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

Contenu

Introduction
Conditions préalables
Conditions requises
Components Used
Conventions
Configuration
Diagramme du réseau
Configurations
Pare-feu Checkpoint
Commandes debug, show et clear
Pare-feu Cisco PIX
Point de contrôle :
Dépannage
Récapitulation de réseau
Exemple de sortie de débogage du PIX
Informations connexes

Introduction

Cet exemple de configuration montre comment former un tunnel IPSec avec des clés pré-partagées pour rejoindre deux réseaux privés. Dans notre exemple, les réseaux joints sont le réseau privé 192.168.1.X à l'intérieur du pare-feu Cisco Secure Pix Firewall (PIX) et le réseau privé 10.32.50.X à l'intérieur du Checkpoint. Il est supposé que le trafic de l'intérieur du PIX et de l'intérieur du Pare-feu Checkpoint 4.1 vers 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.

Components Used

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

- Logiciel PIX version 5.3.1
- 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.

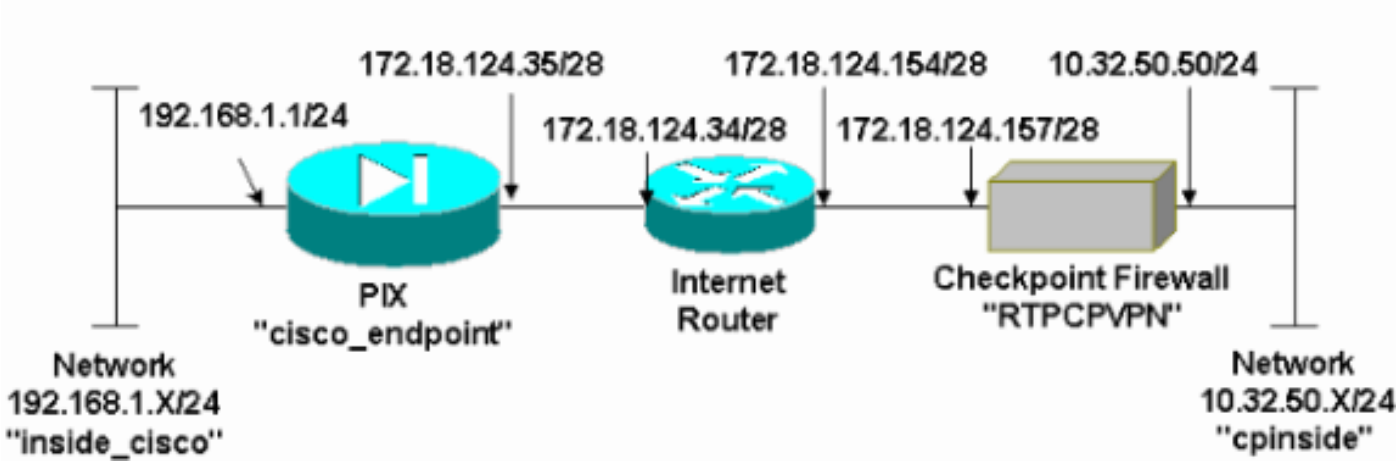
Configuration

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

Remarque : Pour en savoir plus sur les commandes utilisées dans le présent document, utilisez l'outil de recherche de commandes (clients inscrits seulement).

Diagramme du réseau

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



Configurations

Ce document utilise les configurations indiquées dans cette section.

Configuration PIX

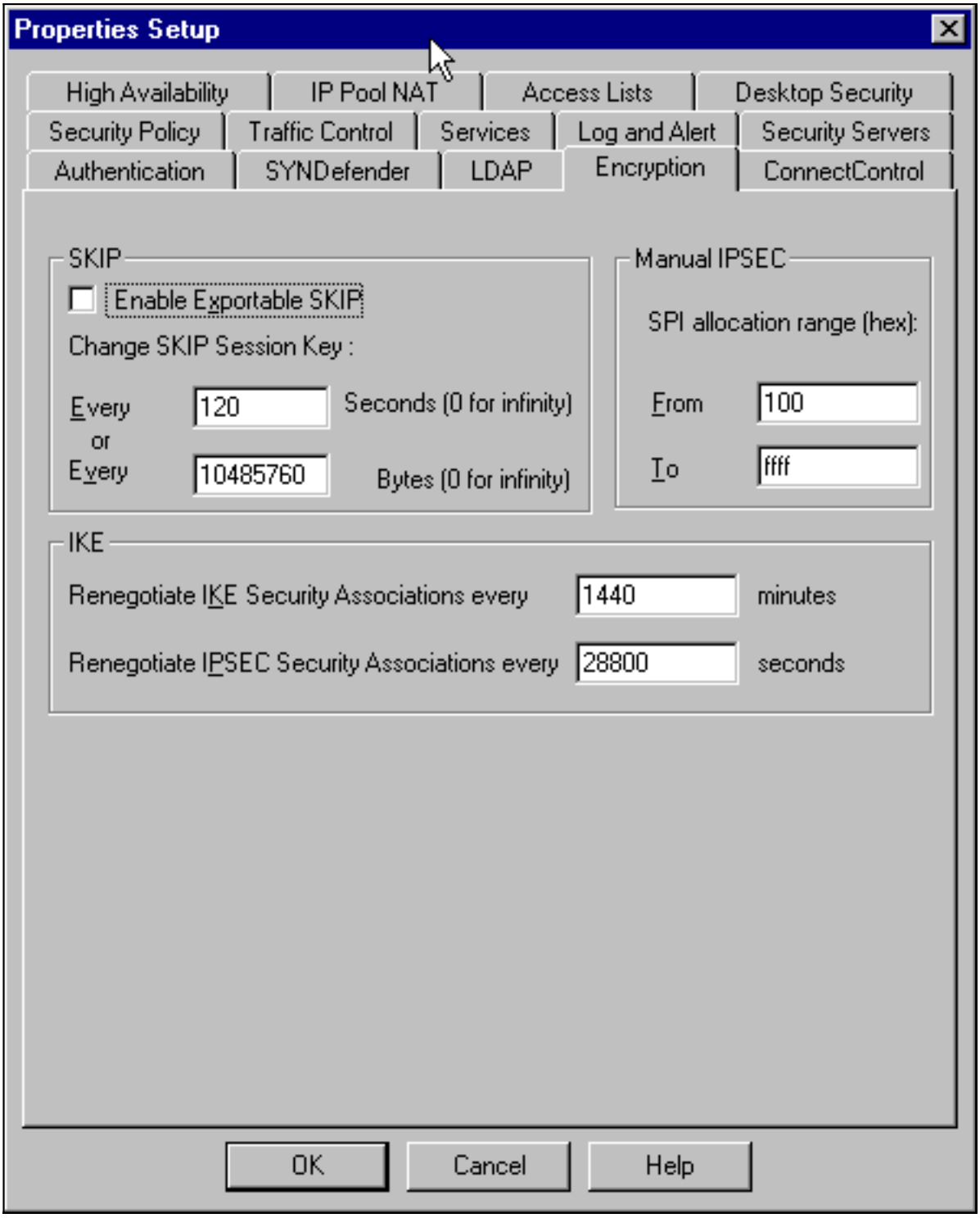
```
PIX Version 5.3(1)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname cisco_endpoint
```

```
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
```

