

Configuration d'un tunnel IPSec entre un contrôleur NG et un routeur

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Diagramme du réseau](#)

[Conventions](#)

[Configuration du routeur VPN Cisco 1751](#)

[Configurer le contrôleur NG](#)

[Vérification](#)

[Vérification du routeur Cisco](#)

[Vérifier le point de contrôle NG](#)

[Dépannage](#)

[Routeur Cisco](#)

[Informations connexes](#)

Introduction

Il explique comment créer un tunnel IPSec avec des clés pré-partagées afin de joindre deux réseaux privés :

- Le réseau privé 172.16.15.x à l'intérieur du routeur.
- Le réseau privé 192.168.10.x à l'intérieur de la nouvelle génération ^{Checkpoint™} (NG).

Conditions préalables

Conditions requises

Les procédures décrites dans le présent document sont fondées sur ces hypothèses.

- La stratégie de base ^{Checkpoint™} NG est définie.
- Toutes les configurations d'accès, de traduction d'adresses de réseau (NAT) et de routage sont configurées.
- Le trafic de l'intérieur du routeur et de l'intérieur du ^{Checkpoint™} NG vers Internet circule.

Components Used

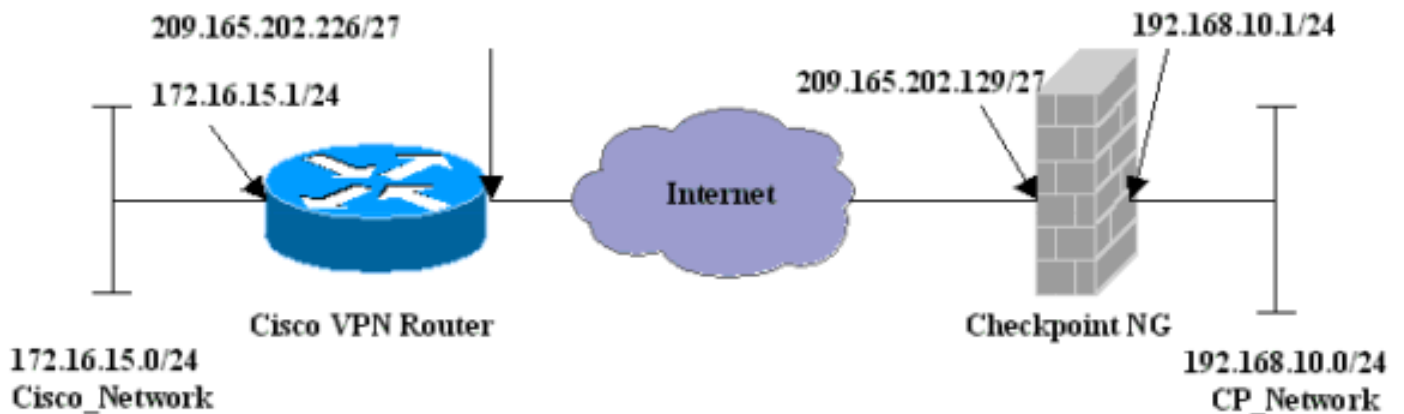
Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Routeur Cisco 1751
- Logiciel Cisco IOS® (C1700-K9O3SY7-M), version 12.2(8)T4, VERSION LOGICIELLE (fc1)
- Checkpoint™ NG Build 50027

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Conventions

Pour plus d'informations sur les conventions des documents, référez-vous aux [Conventions utilisées pour les conseils techniques de Cisco](#).

Configuration du routeur VPN Cisco 1751

```
Router VPN Cisco 1751

version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
hostname sv1-6
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

```

Configurer le contrôleur NG

Le NG Checkpoint™ est une configuration orientée objet. Les objets et les règles réseau sont définis pour constituer la stratégie relative à la configuration VPN à configurer. Cette stratégie est ensuite installée à l'aide de l'Éditeur de stratégie Checkpoint™ NG pour terminer le côté Checkpoint™ NG de la configuration VPN.

1. Créez le sous-réseau du réseau Cisco et le sous-réseau Checkpoint™ NG en tant qu'objets réseau. C'est ce qui est chiffré. Pour créer les objets, sélectionnez **Gérer > Objets réseau**, puis sélectionnez **Nouveau > Réseau**. Entrez les informations réseau appropriées, puis cliquez sur **OK**. Ces exemples montrent un ensemble d'objets appelés CP_Network et

Network Properties - CP_Network

General NAT

Name: CP_Network

IP Address: 192.168.10.0

Net Mask: 255.255.255.0

Comment:

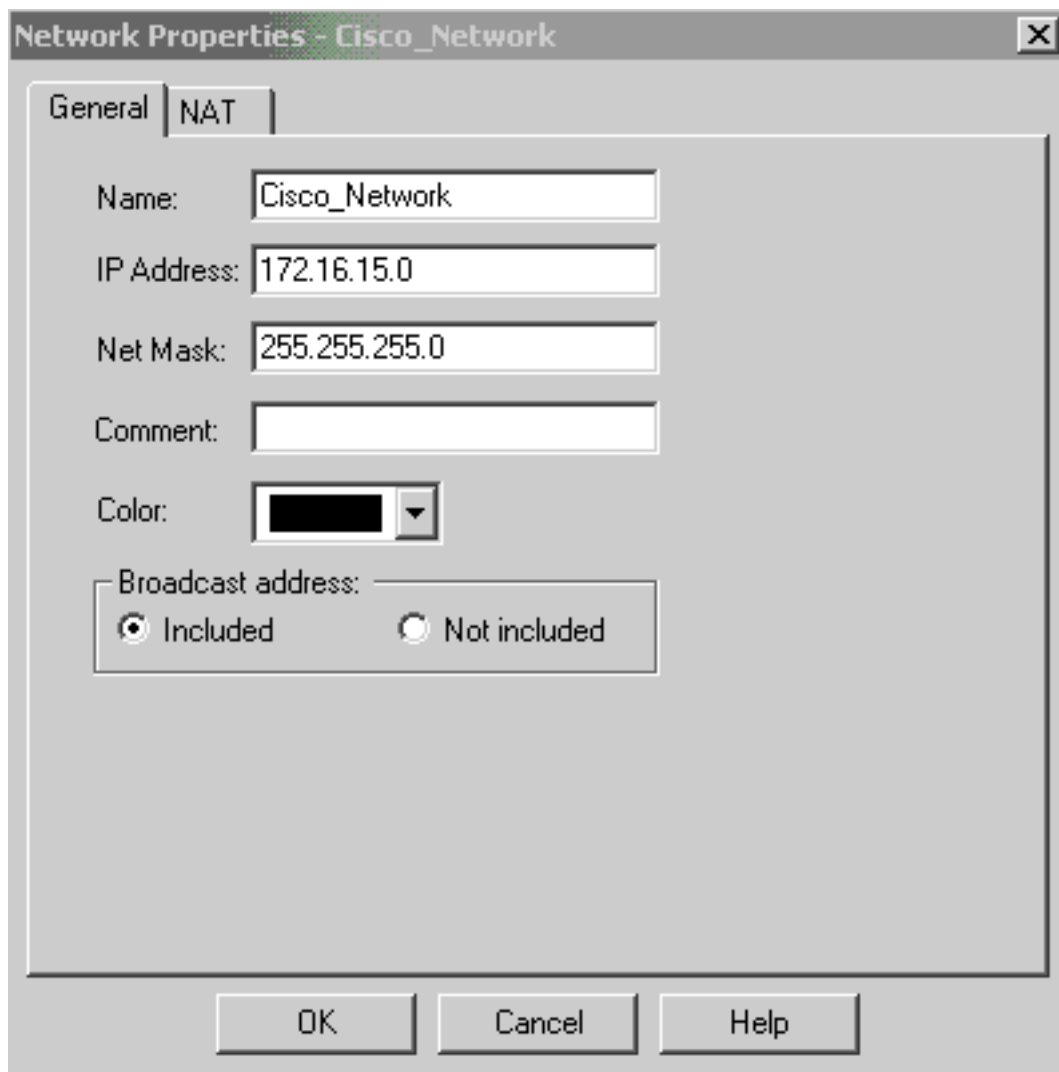
Color:

