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

Contenu

Introduction

Cette configuration d'échantillon explique comment former un tunnel d'IPSec avec des clés pré-partagées pour joindre deux réseaux privés. Dans notre exemple, les réseaux joints sont le réseau 192.168.1.X privé à l'intérieur du Pare-feu Cisco Secure de Pix (PIX) et le réseau 10.32.50.X privé à l'intérieur du point de reprise. On le suppose que le trafic de l'intérieur du PIX et de l'intérieur que le pare-feu Checkpoint 4.1 à l'Internet (représenté ici par les réseaux 172.18.124.X) circule avant de commencer cette configuration.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

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

- Version du logiciel PIX 5.3.1
- Pare-feu Checkpoint 4.1

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

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

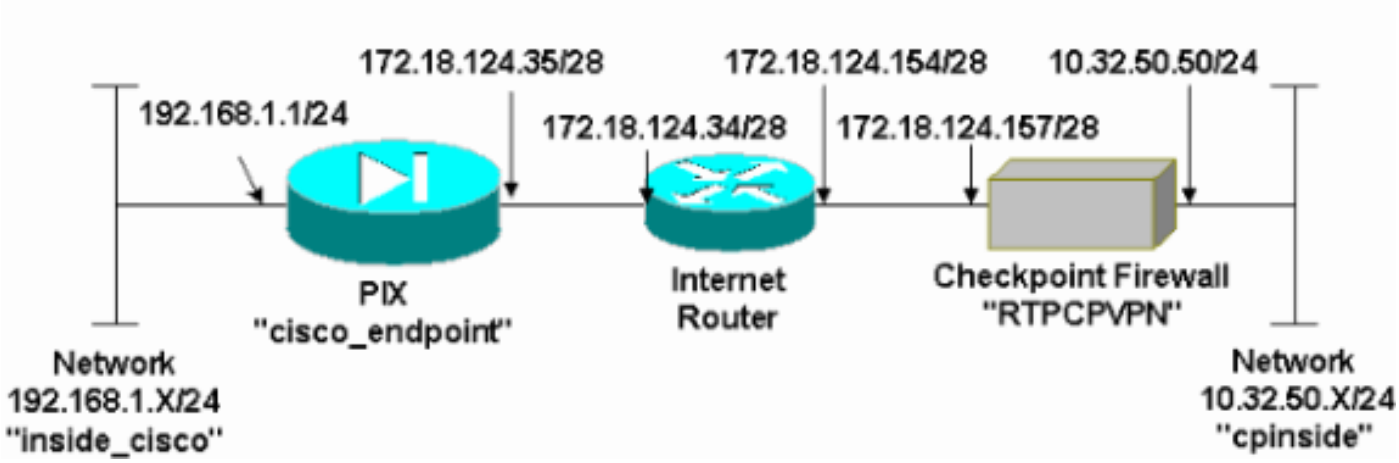
Configurez

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

Remarque: Pour obtenir des informations supplémentaires sur les commandes utilisées dans ce document, utilisez l'Outil de recherche de commande (clients enregistrés seulement).

Diagramme du réseau

Ce document utilise la configuration réseau indiquée dans le diagramme suivant :



Configurations

Ce document utilise les configurations affichées dans cette section.

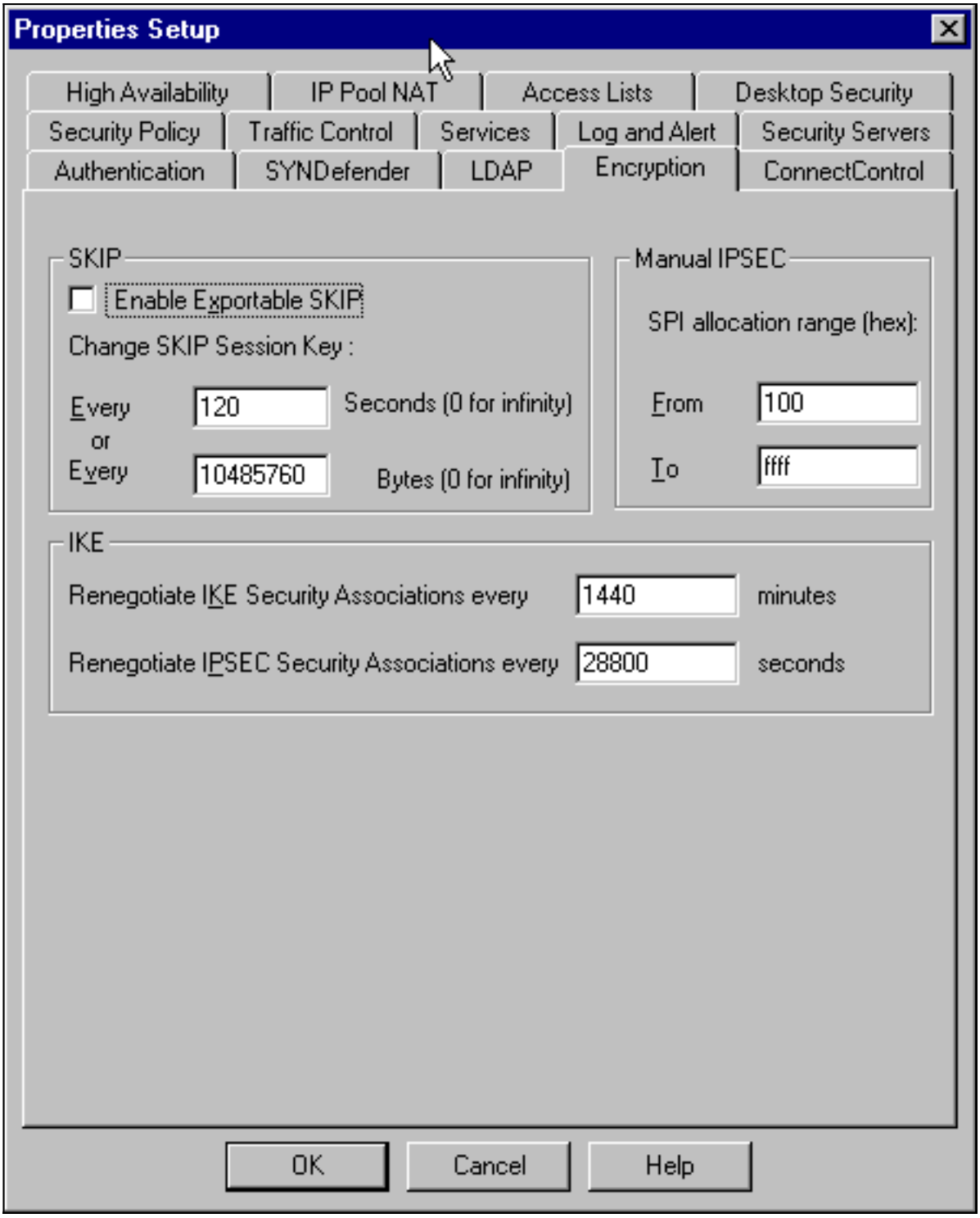
Configuration PIX

```
PIX Version 5.3(1)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname cisco_endpoint
```

