

Configuration d'un tunnel IPsec entre un routeur Cisco et un pare-feu Checkpoint Firewall 4.1

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Conventions](#)

[Configuration](#)

[Diagramme du réseau](#)

[Configurations](#)

[Vérification](#)

[Dépannage](#)

[Dépannage des commandes](#)

[Récapitulation de réseau](#)

[Point de contrôle](#)

[Exemple de sortie de débogage](#)

[Informations connexes](#)

[Introduction](#)

Il explique comment créer un tunnel IPSec avec des clés pré-partagées afin de joindre deux réseaux privés : le réseau privé 192.168.1.x interne au routeur Cisco et le réseau privé 10.32.50.x interne au Pare-feu checkpoint.

[Conditions préalables](#)

[Conditions requises](#)

Cet exemple de configuration suppose que le trafic à partir de l'intérieur du routeur et à l'intérieur du point de contrôle vers Internet (représenté ici par les réseaux 172.18.124.x) circule avant de commencer la configuration.

[Components Used](#)

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

- Routeur Cisco 3600

- Logiciel Cisco IOS® (C3640-JO3S56I-M), version 12.1(5)T, VERSION LOGICIELLE (fc1)
- Pare-feu Checkpoint 4.1

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.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à [Conventions relatives aux conseils techniques Cisco](#).

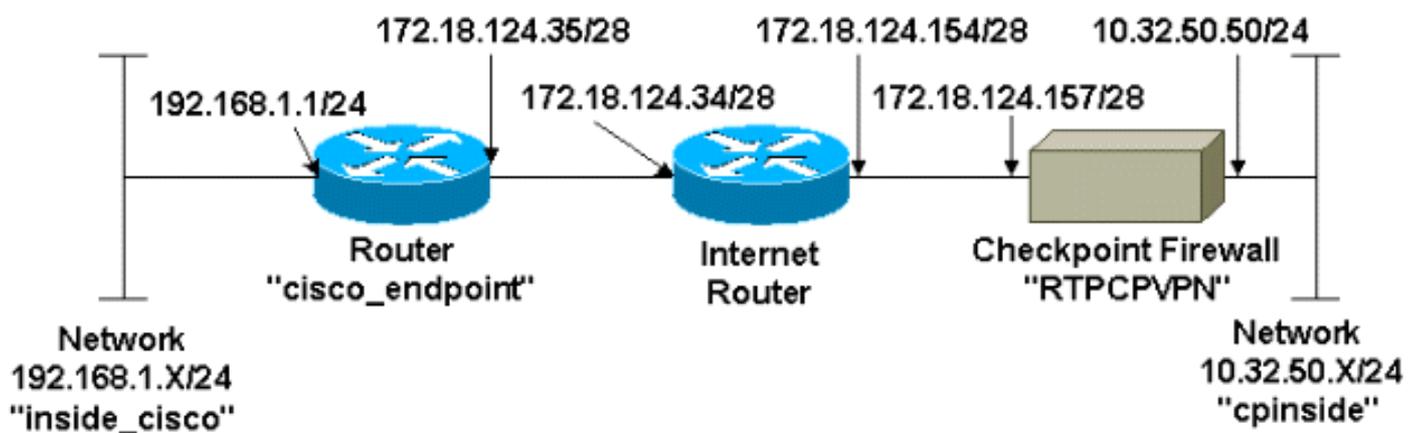
Configuration

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Remarque : Utilisez [l'outil de recherche de commandes](#) (clients [inscrits](#) seulement) pour en savoir plus sur les commandes figurant dans le présent document.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Configurations

Ce document utilise les configurations suivantes.

- [Configuration du routeur](#)
- [Configuration du pare-feu Checkpoint](#)

Configuration du routeur

Configuration du routeur Cisco 3600

```
Current configuration : 1608 bytes
!
version 12.1
```

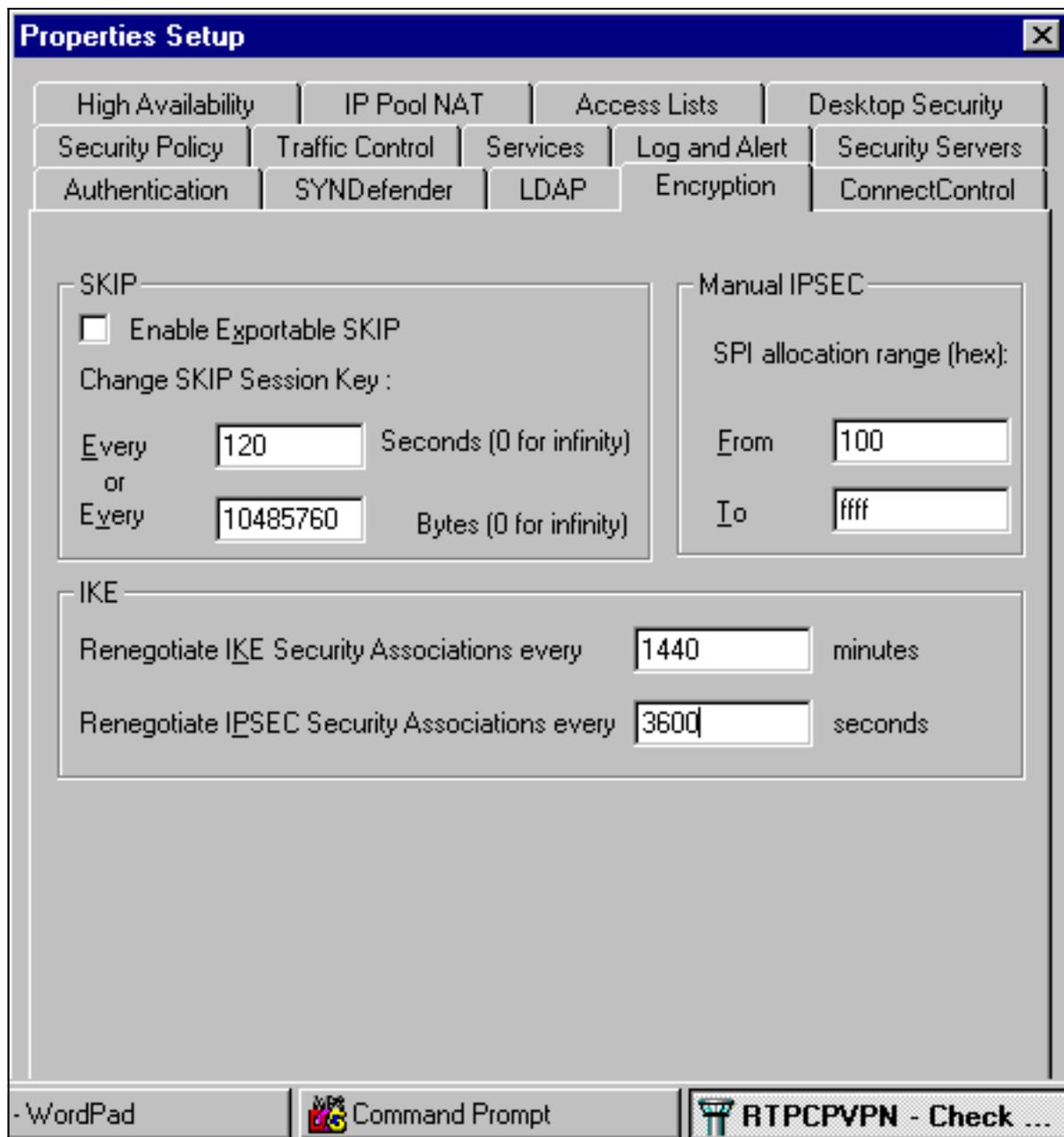
```
no service single-slot-reload-enable
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname cisco_endpoint
!
logging rate-limit console 10 except errors
!
ip subnet-zero
!
no ip finger
!
ip audit notify log
ip audit po max-events 100
!
!--- Internet Key Exchange (IKE) configuration crypto
isakmp policy 1
authentication pre-share
crypto isakmp key ciscorules address 172.18.124.157
!
!--- IPsec configuration crypto ipsec transform-set
rtpset esp-des esp-sha-hmac
!
crypto map rtp 1 ipsec-isakmp
set peer 172.18.124.157
set transform-set rtpset
match address 115
!
call rsvp-sync
cns event-service server
!
controller T1 1/0
!
controller T1 1/1
!
interface Ethernet0/0
ip address 172.18.124.35 255.255.255.240
ip nat outside
no ip mroute-cache
half-duplex
crypto map rtp
!
interface Ethernet0/1
ip address 192.168.1.1 255.255.255.0
ip nat inside
half-duplex
!
interface FastEthernet1/0
no ip address
shutdown
duplex auto
speed auto
!
ip kerberos source-interface any
ip nat pool INTERNET 172.18.124.36 172.18.124.36 netmask
255.255.255.240
ip nat inside source route-map nonat pool INTERNET
ip classless
ip route 0.0.0.0 0.0.0.0 172.18.124.34
no ip http server
!
access-list 101 deny ip 192.168.1.0 0.0.0.255 10.32.50.0
0.0.0.255
```

```
access-list 101 permit ip 192.168.1.0 0.0.0.255 any
access-list 115 permit ip 192.168.1.0 0.0.0.255
10.32.50.0 0.0.0.255
access-list 115 deny ip 192.168.1.0 0.0.0.255 any
route-map nonat permit 10
match ip address 101
!
dial-peer cor custom
!
line con 0
transport input none
line aux 0
line vty 0 4
login
!
end
```