Broadcast address:

Included Not included

OK Cancel Help

Cisco_Network.



2. Créez les objets Cisco_Router et Checkpoint_NG en tant qu'objets de station de travail. Il s'agit des périphériques VPN. Pour créer les objets, sélectionnez **Gérer > Objets réseau**, puis sélectionnez **Nouveau > Station de travail**. Notez que vous pouvez utiliser l'objet de station de travail ^{Checkpoint™} NG créé lors de la configuration initiale de ^{Checkpoint™} NG. Sélectionnez les options pour définir la station de travail en tant que **passerelle** et **périphérique VPN interopérable**. Ces exemples montrent un ensemble d'objets appelés chef et 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

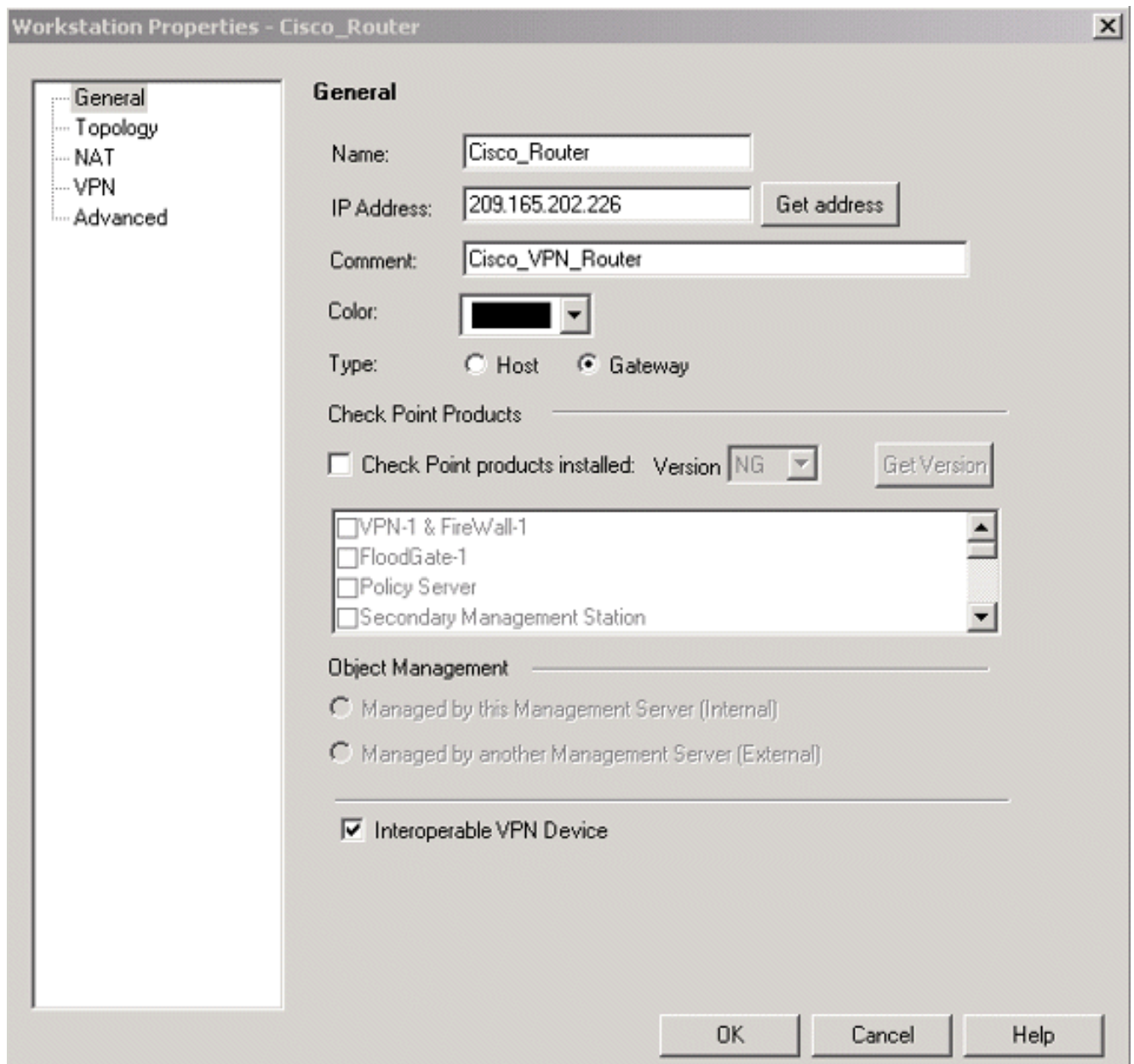
DN: cn=cp_mgmt,o=chef.6h9tua