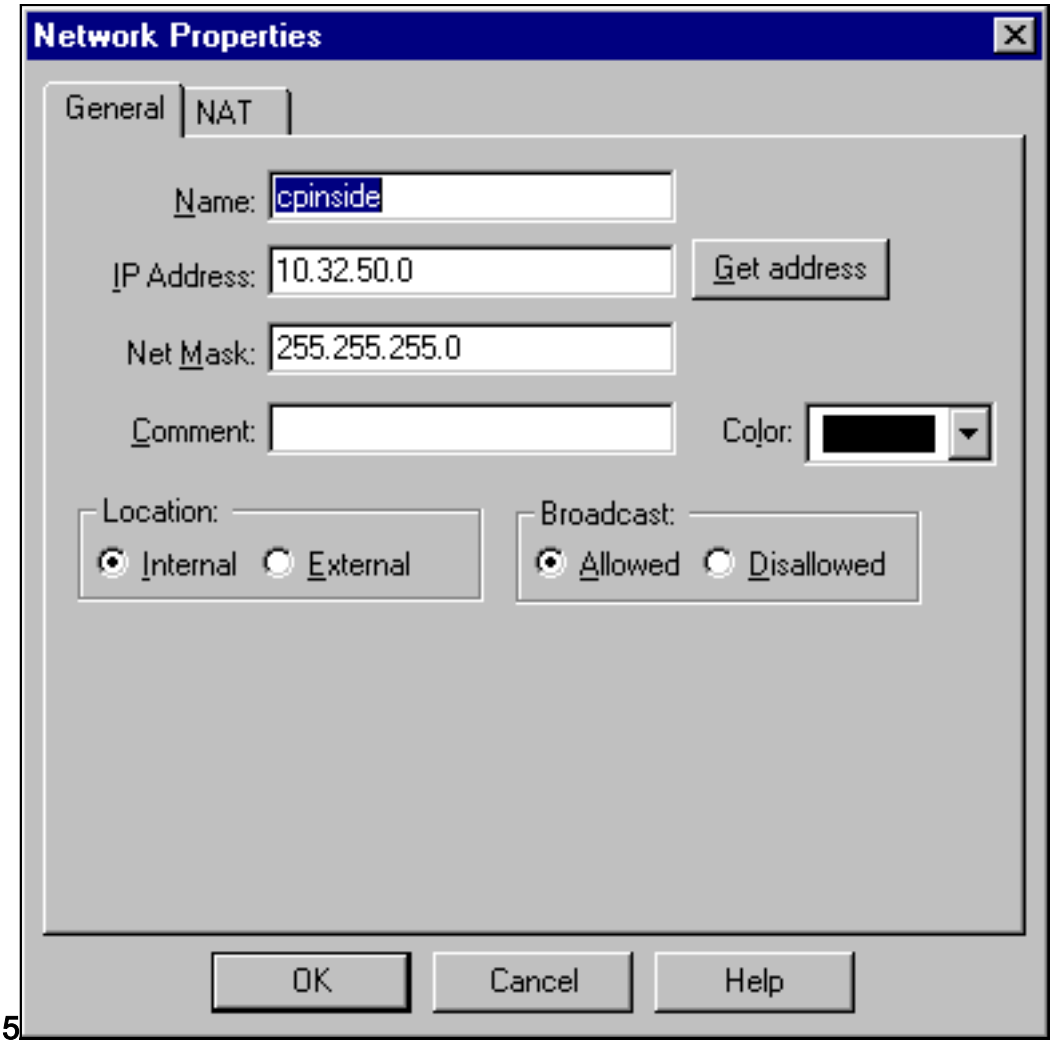
```
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
names
access-list 115 permit ip 192.168.1.0 255.255.255.0
10.32.50.0 255.255.255.0 access-list 115 deny ip
192.168.1.0 255.255.255.0 any pager lines 24 logging on
no logging timestamp no logging standby no logging
console logging monitor debugging no logging buffered
logging trap debugging no logging history logging
facility 20 logging queue 512 interface ethernet0 auto
interface ethernet1 auto mtu outside 1500 mtu inside
1500 ip address outside 172.18.124.35 255.255.255.240 ip
address inside 192.168.1.1 255.255.255.0 ip audit info
action alarm ip audit attack action alarm no failover
failover timeout 0:00:00 failover poll 15 failover ip
address outside 0.0.0.0 failover ip address inside
0.0.0.0 arp timeout 14400 global (outside) 1
172.18.124.36 nat (inside) 0 access-list 115 nat
(inside) 1 0.0.0.0 0.0.0.0 0 0 route outside 0.0.0.0
0.0.0.0 172.18.124.34 1 timeout xlate 3:00:00g SA
0x80bd6a10, conn_id = 0 timeout conn 1:00:00 half-closed
0:10:00 udp 0:02:00 rpc 0:10:00 h323 0:05:00 sip 0:30:00
sip_media 0:02:00 timeout uauth 0:05:00 absolute aaa-
server TACACS+ protocol tacacs+ aaa-server RADIUS
protocol radius no snmp-server location no snmp-server
contact snmp-server community public no snmp-server
enable traps floodguard enable !--- IPSec configuration
sysopt connection permit-ipsec no sysopt route dnat
crypto ipsec transform-set myset esp-des esp-sha-hmac
crypto map rtpmap 10 ipsec-isakmp crypto map rtpmap 10
match address 115 crypto map rtpmap 10 set peer
172.18.124.157 crypto map rtpmap 10 set transform-set
myset crypto map rtpmap 10 set security-association
lifetime seconds 3600 kilobytes 4608000 crypto map
rtpmap interface outside !--- IKE configuration isakmp
enable outside isakmp key ******** address
172.18.124.157 netmask 255.255.255.240 isakmp identity
address isakmp policy 10 authentication pre-share isakmp
policy 10 encryption des isakmp policy 10 hash sha
isakmp policy 10 group 1 isakmp policy 10 lifetime 86400
telnet timeout 5 ssh timeout 5 terminal width 80
Cryptochecksum:dc43c44e4513d3633a3fc7b1c3802c79 : end
[OK]
```

Pare-feu checkpoint

1. Puisque l'IKE et les vies par défaut d'IPSec diffèrent entre les constructeurs, **Properties** choisi **>** le **cryptage** pour placer les durées de vie du point de contrôle pour être d'accord avec le PIX se transfère.Le durée de vie IKE par défaut du PIX est de 86400 secondes (minutes =1440), de modifiable par cette commande : **stratégie d'ISAKMP # vie 86400**La vie d'IKE PIX peut être configurée entre 60-86400 secondes.La vie d'IPSec de par défaut PIX est de 28800 secondes, de modifiable par cette commande : **le crypto ipsec security-association lifetime seconde #**Vous pouvez configurer une vie PIX IPSec entre 120-86400 secondes.