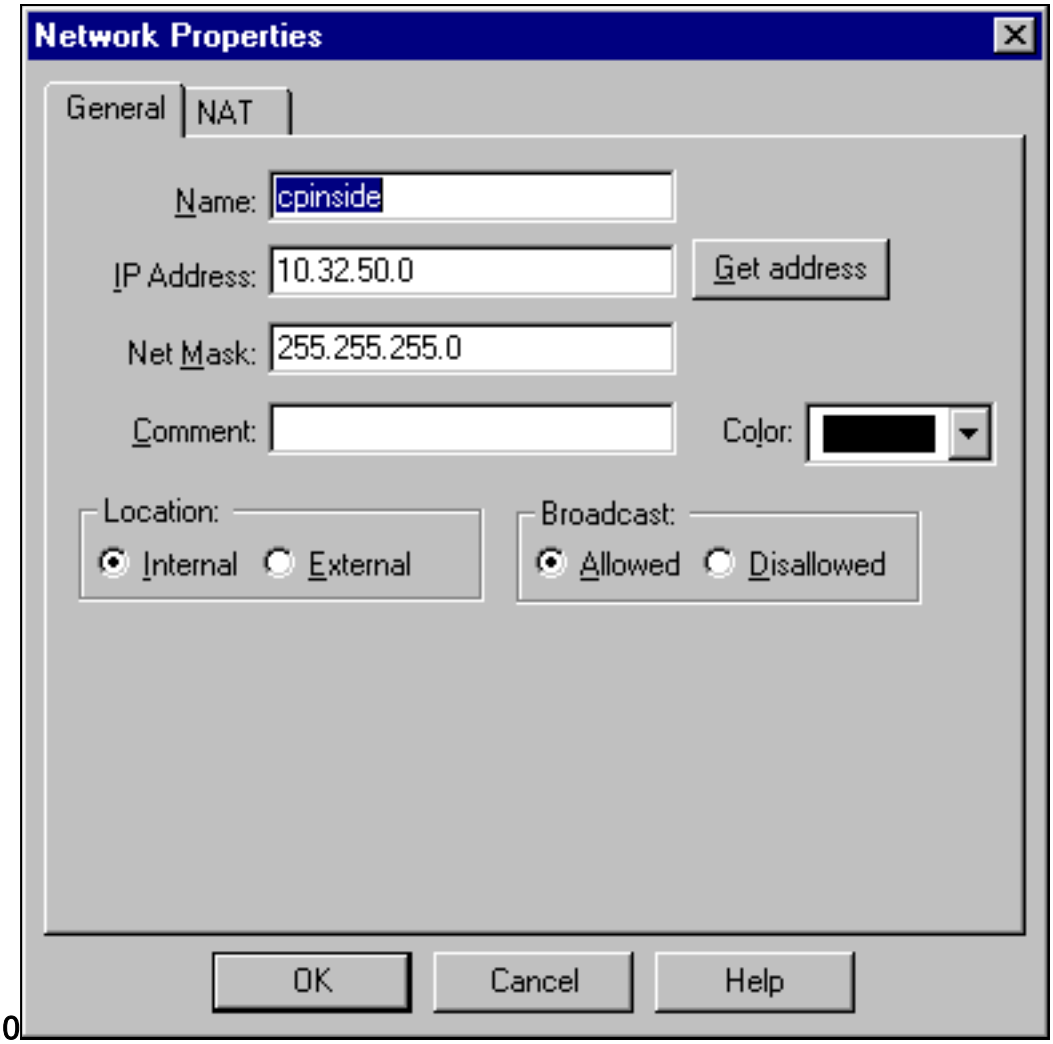
```
isakmp key ******** address 172.18.124.157 netmask
255.255.255.240
isakmp identity address
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption des
isakmp policy 10 hash sha
isakmp policy 10 group 1
isakmp policy 10 lifetime 86400
telnet timeout 5
ssh timeout 5
terminal width 80
Cryptochecksum:dc43c44e4513d3633a3fc7b1c3802c79
: end
[OK]
```

Pare-feu Checkpoint

1. 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 PIX par défaut.La durée de vie IKE par défaut du PIX est de 86 400 secondes (=1 440 minutes), modifiable par cette commande : **isakmp policy # life 86400**La durée de vie de PIX IKE peut être configurée entre 60 et 86 400 secondes.La durée de vie IPSec par défaut de PIX est de 28 800 secondes, modifiable par cette commande : **crypto ipsec security-association life seconds #**Vous pouvez configurer une durée de vie IPSec PIX comprise entre 120 et 86 400
   secondes.

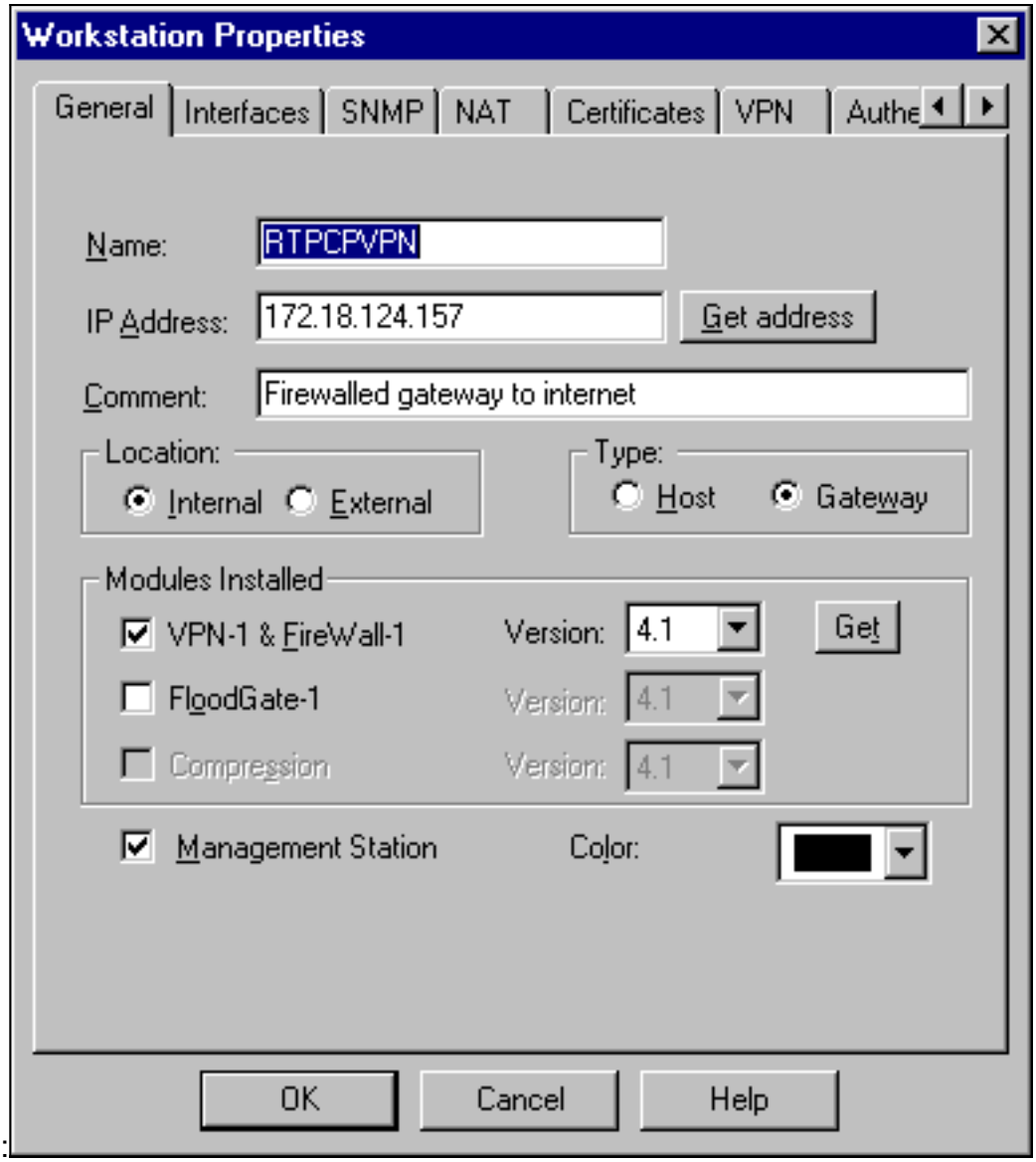


2. Sélectionnez **Gérer > Objets réseau > Nouveau (ou Modifier) > Réseau** pour configurer l'objet pour le réseau interne (« cpinside ») derrière le point de contrôle.Ceci doit être en accord avec le réseau de destination (deuxième) dans cette commande PIX : **access-list 115 permit ip 192.168.1.0 255.255.255.0 10.32.50.0**