 Interoperable VPN Device

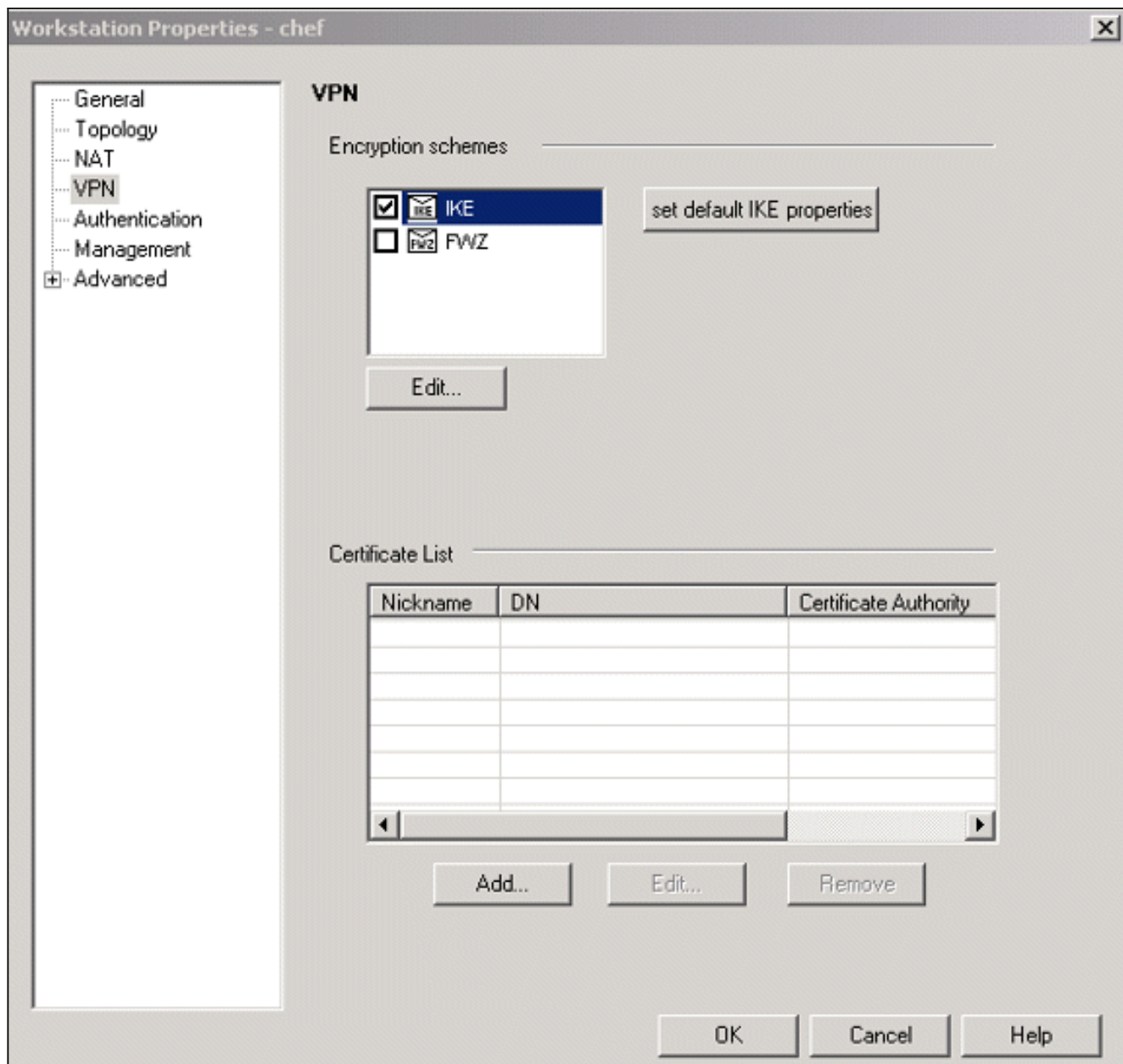
OK

Cancel

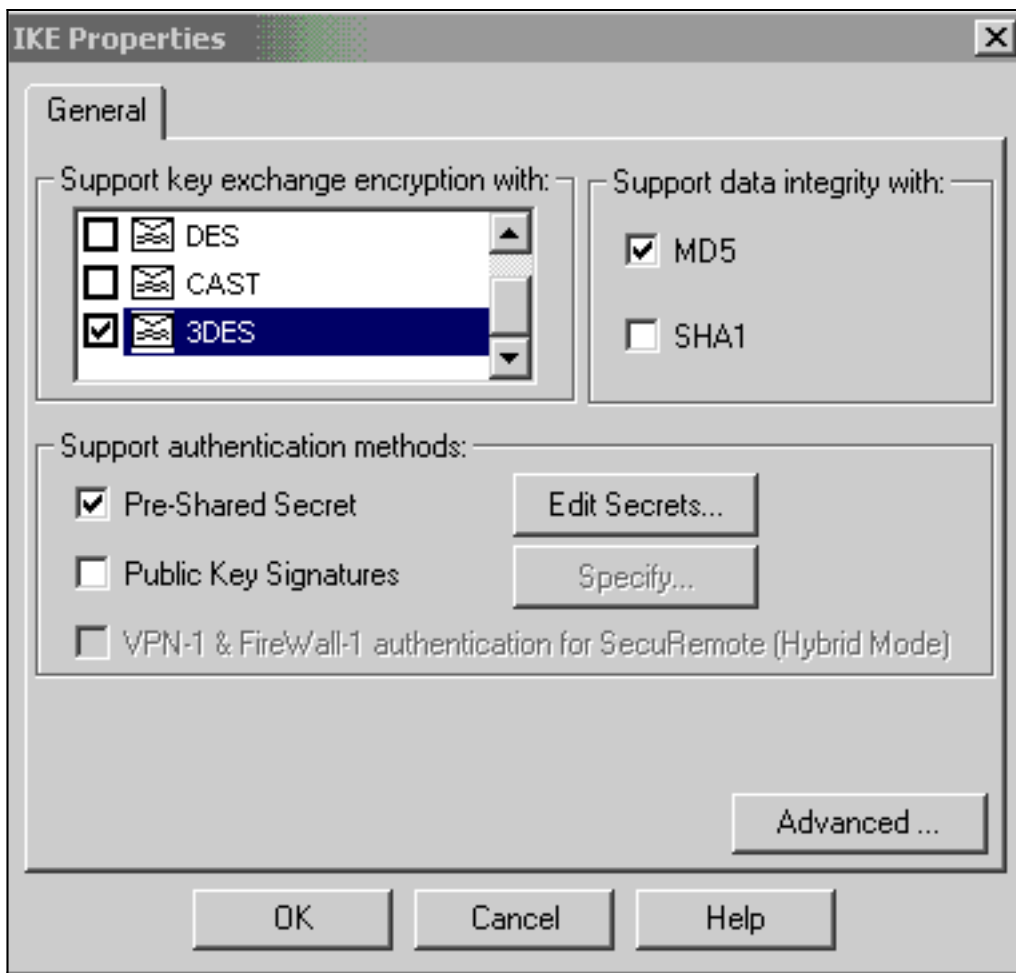
Help



3. Configurez IKE dans l'onglet VPN, puis cliquez sur **Edit**.

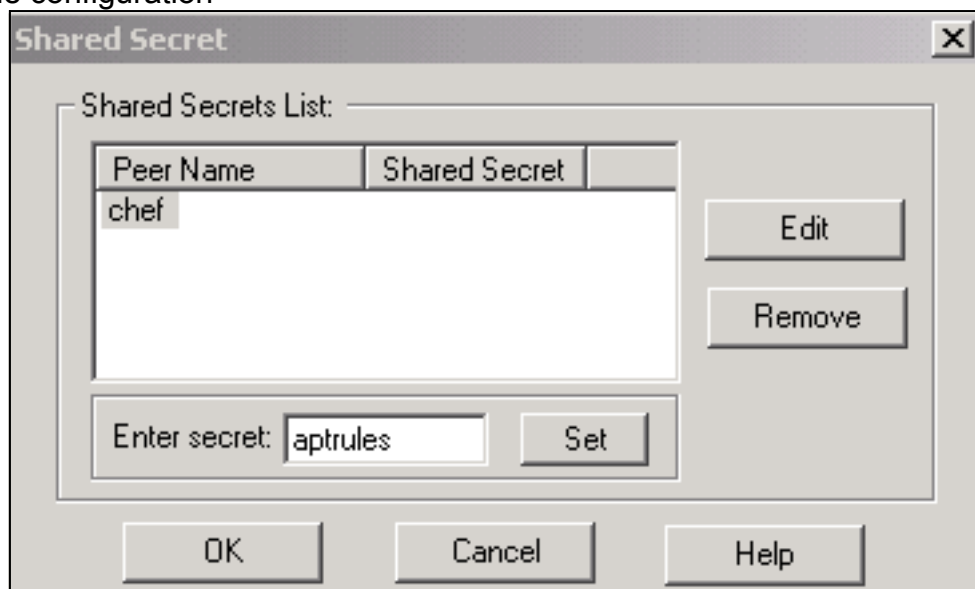


4. Configurez la stratégie d'échange de clés, puis cliquez sur **Modifier les**



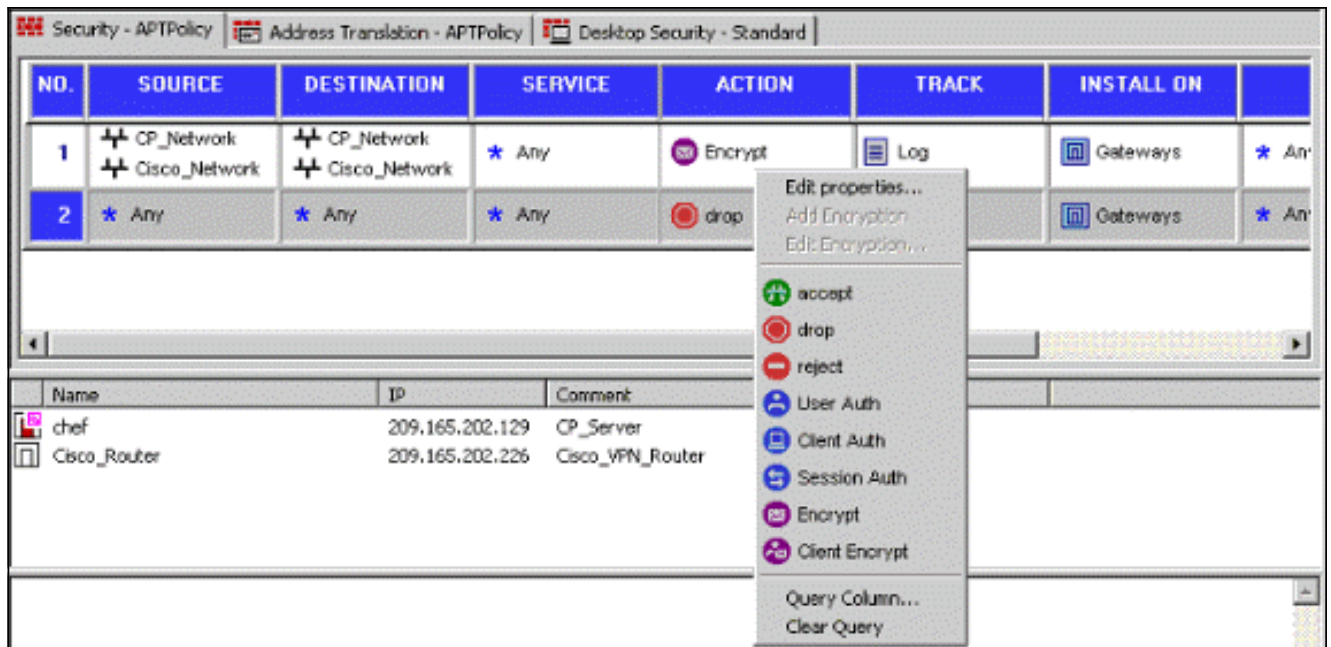
secrets.

