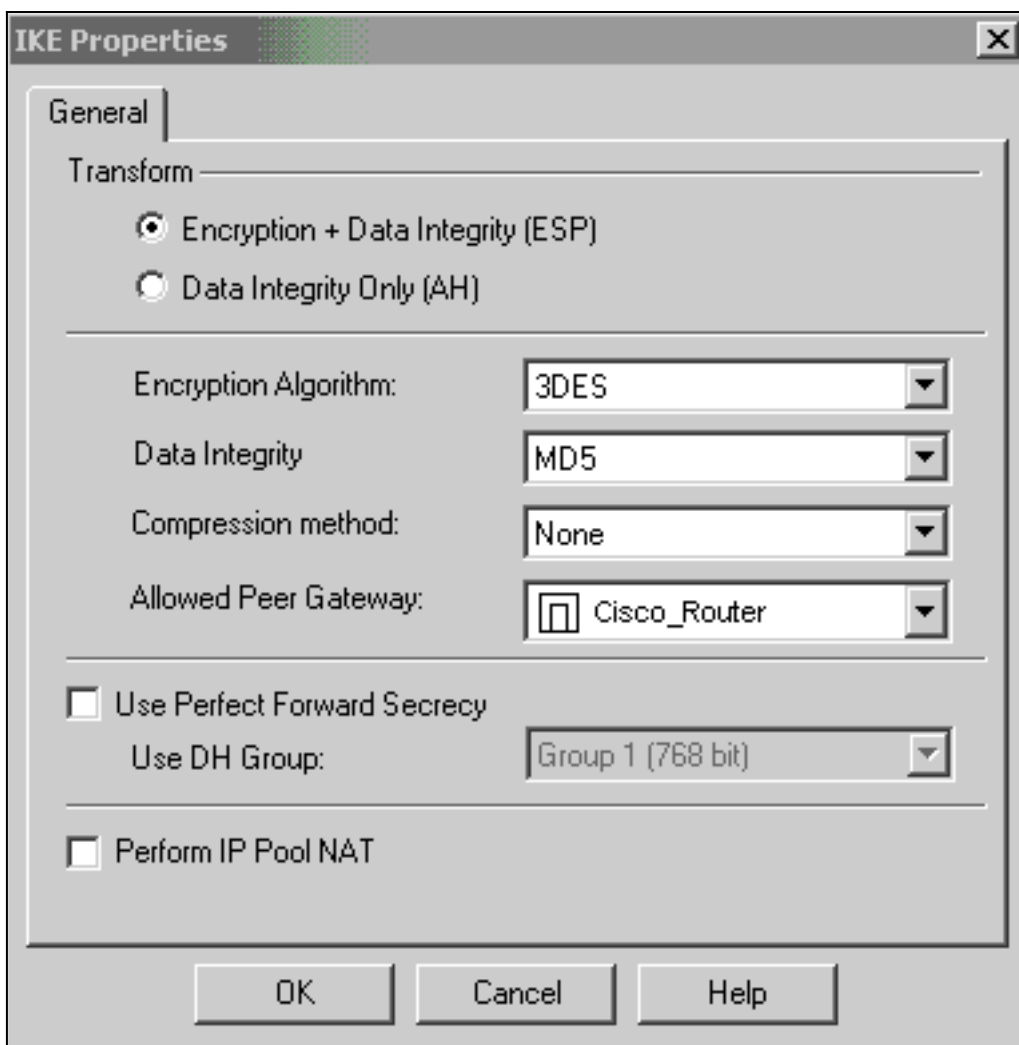


7. Con IKE selezionato ed evidenziato, fare clic su