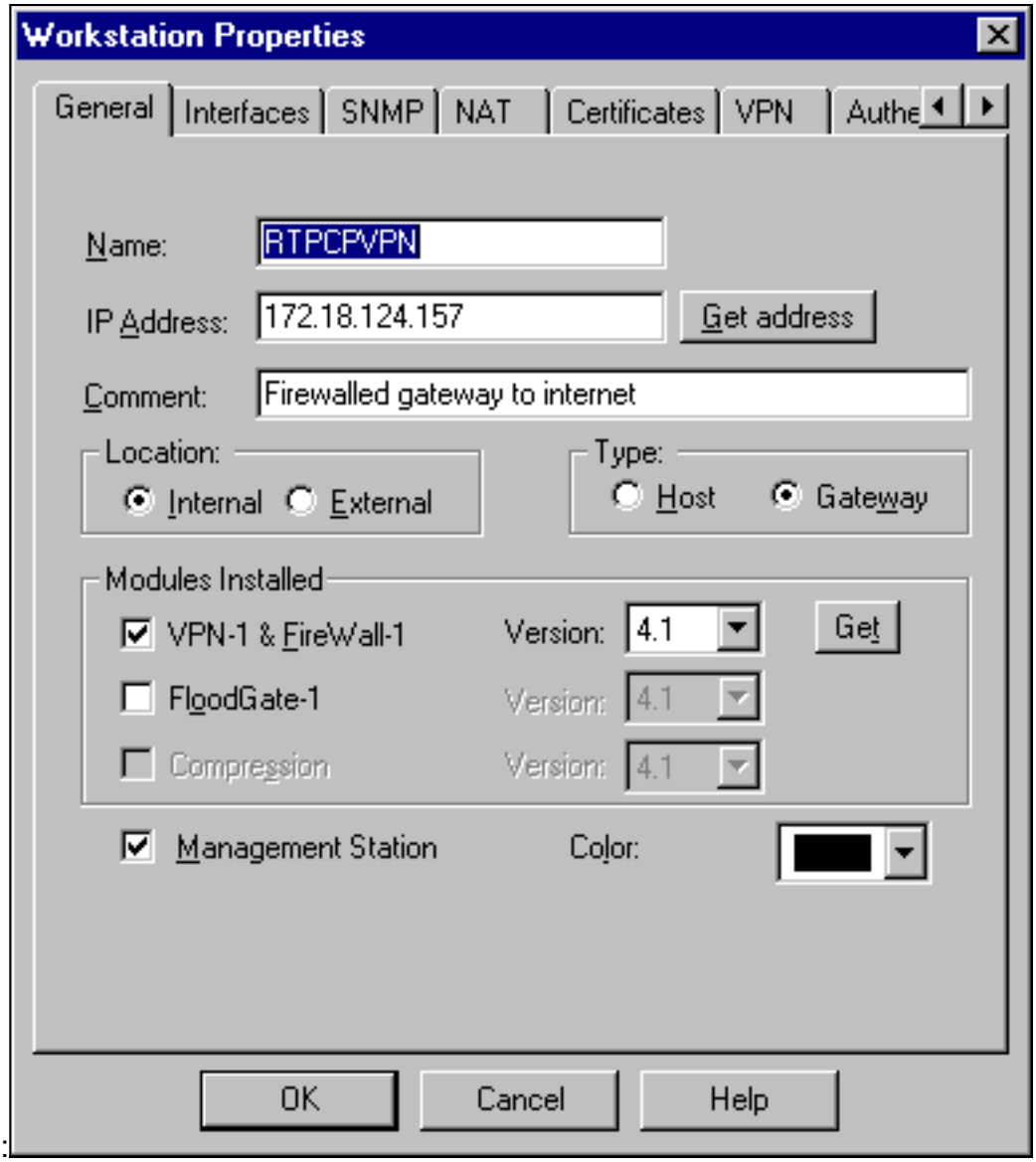


2. Choisi **gérez** > des **objets de réseau** > **nouveau (ou éditez)** > **réseau** pour configurer l'objet pour (« cpinside ») le réseau interne derrière le point de reprise.Ceci doit être conforme au réseau de destination (en second lieu) dans cette commande PIX : **IP 192.168.1.0 255.255.255.0 10.32.50.0 255.255.255.0 d'autorisation de la liste d'accès**



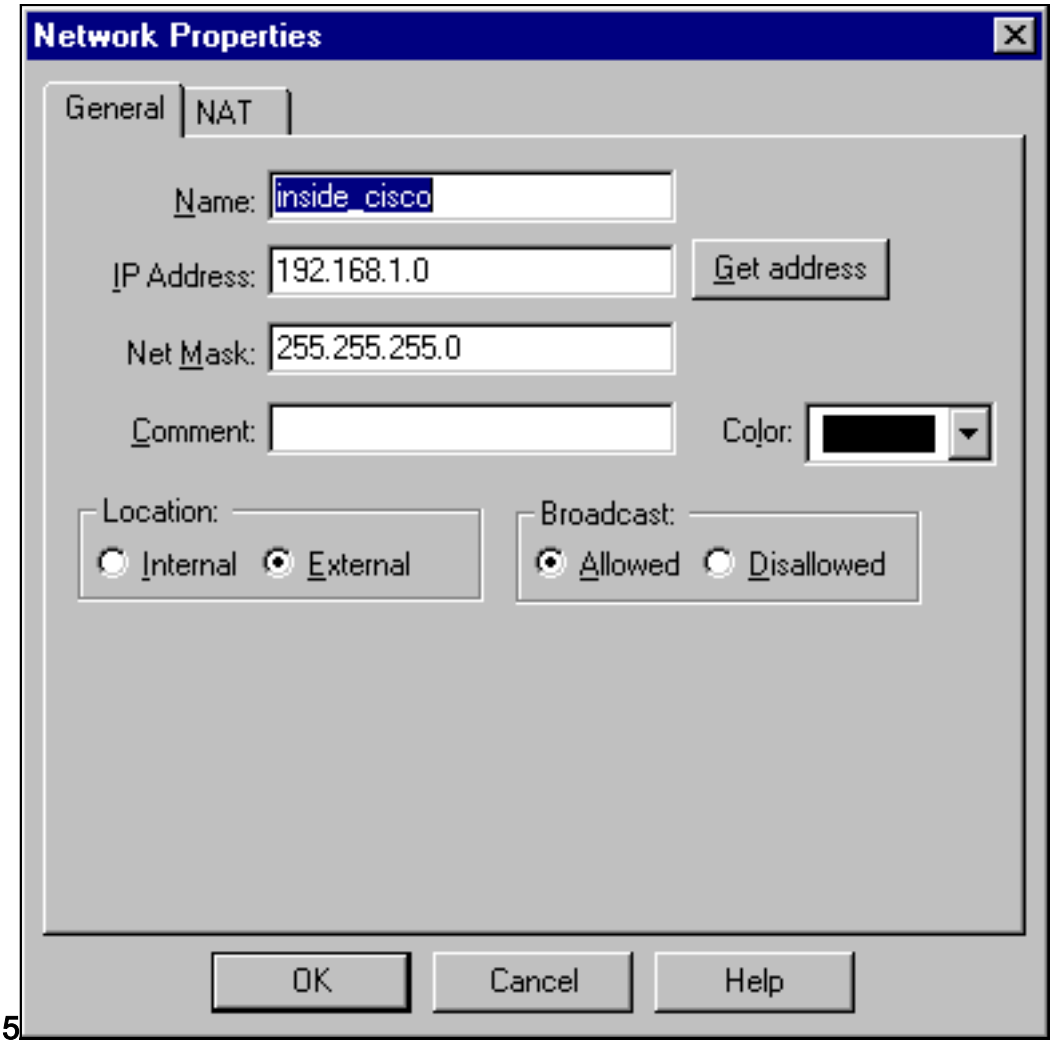
115

3. Choisi **gérez** > des **objets de réseau** > **éditent** pour éditer l'objet pour point final de passerelle (point de reprise le « RTPCPVPN ») ce les points PIX à dans cette commande : **le nom de carte de chiffrement # a placé des ip_address de pair**Sous l'emplacement, **interne** choisi. Pour le type, **passerelle** choisie. Sous des modules installés, sélectionnez la case à cocher **VPN-1 et FireWall-1**, et sélectionnez également la case à cocher de **station de Gestion**



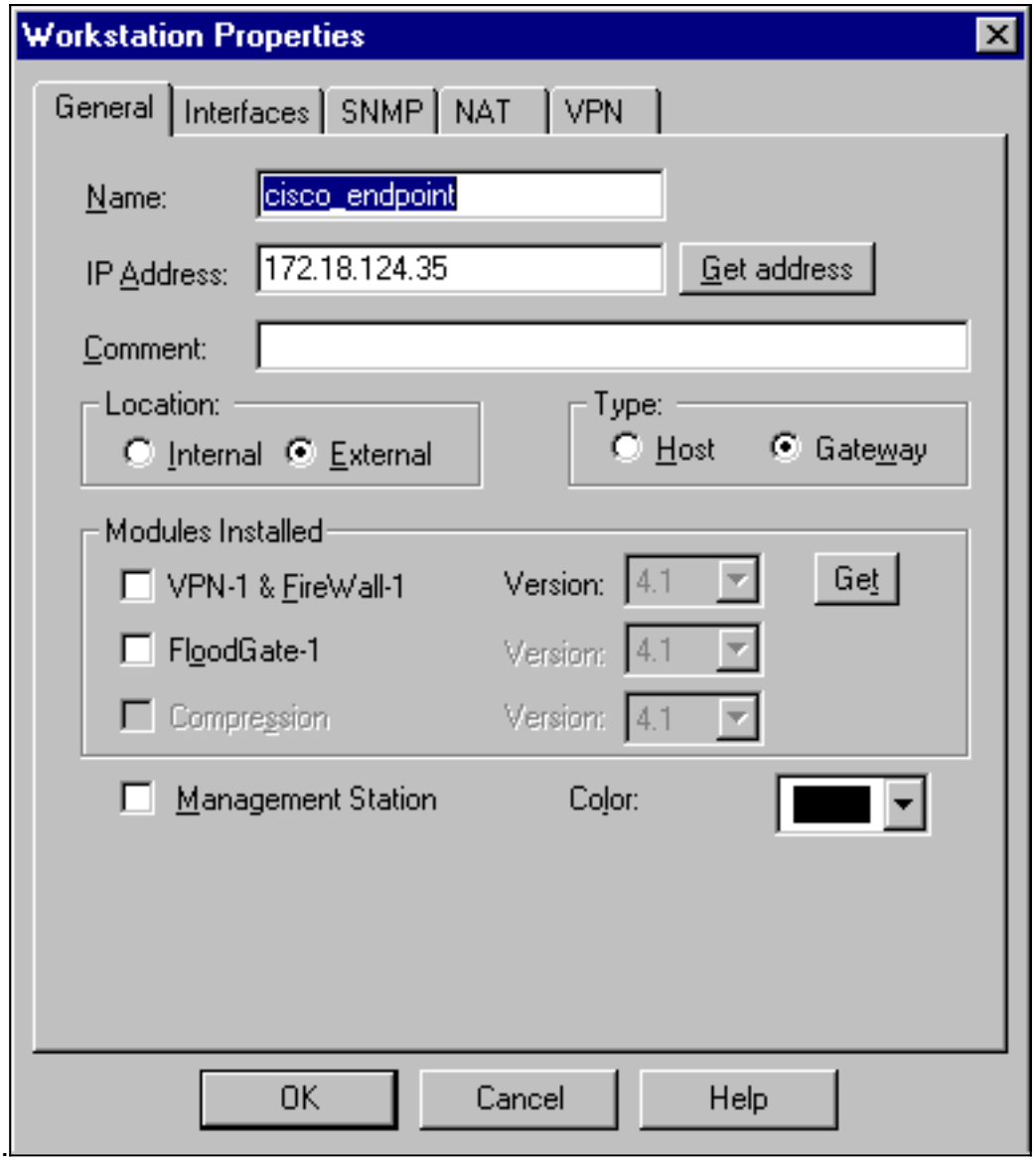
:

4. Choisi **gérez** > des **objets de réseau** > **nouveau** > **réseau** pour configurer l'objet pour (« inside_cisco ») le réseau externe derrière le PIX.Ceci doit être conforme au premier) réseau de source (dans cette commande PIX : **IP 192.168.1.0 255.255.255.0 10.32.50.0 255.255.255.0 d'autorisation de la liste d'accès**

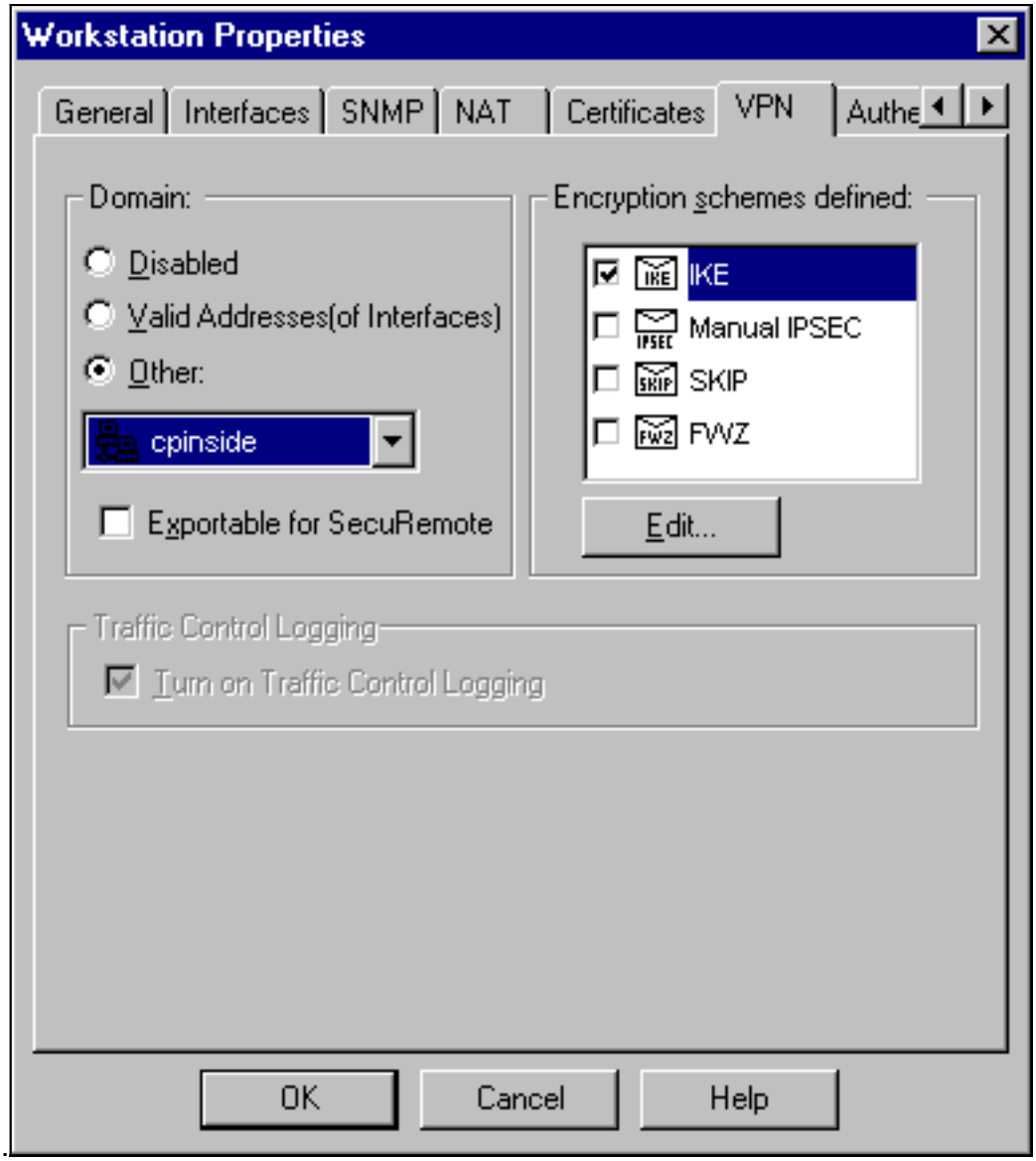


115

5. Choisi **gérez** > des **objets de réseau** > **nouveau** > **poste de travail** pour ajouter un objet pour (« cisco_endpoint ») la passerelle PIX externe. C'est l'interface PIX à laquelle cette commande est appliquée : **interface de nom de carte de chiffrement dehors**Sous l'emplacement, **externe** choisi. Pour le type, **passerelle** choisie.**Remarque:** Ne sélectionnez pas la case à cocher VPN-1/FireWall-

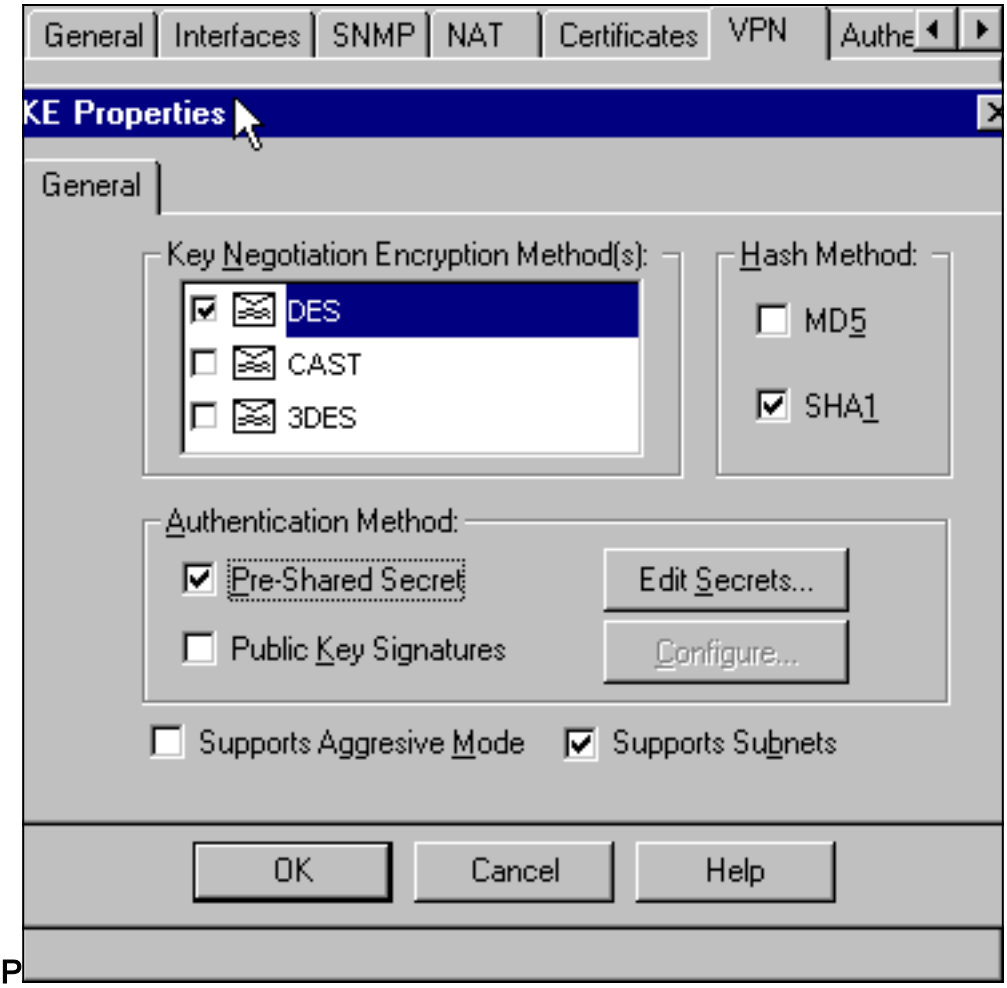
1. 