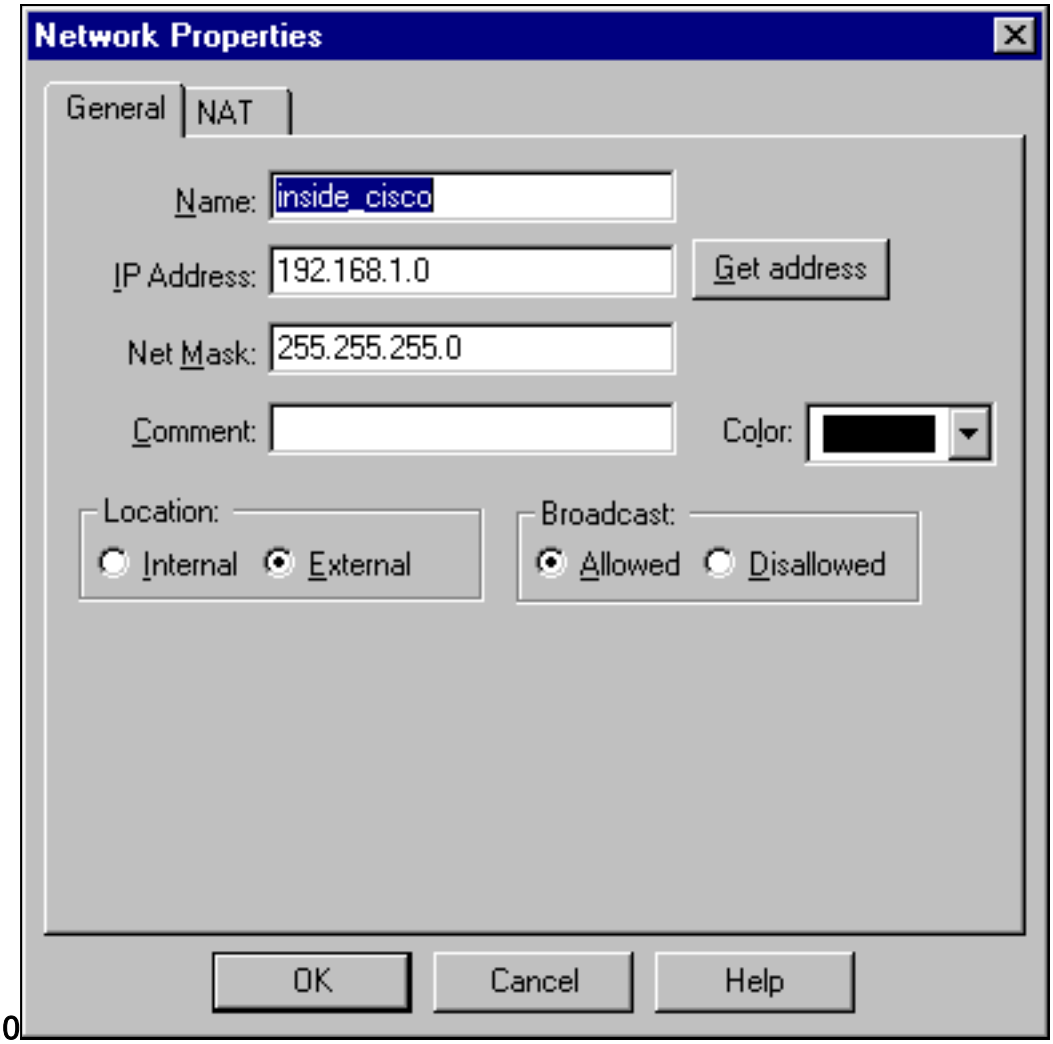
255.255.255.0

3. Sélectionnez **Manage > Network Objects > Edit** pour modifier l'objet du point de terminaison de passerelle (« RTPCPVPN » Checkpoint) auquel le PIX pointe dans cette commande : **crypto map name # set peer ip_address**Sous Emplacement, sélectionnez **Interne**. 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**



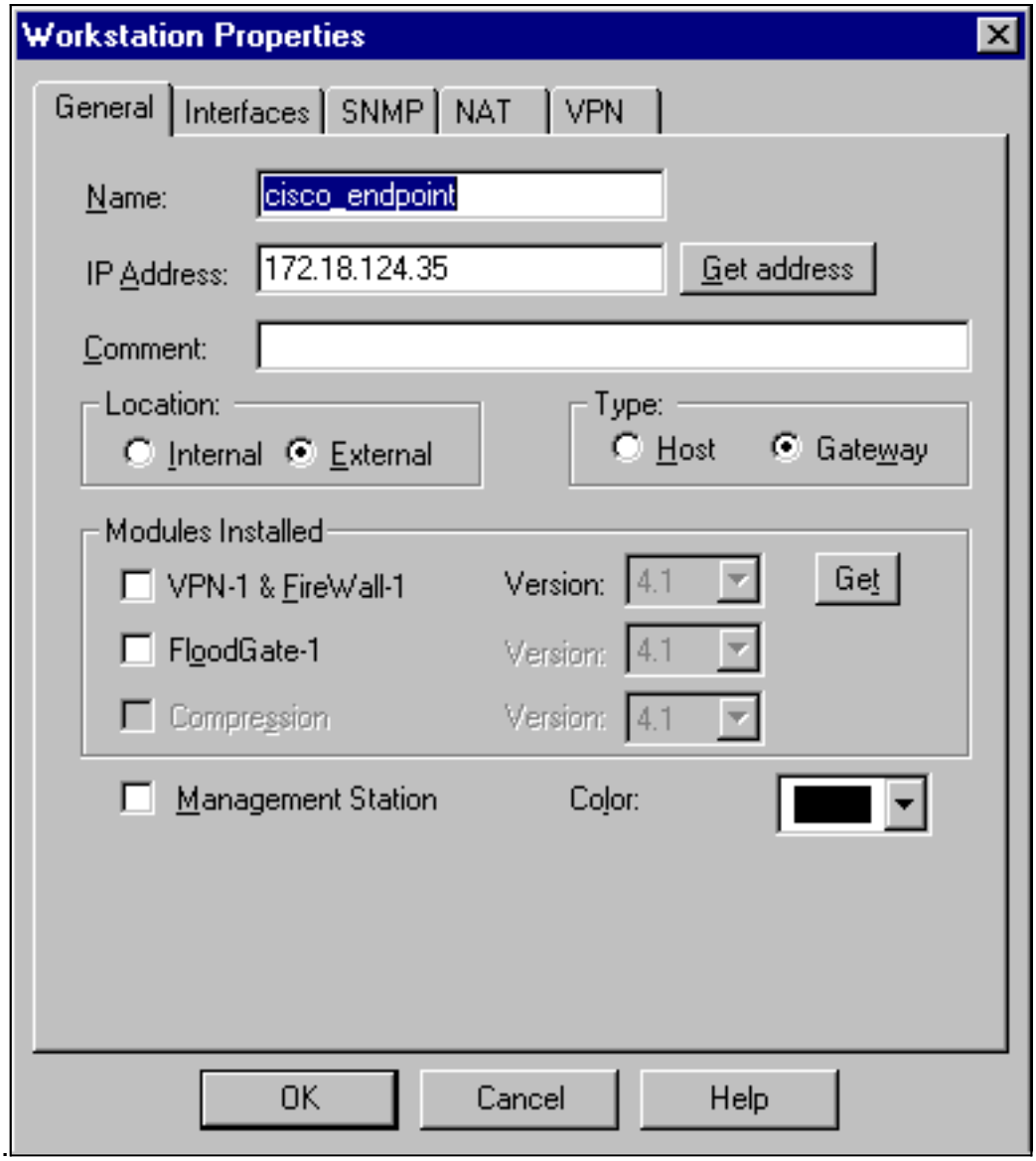
:

4. Sélectionnez **Manage > Network Objects > New > Network** pour configurer l'objet pour le réseau externe (« inside_cisco ») derrière le PIX.Ceci doit être en accord avec le réseau source (premier) dans cette commande PIX : **access-list 115 permit ip 192.168.1.0 255.255.255.0 10.32.50.0**



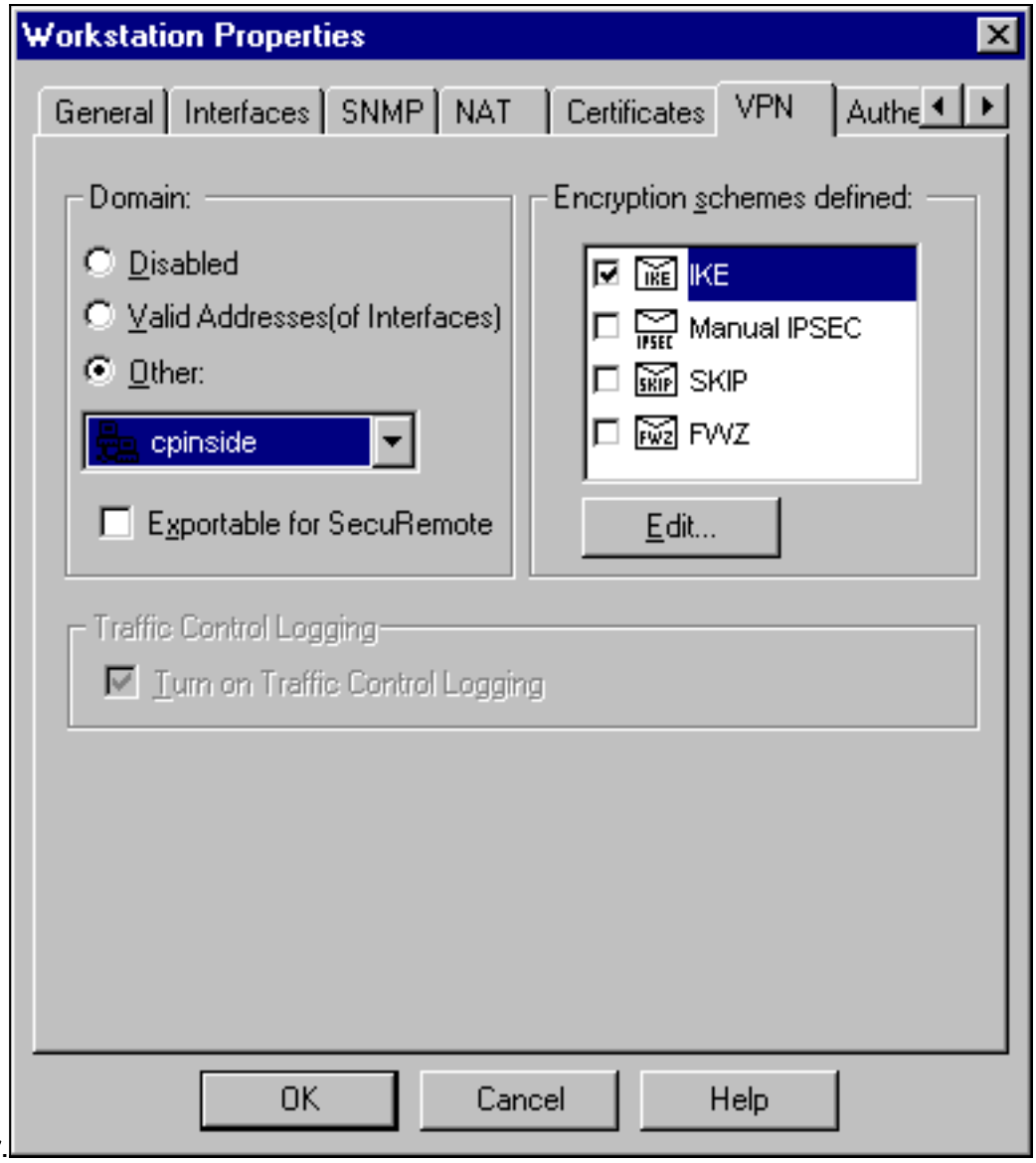
255.255.255.0

5. Sélectionnez **Manage > Network Objects > New > Workstation** pour ajouter un objet pour la passerelle PIX externe (« cisco_endpoint »). Il s'agit de l'interface PIX à laquelle cette commande est appliquée : **interface de *nom de* crypto-carte**Sous Emplacement, sélectionnez **Externe**. Pour Type, sélectionnez **Passerelle**.**Remarque :** Ne cochez pas la case VPN-