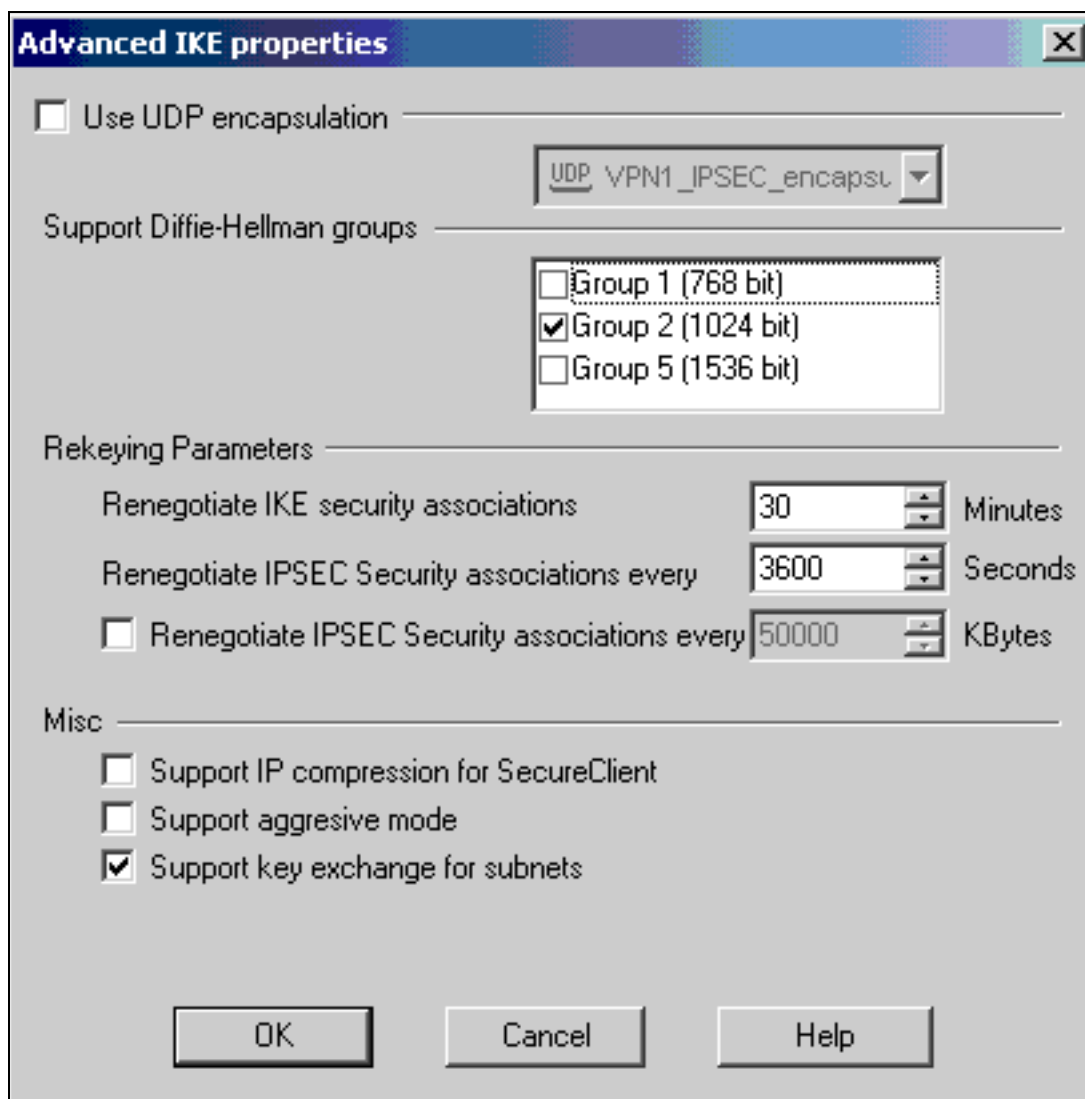
Modifica.

8. Confermare la configurazione



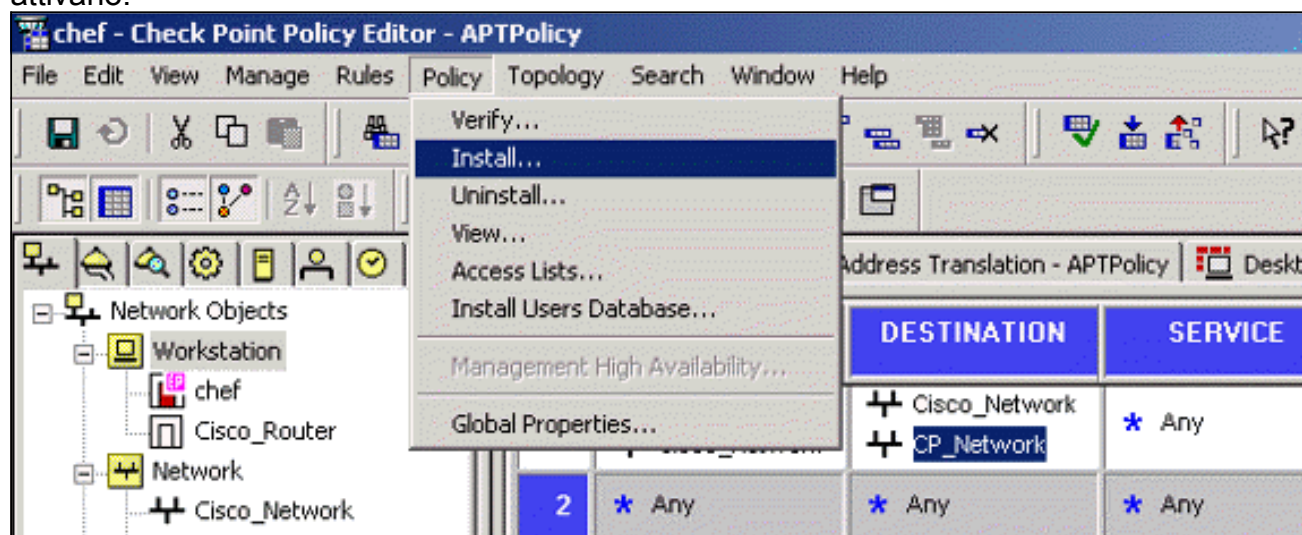
IKE.