6. Choisi **gérez** > des **objets de réseau** > **éditent** pour éditer onglet VPN de point d'extrémité de passerelle avec point de contrôle (appelé le le « RTPCPVPN »). Sous le domaine, sélectionnez **autre** et puis sélectionnez l'intérieur du réseau de points de contrôle (appelé le « cpinside ») de la liste déroulante. Sous des structures de chiffrement définies, l'**IKE** choisi, et cliquent sur Edit



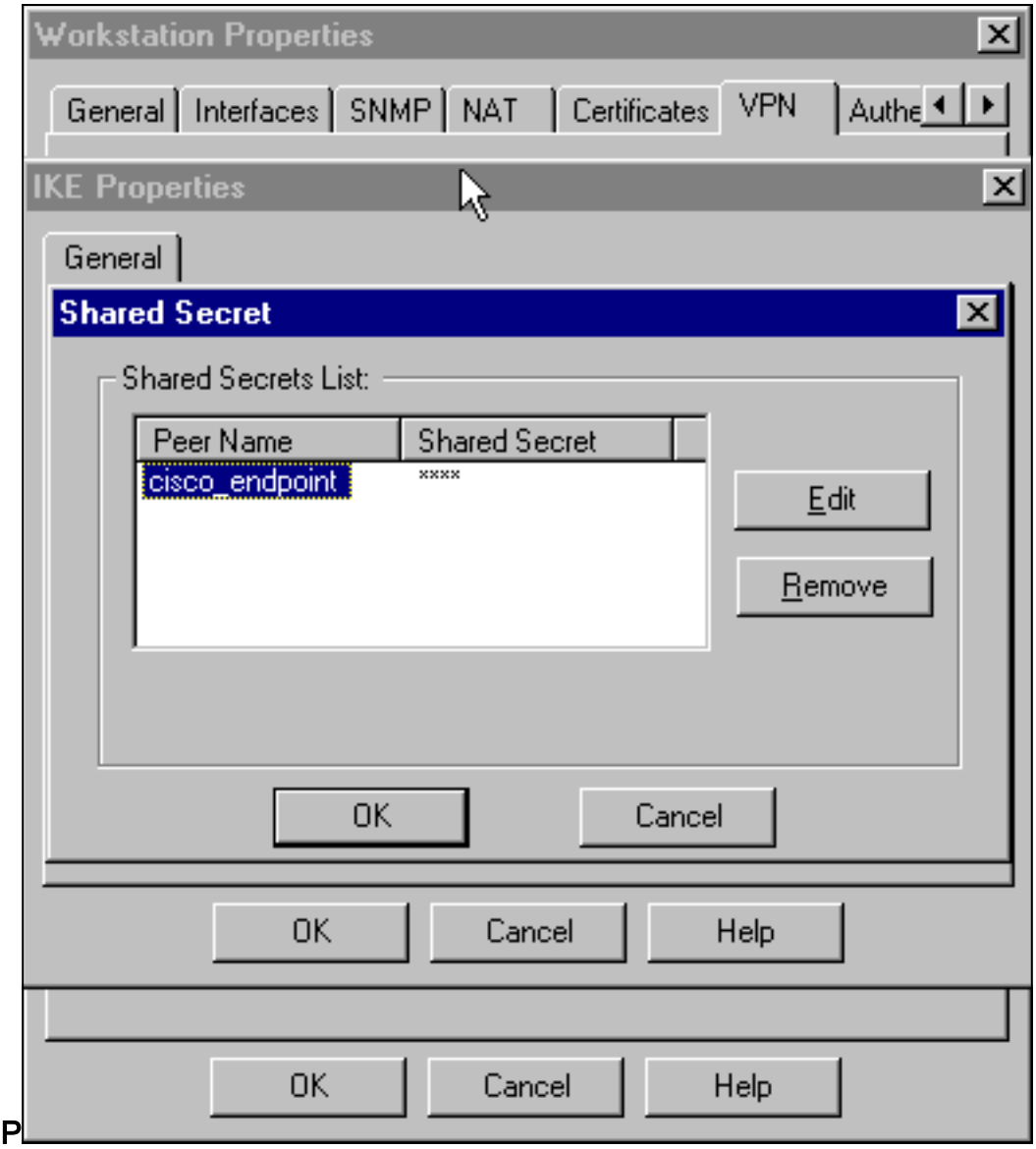
alors.

7. Changez les propriétés IKE pour le chiffrement DES pour être d'accord avec cette commande :**DES de stratégie # de cryptage d'ISAKMP**
8. Changez les propriétés IKE au hachage SHA1 pour être d'accord avec cette commande :**stratégie d'ISAKMP # SHA d'informations parasites**Changez ces configurations :Retirez le **mode agressif**.Sélectionnez la case à cocher de **sous-réseaux de supports**.Sous la méthode d'authentification, sélectionnez la case à cocher **secrète pré-partagée**. Ceci est conforme à cette commande :**stratégie # authentication pre-share**



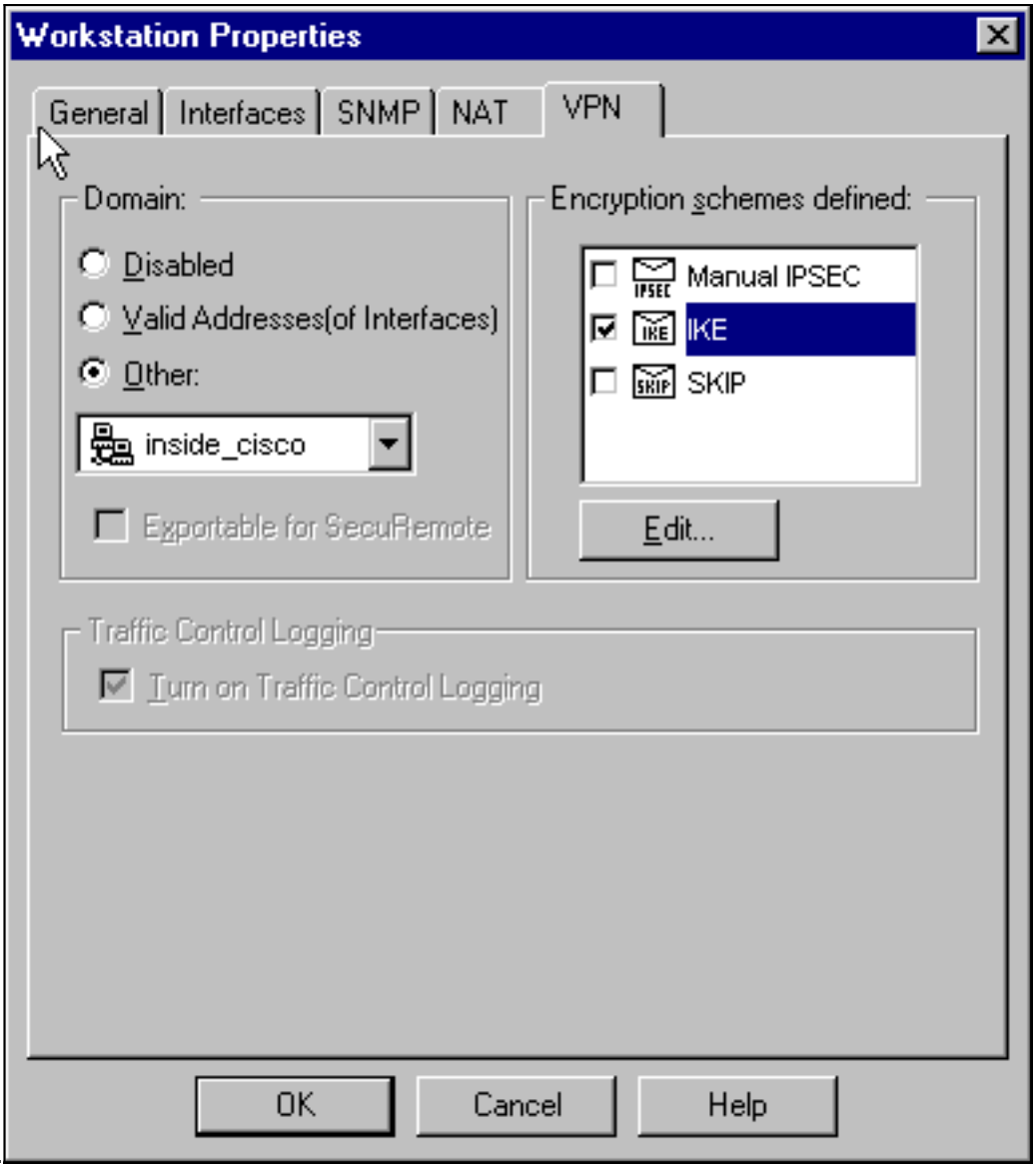
d'ISAKMP

9. Cliquez sur Edit les **secrets** pour placer la clé pré-partagée pour être d'accord avec la commande PIX :*netmask principal* **principal de netmask d'address address**