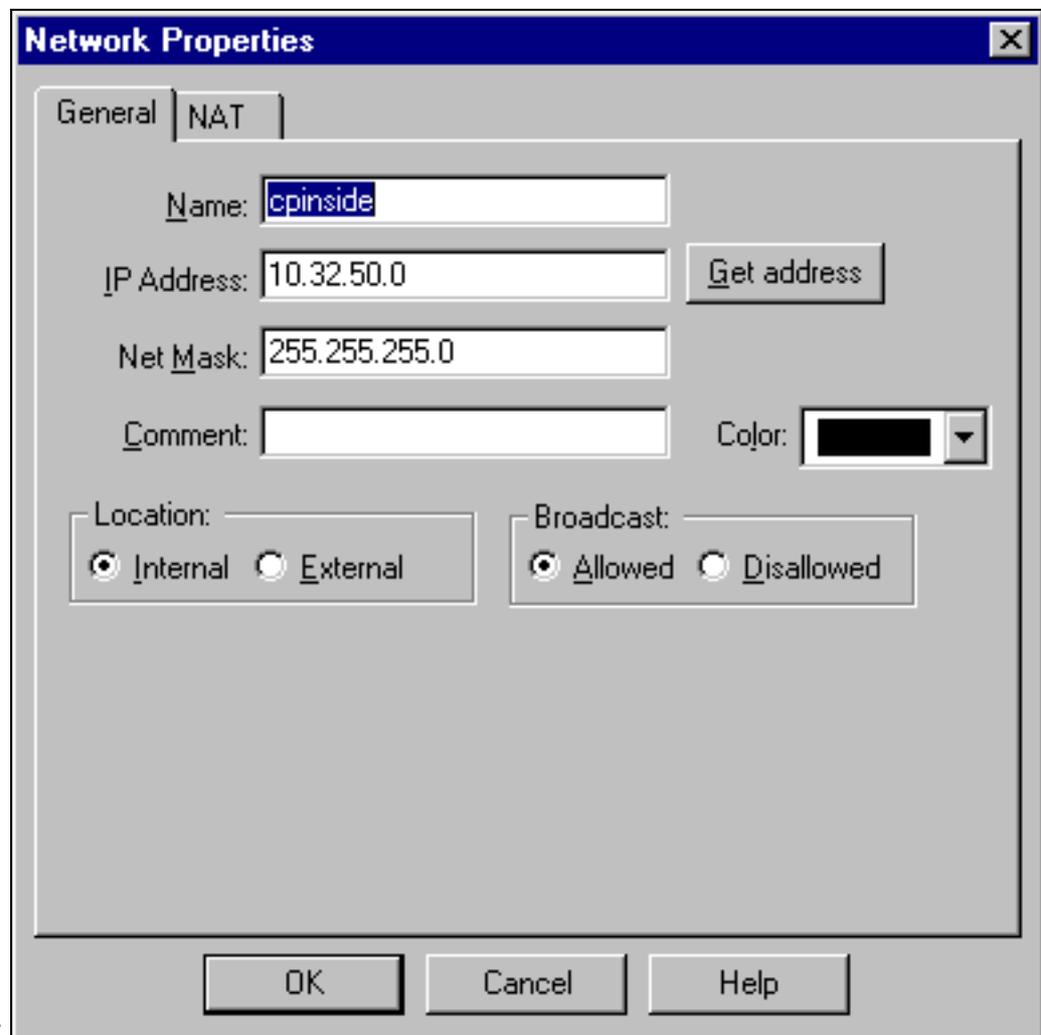
[Configuration du pare-feu Checkpoint](#)

Exécutez ces étapes pour configurer le pare-feu Checkpoint.

1. Étant donné que les durées de vie par défaut IKE et IPsec diffèrent d'un fournisseur à l'autre, sélectionnez **Propriétés > Cryptage** pour définir les durées de vie du point de contrôle en accord avec les valeurs par défaut de Cisco. La durée de vie IKE par défaut de Cisco est de 86 400 secondes (= 1 440 minutes) et peut être modifiée par les commandes suivantes : **crypto isakmp policy n°# de vie**. La durée de vie configurable de Cisco IKE est comprise entre 60 et 86 400 secondes. La durée de vie IPsec par défaut de Cisco est de 3600 secondes, et elle peut être modifiée par la commande **crypto ipsec security-association lifetime seconds #**. La durée de vie configurable de Cisco IPsec est comprise entre 120 et 86 400 secondes.

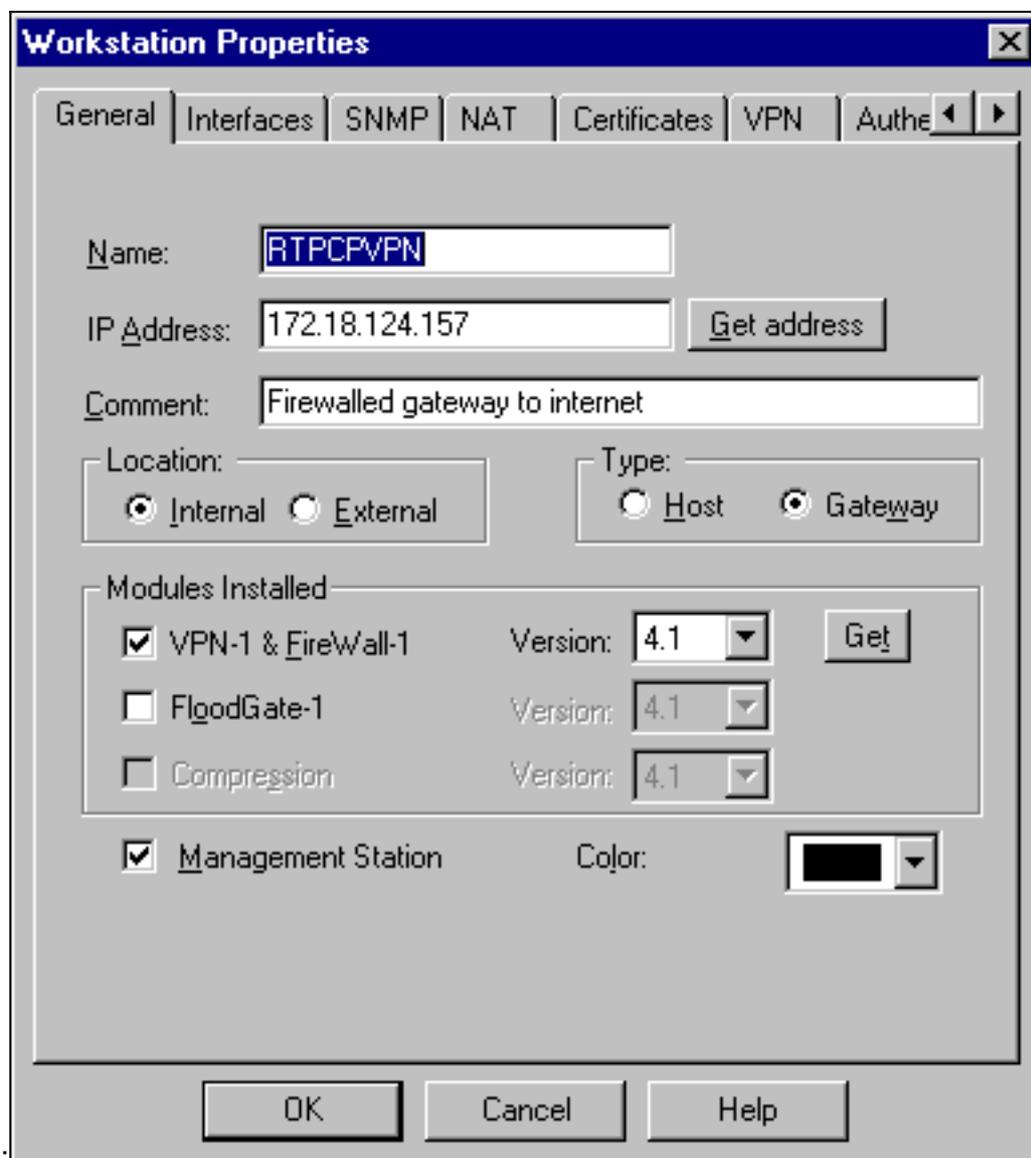


2. Sélectionnez **Gérer > Objets réseau > Nouveau (ou Modifier) > Réseau** pour configurer l'objet pour le réseau interne (appelé « cpinside ») derrière le Checkpoint. Ceci doit être conforme à la commande destination (second) network dans la **liste d'accès 115 permit ip 192.168.1.0 0.0.0.255 10.32.50.0 0.0.0.255**. Sélectionnez **Interne** sous