9. Uno dei problemi principali con l'esecuzione della VPN tra i dispositivi Cisco e altri dispositivi IPsec è la rinegoziazione dello scambio di chiavi. Verificare che l'impostazione per lo scambio IKE sul router Cisco sia esattamente la stessa di quella configurata sul <sup>checkpointTM</sup> NG. **Nota:** il valore effettivo di questo parametro dipende dal criterio di sicurezza aziendale specifico. Nell'esempio, la [configurazione IKE sul router](#) è stata impostata su 30 minuti con il comando **lifetime 1800**. Lo stesso valore deve essere impostato sul <sup>checkpointTM</sup> NG. Per impostare questo valore su <sup>CheckpointTM</sup> NG, selezionare **Gestisci oggetto di rete**, quindi selezionare l'oggetto <sup>CheckpointTM</sup> NG e fare clic su **Modifica**. Quindi selezionare **VPN** e modificare IKE. Selezionare **Avanzamento** e configurare i parametri di rigenerazione delle chiavi. Dopo aver configurato lo scambio di chiave per l'oggetto di rete <sup>CheckpointTM</sup> NG, eseguire la stessa configurazione della rinegoziazione dello scambio di chiave per l'oggetto di rete Cisco\_Router. **Nota:** verificare di aver selezionato il gruppo Diffie-Hellman corretto in modo che corrisponda a quello configurato sul

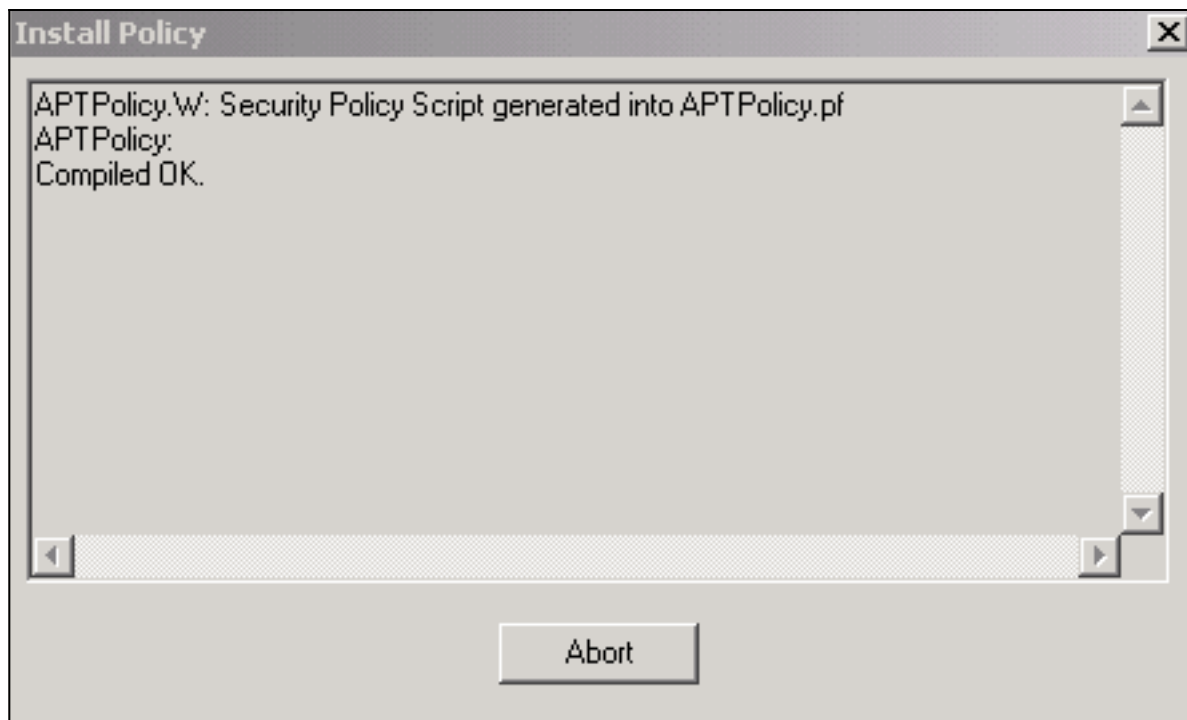


router.