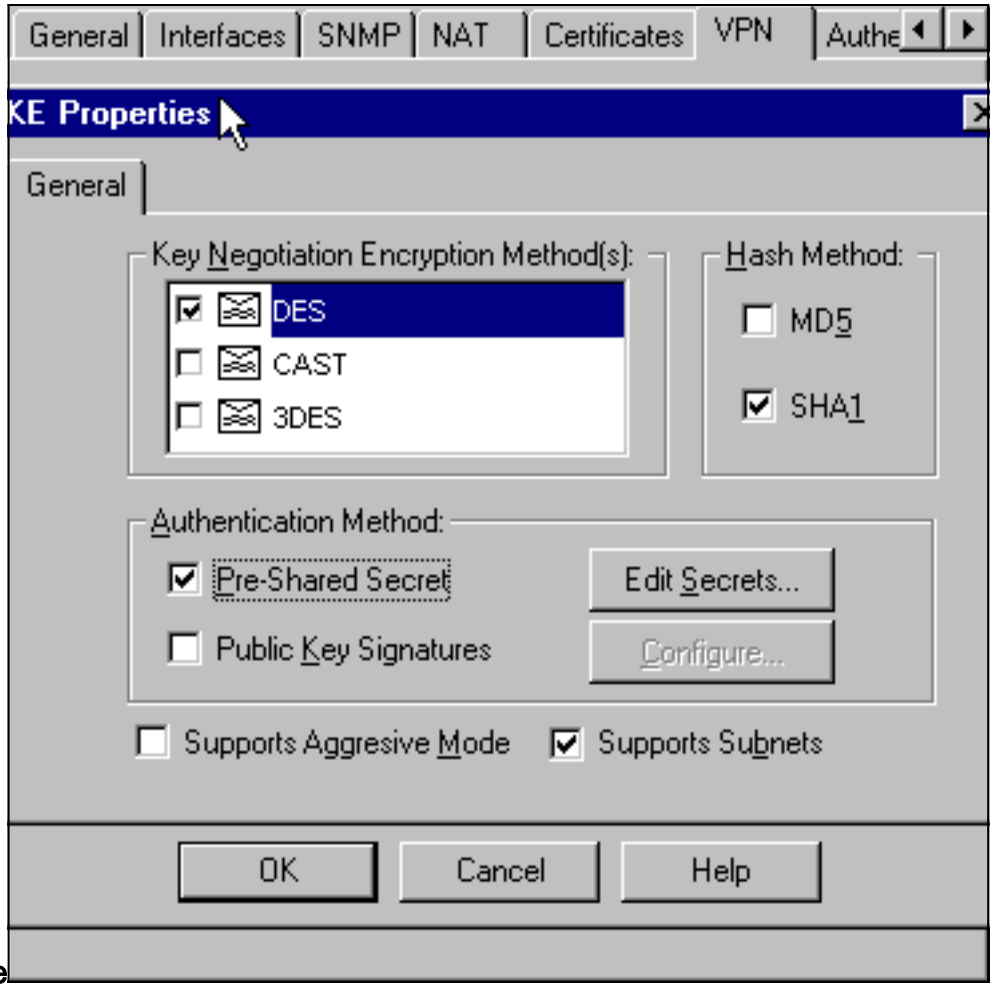
1/FireWall-1.

6. Sélectionnez **Manage > Network Objects > Edit** 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



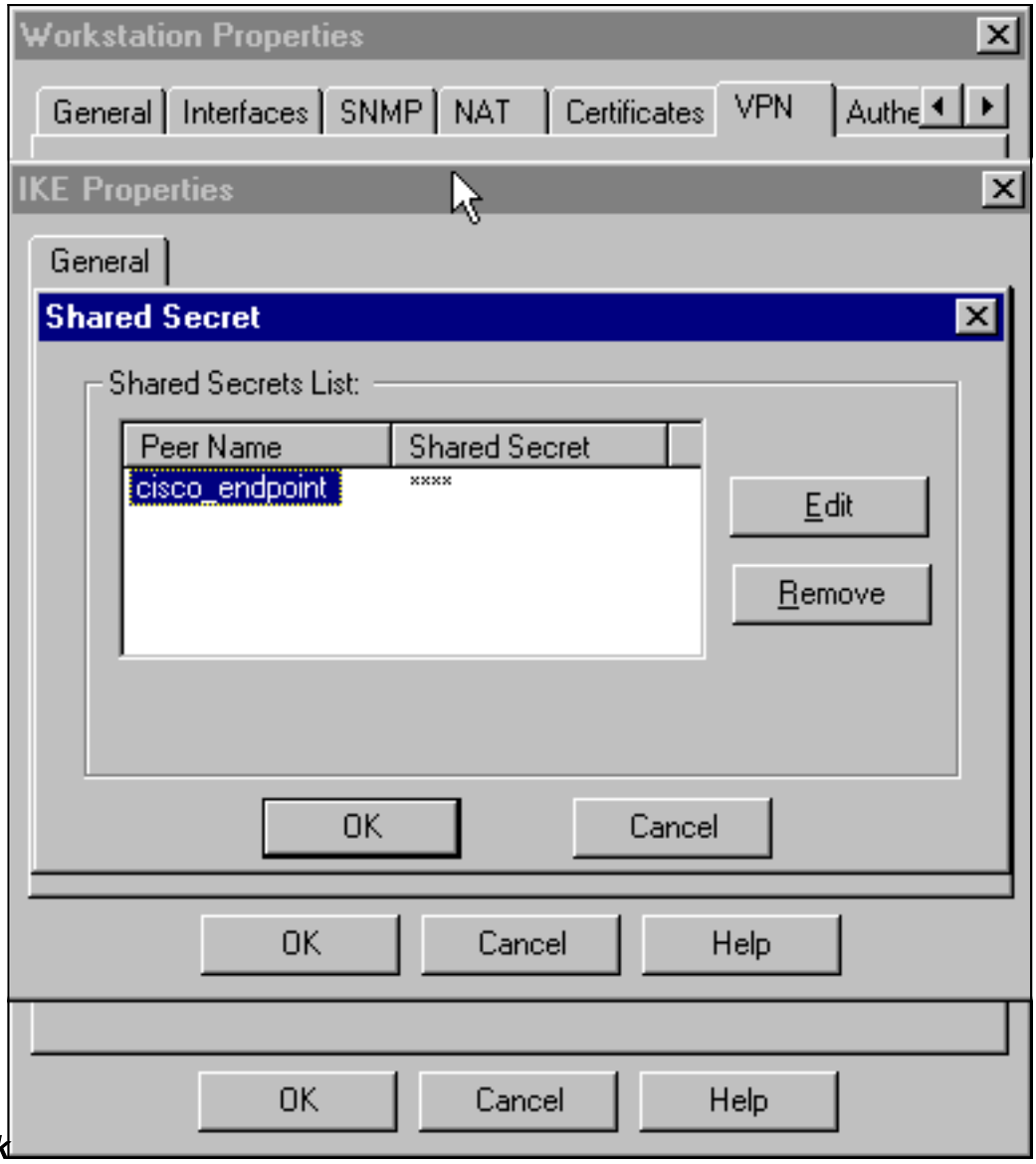
Modifier.

7. Modifiez les propriétés IKE pour le chiffrement DES pour qu'elles soient compatibles avec cette commande :**isakmp policy # encryption des**
8. Remplacez les propriétés IKE par le hachage SHA1 pour accepter cette commande :**isakmp policy # hash sha**Modifiez ces paramètres :Désélectionnez **Mode agressif**.Cochez la case **Supports Subnets**.Sous Authentication Method, activez la case à cocher **Pre-Shared Secret**. Ceci est d'accord avec cette commande :**isakmp policy # authentication pre-**