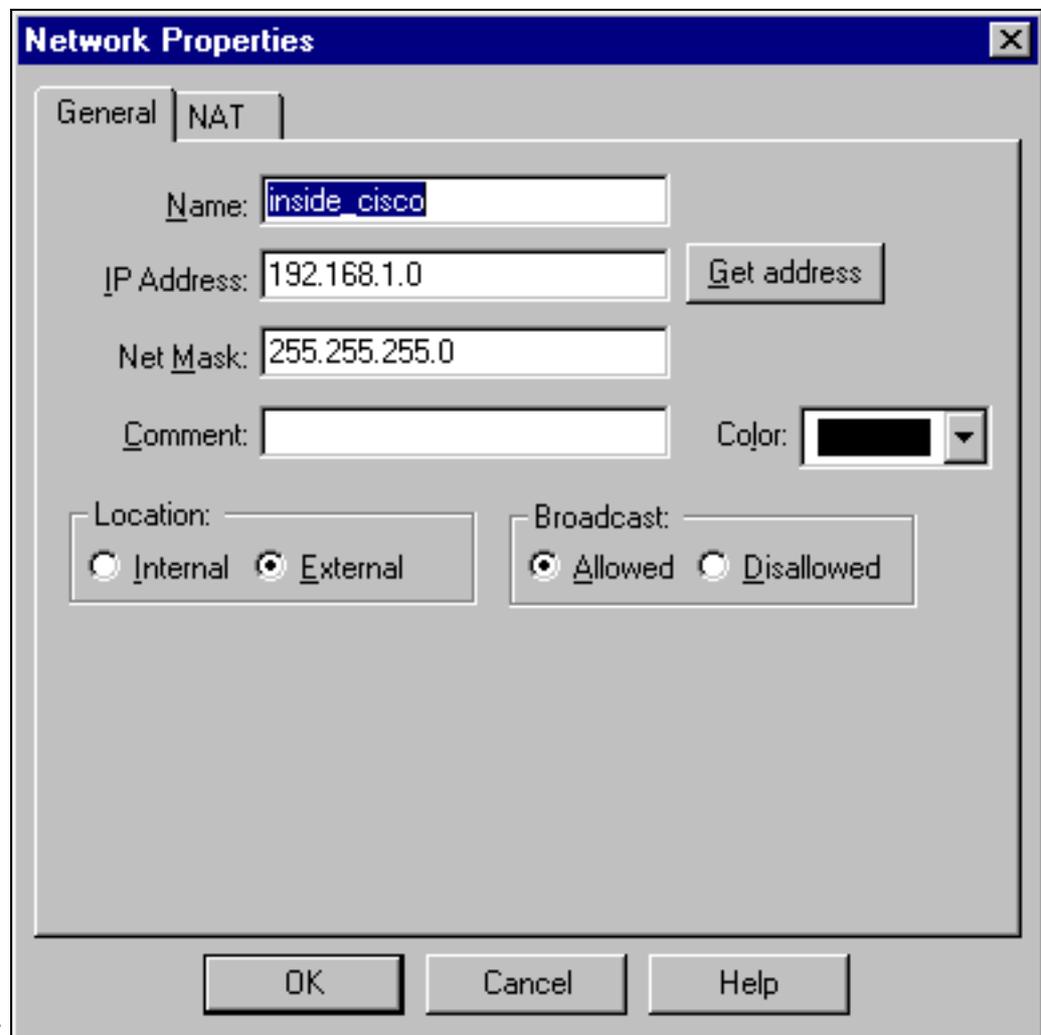


Emplacement.

3. Sélectionnez **Gérer > Objets réseau > Modifier** pour modifier l'objet du point de terminaison RTPCPVPN Checkpoint (passerelle) auquel le routeur Cisco pointe dans la commande **set peer 172.18.124.157**. Sélectionnez **Interne** sous Emplacement. Pour Type, sélectionnez **Passerelle**. Sous Modules installés, activez la case à cocher **VPN-1 et FireWall-1**, et activez également la case à cocher **Station de gestion**

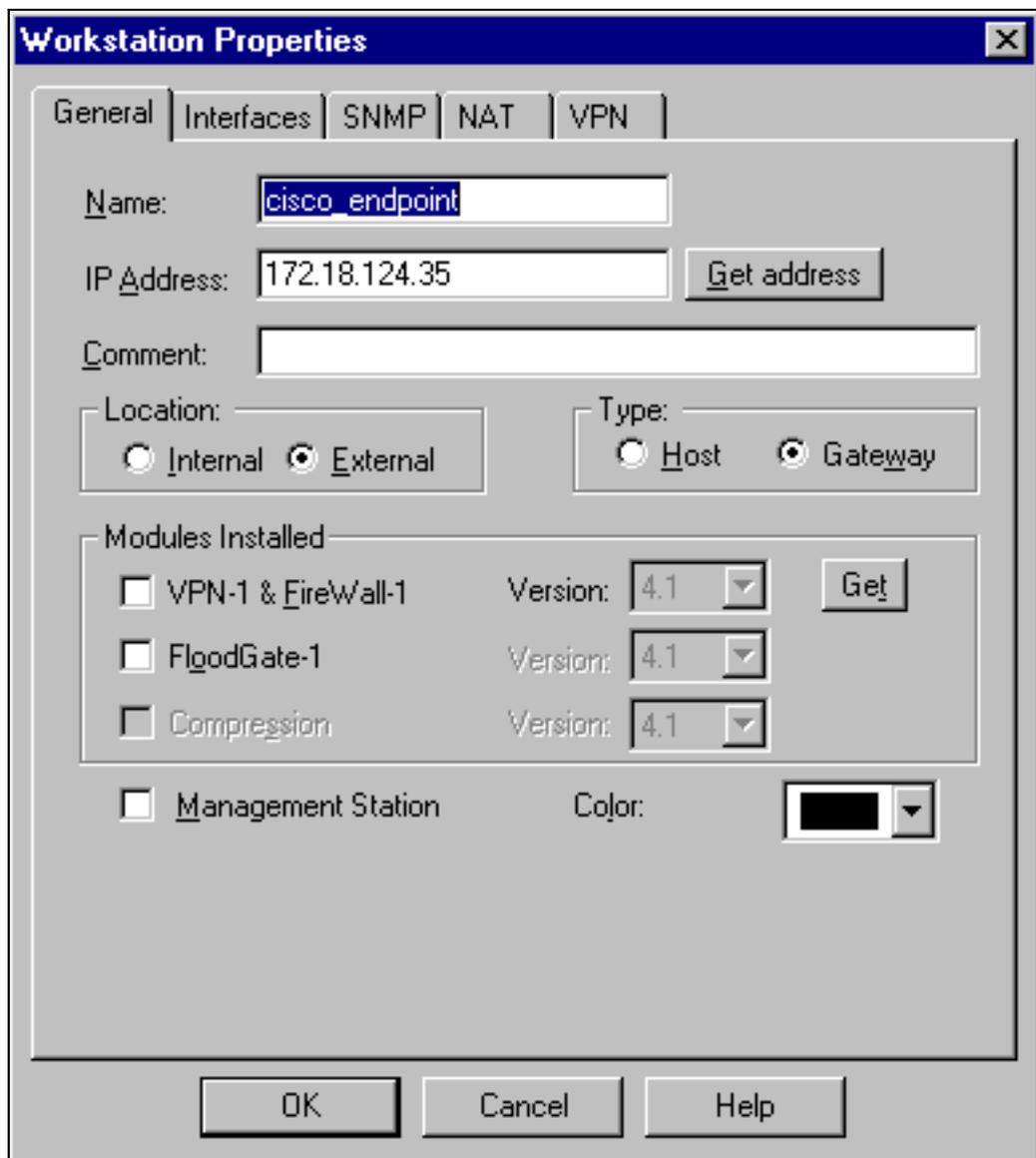


4. Sélectionnez **Gérer > Objets réseau > Nouveau > Réseau** pour configurer l'objet pour le réseau externe (appelé « inside_cisco ») derrière le routeur Cisco. Ceci doit être conforme à la commande source (premier) network dans la liste d'accès 115 permit ip 192.168.1.0 0.0.0.255 10.32.50.0 0.0.0.255. Sélectionnez **Externe** sous