10. Configurazione dei criteri completata. Salvare il criterio e selezionare **Criterio > Installa** per attivarlo.

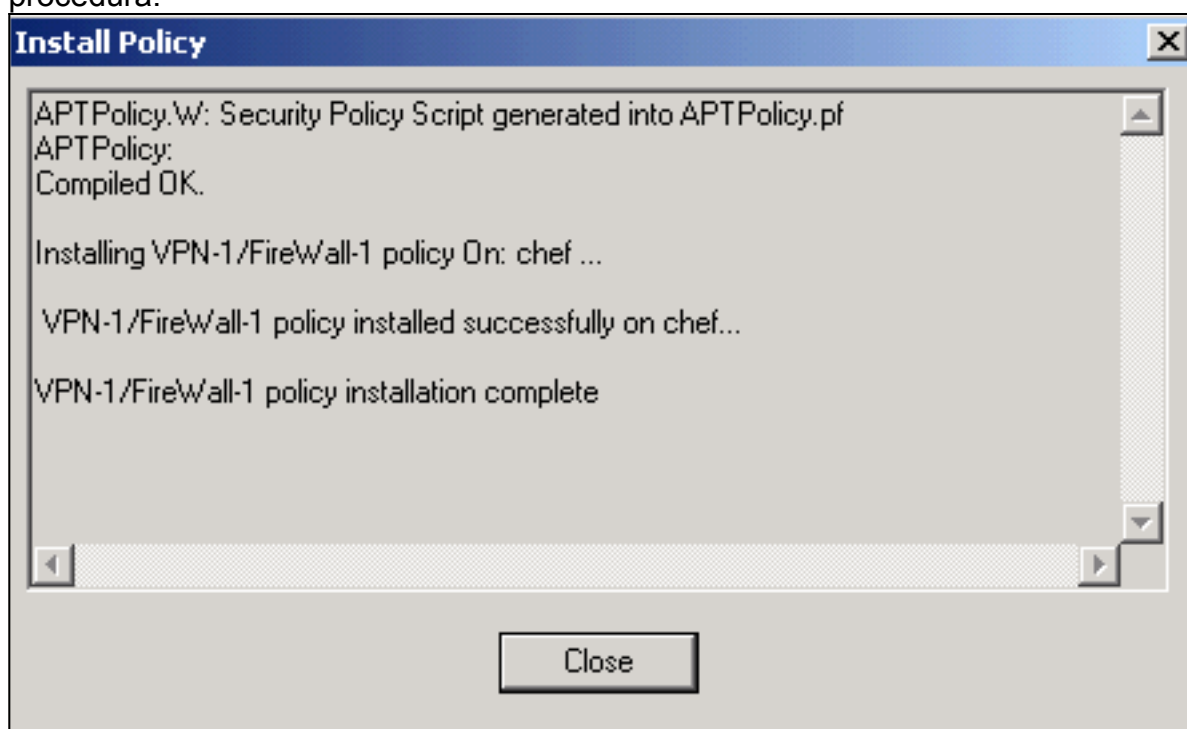


Durante la compilazione del criterio, nella finestra di installazione vengono visualizzate note sullo stato di avanzamento.



Quand

o la finestra di installazione indica che l'installazione del criterio è stata completata, fare clic su **Chiudi** per completare la procedura.



## [Verifica](#)

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

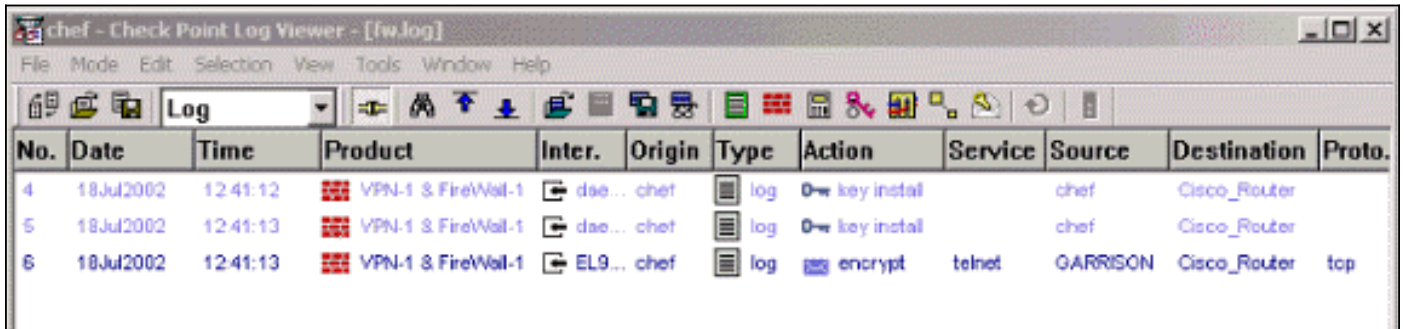
### [Verifica del router Cisco](#)

