Configuration d'IPSec entre un serveur Microsoft Windows 2000 et un périphérique Cisco

Contenu

Introduction

Ce document explique comment créer un tunnel IPSec avec des clés prépartagées afin de joindre deux réseaux privés : un réseau privé (192.168.I.X) au sein d'un périphérique Cisco et un réseau privé (10.32.50.X) au sein d'un serveur Microsoft 2000. Nous supposons que le trafic allant du périphérique Cisco et du serveur 2000 vers Internet (représenté ici par les réseaux 172.18.124.X) circule déjà avant le début de la configuration.

Vous trouverez des informations détaillées sur la configuration du serveur Microsoft Windows 2000 sur le site Web de Microsoft :
http://support.microsoft.com/support/kb/articles/Q252/7/35.ASP

Avant de commencer

Conventions

Pour plus d'informations sur les conventions des documents, référez-vous aux Conventions

utilisées pour les conseils techniques de Cisco.

Conditions préalables

Aucune condition préalable spécifique n'est requise pour ce document.

Components Used

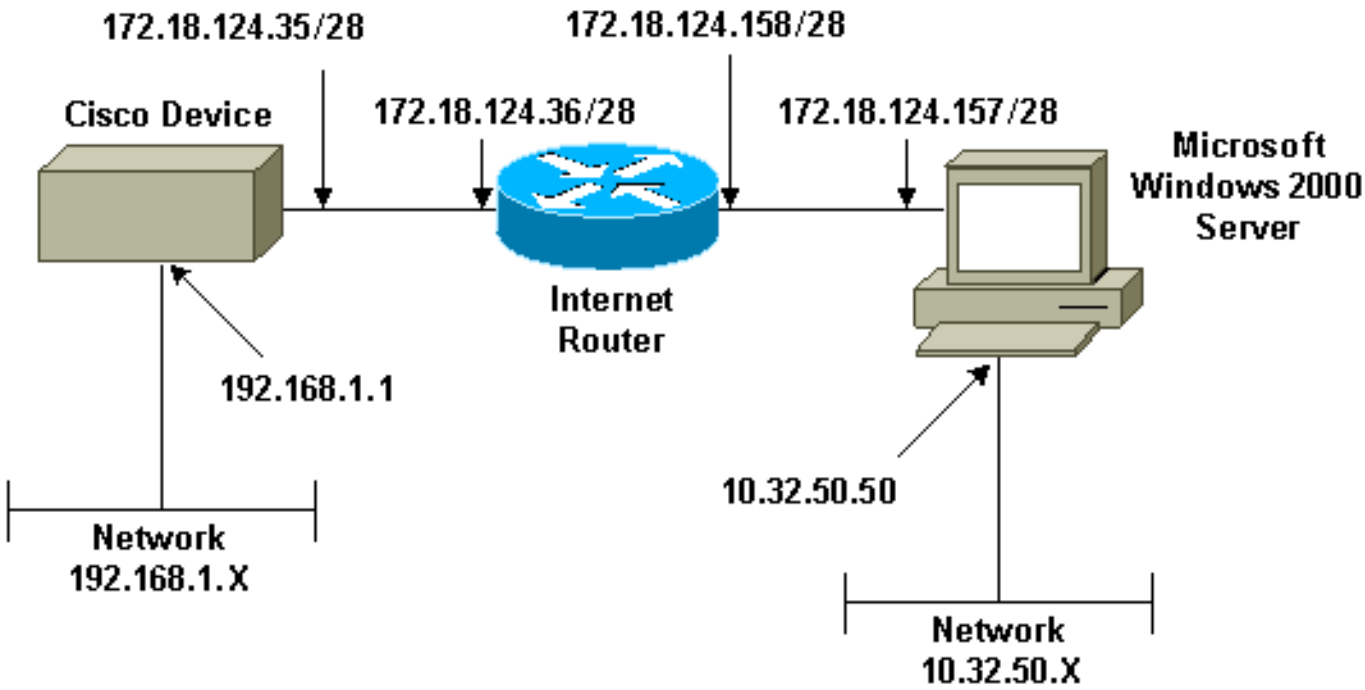
Ces configurations ont été développées et testées à l'aide des versions logicielles et matérielles ci-dessous.

- Microsoft Windows 2000 Server 5.00.2195
- Routeur Cisco 3640 avec logiciel Cisco IOS® version c3640-ik2o3s-mz.121-5.T.bin
- Cisco Secure PIX Firewall avec logiciel PIX version 5.2.1
- Concentrateur Cisco VPN 3000 avec concentrateur VPN 3000 Version 2.5.2.F
- Concentrateur VPN Cisco 5000 avec concentrateur VPN 5000 Version 5.2.19

Les informations présentées dans ce document ont été créées à partir de périphériques dans un environnement de laboratoire spécifique. All of the devices used in this document started with a cleared (default) configuration. Si vous travaillez dans un réseau opérationnel, assurez-vous de bien comprendre l'impact potentiel de toute commande avant de l'utiliser.

Diagramme du réseau

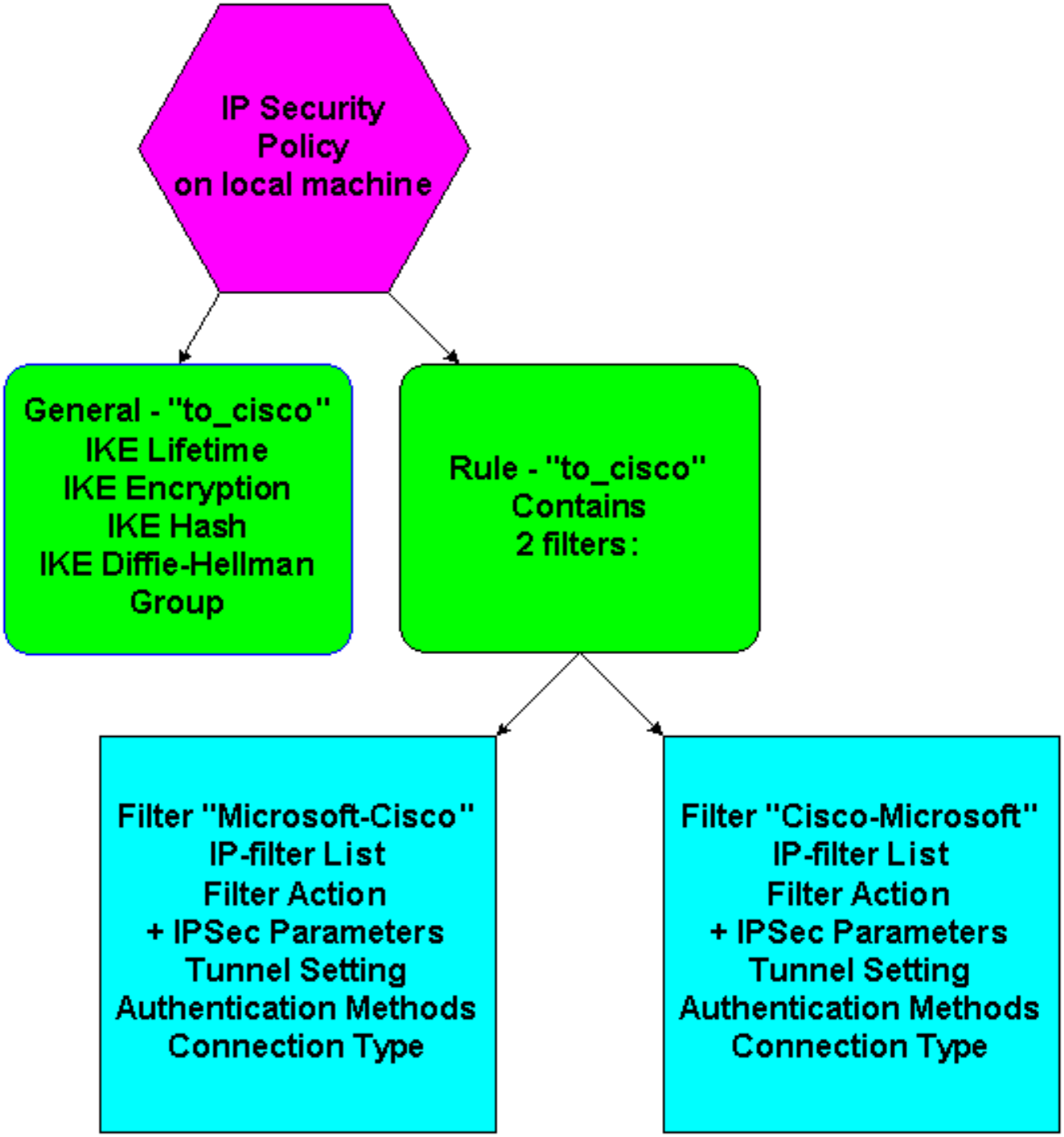
Ce document utilise la configuration réseau indiquée dans le diagramme suivant :



Configuration du serveur Microsoft Windows 2000 pour qu'il fonctionne avec les périphériques Cisco