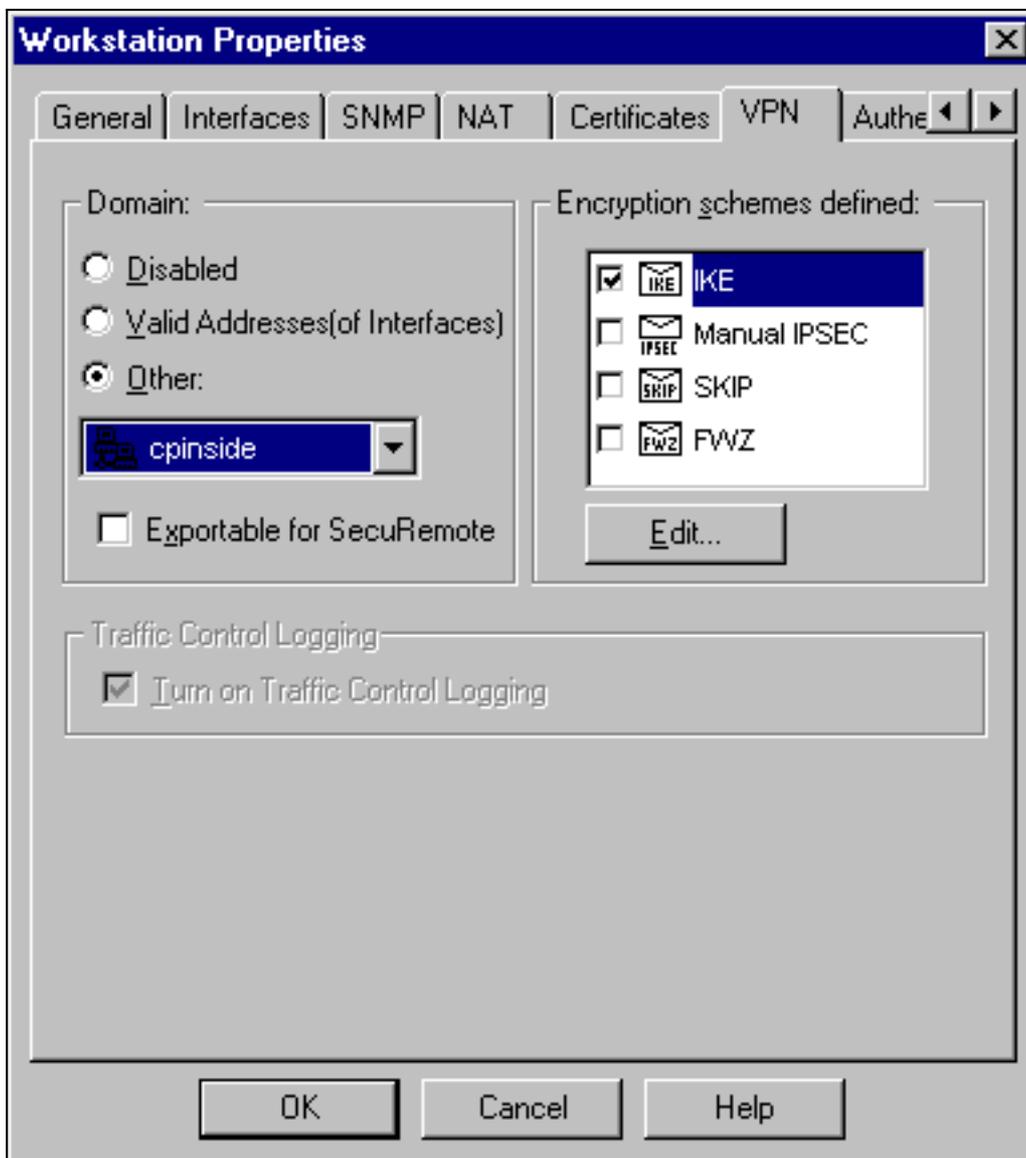
Emplacement.

5. Sélectionnez **Gérer > Objets réseau > Nouveau > Station de travail** pour ajouter un objet pour la passerelle de routeur Cisco externe (appelé « cisco_endpoint »). Il s'agit de l'interface Cisco à laquelle la commande **crypto map name** est appliquée. Sélectionnez **Externe** sous Emplacement. Pour Type, sélectionnez **Passerelle**. **Remarque** : Ne cochez pas la case VPN-



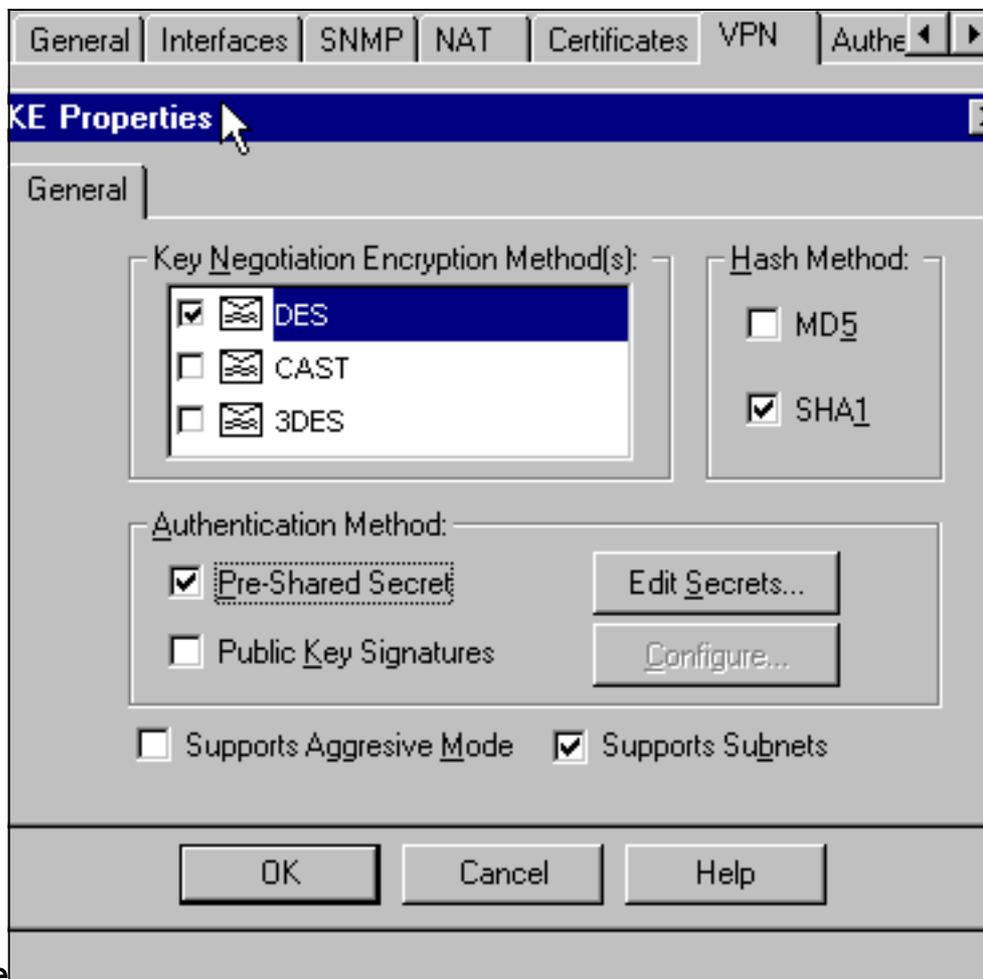
1/FireWall-1.

6. Sélectionnez **Gérer > Objets réseau > Modifier** pour modifier l'onglet VPN du point de terminaison de passerelle Checkpoint (appelé RTPCPVPN). Sous Domaine, sélectionnez **Autre**, puis sélectionnez l'intérieur du réseau Checkpoint (appelé « cpinside ») dans la liste déroulante. Sous Schémas de chiffrement définis, sélectionnez **IKE**, puis cliquez sur