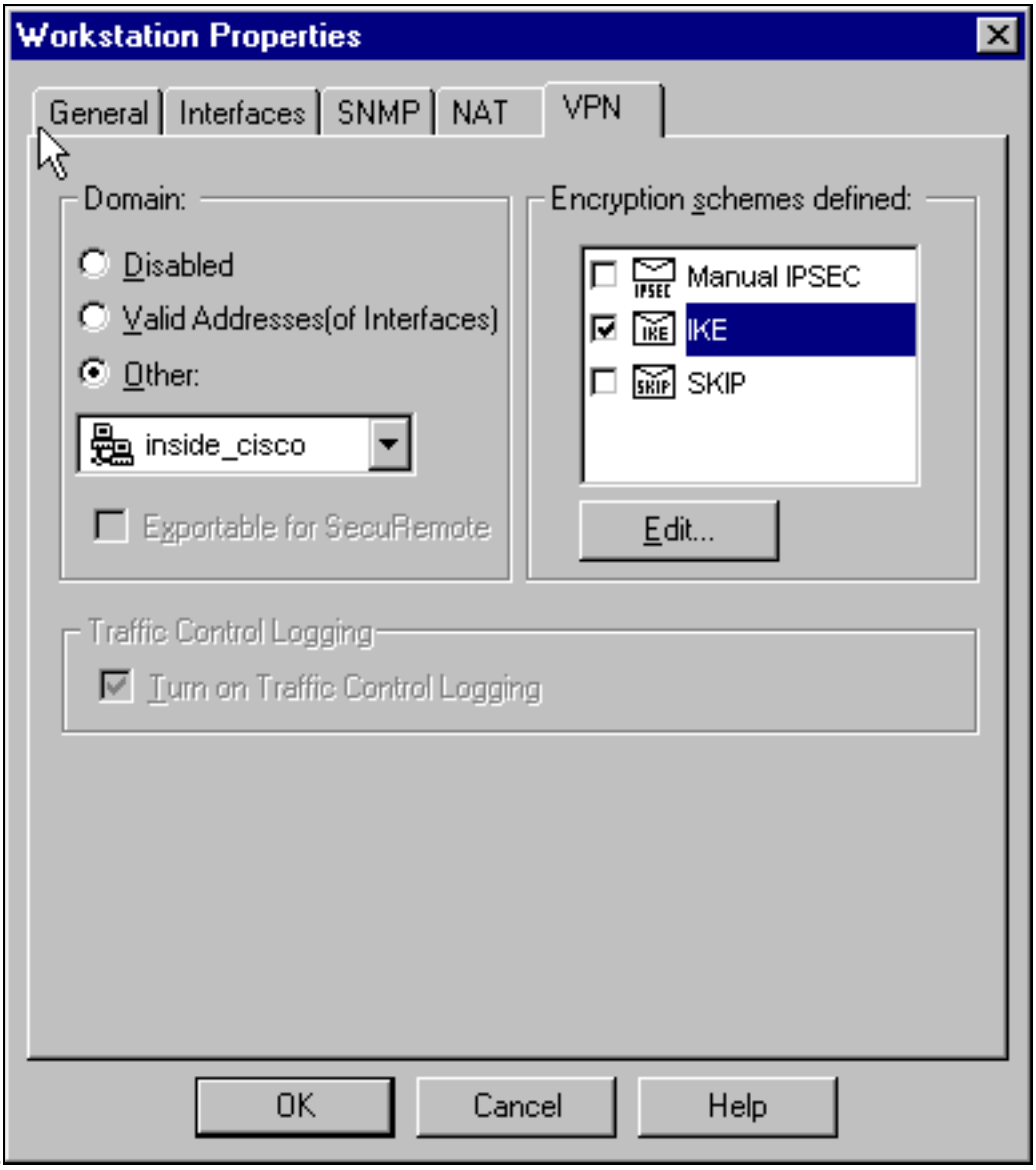
share

9. Cliquez sur **Modifier les secrets** pour définir la clé pré-partagée de manière à accepter la commande PIX :**isakmp key key** ***key*** **address** ***address*** **netmask**



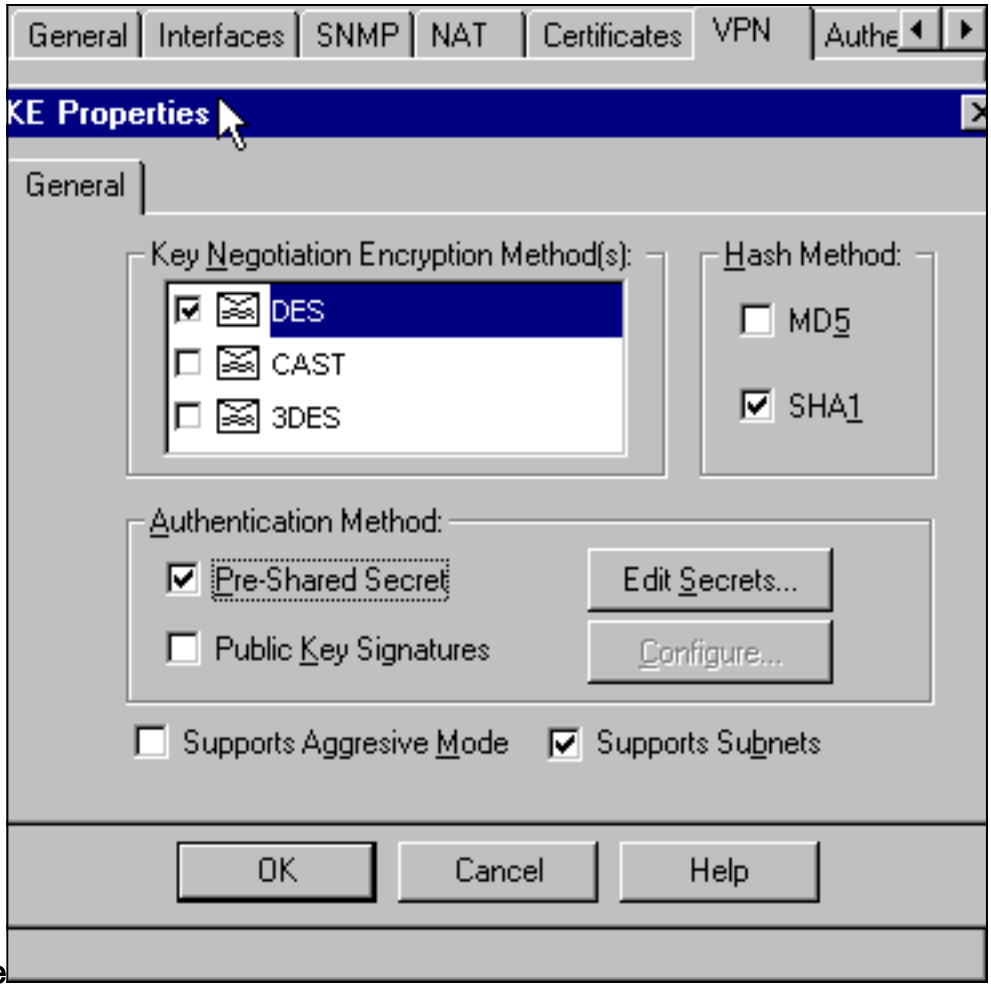
netmask

10. Sélectionnez **Manage > Network Objects > Edit** pour modifier l'onglet VPN « cisco_endpoint ». Sous Domaine, sélectionnez **Autre**, puis sélectionnez l'intérieur du réseau PIX (appelé « inside_cisco »). Sous Schémas de chiffrement définis, sélectionnez **IKE**, puis cliquez sur