Tâches effectuées

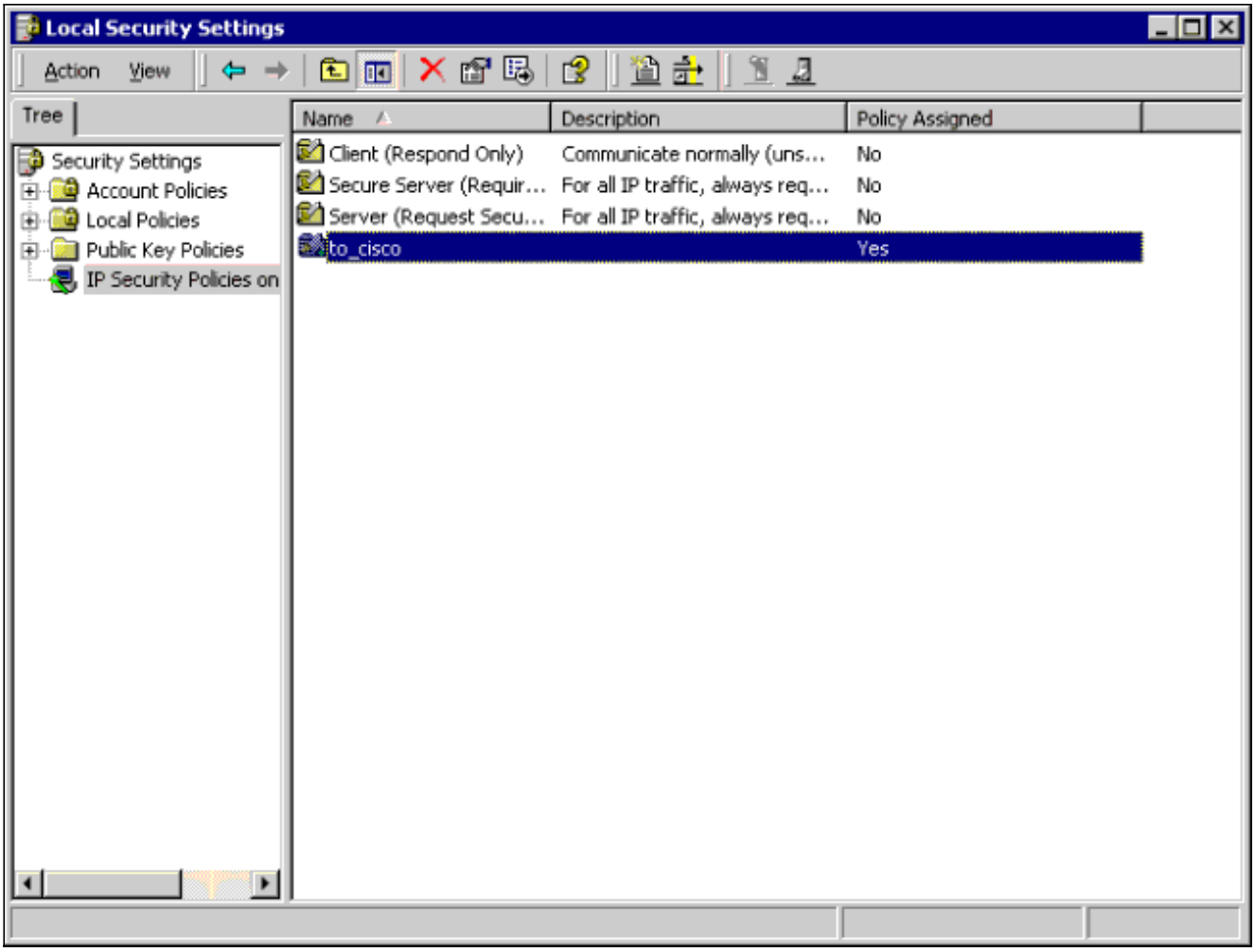
Ce diagramme montre les tâches effectuées dans la configuration du serveur Microsoft Windows 2000 :



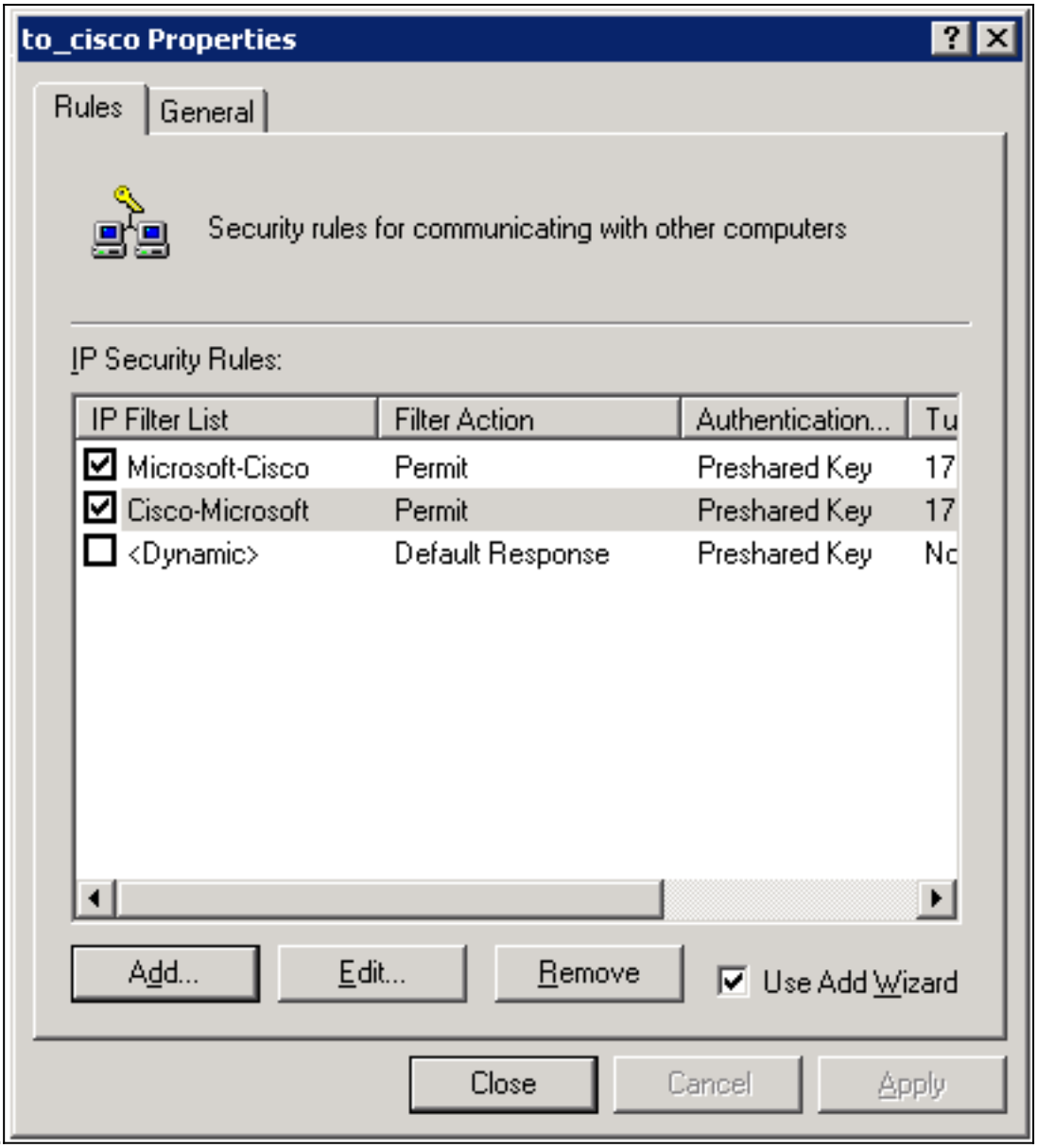
Step-by-Step Instructions

Une fois que vous avez suivi les instructions de configuration sur le site Web de Microsoft, procédez comme suit pour vérifier que votre configuration peut fonctionner avec les périphériques Cisco. Les commentaires et les modifications sont notés avec les captures d'écran.

1. Cliquez sur **Démarrer > Exécuter > secpol.msc** sur Microsoft Windows 2000 Server, puis vérifiez les informations sur les écrans suivants.Une fois que les instructions du site Web de Microsoft ont été utilisées pour configurer un serveur 2000, les informations de tunnel suivantes ont été affichées.**Remarque :** la règle d'exemple est appelée « to_cisco ».