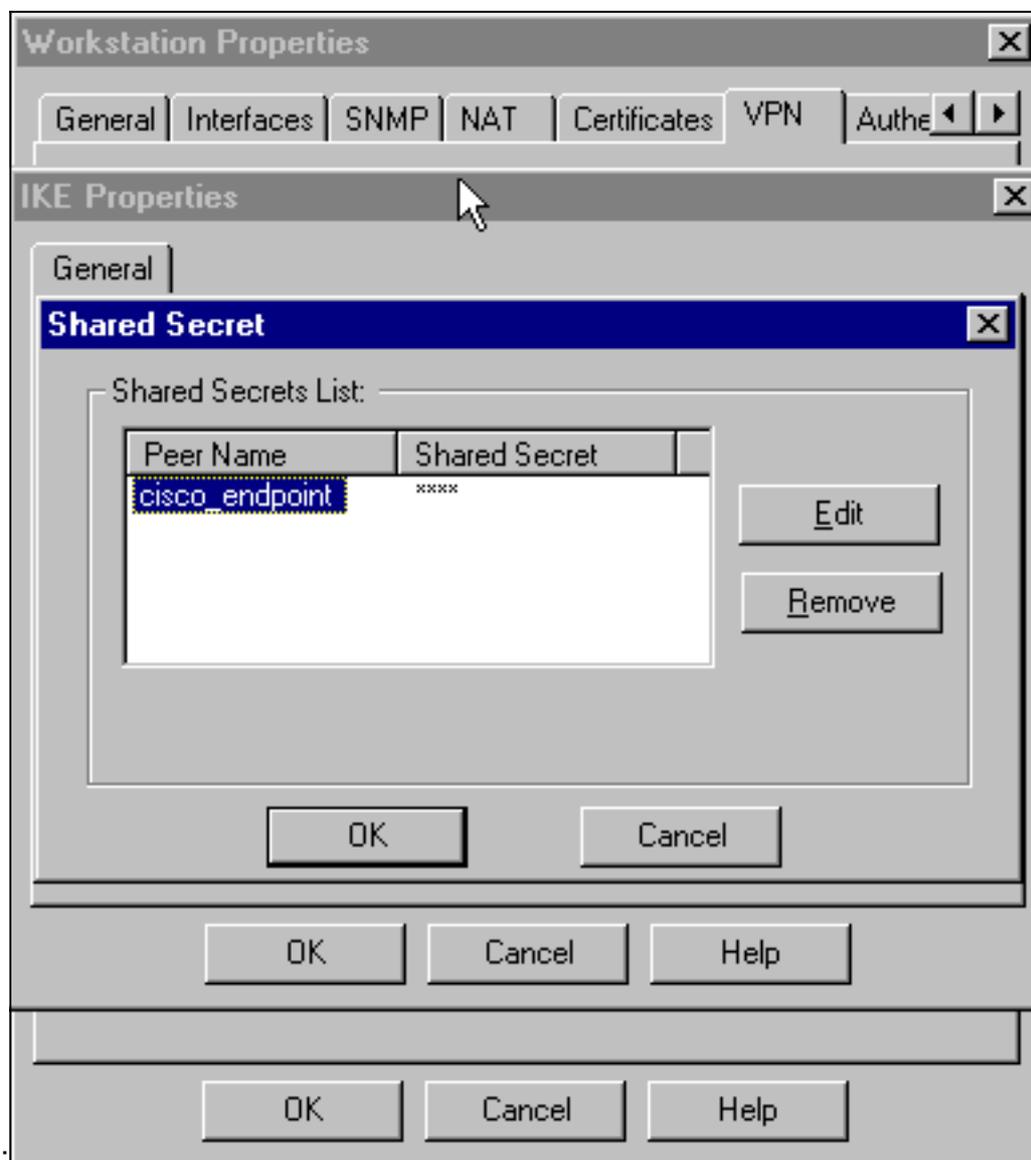
Modifier.

7. Modifiez les propriétés IKE pour le chiffrement DES afin qu'elles soient compatibles avec ces commandes :**crypto isakmp policy n°cryptage des****Remarque** : le chiffrement DES est le mode par défaut, de sorte qu'il n'est pas visible dans la configuration Cisco.
8. Remplacez les propriétés IKE par le hachage SHA1 pour accepter ces commandes :**crypto isakmp policy n°hash sha****Remarque** : l'algorithme de hachage SHA est l'algorithme par défaut. Il n'est donc pas visible dans la configuration Cisco.Modifiez ces paramètres :**Désélectionnez Mode agressif.Cochez Support Subnets.Cochez Pre-Shared Secret** sous Authentication Method. Ceci est en accord avec ces commandes :**crypto isakmp policy n°authentication pre-**

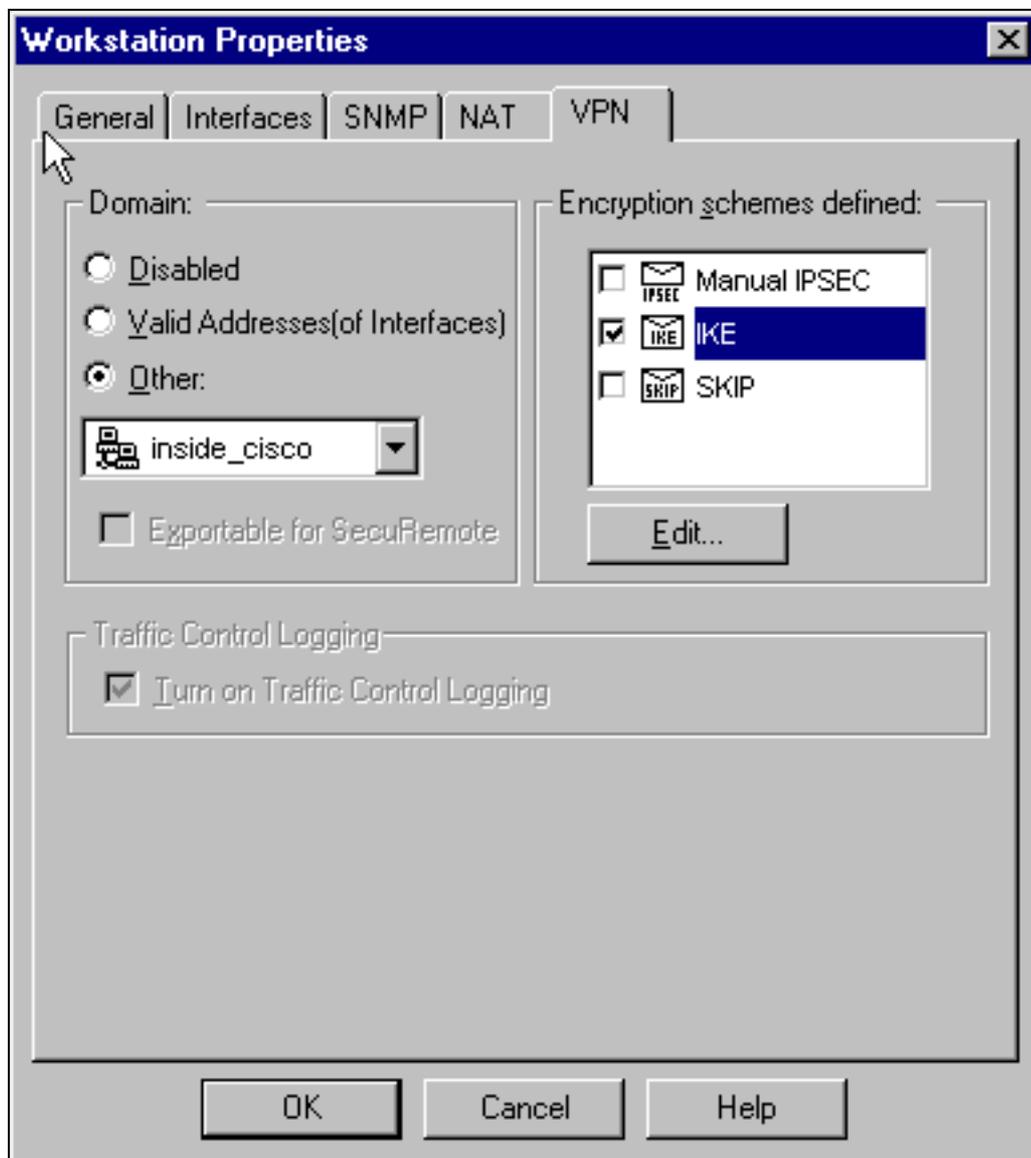


share

9. Cliquez sur **Modifier les secrets** pour définir la clé pré-partagée de manière à accepter la commande Cisco `crypto isakmp key key address`