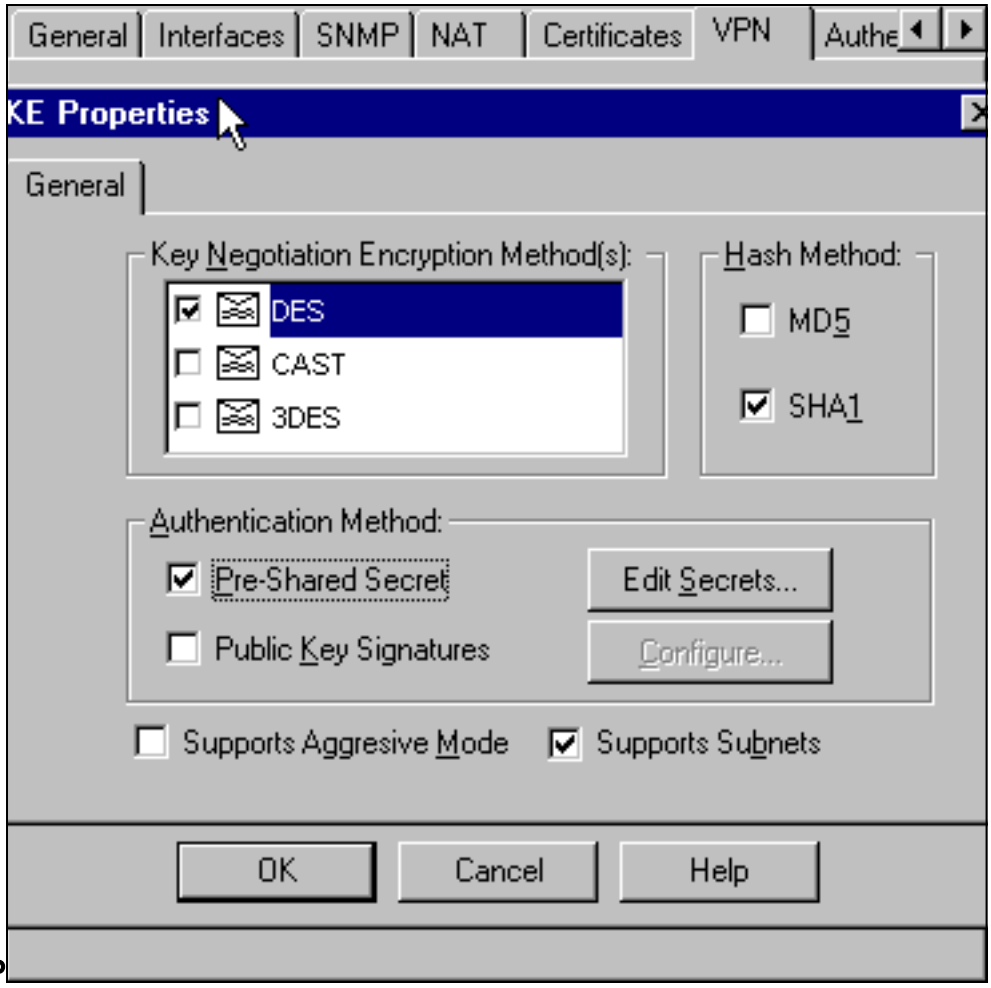
d'ISAKMP

10. Choisi **gérez** > des **objets de réseau** > **éditent** pour éditer l'onglet VPN de « cisco_endpoint ». Sous le domaine, sélectionnez **autre**, et puis sélectionnez l'intérieur du réseau PIX (appelé le « inside_cisco »). Sous des structures de chiffrement définies, l'**IKE** choisi, et cliquent sur Edit



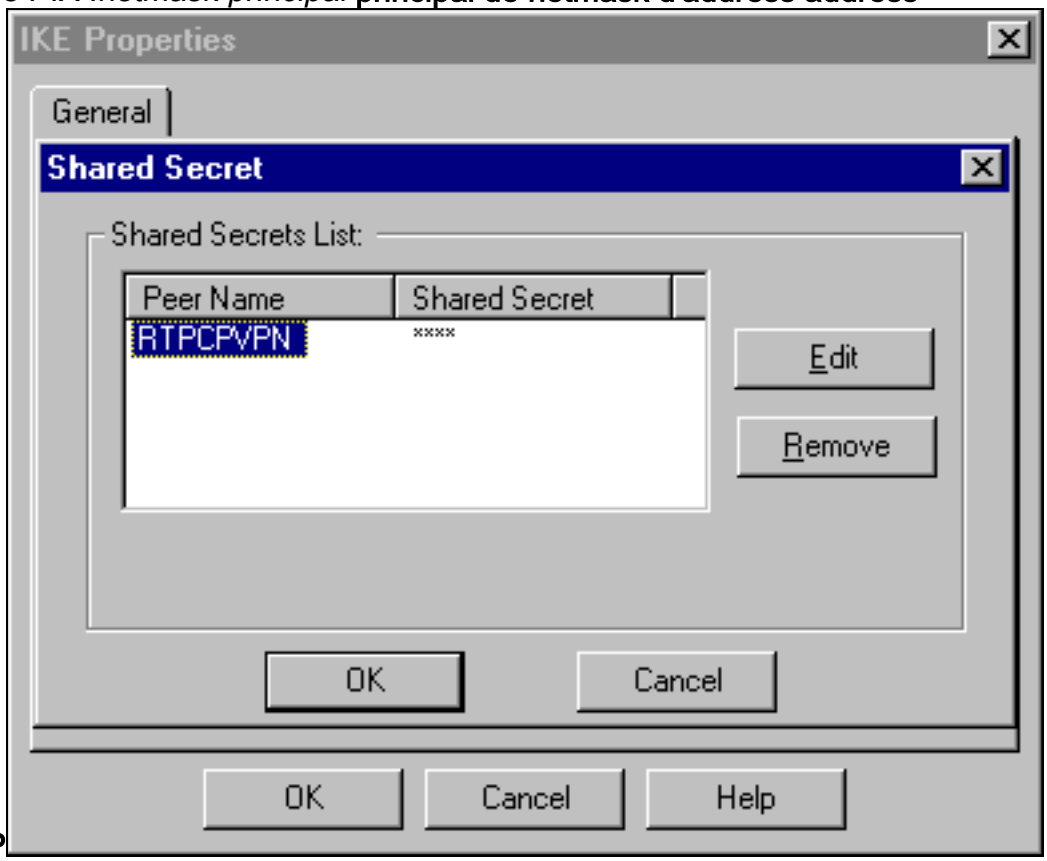
alors.