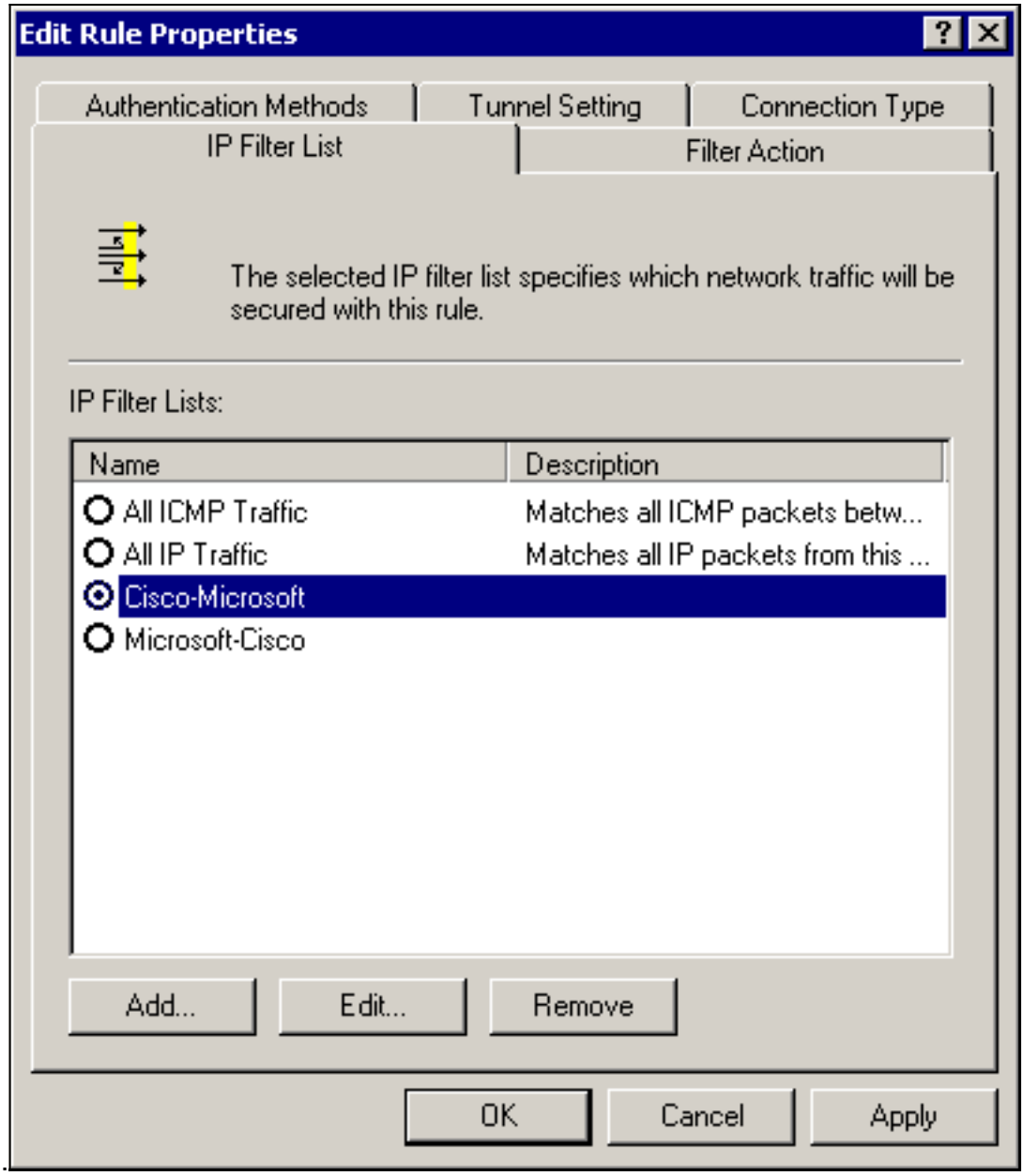


2. Cette règle d'exemple contient deux filtres : Microsoft-Cisco et Cisco-



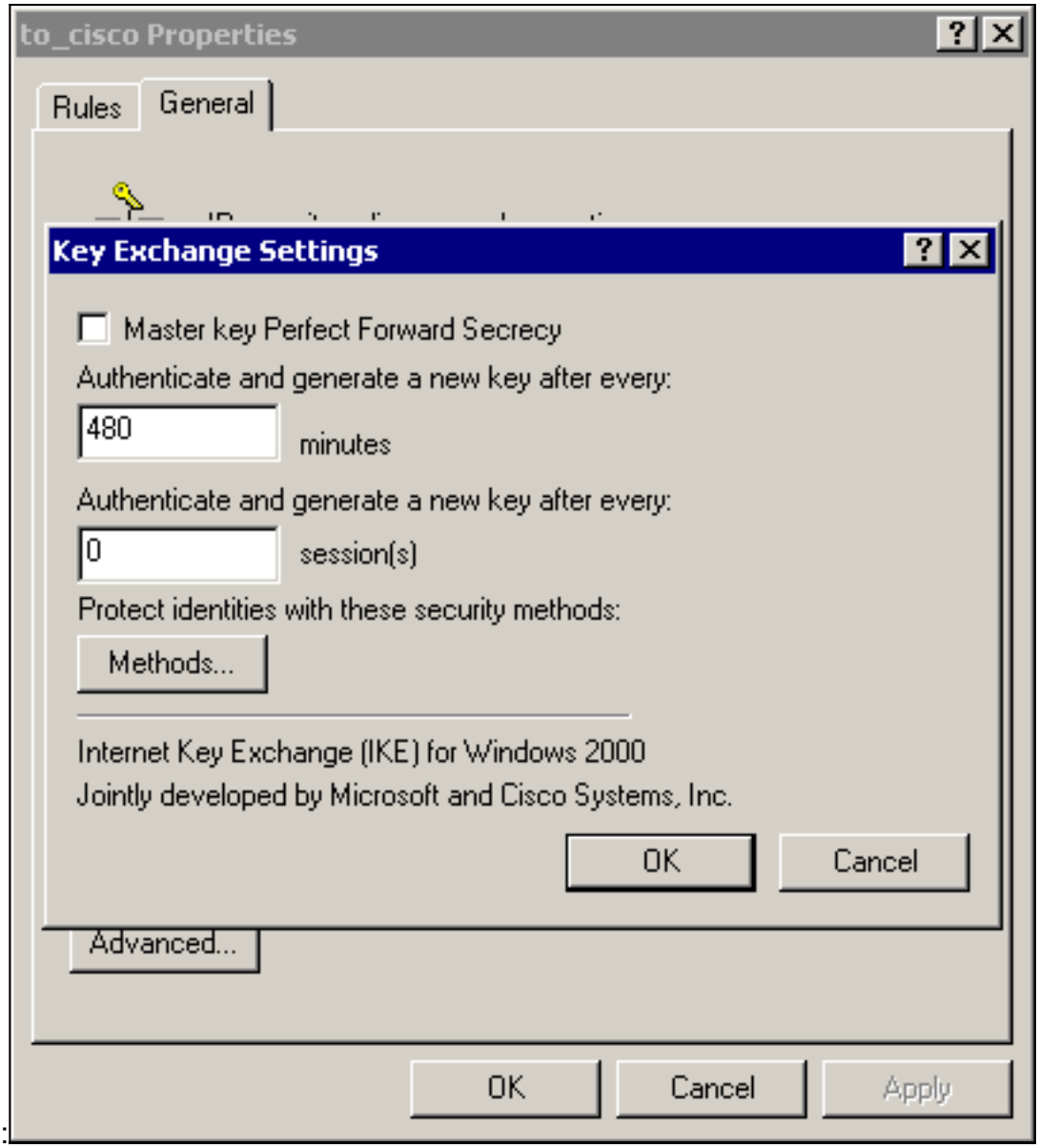
Microsoft.

3. Sélectionnez la règle de sécurité IP Cisco-Microsoft, puis cliquez sur **Modifier** pour afficher/ajouter/modifier les listes de filtres



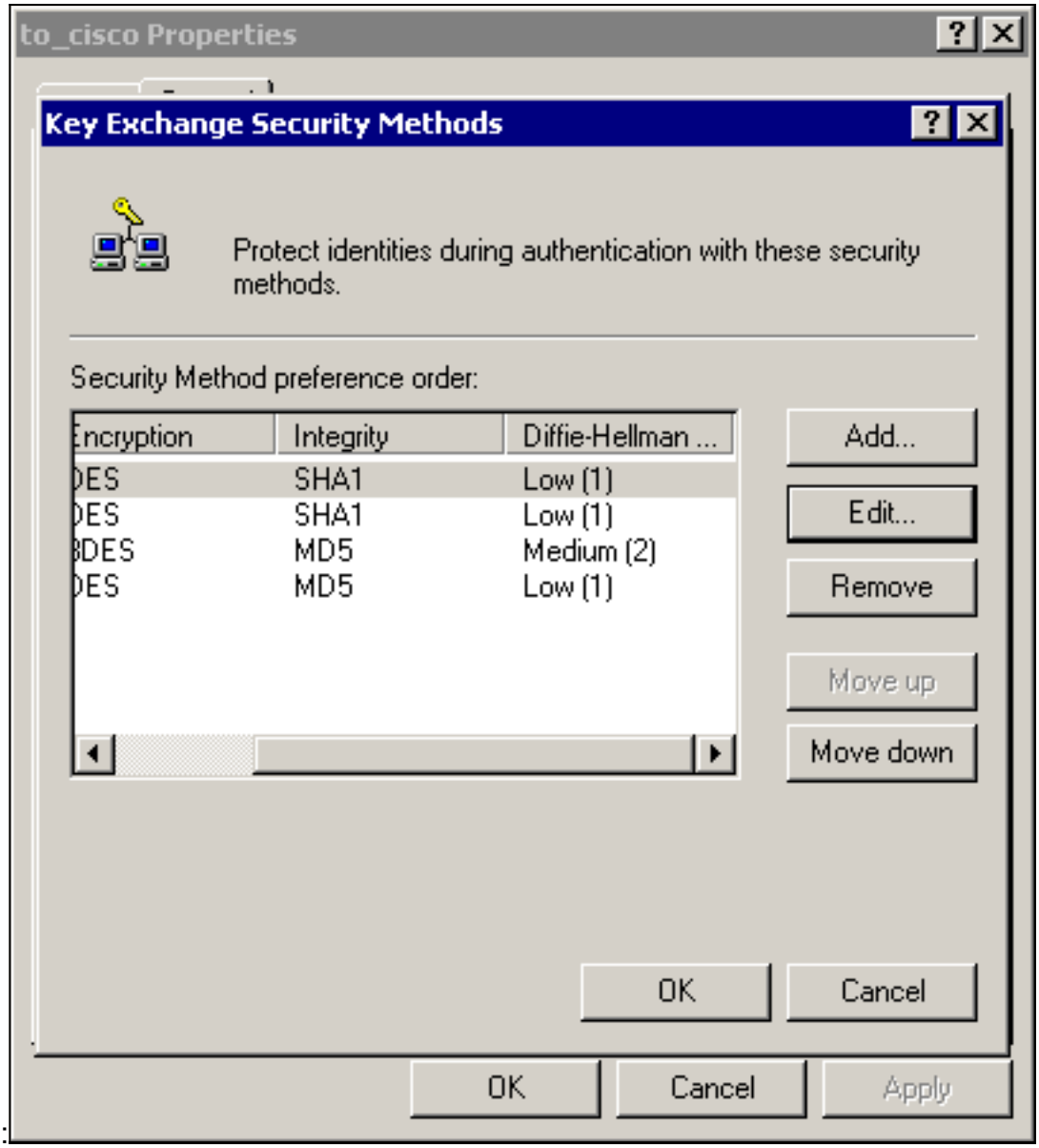
IP.