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

- **show crypto isakmp sa:** visualizza tutte le associazioni di sicurezza IKE correnti in un peer.
- **show crypto ipsec sa:** visualizza le impostazioni utilizzate dalle associazioni di protezione correnti.

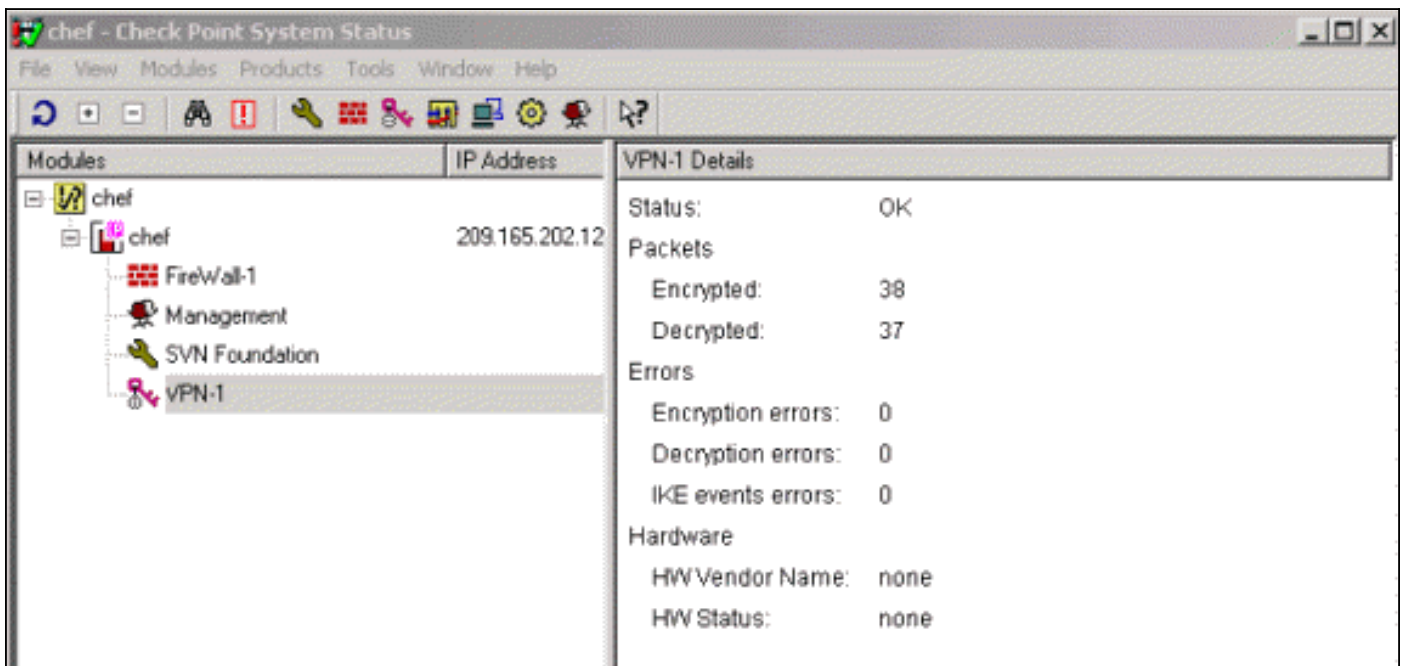
## Verifica NG checkpoint

Per visualizzare i log, selezionare **Finestra > Log Viewer**.



No.	Date	Time	Product	Inter.	Origin	Type	Action	Service	Source	Destination	Proto.
4	18Jul2002	12:41:12	VPN-1 & FireWall-1	dae...	chef	log	key instal		chef	Cisco_Router	
5	18Jul2002	12:41:13	VPN-1 & FireWall-1	dae...	chef	log	key instal		chef	Cisco_Router	
6	18Jul2002	12:41:13	VPN-1 & FireWall-1	EL9...	chef	log	encrypt	telnet	GARRISON	Cisco_Router	tcp

Per visualizzare lo stato del sistema, selezionare **Finestra > Stato sistema**.