5. Définissez les clés pré-partagées à utiliser, puis cliquez plusieurs fois sur **OK** jusqu'à ce que les fenêtres de configuration

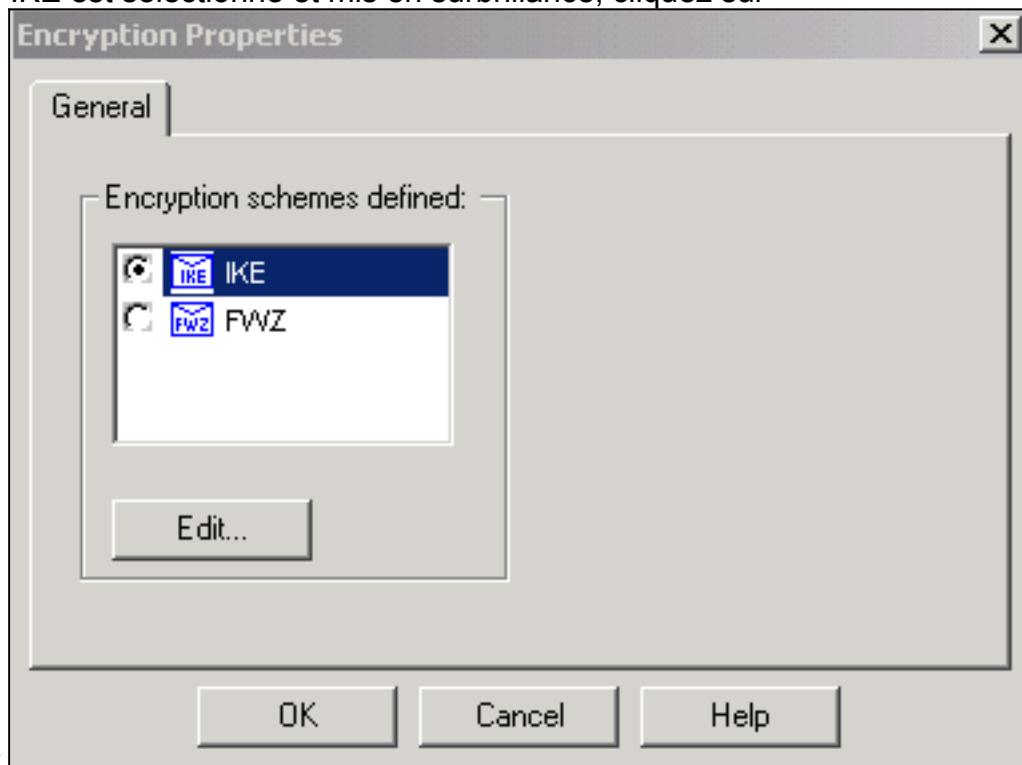


disparaissent.

6. Sélectionnez **Règles > Ajouter des règles > Haut** pour configurer les règles de chiffrement de la stratégie. La règle supérieure est la première règle exécutée avant toute autre règle qui peut contourner le chiffrement. Configurez la source et la destination pour inclure le CP_Network et le Cisco_Network, comme indiqué ici. Une fois que vous avez ajouté la section Action de chiffrement de la règle, cliquez avec le bouton droit sur **Action** et sélectionnez **Modifier les propriétés**.