4. L'onglet **Général > Avancé de** la règle a la **durée de vie IKE** (480 minutes = 28800 secondes)



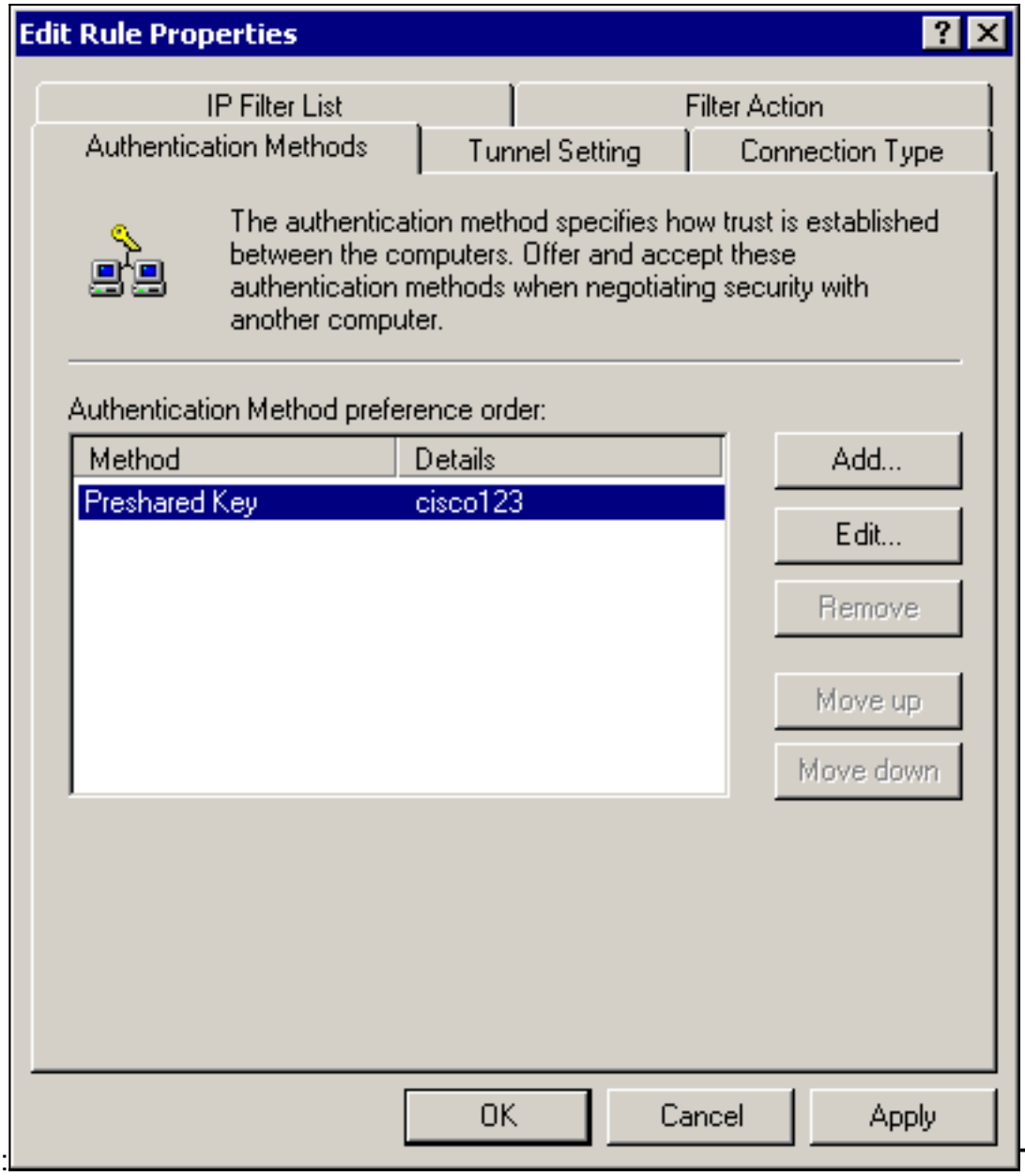
:

5. L'onglet **Général > Avancé > Méthodes** de la règle comporte la **méthode de chiffrement IKE** (DES), le **hachage IKE** (SHA1) et le **groupe Diffie-Helman** (Low(1)

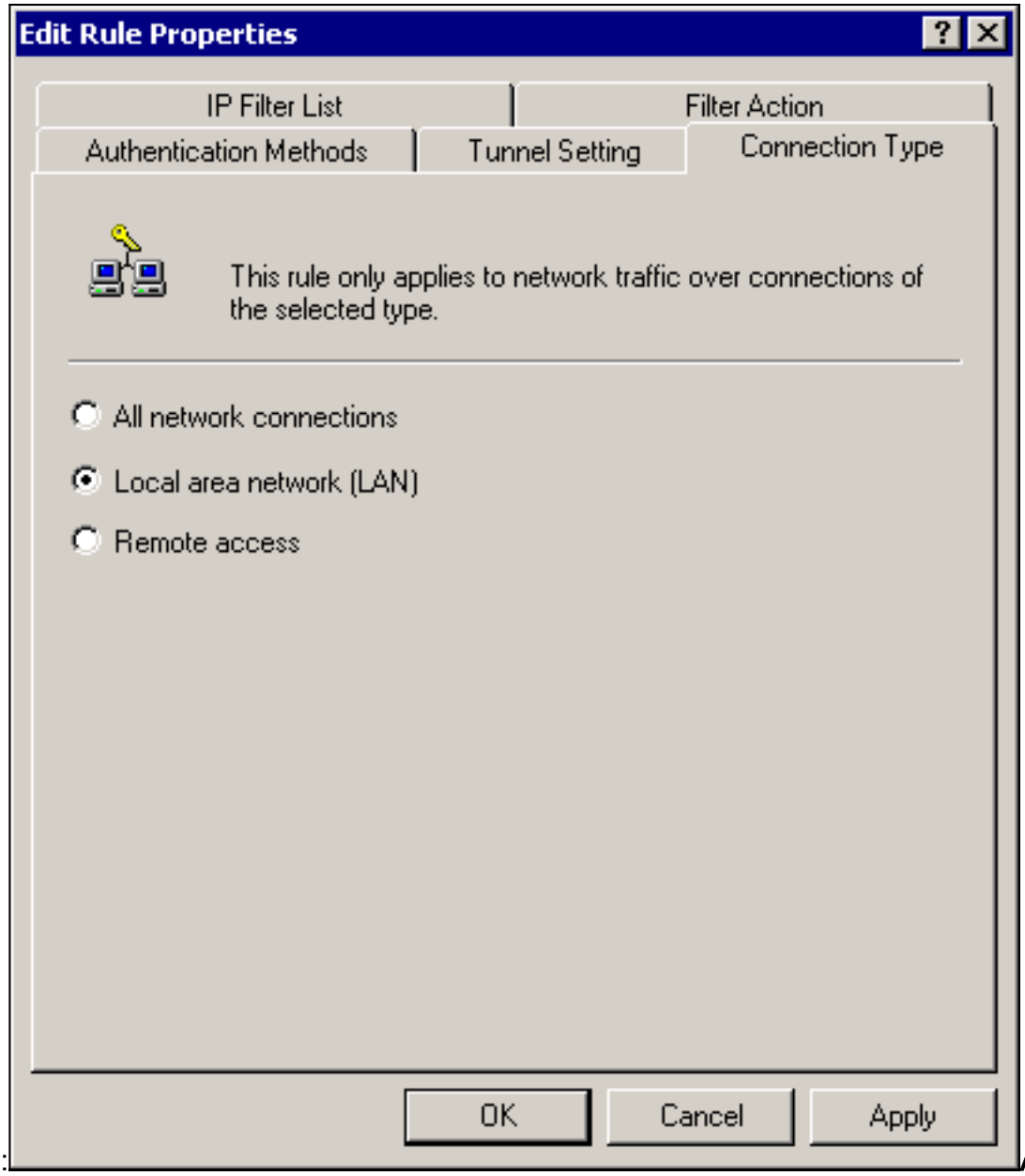


:

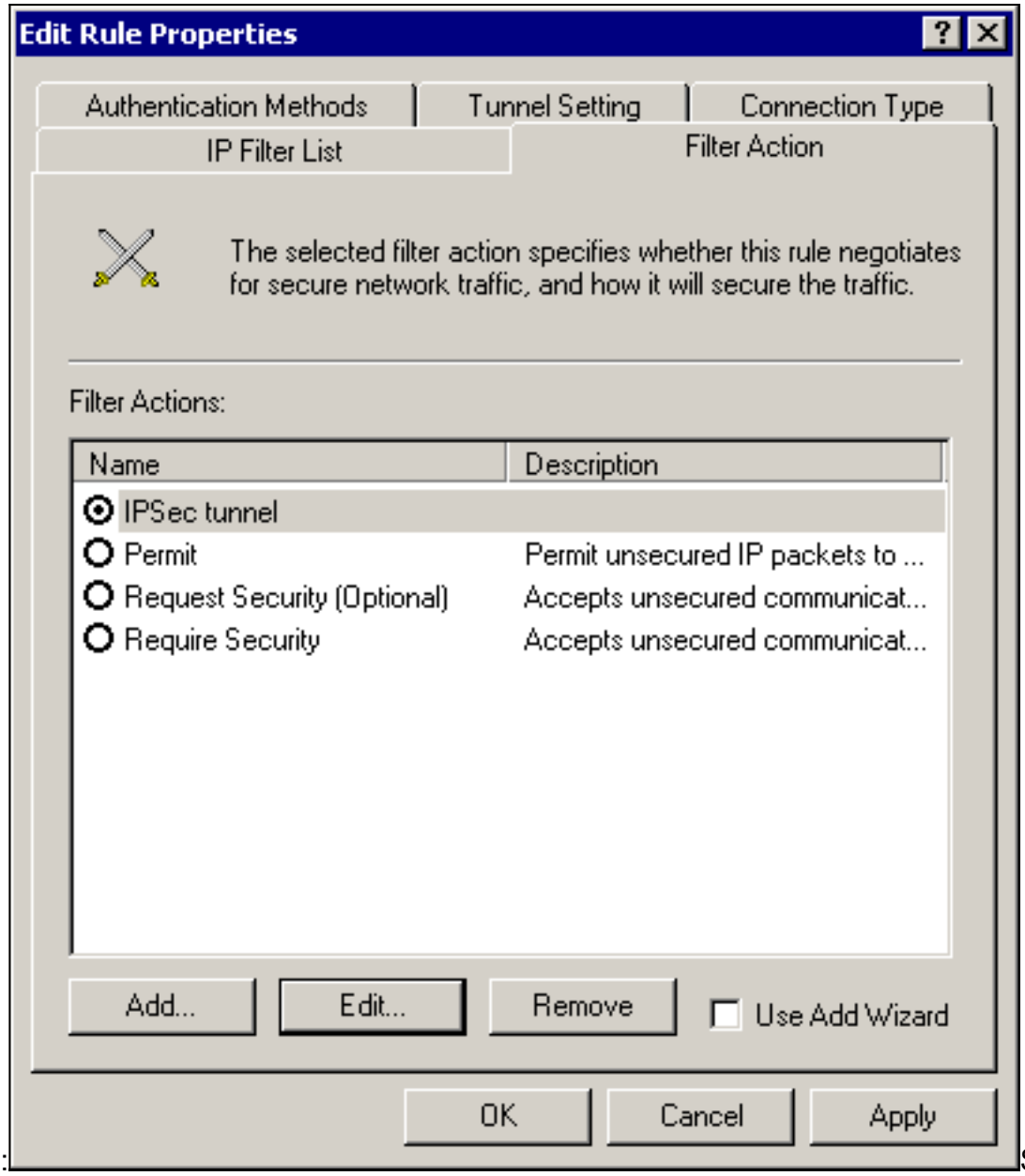
6. Chaque filtre comporte 5 onglets :**Méthodes d'authentification** (clés prépartagées pour l'échange de clés Internet [IKE])



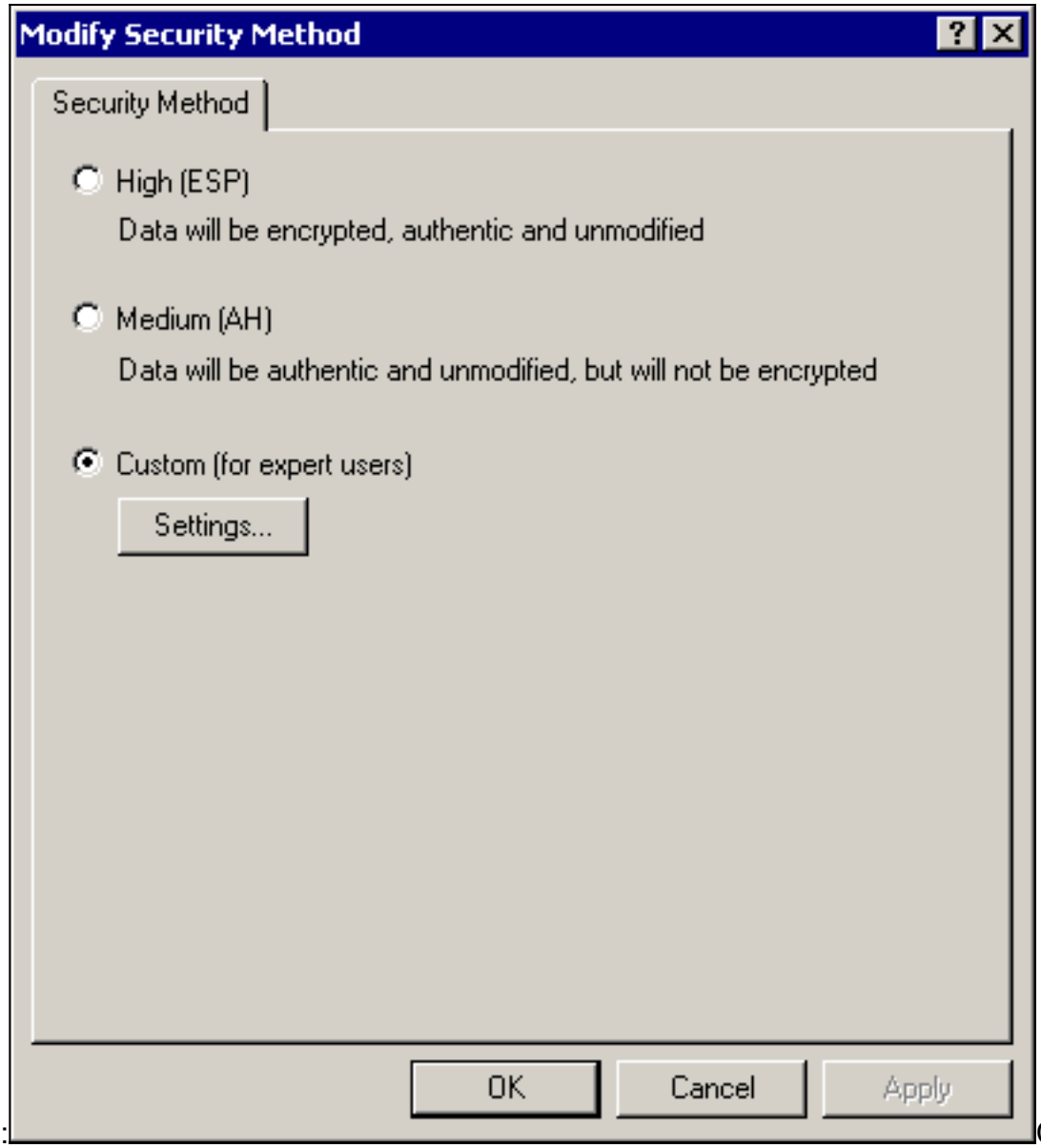
:**Type de connexion** (LAN)