Modules	IP Address	VPN-1 Details
chef		Status: OK
chef	209.165.202.12	Packets
FireWall-1		Encrypted: 38
Management		Decrypted: 37
SVN Foundation		Errors
VPN-1		Encryption errors: 0
		Decryption errors: 0
		IKE events errors: 0
		Hardware
		HW Vendor Name: none
		HW Status: none

## Risoluzione dei problemi

### Cisco Router

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

Per ulteriori informazioni sulla risoluzione dei problemi, consultare il documento sulla [risoluzione dei problemi di sicurezza IP - descrizione e uso dei comandi di debug](#).

**Nota:** prima di usare i comandi di **debug**, consultare le [informazioni importanti sui comandi di debug](#).

- **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.
- **clear crypto isakmp:** cancella tutte le connessioni IKE attive.
- **clear crypto sa:** cancella tutte le SA IPsec.

## Output log di debug riuscito

```

18:05:32: ISAKMP (0:0): received packet from
      209.165.202.129 (N) NEW SA
18:05:32: ISAKMP: local port 500, remote port 500
18:05:32: ISAKMP (0:1): Input = IKE_MSG_FROM_PEER,
      IKE_MM_EXCH
Old State = IKE_READY New State = IKE_R_MM1
18:05:32: ISAKMP (0:1): processing SA payload. message ID = 0
18:05:32: ISAKMP (0:1): processing vendor id payload
18:05:32: ISAKMP (0:1): vendor ID seems Unity/DPD
      but bad major
18:05:32: ISAKMP (0:1): found peer pre-shared key
      matching 209.165.202.129
18:05:32: ISAKMP (0:1): Checking ISAKMP transform 1
      against priority 1 policy
18:05:32: ISAKMP: encryption 3DES-CBC
18:05:32: ISAKMP: hash MD5
18:05:32: ISAKMP: auth pre-share
18:05:32: ISAKMP: default group 2
18:05:32: ISAKMP: life type in seconds
18:05:32: ISAKMP: life duration (VPI) of 0x0 0x0 0x7 0x8
18:05:32: ISAKMP (0:1): atts are acceptable. Next payload is 0
18:05:33: ISAKMP (0:1): processing vendor id payload
18:05:33: ISAKMP (0:1): vendor ID seems Unity/DPD but bad major
18:05:33: ISAKMP (0:1): Input = IKE_MSG_INTERNAL,
      IKE_PROCESS_MAIN_MODE
Old State = IKE_R_MM1 New State = IKE_R_MM1
18:05:33: ISAKMP (0:1): sending packet to 209.165.202.129 (R)
      MM_SA_SETUP
18:05:33: ISAKMP (0:1): Input = IKE_MSG_INTERNAL,
      IKE_PROCESS_COMPLETE
Old State = IKE_R_MM1 New State = IKE_R_MM2
18:05:33: ISAKMP (0:1): received packet from 209.165.202.129 (R)
      MM_SA_SETUP
18:05:33: ISAKMP (0:1): Input = IKE_MSG_FROM_PEER,
      IKE_MM_EXCH
Old State = IKE_R_MM2 New State = IKE_R_MM3
18:05:33: ISAKMP (0:1): processing KE payload.
      message ID = 0
18:05:33: ISAKMP (0:1): processing NONCE payload.
      message ID = 0
18:05:33: ISAKMP (0:1): found peer pre-shared key
      matching 209.165.202.129
18:05:33: ISAKMP (0:1): SKEYID state generated
18:05:33: ISAKMP (0:1): Input = IKE_MSG_INTERNAL,
      IKE_PROCESS_MAIN_MODE
Old State = IKE_R_MM3 New State = IKE_R_MM3
18:05:33: ISAKMP (0:1): sending packet to 209.165.202.129 (R)
      MM_KEY_EXCH
18:05:33: ISAKMP (0:1): Input = IKE_MSG_INTERNAL,
      IKE_PROCESS_COMPLETE
Old State = IKE_R_MM3 New State = IKE_R_MM4
18:05:33: ISAKMP (0:1): received packet from 209.165.202.129 (R)