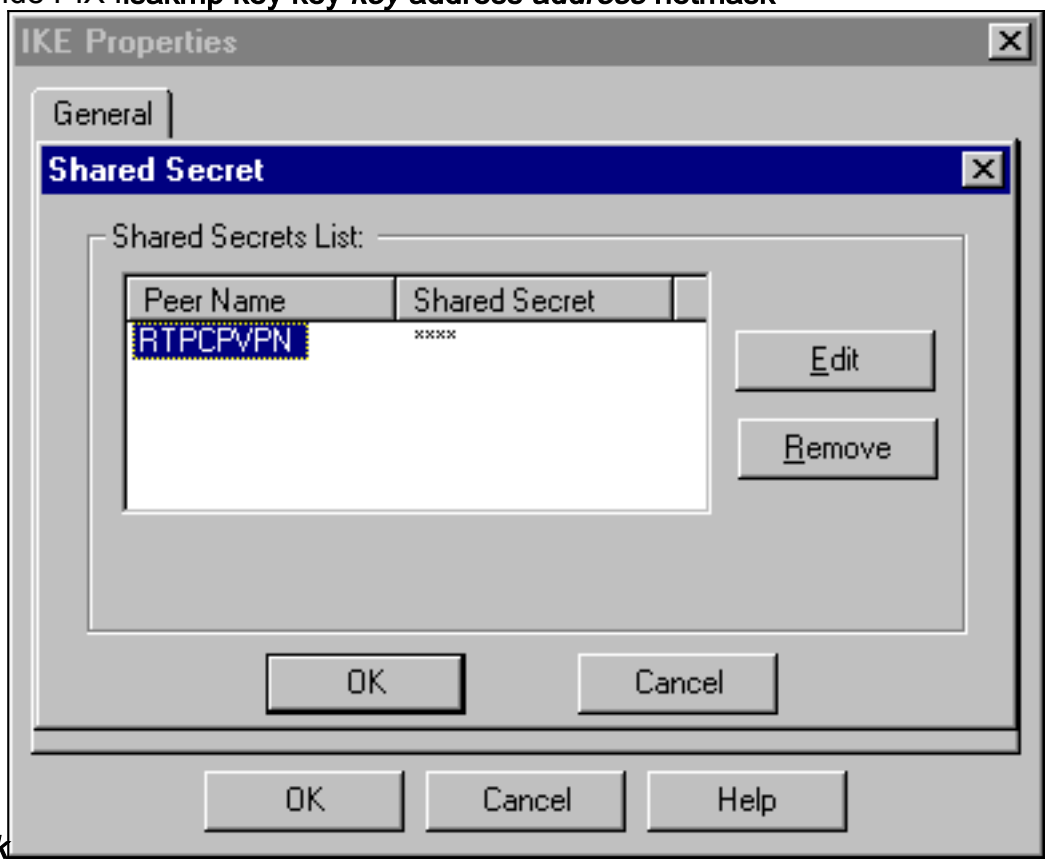
Modifier.

11. Modifiez les propriétés IKE du chiffrement DES pour accepter cette commande :**isakmp policy # encryption des**
12. Remplacez les propriétés IKE par le hachage SHA1 pour accepter cette commande :**crypto isakmp policy # hash sha**Modifiez ces paramètres :Désélectionnez **Mode agressif**.Cochez la case **Supports Subnets**.Sous Authentication Method, activez la case à cocher **Pre-Shared Secret**. Cette action est en accord avec cette commande :**isakmp policy # authentication pre-**



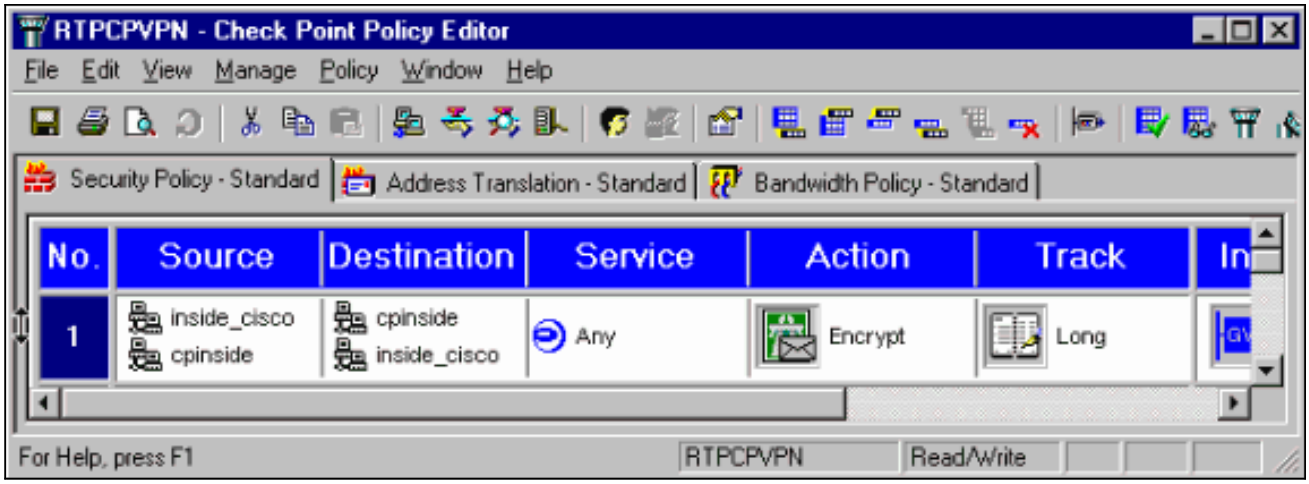
share

13. Cliquez sur **Modifier les secrets** pour définir la clé pré-partagée en accord avec cette commande PIX :**isakmp key key *key* address *address* netmask**