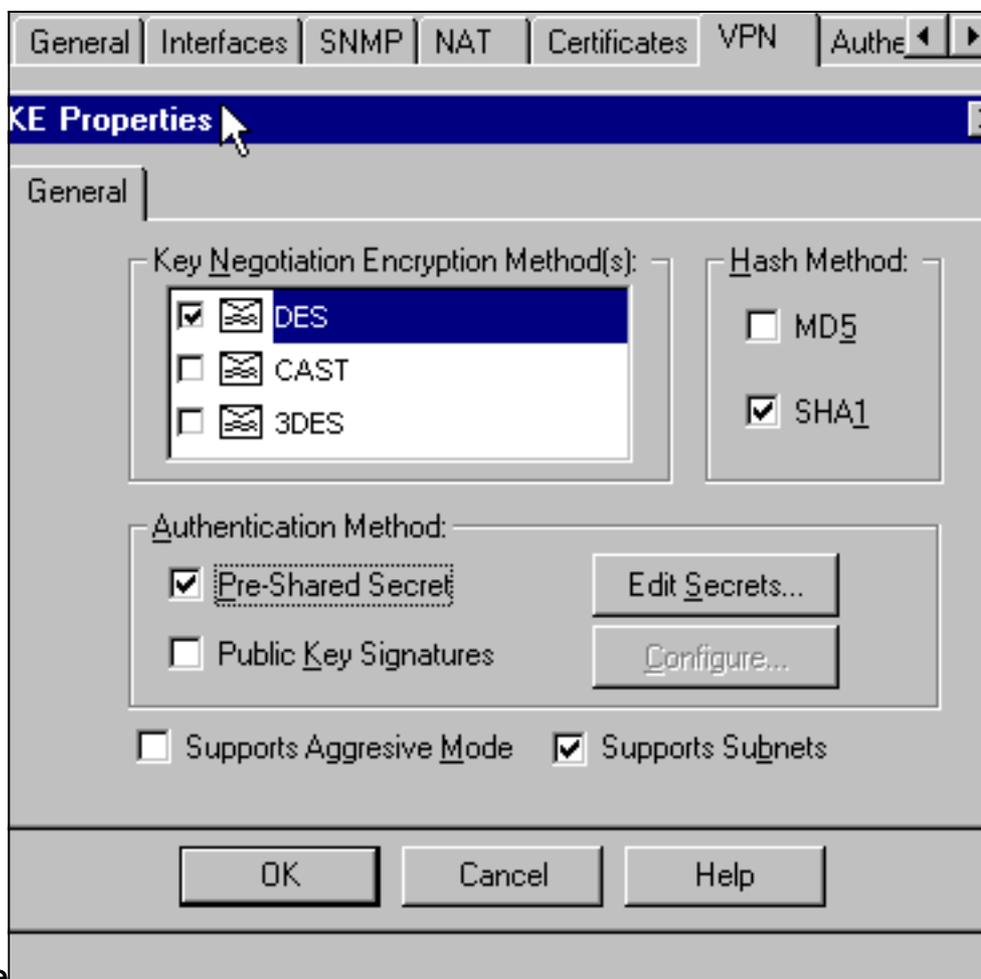


10. Sélectionnez **Gérer > Objets réseau > Modifier** pour modifier l'onglet VPN « cisco_endpoint ». Sous Domaine, sélectionnez **Autre**, puis sélectionnez l'intérieur du réseau Cisco (appelé « inside_cisco »). Sous Schémas de chiffrement définis, sélectionnez **IKE**, puis cliquez sur



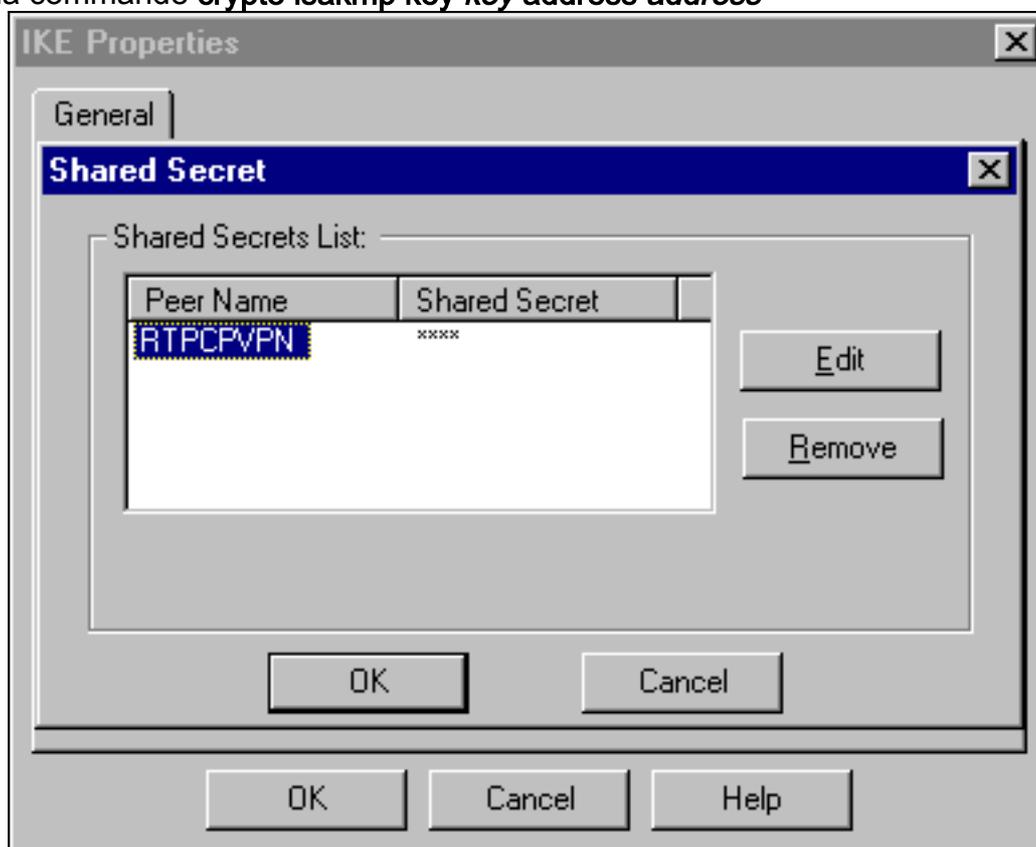
Modifier.

11. Modifiez les propriétés IKE du chiffrement DES pour qu'elles soient compatibles avec ces commandes :**crypto isakmp policy n°cryptage des****Remarque** : le chiffrement DES est le mode par défaut, de sorte qu'il n'est pas visible dans la configuration Cisco.
12. Remplacez les propriétés IKE par le hachage SHA1 pour accepter ces commandes :**crypto isakmp policy n°hash sha****Remarque** : l'algorithme de hachage SHA est l'algorithme par défaut. Il n'est donc pas visible dans la configuration Cisco. Modifiez ces paramètres : Désélectionnez **Mode agressif**. Cochez **Support Subnets**. Cochez **Pre-Shared Secret** sous Authentication Method. Ceci est en accord avec ces commandes :**crypto isakmp policy n°authentication pre-**



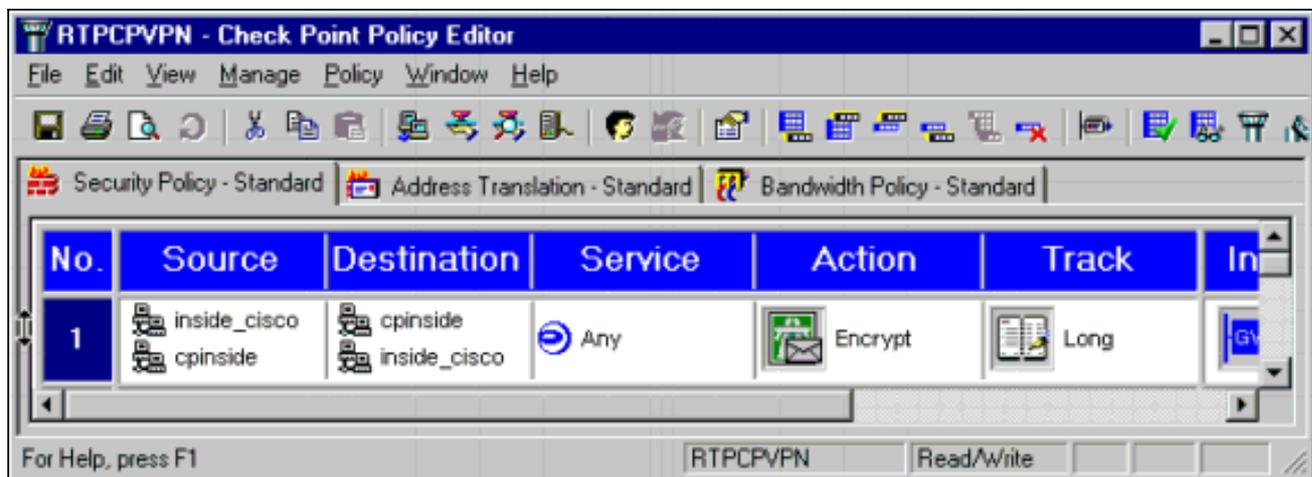
share

13. Cliquez sur **Modifier les secrets** pour définir la clé pré-partagée de manière à être d'accord avec la commande `crypto isakmp key key address address`