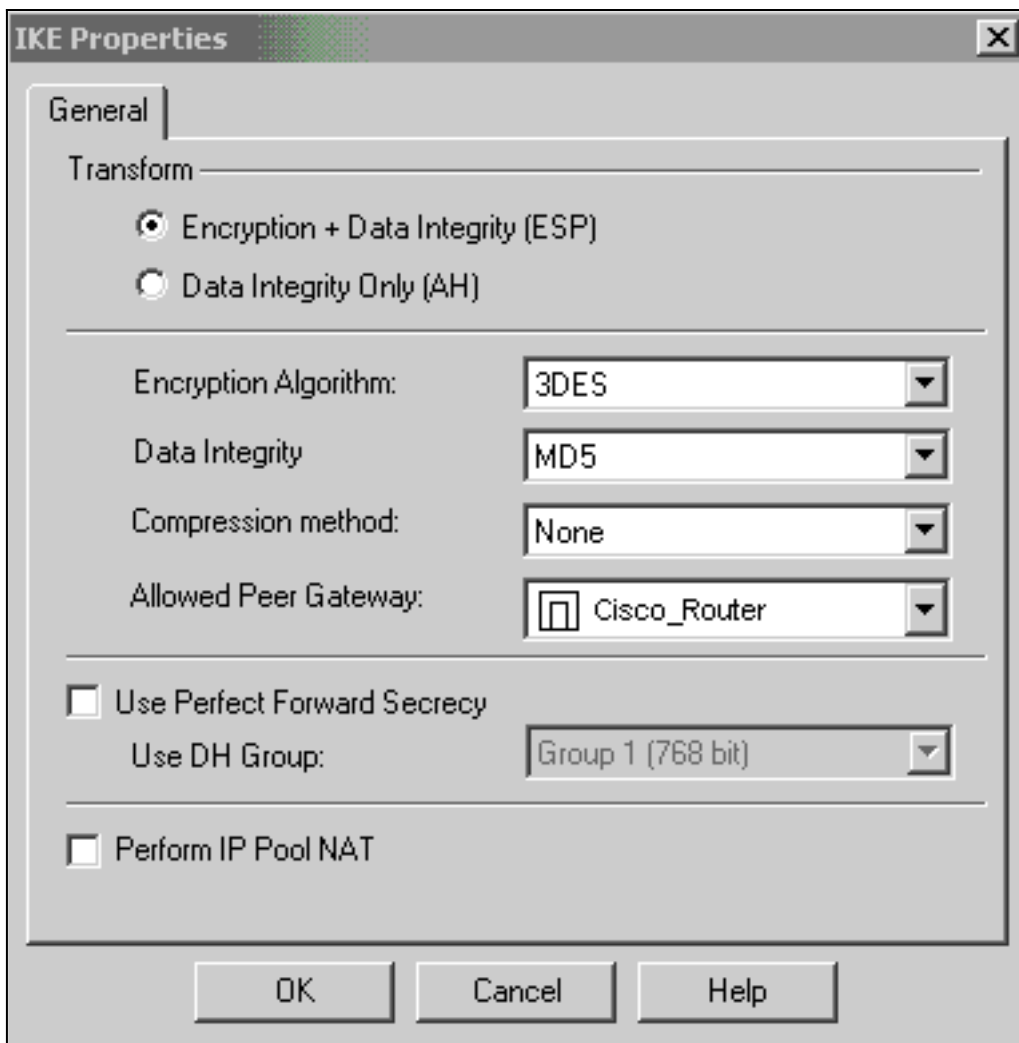


7. Lorsque IKE est sélectionné et mis en surbrillance, cliquez sur



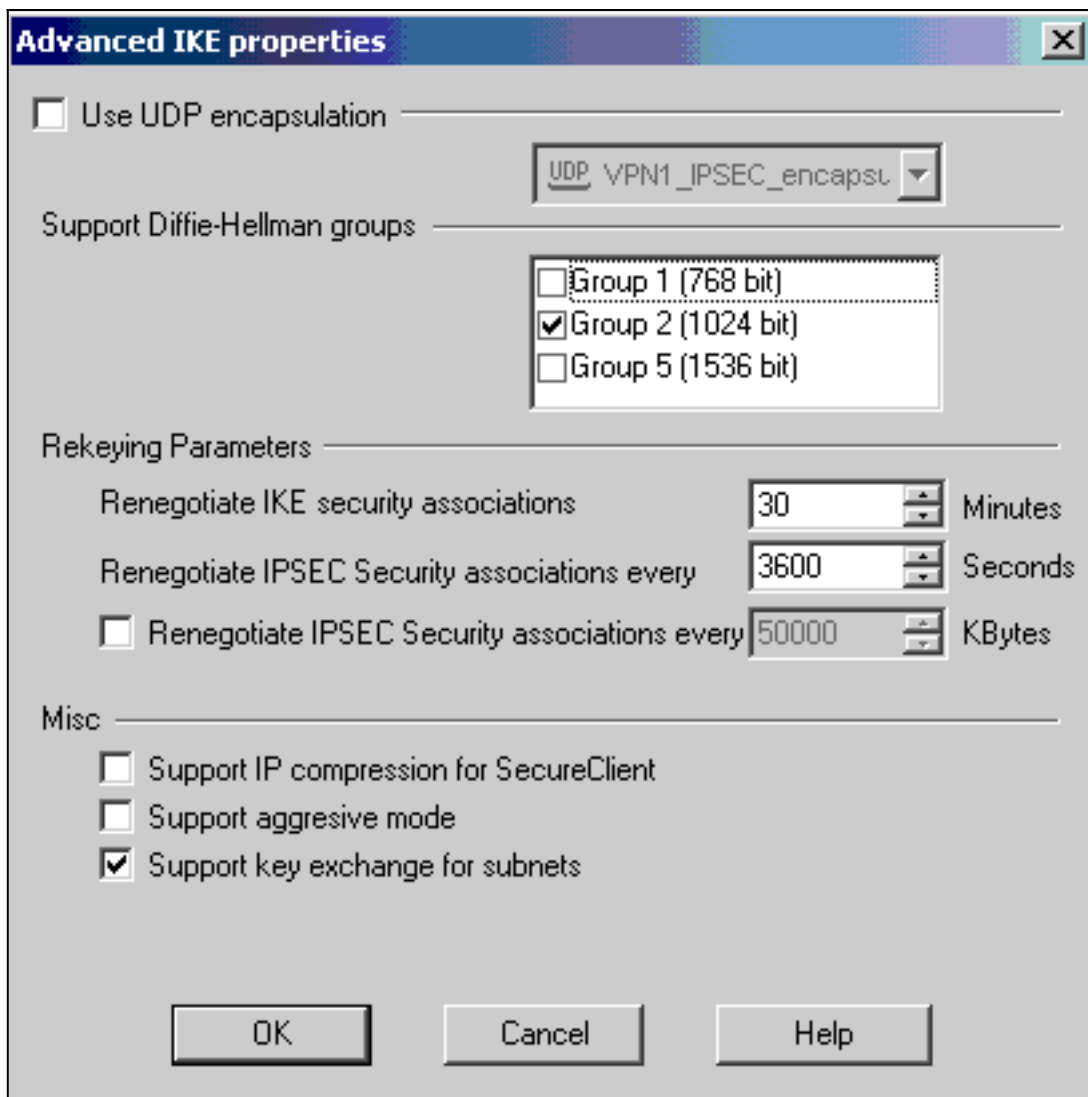
Modifier.

8. Confirmez la configuration



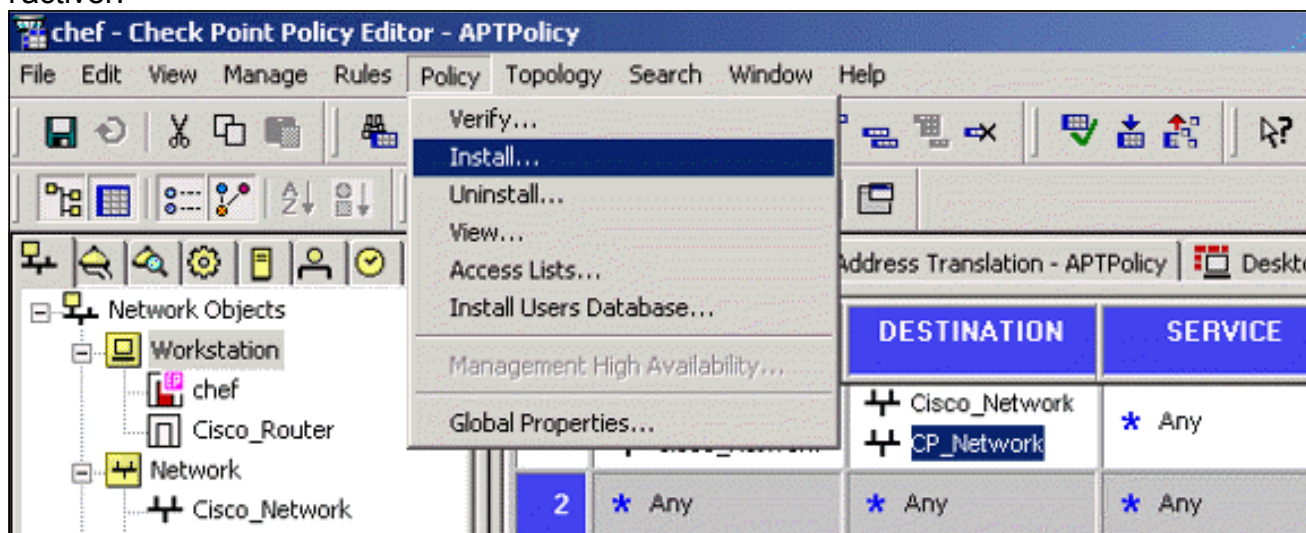
IKE.