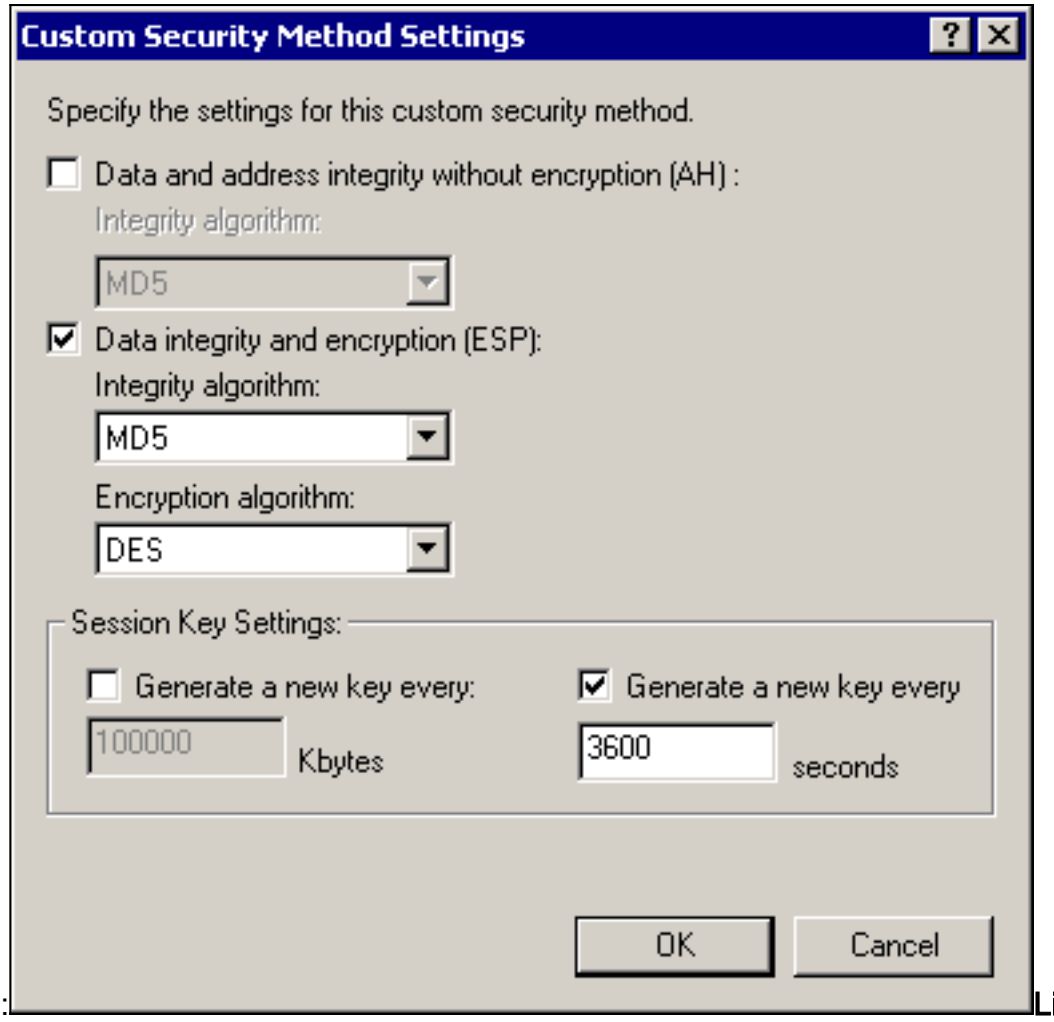
: **Action de filtre** (IPSec)



:Sélectionnez **Action de filtre > tunnel IPSec > Modifier > Modifier**, puis cliquez sur **Personnalisé**



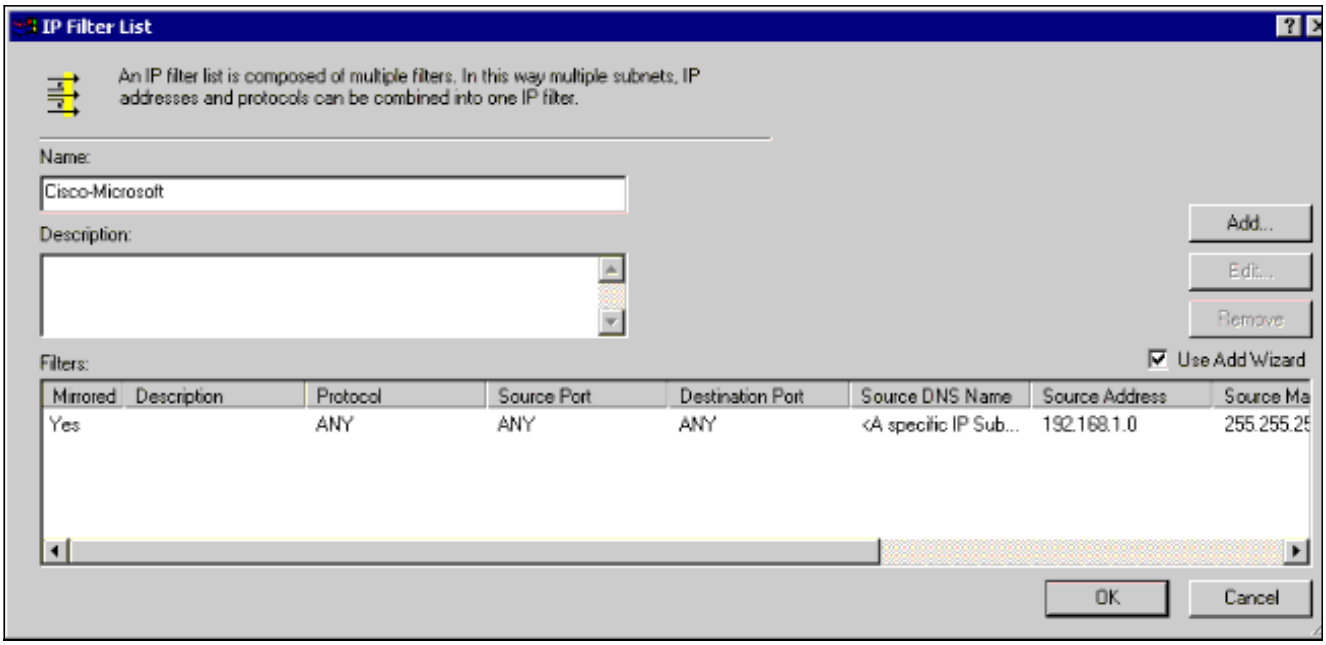
:Cliquez sur **Paramètres - IPSec transforme** et **durée de vie IPSec**



:**Liste de filtres IP :**

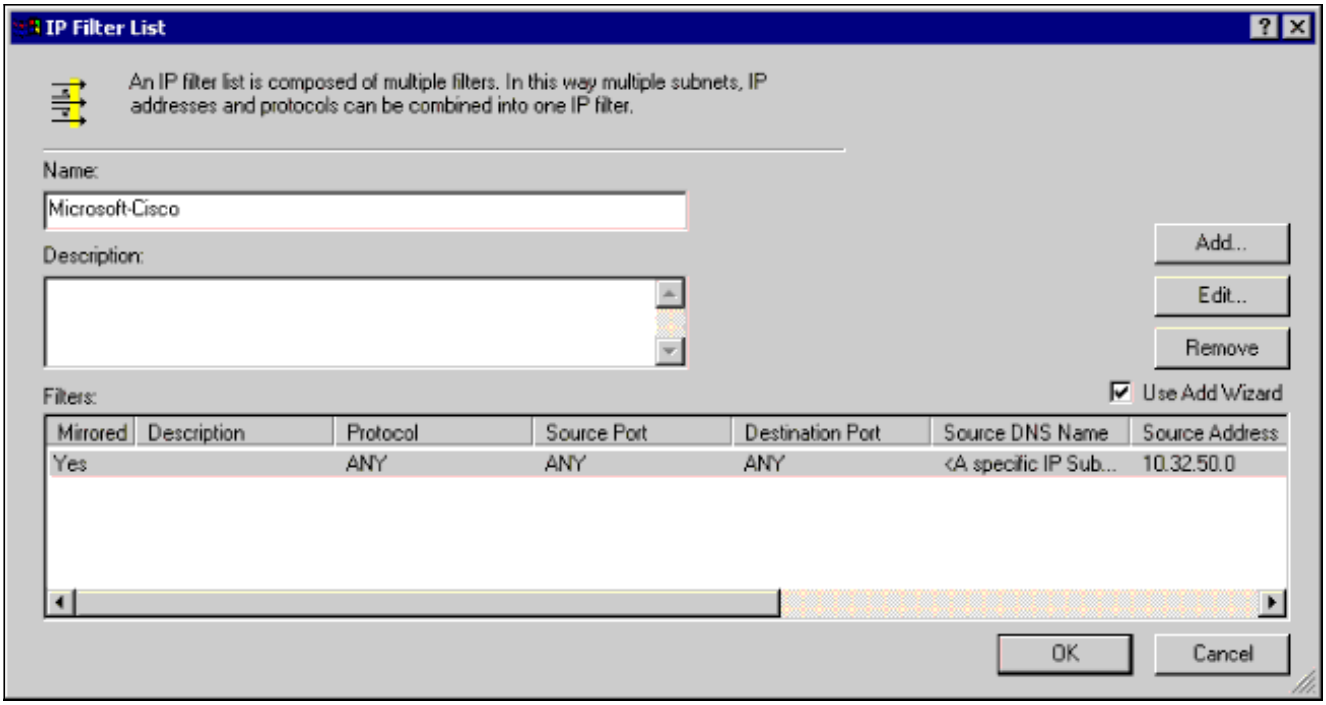
les réseaux **source** et **de destination** doivent être chiffrés :Pour Cisco-Microsoft

:

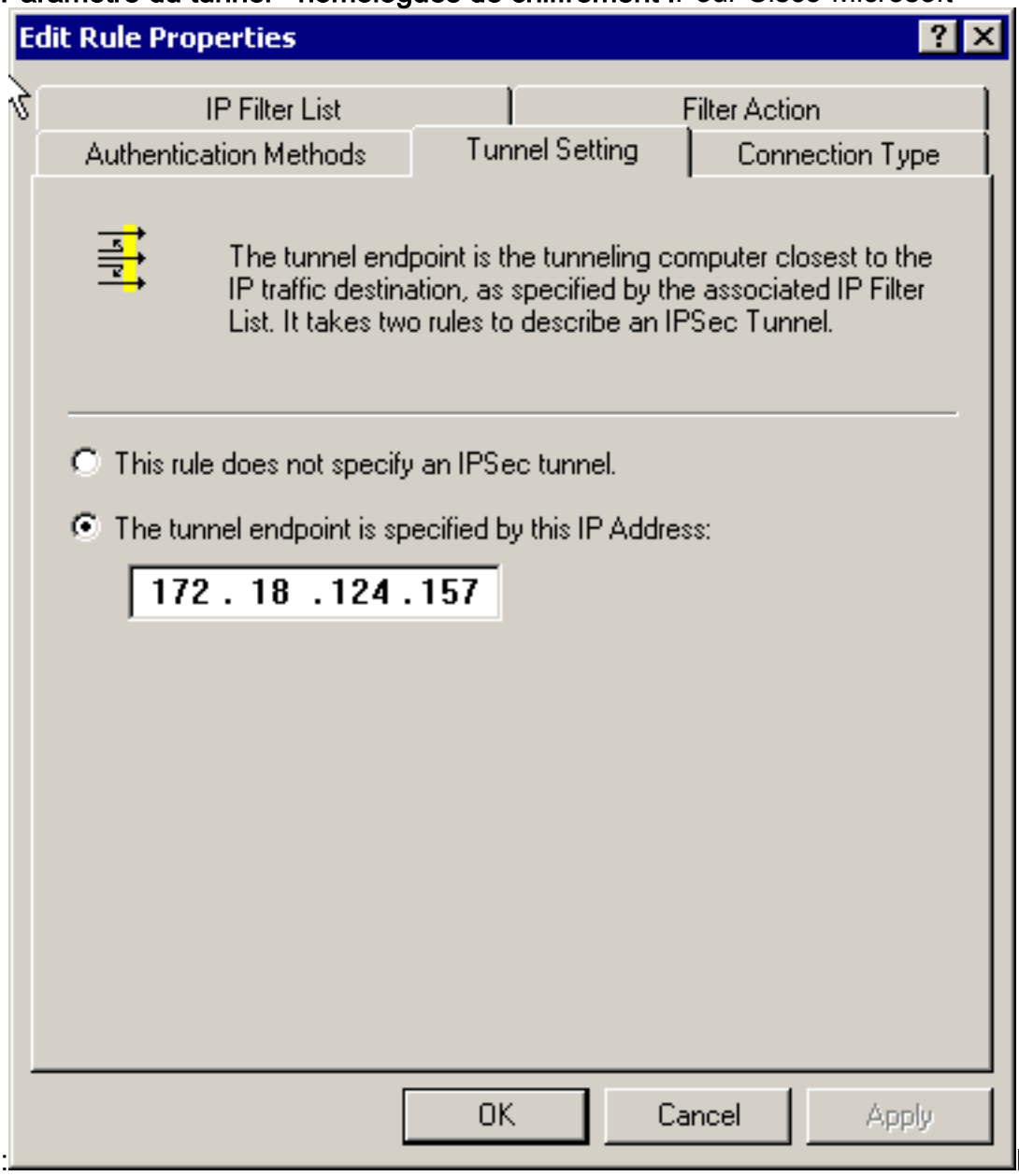


Pour Microsoft-Cisco

:

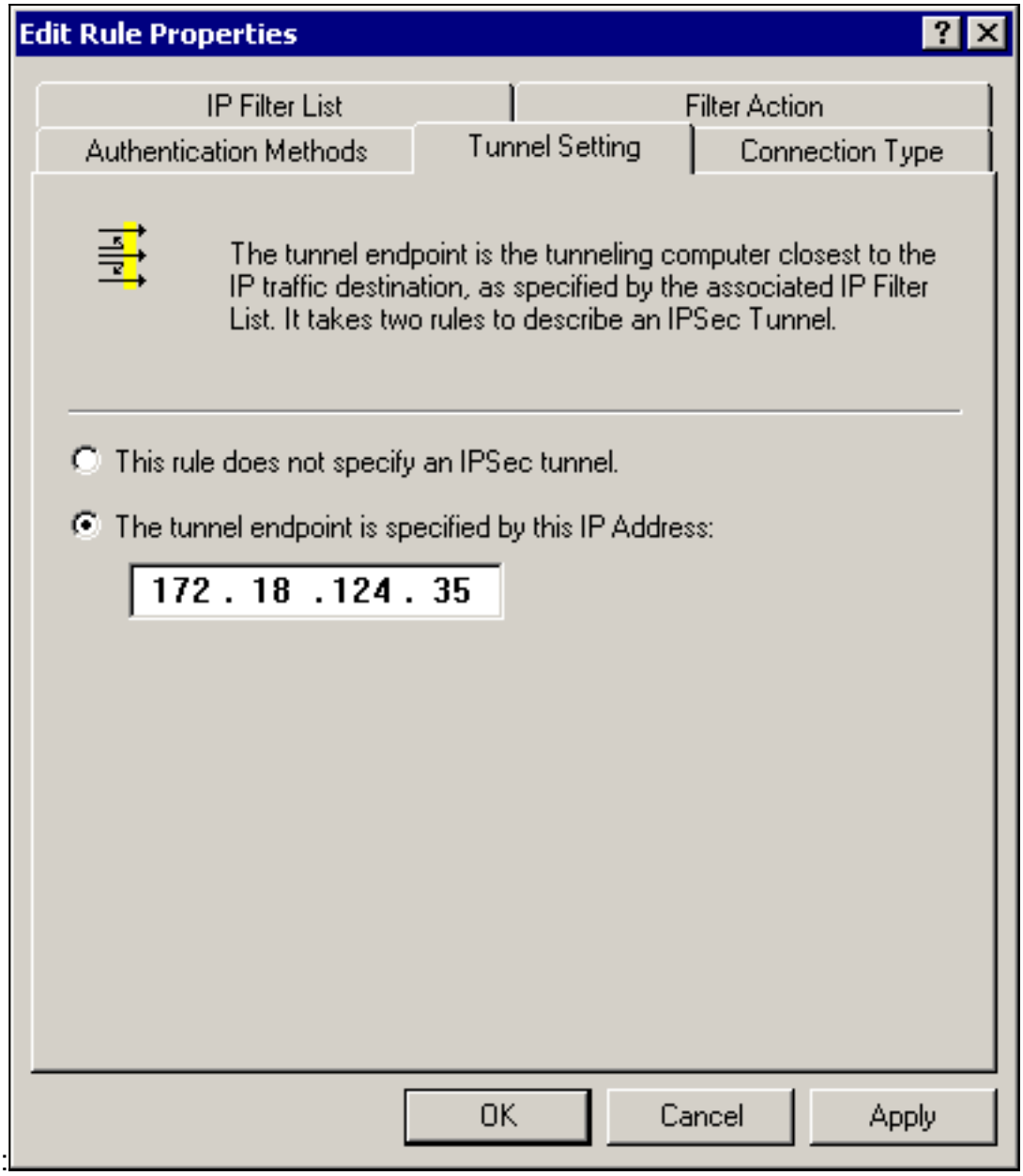


Paramètre du tunnel - homologues de chiffrement : Pour Cisco-Microsoft



:Pour Microsoft-

Cisco :



Configuration des périphériques Cisco

Configurez le routeur Cisco, les concentrateurs PIX et VPN, comme indiqué dans les exemples ci-dessous.

- Routeur Cisco 3640
- PIX
- Concentrateur VPN 3000
- Concentrateur VPN 5000

Configuration du routeur Cisco 3640

Routeur Cisco 3640

`Current configuration : 1840 bytes`
`!`
`version 12.1`
`no service single-slot-reload-enable`

```
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname moss
!
logging rate-limit console 10 except errors
!
ip subnet-zero
!
no ip finger
!
ip audit notify log
ip audit po max-events 100
!
crypto isakmp policy 1
!--- The following are IOS defaults so they do not
appear: !--- IKE encryption method encryption des !---
IKE hashing hash sha !--- Diffie-Hellman group group 1
!--- Authentication method authentication pre-share
!--- IKE lifetime lifetime 28800
!--- encryption peer crypto isakmp key cisco123 address
172.18.124.157
!
!--- The following is the IOS default so it does not
appear: !--- IPSec lifetime crypto ipsec security-
association lifetime seconds 3600 ! !--- IPSec
transforms crypto ipsec transform-set rtpset esp-des
esp-md5-hmac
!
crypto map rtp 1 ipsec-isakmp
!--- Encryption peer set peer 172.18.124.157
set transform-set rtpset
!--- Source/Destination networks defined match address
115
!
call rsvp-sync
!
interface Ethernet0/0
ip address 192.168.1.1 255.255.255.0
ip nat inside
half-duplex
!
interface Ethernet0/1
ip address 172.18.124.35 255.255.255.240
ip nat outside
half-duplex
crypto map rtp
!
ip nat pool INTERNET 172.18.124.35 172.18.124.35 netmask
255.255.255.240
ip nat inside source route-map nonat pool INTERNET
ip classless
ip route 0.0.0.0 0.0.0.0 172.18.124.36
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
!--- Source/Destination networks defined 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
```

```
!
line con 0
transport input none
line 65 94
line aux 0
line vty 0 4
!
end
```