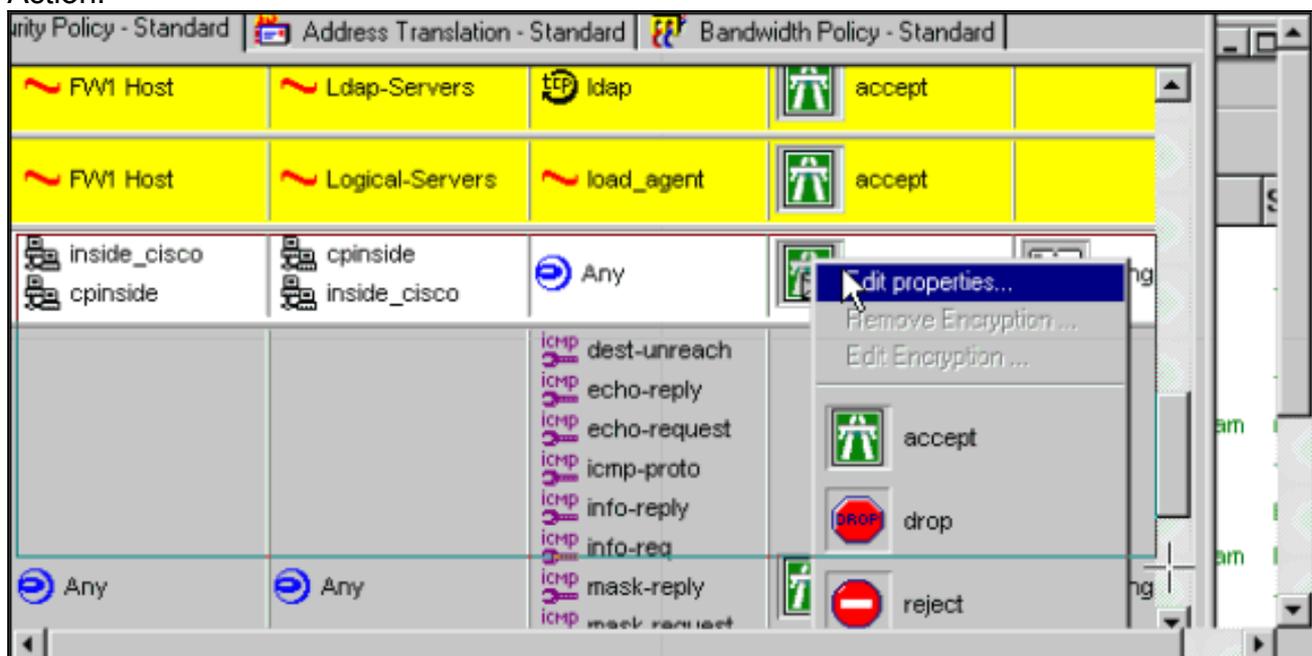


Cisco.

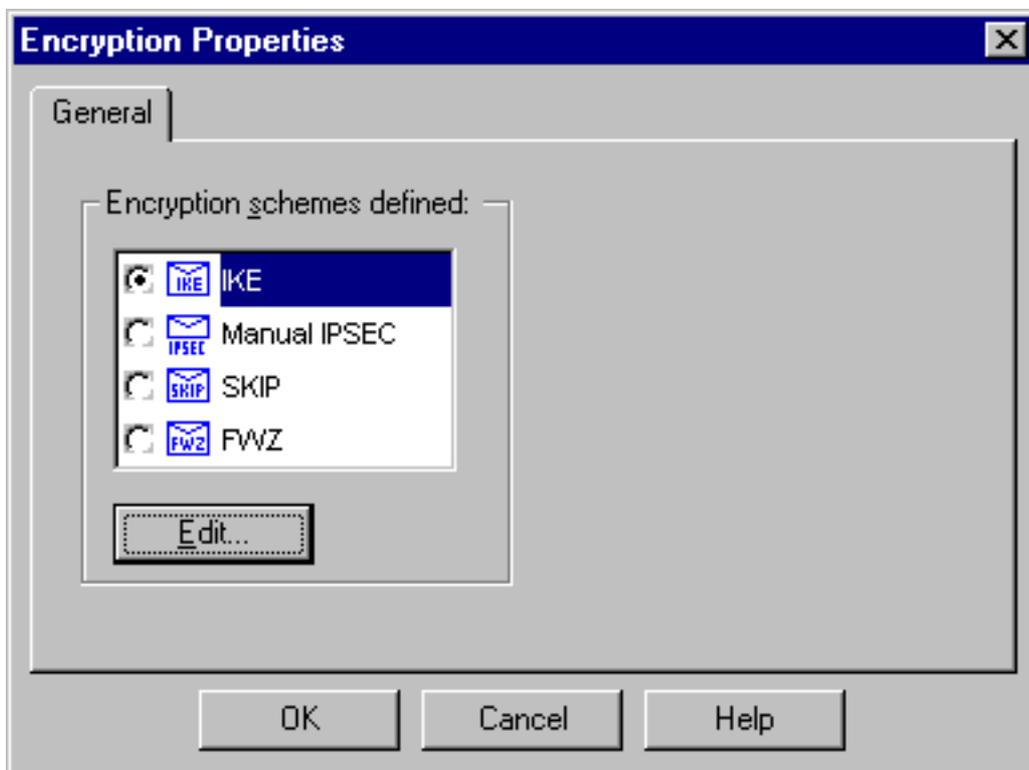
14. Dans la fenêtre Éditeur de stratégie, insérez une règle avec Source et Destination comme « inside_cisco » et « cinside » (bidirectionnel). Définir **Service=Any**, **Action=Encrypt** et **Track=Long**.



15. Cliquez sur l'icône **Chiffrement** verte et sélectionnez **Modifier les propriétés** pour configurer les stratégies de chiffrement sous l'en-tête Action.



16. Sélectionnez **IKE**, puis cliquez sur



Modifier.

17. Dans la fenêtre Propriétés IKE, modifiez ces propriétés pour qu'elles correspondent aux transformations Cisco IPsec dans la commande `crypto ipsec transform-set rpset esp-des esp-sha-hmac` : Sous Transform, sélectionnez **Encryption + Data Integrity (ESP)**. L'algorithme de chiffrement doit être **DES**, l'intégrité des données doit être **SHA1** et la passerelle d'homologue autorisée doit être la passerelle de routeur externe (appelée « cisco_endpoint »). Click



OK.

18. Après avoir configuré le point de contrôle, sélectionnez **Policy > Install** dans le menu Checkpoint pour que les modifications prennent effet.

Vérification

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

L'[Outil Interpréteur de sortie \(clients enregistrés uniquement\) \(OIT\) prend en charge certaines commandes show](#). Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show**.

- **show crypto isakmp sa** - Affichez toutes les associations de sécurité IKE (SA) actuelles sur un homologue.
- **show crypto ipsec sa** - Affichez les paramètres utilisés par les SA actuelles.

Dépannage

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

Dépannage des commandes

Remarque : Consulter les [renseignements importants sur les commandes de débogage](#) avant d'utiliser 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.

Récapitulation de réseau

Lorsque plusieurs réseaux internes adjacents sont configurés dans le domaine de chiffrement sur le point de contrôle, le périphérique peut automatiquement les résumer en fonction du trafic intéressant. Si le routeur n'est pas configuré pour correspondre, le tunnel risque d'échouer. Par exemple, si les réseaux internes 10.0.0.0 /24 et 10.0.1.0 /24 sont configurés pour être inclus dans le tunnel, ils peuvent être résumés sur 10.0.0.0 /23.

Point de contrôle

Comme le suivi a été défini sur Long dans la fenêtre Éditeur de stratégie, le trafic refusé doit apparaître en rouge dans la Visionneuse de journaux. Vous pouvez obtenir plus de débogage détaillé avec :

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

et dans une autre fenêtre :

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

Remarque : Il s'agissait d'une installation de Microsoft Windows NT.

Émettez ces commandes pour effacer les SA sur le point de contrôle :

```
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
```

Répondez oui à la question Êtes-vous sûr ? activer.

Exemple de sortie de débogage

Configuration register is 0x2102

```
cisco_endpoint#debug crypto isakmp
Crypto ISAKMP debugging is on
cisco_endpoint#debug crypto isakmp
Crypto IPSEC debugging is on
cisco_endpoint#debug crypto engine
Crypto Engine debugging is on
cisco_endpoint#
20:54:06: IPSEC(sa_request): ,
    (key eng. msg.) src= 172.18.124.35, dest= 172.18.124.157,
    src_proxy= 192.168.1.0/255.255.255.0/0/0 (type=4),
    dest_proxy= 10.32.50.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-des esp-sha-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0xA29984CA(2727969994), conn_id= 0, keysize= 0, flags= 0x4004
20:54:06: ISAKMP: received ke message (1/1)
20:54:06: ISAKMP: local port 500, remote port 500
20:54:06: ISAKMP (0:1): beginning Main Mode exchange
20:54:06: ISAKMP (0:1): sending packet to 172.18.124.157 (I) MM_NO_STATE
20:54:06: ISAKMP (0:1): received packet from 172.18.124.157 (I) MM_NO_STATE
20:54:06: ISAKMP (0:1): processing SA payload. message ID = 0
20:54:06: ISAKMP (0:1): found peer pre-shared key matching 172.18.124.157
20:54:06: ISAKMP (0:1): Checking ISAKMP transform 1 against priority 1 policy
20:54:06: ISAKMP:      encryption DES-CBC
20:54:06: ISAKMP:      hash SHA
20:54:06: ISAKMP:      default group 1
20:54:06: ISAKMP:      auth pre-share
20:54:06: ISAKMP (0:1): atts are acceptable. Next payload is 0
20:54:06: CryptoEngine0: generate alg parameter
20:54:06: CRYPTO_ENGINE: Dh phase 1 status: 0
20:54:06: CRYPTO_ENGINE: Dh phase 1 status: 0
20:54:06: ISAKMP (0:1): SA is doing pre-shared key authentication
    using id type ID_IPV4_ADDR
20:54:06: ISAKMP (0:1): sending packet to 172.18.124.157 (I) MM_SA_SETUP
20:54:06: ISAKMP (0:1): received packet from 172.18.124.157 (I) MM_SA_SETUP
20:54:06: ISAKMP (0:1): processing KE payload. message ID = 0
20:54:06: CryptoEngine0: generate alg parameter
20:54:06: ISAKMP (0:1): processing NONCE payload. message ID = 0
20:54:06: ISAKMP (0:1): found peer pre-shared key matching 172.18.124.157
20:54:06: CryptoEngine0: create ISAKMP SKEYID for conn id 1
20:54:06: ISAKMP (0:1): SKEYID state generated
20:54:06: ISAKMP (1): ID payload
    next-payload : 8
    type          : 1
    protocol      : 17
    port          : 500
    length        : 8
20:54:06: ISAKMP (1): Total payload length: 12
20:54:06: CryptoEngine0: generate hmac context for conn id 1
20:54:06: ISAKMP (0:1): sending packet to 172.18.124.157 (I) MM_KEY_EXCH
20:54:06: ISAKMP (0:1): received packet from 172.18.124.157 (I) MM_KEY_EXCH
```