11. Changez le chiffrement DES de propriétés IKE pour être d'accord avec cette commande :**DES de stratégie # de cryptage d'ISAKMP**
12. Changez les propriétés IKE au hachage SHA1 pour être d'accord avec cette commande :**crypto isakmp policy # SHA d'informations parasites**Changez ces configurations :Retirez le **mode agressif**.Sélectionnez la case à cocher de **sous-réseaux de supports**.Sous la méthode d'authentification, sélectionnez la case à cocher **secrète pré-partagée**. Cette action est conforme à cette commande :**stratégie # authentication pre-share**



d'ISAKMP

13. Cliquez sur Edit les **secrets** pour placer la clé pré-partagée pour être d'accord avec cette commande PIX :*netmask principal* **principal de netmask d'address address**

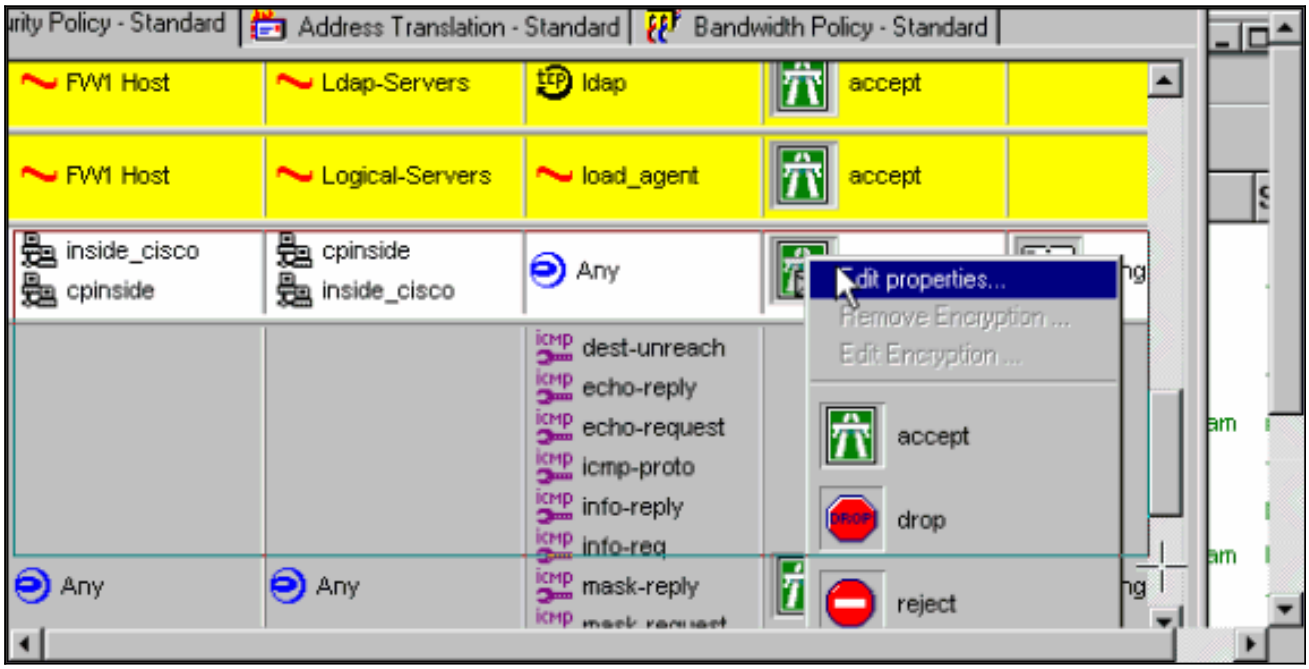


d'ISAKMP

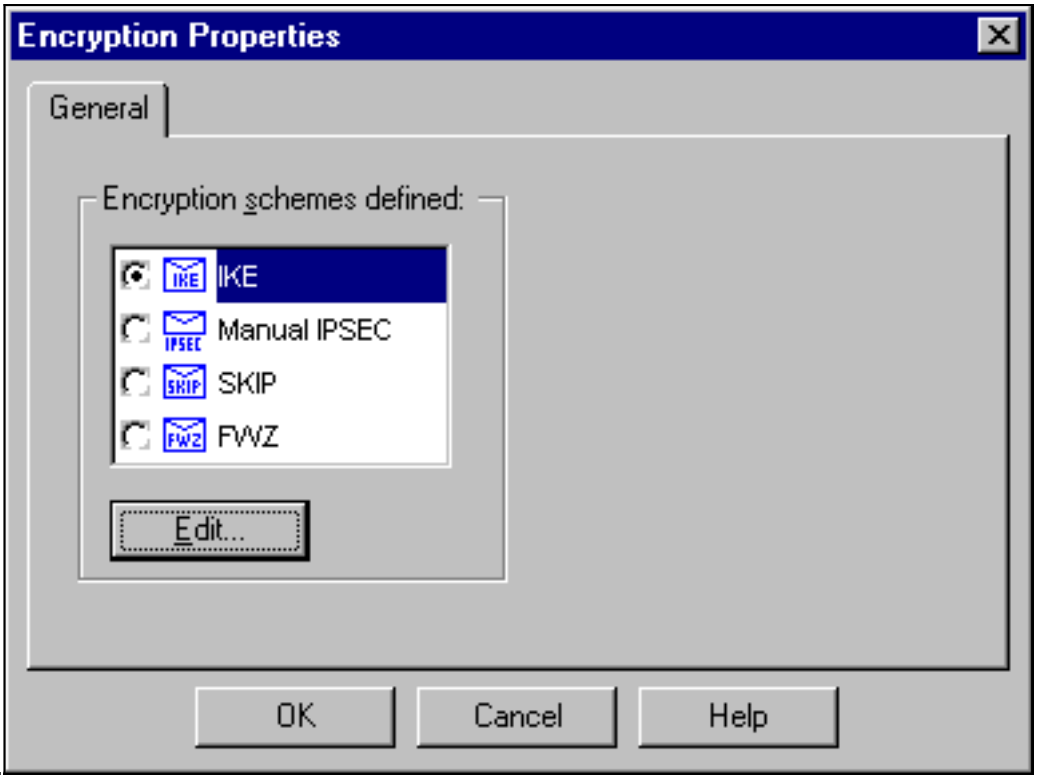
14. Dans la fenêtre de l'éditeur de stratégie, insérez une règle avec la source et la destination en tant que le « inside_cisco » et « cpinside » (bidirectionnel). Placez **Service=Any**, **Action=Encrypt**, et

Track=Long.

15. Sous le titre d'action, cliquez sur l'icône verte chiffrement et choisi **éditez les propriétés** pour configurer des stratégies de chiffrement.

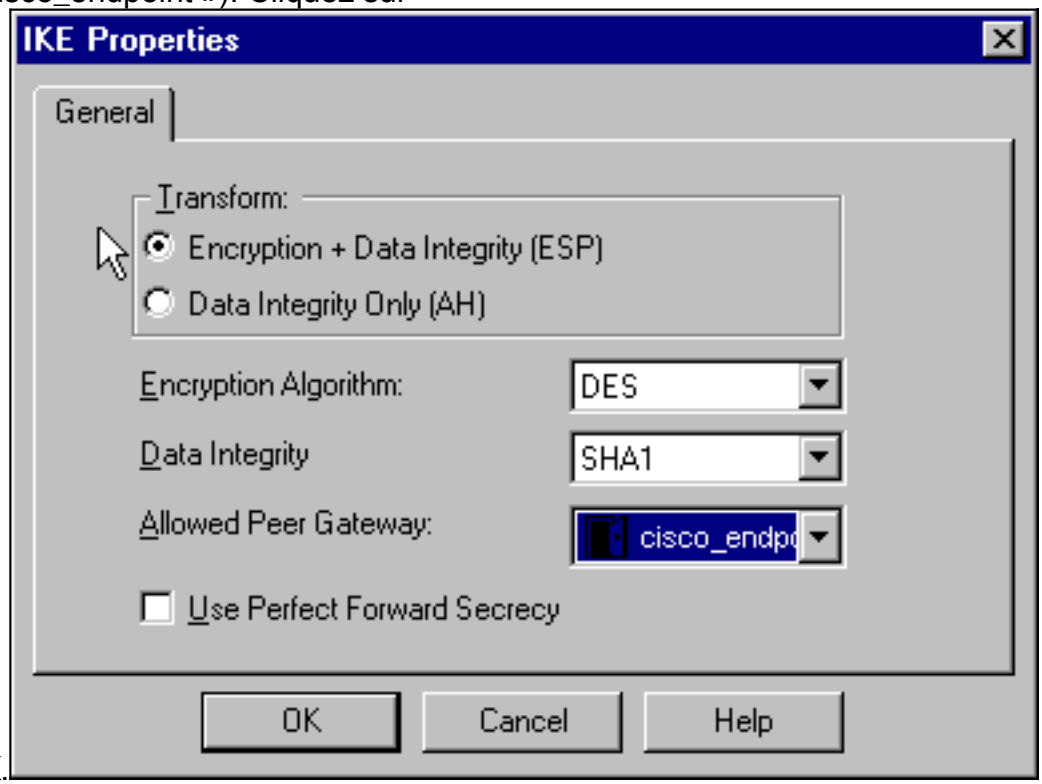


16. **L'IKE** choisi, et cliquent sur Edit



alors.