Configuration de PIX

PIX

```
PIX Version 5.2(1)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pixfirewall
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
!--- Source/Destination networks defined 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
no logging monitor
no logging buffered
no logging trap
no logging history
logging facility 20
logging queue 512
interface ethernet0 auto
interface ethernet1 10baset
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
!--- Except Source/Destination from Network Address
Translation (NAT): nat (inside) 0 access-list 115
route outside 0.0.0.0 0.0.0.0 172.18.124.36 1
timeout xlate 3:00:00
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
sysopt connection permit-ipsec
no sysopt route dnat
!--- IPSec transforms crypto ipsec transform-set myset
esp-des esp-md5-hmac
!--- IPSec lifetime crypto ipsec security-association
lifetime seconds 3600
crypto map rtpmap 10 ipsec-isakmp
!--- Source/Destination networks crypto map rtpmap 10
match address 115
!--- Encryption peer crypto map rtpmap 10 set peer
172.18.124.157
crypto map rtpmap 10 set transform-set myset
crypto map rtpmap interface outside
isakmp enable outside
!--- Encryption peer isakmp key ******** address
172.18.124.157 netmask 255.255.255.240
isakmp identity address
!--- Authentication method isakmp policy 10
authentication pre-share
!--- IKE encryption method isakmp policy 10 encryption
des
!--- IKE hashing isakmp policy 10 hash sha
!--- Diffie-Hellman group isakmp policy 10 group 1
!--- IKE lifetime isakmp policy 10 lifetime 28800
telnet timeout 5
ssh timeout 5
terminal width 80
Cryptochecksum:c237ed11307abea7b530bbd0c2b2ec08
: end
```

Configuration du concentrateur VPN 3000

Utilisez les options de menu et les paramètres indiqués ci-dessous pour configurer le concentrateur VPN si nécessaire.

- Pour ajouter une proposition IKE, sélectionnez **Configuration > Système > Protocoles de tunnellisation > IPSec > Propositions IKE > Ajouter une proposition.**

  ```
  Proposal Name = DES-SHA
  !--- Authentication method Authentication Mode = Preshared Keys !--- IKE hashing
  Authentication Algorithm = SHA/HMAC-160 !--- IKE encryption method Encryption Algorithm =
  DES-56 !--- Diffie-Hellman group Diffie Hellman Group = Group 1 (768-bits) Lifetime
  Measurement = Time Date Lifetime = 10000 !--- IKE lifetime Time Lifetime = 28800
  ```

- Pour définir le tunnel LAN à LAN, sélectionnez **Configuration > System > Tunneling Protocols > IPSec LAN à LAN.**

  ```
  Name = to_2000
  Interface = Ethernet 2 (Public) 172.18.124.35/28
  !--- Encryption peer Peer = 172.18.124.157 !--- Authentication method Digital Certs = none
  (Use Pre-shared Keys) Pre-shared key = cisco123 !--- IPSec transforms Authentication =
  ESP/MD5/HMAC-128 Encryption = DES-56 !--- Use the IKE proposal IKE Proposal = DES-SHA
  Autodiscovery = off !--- Source network defined Local Network Network List = Use IP
  ```

```
Address/Wildcard-mask below IP Address 192.168.1.0 Wildcard Mask = 0.0.0.255 !---
Destination network defined Remote Network Network List = Use IP Address/Wildcard-mask below
IP Address 10.32.50.0 Wildcard Mask 0.0.0.255
```

- Pour modifier l'association de sécurité, sélectionnez **Configuration > Policy Management > Traffic Management > Security Associations > Modify.**

```
SA Name = L2L-to_2000
Inheritance = From Rule
IPSec Parameters
!--- IPSec transforms Authentication Algorithm = ESP/MD5/HMAC-128 Encryption Algorithm =
DES-56 Encapsulation Mode = Tunnel PFS = Disabled Lifetime Measurement = Time Data Lifetime
= 10000 !--- IPSec lifetime Time Lifetime = 3600 Ike Parameters !--- Encryption peer IKE
Peer = 172.18.124.157 Negotiation Mode = Main !--- Authentication method Digital Certificate
= None (Use Preshared Keys) !--- Use the IKE proposal IKE Proposal DES-SHA
```

Configuration du concentrateur VPN 5000

Concentrateur VPN 5000

```
[ IP Ethernet 1:0 ]
Mode = Routed
SubnetMask = 255.255.255.240
IPAddress = 172.18.124.35

[ General ]
IPSecGateway = 172.18.124.36
DeviceName = "cisco"
EthernetAddress = 00:00:a5:f0:c8:00
DeviceType = VPN 5002/8 Concentrator
ConfiguredOn = Timeserver not configured
ConfiguredFrom = Command Line, from Console

[ IP Ethernet 0:0 ]
Mode = Routed
SubnetMask = 255.255.255.0
IPAddress = 192.168.1.1

[ Tunnel Partner VPN 1 ]
 !--- Encryption peer Partner = 172.18.124.157 !---
IPSec lifetime KeyLifeSecs = 3600 BindTo = "ethernet
1:0" !--- Authentication method SharedKey = "cisco123"
KeyManage = Auto !--- IPSec transforms Transform =
esp(md5,des) Mode = Main !--- Destination network
defined Peer = "10.32.50.0/24" !--- Source network
defined LocalAccess = "192.168.1.0/24" [ IP Static ]
10.32.50.0 255.255.255.0 VPN 1 1 [ IP VPN 1 ] Mode =
Routed Numbered = Off [ IKE Policy ] !--- IKE hashing,
encryption, Diffie-Hellman group Protection = SHA_DES_G1
Configuration size is 1088 out of 65500 bytes.
```

Vérification

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner vos configurations.

Dépannage des commandes

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.

Note : Avant d'émettre des commandes **debug**, consultez Informations importantes sur les commandes de débogage.

Routeur Cisco 3640

- **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** - Affiche toutes les associations de sécurité IKE (SA) actuelles sur un homologue.
- **show crypto ipsec sa** - Affiche les paramètres utilisés par les associations de sécurité actuelles.
- **clear crypto isakmp** - (à partir du mode de configuration) Efface toutes les connexions IKE actives.
- **clear crypto sa** - (à partir du mode de configuration) Supprime toutes les associations de sécurité IPSec.

PIX

- **debug crypto ipsec** - Affiche les négociations IPSec de la phase 2.
- **debug crypto isakmp** - Affiche les négociations de la phase 1 de l'ISAKMP (Internet Security Association and Key Management Protocol).
- **debug crypto engine** - Affiche le trafic chiffré.
- **show crypto ipsec sa** - Affiche les associations de sécurité de phase 2.
- **show crypto isakmp sa** - Affiche les associations de sécurité de phase 1.
- **clear crypto isakmp** - (à partir du mode de configuration) Efface les associations de sécurité IKE (Internet Key Exchange).
- **clear crypto ipsec sa** - (à partir du mode de configuration) Efface les associations de sécurité IPSec.

Concentrateur VPN 3000

- - Démarrez le débogage du concentrateur VPN 3000 en sélectionnant **Configuration > System > Events > Classes > Modify** (Severity to Log=1-13, Severity to Console=1-3) : IKE, IKEDBG, IKEDECODE, IPSEC, IPSECDBG, IPSECDECODE
- - Le journal des événements peut être effacé ou récupéré en sélectionnant **Monitoring > Event Log**.
- - Le trafic de tunnel LAN à LAN peut être surveillé dans **Monitoring > Sessions**.
- - Le tunnel peut être effacé dans **Administration > Admin Sessions > LAN-to-LAN sessions > Actions - Logout.**

Concentrateur VPN 5000

- **vpn trace dump all** - Affiche des informations sur toutes les connexions VPN correspondantes, y compris des informations sur l'heure, le numéro VPN, l'adresse IP réelle de l'homologue, les scripts qui ont été exécutés, et en cas d'erreur, la routine et le numéro de ligne du code logiciel où l'erreur s'est produite.
- **show vpn statistics** - Affiche les informations suivantes pour les utilisateurs, les partenaires et le total pour les deux. (Pour les modèles modulaires, l'affichage comprend une section pour chaque logement de module.) Current Active : connexions actives en cours. In Negot - Les relations actuellement en cours de négociation. Eau élevée : nombre le plus élevé de connexions actives simultanées depuis le dernier redémarrage. Total cumulé : nombre total de connexions ayant réussi depuis le dernier redémarrage. Tunnel Starts : nombre de démarrages du tunnel. Tunnel OK : nombre de tunnels pour lesquels aucune erreur n'a été détectée. Tunnel Error (Erreur de tunnel) : nombre de tunnels comportant des erreurs.
- **show vpn statistics verbose** - Affiche les statistiques de négociation ISAKMP et beaucoup plus de statistiques de connexion actives.

Informations connexes

- Annonce de fin de commercialisation des concentrateurs Cisco VPN 5000
- Configuration de la sécurité des réseaux IPSec
- Configuration du protocole IKE (Internet Key Exchange)
- Support technique - Cisco Systems