20:54:06: ISAKMP (0:1): processing ID payload. message ID = 0
20:54:06: ISAKMP (0:1): processing HASH payload. message ID = 0
20:54:06: CryptoEngine0: generate hmac context for conn id 1
20:54:06: ISAKMP (0:1): SA has been authenticated with 172.18.124.157
20:54:06: ISAKMP (0:1): beginning Quick Mode exchange, M-ID of 1855173267
20:54:06: CryptoEngine0: generate hmac context for conn id 1
20:54:06: ISAKMP (0:1): sending packet to 172.18.124.157 (I) QM_IDLE
20:54:06: CryptoEngine0: clear dh number for conn id 1
20:54:06: ISAKMP (0:1): received packet from 172.18.124.157 (I) QM_IDLE
20:54:06: CryptoEngine0: generate hmac context for conn id 1
20:54:06: ISAKMP (0:1): processing HASH payload. message ID = 1855173267
20:54:06: ISAKMP (0:1): processing SA payload. message ID = 1855173267
20:54:06: ISAKMP (0:1): Checking IPsec proposal 1
20:54:06: ISAKMP: transform 1, ESP_DES
20:54:06: ISAKMP: attributes in transform:
20:54:06: ISAKMP: encaps is 1
20:54:06: ISAKMP: SA life type in seconds
20:54:06: ISAKMP: SA life duration (basic) of 3600
20:54:06: ISAKMP: SA life type in kilobytes
20:54:06: ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0
20:54:06: ISAKMP: authenticator is HMAC-SHA
20:54:06: validate proposal 0
20:54:06: ISAKMP (0:1): atts are acceptable.
20:54:06: IPSEC(validate_proposal_request): proposal part #1,
 (key eng. msg.) dest= 172.18.124.157, src= 172.18.124.35,
 dest_proxy= 10.32.50.0/255.255.255.0/0/0 (type=4),
 src_proxy= 192.168.1.0/255.255.255.0/0/0 (type=4),
 protocol= ESP, transform= esp-des esp-sha-hmac ,
 lifedur= 0s and 0kb,
 spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
20:54:06: validate proposal request 0
20:54:06: ISAKMP (0:1): processing NONCE payload. message ID = 1855173267
20:54:06: ISAKMP (0:1): processing ID payload. message ID = 1855173267
20:54:06: ISAKMP (0:1): processing ID payload. message ID = 1855173267
20:54:06: CryptoEngine0: generate hmac context for conn id 1
20:54:06: ipsec allocate flow 0
20:54:06: ipsec allocate flow 0
20:54:06: ISAKMP (0:1): Creating IPsec SAs
20:54:06: inbound SA from 172.18.124.157 to 172.18.124.35
 (proxy 10.32.50.0 to 192.168.1.0)
20:54:06: has spi 0xA29984CA and conn_id 2000 and flags 4
20:54:06: lifetime of 3600 seconds
20:54:06: lifetime of 4608000 kilobytes
20:54:06: outbound SA from 172.18.124.35 to 172.18.124.157
 (proxy 192.168.1.0 to 10.32.50.0)
20:54:06: has spi 404516441 and conn_id 2001 and flags 4
20:54:06: lifetime of 3600 seconds
20:54:06: lifetime of 4608000 kilobytes
20:54:06: ISAKMP (0:1): sending packet to 172.18.124.157 (I) QM_IDLE
20:54:06: ISAKMP (0:1): deleting node 1855173267 error FALSE reason ""
20:54:06: IPSEC(key_engine): got a queue event...
20:54:06: IPSEC(initialize_sas): ,
 (key eng. msg.) dest= 172.18.124.35, src= 172.18.124.157,
 dest_proxy= 192.168.1.0/255.255.255.0/0/0 (type=4),
 src_proxy= 10.32.50.0/255.255.255.0/0/0 (type=4),
 protocol= ESP, transform= esp-des esp-sha-hmac ,
 lifedur= 3600s and 4608000kb,
 spi= 0xA29984CA(2727969994), conn_id= 2000, keysize= 0, flags= 0x4
20:54:06: IPSEC(initialize_sas): ,
 (key eng. msg.) src= 172.18.124.35, dest= 172.18.124.157,
 src_proxy= 192.168.1.0/255.255.255.0/0/0 (type=4),
 dest_proxy= 10.32.50.0/255.255.255.0/0/0 (type=4),
 protocol= ESP, transform= esp-des esp-sha-hmac ,
 lifedur= 3600s and 4608000kb,

```
spi= 0x181C6E59(404516441), conn_id= 2001, keysize= 0, flags= 0x4
20:54:06: IPSEC(create_sa): sa created,
(sa) sa_dest= 172.18.124.35, sa_prot= 50,
sa_spi= 0xA29984CA(2727969994),
sa_trans= esp-des esp-sha-hmac , sa_conn_id= 2000
20:54:06: IPSEC(create_sa): sa created,
(sa) sa_dest= 172.18.124.157, sa_prot= 50,
sa_spi= 0x181C6E59(404516441),
sa_trans= esp-des esp-sha-hmac , sa_conn_id= 2001
cisco_endpoint#sho cry ips sa
```

```
interface: Ethernet0/0
```

```
Crypto map tag: rtp, local addr. 172.18.124.35
```

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

```
remote ident (addr/mask/prot/port): (10.32.50.0/255.255.255.0/0/0)
```

```
current_peer: 172.18.124.157
```

```
PERMIT, flags={origin_is_acl,}
```

```
#pkts encaps: 14, #pkts encrypt: 14, #pkts digest 14
```

```
#pkts decaps: 14, #pkts decrypt: 14, #pkts verify 14
```

```
#pkts compressed: 0, #pkts decompressed: 0
```

```
#pkts not compressed: 0, #pkts compr. failed: 0,
```

```
#pkts decompress failed: 0, #send errors 1, #recv errors 0
```

```
local crypto endpt.: 172.18.124.35, remote crypto endpt.: 172.18.124.157
```

```
path mtu 1500, media mtu 1500
```

```
current outbound spi: 181C6E59
```

```
inbound esp sas:
```

```
spi: 0xA29984CA(2727969994)
```

```
transform: esp-des esp-sha-hmac ,
```

```
in use settings = {Tunnel, }
```

```
slot: 0, conn id: 2000, flow_id: 1, crypto map: rtp
```

```
--More-- sa timing: remaining key lifetime (k/sec):
(4607998/3447)
```

```
IV size: 8 bytes
```

```
replay detection support: Y
```

```
inbound ah sas:
```

```
inbound pcp sas:
```

```
outbound esp sas:
```

```
spi: 0x181C6E59(404516441)
```

```
transform: esp-des esp-sha-hmac ,
```

```
in use settings = {Tunnel, }
```

```
slot: 0, conn id: 2001, flow_id: 2, crypto map: rtp
```

```
sa timing: remaining key lifetime (k/sec): (4607997/3447)
```

```
IV size: 8 bytes
```

```
replay detection support: Y
```

```
outbound ah sas:
```

```
outbound pcp sas:
```

```
cisco_endpoint#show crypto isakmp sa
```

dst	src	state	conn-id	slot
172.18.124.157	172.18.124.35	QM_IDLE	1	0

```
cisco_endpoint#exit
```

Informations connexes

- [Négociation IPSec/Protocoles IKE](#)
- [Configuration de la sécurité des réseaux IPSec](#)
- [Configuration du protocole IKE \(Internet Key Exchange\)](#)
- [Support et documentation techniques - Cisco Systems](#)