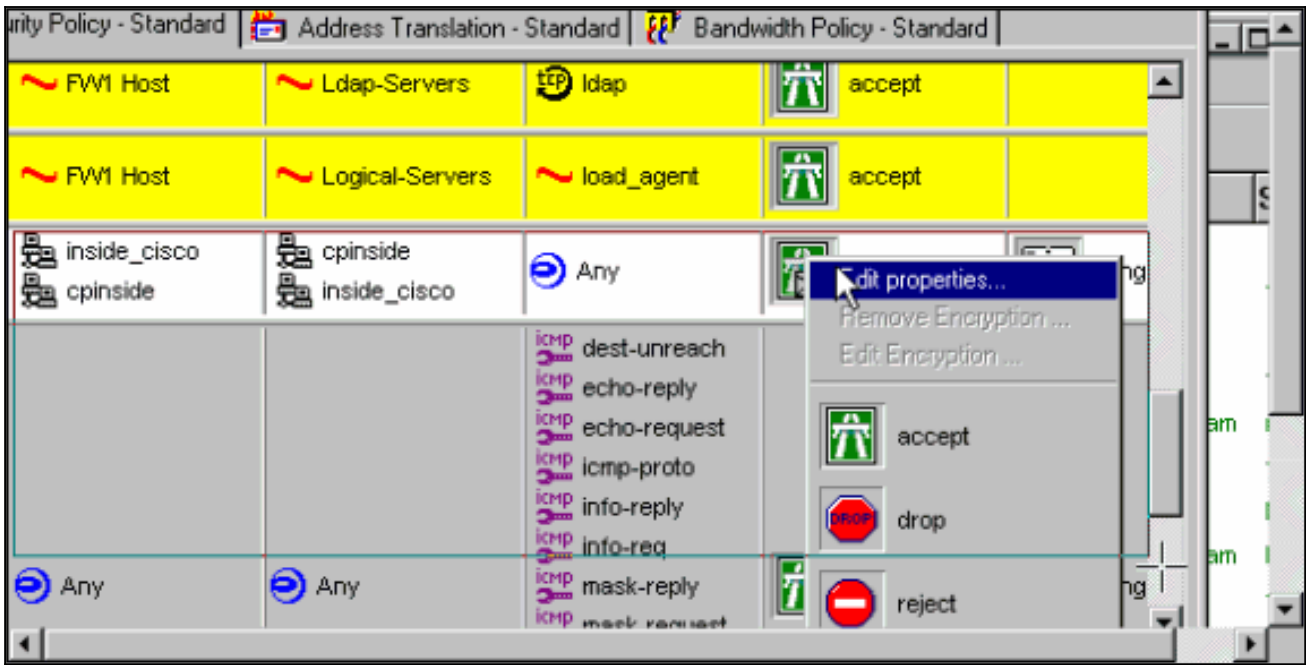


netmask

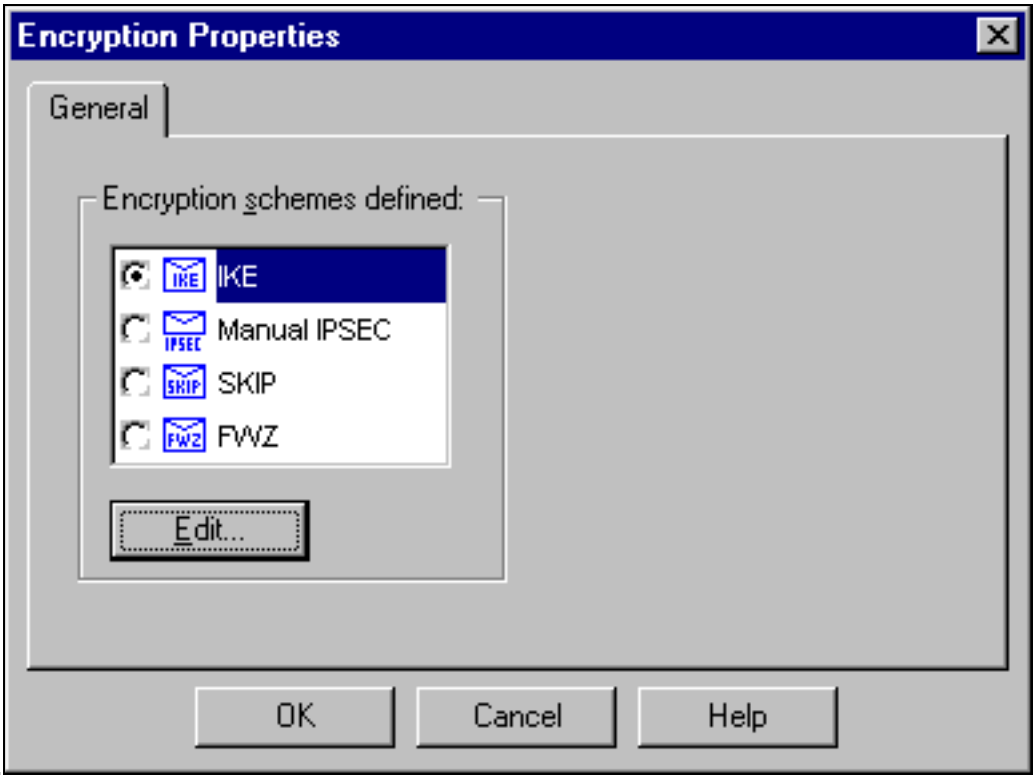
14. Dans la fenêtre Éditeur de stratégie, insérez une règle avec Source et Destination comme « inside_cisco » et « cpinside » (bidirectionnel). Définir **Service=Any**, **Action=Encrypt** et **Track=Long**.

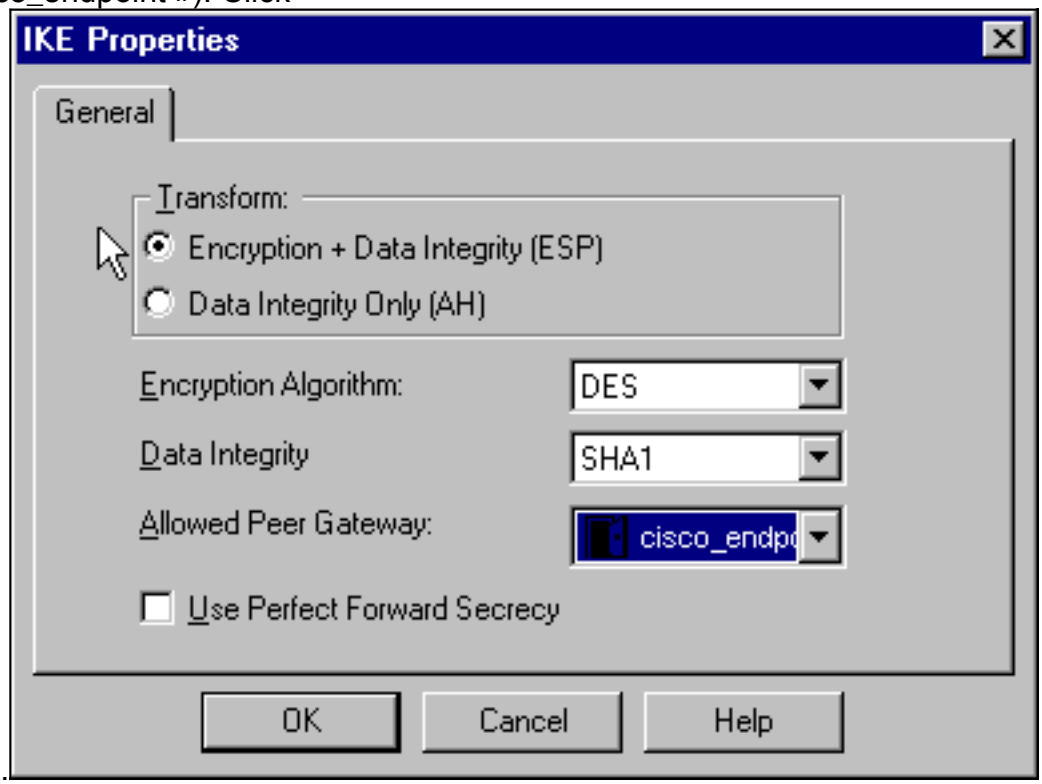


15. Sous l'en-tête Action, cliquez sur l'icône **Chiffrement** vert et sélectionnez **Modifier les propriétés** pour configurer les stratégies de chiffrement.



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

Modifier. 

17. Dans l'écran Propriétés IKE, modifiez ces propriétés pour les mettre en accord avec les transformations IPSec PIX dans cette commande :**crypto ipsec transformer-set myset 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 PIX externe (appelée « cisco_endpoint »). Click OK. 

18. Une fois le point de contrôle configuré, sélectionnez **Stratégie > Installer** dans le menu Point de contrôle afin que les modifications prennent effet.

Commandes debug, show et clear

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** - Affiche les messages de débogage sur les moteurs de chiffrement, qui effectuent le chiffrement et le déchiffrement.
- **debug crypto isakmp** - Affiche les messages relatifs aux événements IKE.
- **debug crypto ipsec** - Affiche les événements IPSec.
- **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 associations de sécurité actuelles.
- **clear crypto isakmp sa** -(à partir du mode de configuration) Effacez toutes les connexions IKE actives.
- **clear crypto ipsec sa** -(à partir du mode de configuration) Supprimez toutes les associations de sécurité IPSec.

Point de contrôle :

Comme le suivi a été défini sur Long dans la fenêtre Éditeur de stratégie illustrée à l'étape 14, le trafic refusé apparaît en rouge dans la Visionneuse de journaux. Vous pouvez obtenir un débogage plus détaillé 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 : Il s'agissait d'une installation de Microsoft Windows NT.

Vous pouvez effacer les SA sur le point de contrôle à l'aide des commandes suivantes :

```
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 de répondre **oui** à l'Êtes-vous sûr? activer.

Dépannage

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

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 la liste de contrôle d'accès de chiffrement sur le PIX n'est pas configurée pour correspondre, le tunnel échouera probablement. 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.

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)
- Configuration de la sécurité des réseaux IPSec
- Configuration du protocole IKE (Internet Key Exchange)
- PIX 5.2 : Configuration d'IPSec
- PIX 5.3 : Configuration d'IPSec
- Page d'assistance IPsec
- Support technique - Cisco Systems