9. L'un des principaux problèmes liés à l'exécution du VPN entre les périphériques Cisco et les autres périphériques IPsec est la renégociation de Key Exchange. Assurez-vous que le paramètre de l'échange IKE sur le routeur Cisco est exactement le même que celui configuré sur le NG ^{Checkpoint™}. **Remarque** : La valeur réelle de ce paramètre dépend de votre stratégie de sécurité d'entreprise particulière. Dans cet exemple, la [configuration IKE sur le routeur](#) a été définie sur 30 minutes avec la commande **lifetime 1800**. La même valeur doit être définie sur le NG ^{Checkpoint™}. Pour définir cette valeur sur ^{Checkpoint™} NG, sélectionnez **Manage Network Object**, puis sélectionnez l'objet ^{Checkpoint™} NG et cliquez sur **Edit**. Sélectionnez ensuite **VPN**, puis modifiez l'IKE. Sélectionnez **Avance** et configurez les paramètres de correction. Après avoir configuré l'échange de clés pour l'objet réseau ^{Checkpoint™} NG, exécutez la même configuration de la renégociation Key Exchange pour l'objet réseau Cisco_Router. **Remarque** : assurez-vous que le groupe Diffie-Hellman correct est sélectionné pour correspondre à celui configuré sur le

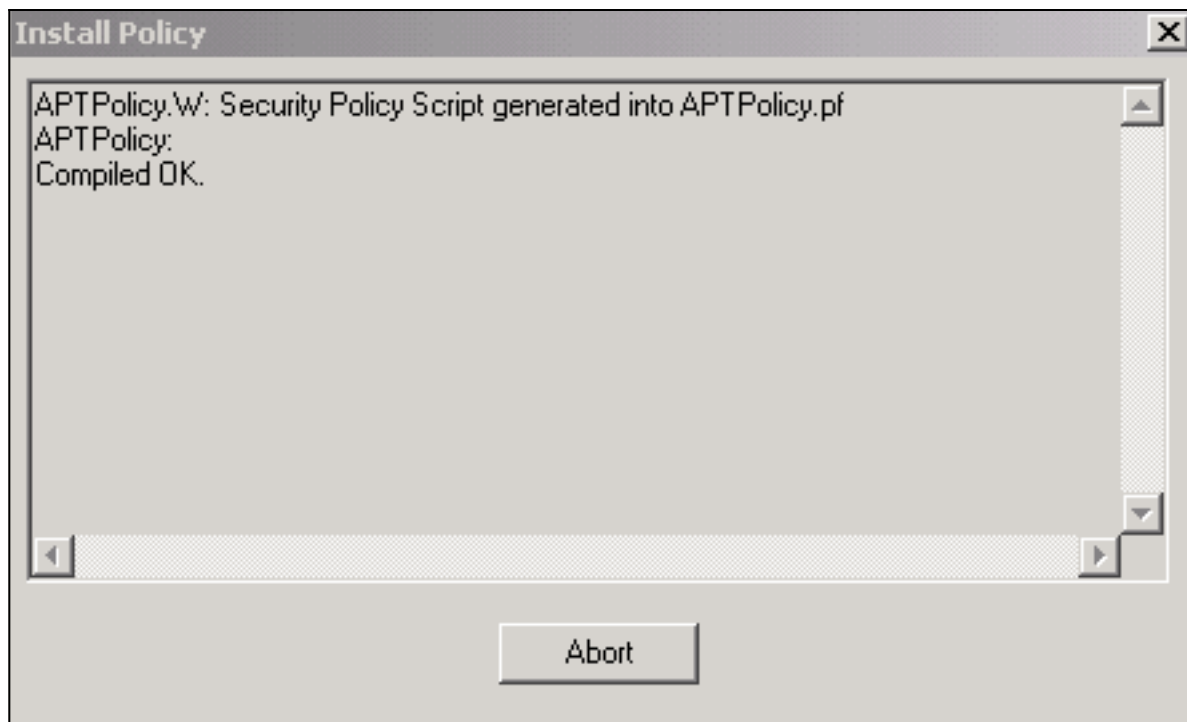


routeur.

- La configuration de la stratégie est terminée. Enregistrez la stratégie et sélectionnez **Stratégie > Installer** pour l'activer.

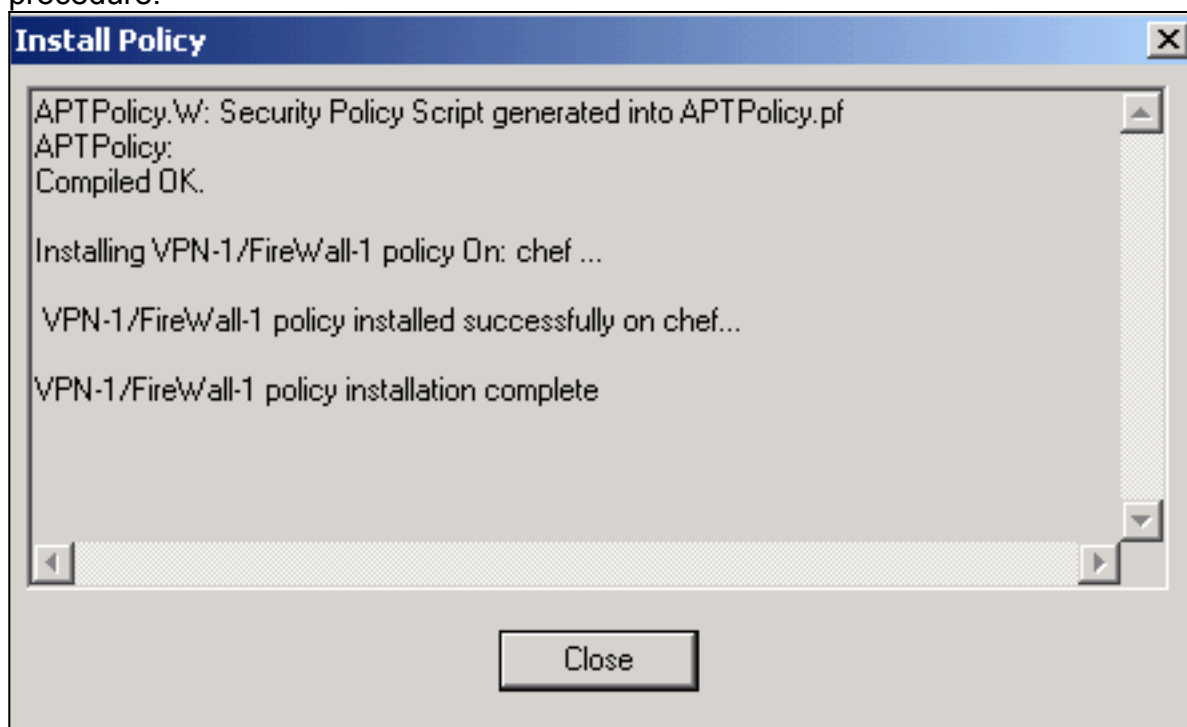


La fenêtre d'installation affiche les notes de progression lors de la compilation de la stratégie.



Lorsqu

e la fenêtre d'installation indique que l'installation de la stratégie est terminée, cliquez sur **Fermer** pour terminer la procédure.



Vérification

Cette section présente des informations que vous pouvez utiliser pour vous assurer que votre configuration fonctionne correctement.