```

```
MM_KEY_EXCH
18:05:33: ISAKMP (0:1): Input = IKE_MESG_FROM_PEER,
    IKE_MM_EXCH
Old State = IKE_R_MM4 New State = IKE_R_MM5
18:05:33: ISAKMP (0:1): processing ID payload.
    message ID = 0
18:05:33: ISAKMP (0:1): processing HASH payload.
    message ID = 0
18:05:33: ISAKMP (0:1): SA has been authenticated
    with 209.165.202.129
18:05:33: ISAKMP (0:1): Input = IKE_MESG_INTERNAL,
    IKE_PROCESS_MAIN_MODE
Old State = IKE_R_MM5 New State = IKE_R_MM5
18:05:33: ISAKMP (0:1): SA is doing pre-shared key authentication
using id type ID_IPV4_ADDR
18:05:33: ISAKMP (1): ID payload
next-payload : 8
type : 1
protocol : 17
port : 500
length : 8
18:05:33: ISAKMP (1): Total payload length: 12
18:05:33: ISAKMP (0:1): sending packet to 209.165.202.129
(R) QM_IDLE
18:05:33: ISAKMP (0:1): Input = IKE_MESG_INTERNAL,
    IKE_PROCESS_COMPLETE
Old State = IKE_R_MM5 New State = IKE_P1_COMPLETE
18:05:33: ISAKMP (0:1): Input = IKE_MESG_INTERNAL,
    IKE_PHASE1_COMPLETE
Old State = IKE_P1_COMPLETE
New State = IKE_P1_COMPLETE
18:05:33: ISAKMP (0:1): received packet from 209.165.202.129 (R)
    QM_IDLE
18:05:33: ISAKMP (0:1): processing HASH payload.
    message ID = -1335371103
18:05:33: ISAKMP (0:1): processing SA payload.
    message ID = -1335371103
18:05:33: ISAKMP (0:1): Checking IPSec proposal 1
18:05:33: ISAKMP: transform 1, ESP_3DES
18:05:33: ISAKMP: attributes in transform:
18:05:33: ISAKMP: SA life type in seconds
18:05:33: ISAKMP: SA life duration (VPI) of 0x0 0x0 0xE 0x10
18:05:33: ISAKMP: authenticator is HMAC-MD5
18:05:33: ISAKMP: encaps is 1
18:05:33: ISAKMP (0:1): atts are acceptable.
18:05:33: IPSEC(validate_proposal_request): proposal part #1,
(key eng. msg.) INBOUND local= 209.165.202.226, remote= 209.165.202.129,
local_proxy= 172.16.15.0/255.255.255.0/0/0 (type=4),
remote_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
18:05:33: ISAKMP (0:1): processing NONCE payload.
    message ID = -1335371103
18:05:33: ISAKMP (0:1): processing ID payload.
    message ID = -1335371103
18:05:33: ISAKMP (0:1): processing ID payload.
    message ID = -1335371103
18:05:33: ISAKMP (0:1): asking for 1 spis from ipsec
18:05:33: ISAKMP (0:1): Node -1335371103,
    Input = IKE_MESG_FROM_PEER, IKE_QM_EXCH
Old State = IKE_QM_READY New State = IKE_QM_SPI_STARVE
18:05:33: IPSEC(key_engine): got a queue event...
18:05:33: IPSEC(spi_response): getting spi 2147492563 for SA
```



from 209.165.202.226 to 209.165.202.129 for prot 3  
18:05:33: ISAKMP: received ke message (2/1)  
18:05:33: ISAKMP (0:1): sending packet to  
209.165.202.129 (R) QM\_IDLE  
18:05:33: ISAKMP (0:1): Node -1335371103,  
Input = IKE\_MESG\_FROM\_IPSEC, IKE\_SPI\_REPLY  
Old State = IKE\_QM\_SPI\_STARVE New State = IKE\_QM\_R\_QM2  
18:05:33: ISAKMP (0:1): received packet  
from 209.165.202.129 (R) QM\_IDLE  
18:05:33: ISAKMP (0:1): Creating IPsec SAs  
18:05:33: inbound SA from 209.165.202.129 to 209.165.202.226  
(proxy 192.168.10.0 to 172.16.15.0)  
18:05:33: has spi 0x800022D3 and conn\_id 200 and flags 4  
18:05:33: lifetime of 3600 seconds  
18:05:33: outbound SA from 209.165.202.226 to 209.165.202.129  
(proxy 172.16.15.0 to 192.168.10.0 )  
18:05:33: has spi -2006413528 and conn\_id 201 and flags C  
18:05:33: lifetime of 3600 seconds  
18:05:33: ISAKMP (0:1): deleting node -1335371103 error  
FALSE reason "quick mode done (await())"  
18:05:33: ISAKMP (0:1): Node -1335371103, Input = IKE\_MESG\_FROM\_PEER,  
IKE\_QM\_EXCH  
**Old State = IKE\_QM\_R\_QM2 New State = IKE\_QM\_PHASE2\_COMPLETE**  
18:05:33: IPSEC(key\_engine): got a queue event...  
18:05:33: IPSEC(initialize\_sas): ,  
(key eng. msg.) INBOUND local= 209.165.202.226,  
remote=209.165.202.129,  
local\_proxy= 172.16.15.0/255.255.255.0/0/0 (type=4),  
remote\_proxy= 192.168.10.0/255.255.255.0/0/0 (type=4),  
protocol= ESP, transform= esp-3des esp-md5-hmac ,  
lifedur= 3600s and 0kb,  
spi= 0x800022D3(2147492563), conn\_id= 200, keysize= 0,  
flags= 0x4  
18:05:33: IPSEC(initialize\_sas): ,  
(key eng. msg.) OUTBOUND local= 209.165.202.226,  
remote=209.165.202.129,  
local\_proxy= 172.16.15.0/255.255.255.0/0/0 (type=4),  
remote\_proxy= 192.168.10.0/255.255.255.0/0/0 (type=4),  
protocol= ESP, transform= esp-3des esp-md5-hmac ,  
lifedur= 3600s and 0kb,  
  