17. Sur les propriétés IKE examinez, changez ces propriétés pour être d'accord avec le PIX IPSec transforme dans cette commande :**ESP-SHA-hmac ESP-DES de myset de crypto ipsec transform-set**Sous transformez, **cryptage + intégrité des données** choisis **(ESP)**. L'algorithme de chiffrement doit être **DES**, intégrité des données doit être **SHA1**, et la passerelle homologue permise doit être la passerelle PIX externe (appelée le « cisco_endpoint »). Cliquez sur



OK.

18. Après que le point de reprise soit configuré, la **stratégie** choisie **> installent** sur le menu du point de contrôle pour que les modifications les prennent effet.

mettez au point, exposition et commandes claires

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

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.

Avant d'émettre des commandes **debug**, reportez-vous aux Informations importantes sur les commandes de débogage.

Pare-feu Cisco PIX

- **debug crypto engine** — Affichez les messages de débogage au sujet des moteurs de chiffrement, qui exécutent le cryptage et le déchiffrement.
- **debug crypto isakmp** — Messages d'affichage au sujet des événements d'IKE.
- **debug crypto ipsec** — Événements d'IPSec d'affichage.
- **show crypto isakmp sa** — Visualisez toutes les associations de sécurité en cours d'IKE (SAS) à un pair.
- **show crypto ipsec sa** — Visualisez les configurations utilisées par les associations de sécurité en cours.
- **clear crypto isakmp SA** — (du mode de configuration) effacez toutes les connexions actives d'IKE.
- **clear crypto ipsec sa** — (du mode de configuration) supprimez toutes les associations de sécurité d'IPSec.

Point de reprise :

Puisque le cheminement a été placé pour long dans la fenêtre de l'éditeur de stratégie affichée dans l'étape 14, refusée le trafic apparaît en rouge dans le visualiseur de log. Un plus bavard mettent au point peut être obtenu en entrant :

```
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: C'était une installation de NT de Microsoft Windows.

Vous pouvez effacer SAS sur le point de reprise avec ces commandes :

```
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
```

et répondant **oui au** êtes-vous sure ? demande.

Dépannez

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

Récapitulation de réseau

Quand des réseaux intérieurs adjacents de multiple sont configurés dans le domaine de cryptage sur le point de reprise, le périphérique peut automatiquement les récapituler en ce qui concerne le trafic intéressant. Si le crypto ACL sur le PIX n'est pas configuré pour s'assortir, le tunnel échoue vraisemblablement. Par exemple, si les réseaux intérieurs de 10.0.0.0 /24 et de 10.0.1.0 /24 sont configurés pour être inclus dans le tunnel, ils peuvent être récapitulés à 10.0.0.0 /23.

Exemple de sortie de débogage du PIX

```
cisco_endpoint# show debug debug crypto ipsec 1 debug crypto isakmp 1 debug crypto engine debug
fover status tx Off rx Off open Off cable Off txdmp Off rxdmp Off ifc Off rxip Off txip Off get
Off put Off verify Off switch Off fail Off fmsg Off cisco_endpoint# term mon cisco_endpoint#
ISAKMP (0): beginning Quick Mode exchange, M-ID of 2112882468:7df00724IPSEC(key_engine): got a
queue event... IPSEC(spi_response): getting spi 0x9d71f29c(2641490588) for SA from
172.18.124.157 to 172.18.124.35 for prot 3 70 crypto_isakmp_process_block: src 172.18.124.157,
dest 172.18.124.35 OAK_QM exchange oakley_process_quick_mode: OAK_QM_IDLE ISAKMP (0): processing
SA payload. message ID = 2112882468 ISAKMP : Checking IPSec proposal 1 ISAKMP: transform 1,
ESP_DES ISAKMP: attributes in transform: ISAKMP: encaps is 1 ISAKMP: SA life type in seconds
ISAKMP: SA life duration (basic) of 28800 ISAKMP: SA life type in kilobytes ISAKMP: SA life
duration (VPI) of 0x0 0x46 0x50 0x0 ISAKMP: authenticator is HMAC-SHA ISAKMP (0): atts are
acceptable.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 ISAKMP (0):
processing NONCE payload. message ID = 2112882468 ISAKMP (0): processing ID payload. message ID
= 2112882468 ISAKMP (0): processing ID payload. message ID = 2112882468map_alloc_entry:
allocating entry 3 map_alloc_entry: allocating entry 4 ISAKMP (0): Creating IPSec SAs inbound SA
from 172.18.124.157 to 172.18.124.35 (proxy 10.32.50.0 to 192.168.1.0) has spi 2641490588 and
conn_id 3 and flags 4 lifetime of 28800 seconds lifetime of 4608000 kilobytes outbound SA from
172.18.124.35 to 172.18.124.157 (proxy 192.168.1.0 to 10.32.50.0) has spi 3955804195 and conn_id
4 and flags 4 lifetime of 28800 seconds lifetime of 4608000 kilobytesIPSEC(key_engine): got a
queue event... 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=
28800s and 4608000kb, spi= 0x9d71f29c(2641490588), conn_id= 3, keysize= 0, flags= 0x4
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= 28800s and 4608000kb, spi=
0xebc8c823(3955804195), conn_id= 4, keysize= 0, flags= 0x4 return status is IKMP_NO_ERROR2303:
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= 28800s and 4608000kb, spi= 0x0(0),
conn_id= 0, keysize= 0, flags= 0x4004 602301: sa created, (sa) sa_dest= 172.18.124.35, sa_prot=
50, sa_spi= 0x9d71f29c(2641490588), sa_trans= esp-des esp-sha-hmac , sa_conn_id= 3 602301: sa
created, (sa) sa_dest= 172.18.124.157, sa_prot= 50, sa_spi= 0xebc8c823(3955804195), sa_trans=
esp-des esp-sha-hmac , sa_conn_id= 4 cisco_endpoint# sho cry ips sa interface: outside Crypto
map tag: rtpmap, 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): (0.0.0.0/0.0.0.0/0/0)
current_peer: 172.18.124.157 PERMIT, flags={origin_is_acl,} #pkts encaps: 0, #pkts encrypt: 0,
#pkts digest 0 #pkts decaps: 0, #pkts decrypt: 0, #pkts verify 0 #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.: 172.18.124.35, remote crypto endpt.:
172.18.124.157 path mtu 1500, ipsec overhead 0, media mtu 1500 current outbound spi: 0 inbound
esp sas: inbound ah sas: inbound pcp sas: outbound esp sas: outbound ah sas: outbound pcp sas:
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: 4, #pkts encrypt: 4, #pkts digest 4 #pkts decaps: 4, #pkts
decrypt: 4, #pkts verify 4 #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, ipsec overhead 56,
media mtu 1500 current outbound spi: ebc8c823 inbound esp sas: spi: 0x9d71f29c(2641490588)
transform: esp-des esp-sha-hmac , in use settings ={Tunnel, } slot: 0, conn id: 3, crypto map:
```

```
rtpmap sa timing: remaining key lifetime (k/sec): (4607999/28777) IV size: 8 bytes replay
detection support: Y inbound ah sas: inbound pcp sas: outbound esp sas: spi:
0xebc8c823(3955804195) transform: esp-des esp-sha-hmac , in use settings ={Tunnel, } slot: 0,
conn id: 4, crypto map: rtpmap sa timing: remaining key lifetime (k/sec): (4607999/28777) IV
size: 8 bytes replay detection support: Y outbound ah sas: outbound pcp sas: cisco_endpoint# sho
cry is sa dst src state pending created 172.18.124.157 172.18.124.35 QM_IDLE 0 2
```

Informations connexes

- Page de support PIX
- Référence des commandes PIX
- Demandes de commentaires (RFC)
- Sécurité des réseaux de configuration d'IPSec
- Configurer le protocole de sécurité IKE
- PIX 5.2 : Configuration d'IPSec
- PIX 5.3 : Configuration d'IPSec
- Page d'assistance IPsec
- Support technique - Cisco Systems