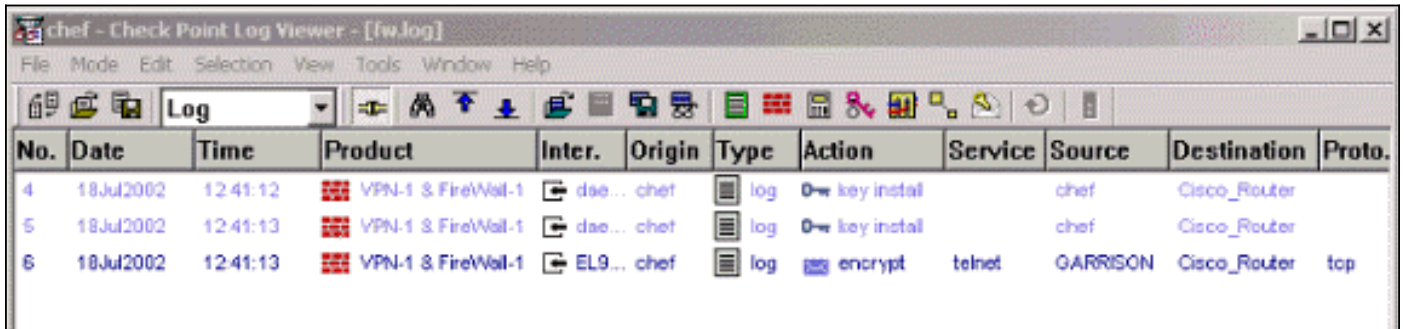
Vérification du routeur Cisco

Certaines commandes **show** sont prises en charge par l'[Output Interpreter Tool](#) (clients enregistrés uniquement), qui vous permet de voir une analyse de la sortie de la commande show.

- **show crypto isakmp sa** - Affiche toutes les associations de sécurité actuelles d'IKE (SA) sur un pair.
- **show crypto ipsec sa** — Affiche les paramètres utilisés par les SA.

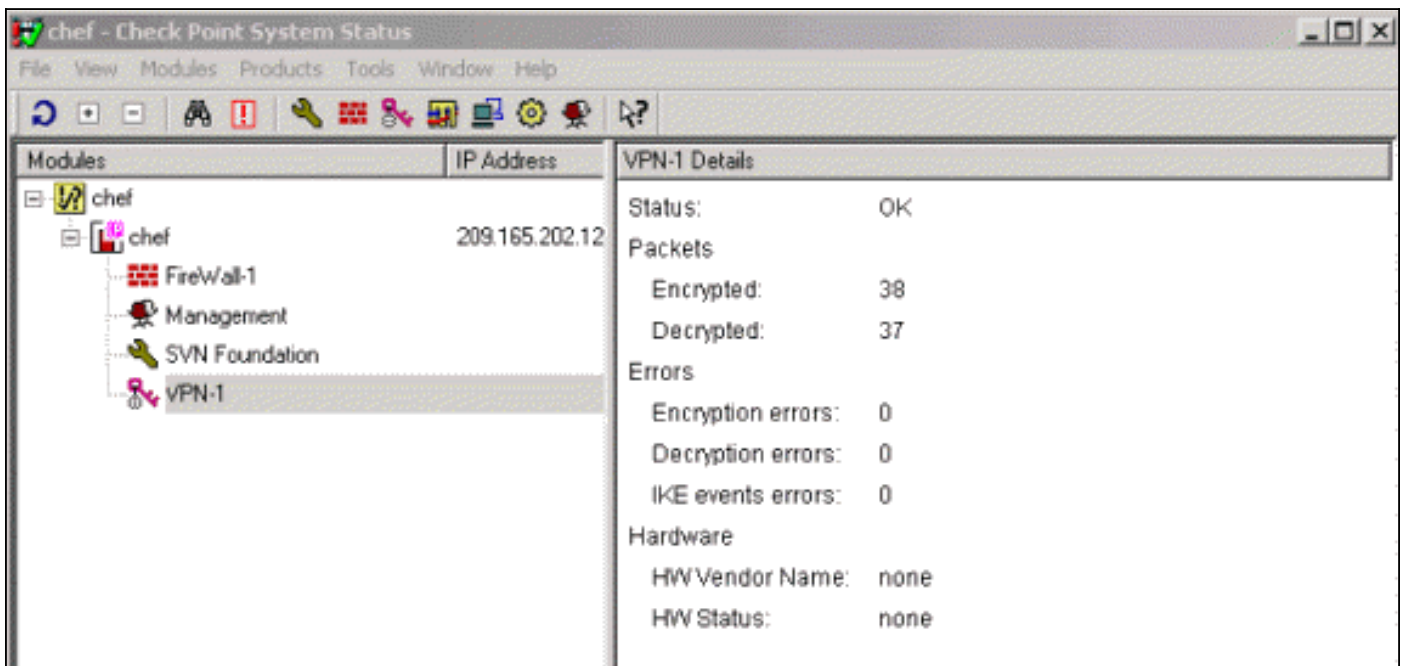
Vérifier le point de contrôle NG

Pour afficher les journaux, sélectionnez **Fenêtre > Visionneuse de journaux**.



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

Pour afficher l'état du système, sélectionnez **Fenêtre > État du système**.



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

Dépannage

Routeur Cisco

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Pour plus d'informations sur le dépannage, consultez [Dépannage de la sécurité IP - Compréhension et utilisation des commandes de débogage](#).

Remarque : avant d'émettre des commandes **debug**, reportez-vous à [Informations importantes sur les commandes de débogage](#).

- **debug crypto engine** - Affiche les messages de débogage sur les moteurs de chiffrement, qui

effectuent le chiffrement et le déchiffrement.

- **debug crypto isakmp**—Affichage de messages d'événements IKE.
- **debug crypto ipsec** — Affiche des événements IPsec.
- **clear crypto isakmp** : efface toutes les connexions IKE actives.
- **clear crypto sa** : efface toutes les SA IPsec.

Sortie du journal de débogage réussie

```
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_MSG_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_MSG_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

```
sv1-6#show crypto isakmp sa
dst src state conn-id slot
209.165.202.226 209.165.202.129 QM_IDLE 1 0
```

```
sv1-6#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:
```

```
sv1-6#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 24
201 Ethernet0/0 209.165.202.226 set HMAC_MD5+3DES_56_C 21 0
```

[Informations connexes](#)

- [Page d'assistance IPsec](#)
- [Support technique - Cisco Systems](#)