spi= 0x88688F28(2288553768), conn\_id= 201, keysize= 0,  
flags= 0xC  
18:05:33: IPSEC(create\_sa): sa created,  
(sa) sa\_dest= 209.165.202.226, sa\_prot= 50,  
sa\_spi= 0x800022D3(2147492563),  
sa\_trans= esp-3des esp-md5-hmac , sa\_conn\_id= 200  
18:05:33: IPSEC(create\_sa): sa created,  
(sa) sa\_dest= 209.165.202.129, sa\_prot= 50,  
sa\_spi= 0x88688F28(2288553768),  
sa\_trans= esp-3des esp-md5-hmac , sa\_conn\_id= 201  
18:05:34: ISAKMP (0:1): received packet  
from 209.165.202.129 (R) QM\_IDLE  
18:05:34: ISAKMP (0:1): phase 2 packet is a duplicate  
of a previous packet.  
18:05:34: ISAKMP (0:1): retransmitting due to retransmit phase 2  
18:05:34: ISAKMP (0:1): ignoring retransmission, because phase2  
node marked dead -1335371103  
18:05:34: ISAKMP (0:1): received packet  
from 209.165.202.129 (R) QM\_IDLE  
18:05:34: ISAKMP (0:1): phase 2 packet is a duplicate  
of a previous packet.

```
18:05:34: ISAKMP (0:1): retransmitting due to retransmit phase 2
18:05:34: ISAKMP (0:1): ignoring retransmission, because phase2
node marked dead -1335371103
```

```
svl-6#show crypto isakmp sa
```

```
dst src state conn-id slot
209.165.202.226 209.165.202.129 QM_IDLE 1 0
```

```
svl-6#show crypto ipsec sa
```

```
interface: Ethernet0/0
Crypto map tag: aptmap, local addr. 209.165.202.226
local ident (addr/mask/prot/port): (172.16.15.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (192.168.10.0/255.255.255.0/0/0)
current_peer: 209.165.202.129
PERMIT, flags={origin_is_acl,}
#pkts encaps: 21, #pkts encrypt: 21, #pkts digest 21
#pkts decaps: 24, #pkts decrypt: 24, #pkts verify 24
#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.: 209.165.202.226, remote crypto endpt.: 209.165.202.129
path mtu 1500, media mtu 1500
current outbound spi: 88688F28
inbound esp sas:
spi: 0x800022D3(2147492563)
transform: esp-3des esp-md5-hmac ,
in use settings = {Tunnel, }
slot: 0, conn id: 200, flow_id: 1, crypto map: aptmap
sa timing: remaining key lifetime (k/sec): (4607997/3559)
IV size: 8 bytes
replay detection support: Y
inbound ah sas:
inbound pcp sas:
outbound esp sas:
spi: 0x88688F28(2288553768)
transform: esp-3des esp-md5-hmac ,
in use settings = {Tunnel, }
slot: 0, conn id: 201, flow_id: 2, crypto map: aptmap
sa timing: remaining key lifetime (k/sec): (4607997/3550)
IV size: 8 bytes
replay detection support: Y
outbound ah sas:
outbound pcp sas:
```

```
svl-6#show crypto engine conn act
```

ID	Interface	IP-	Address	State	Algorithm	Encrypt	Decrypt
1	Ethernet0/0	209.165.202.226	set	HMAC_MD5+3DES_56_C	0	0	
200	Ethernet0/0	209.165.202.226	set	HMAC_MD5+3DES_56_C	0	<b>24</b>	
201	Ethernet0/0	209.165.202.226	set	HMAC_MD5+3DES_56_C	<b>21</b>	0	

## [Informazioni correlate](#)

- [Pagina di supporto per IPsec](#)
- [Supporto tecnico – Cisco Systems](#)