Configuración de IPSec entre un servidor Microsoft Windows 2000 y un dispositivo Cisco

Contenido

Introducción
Antes de comenzar
Convenciones
Prerequisites
Componentes Utilizados
Diagrama de la red
Configuración de Microsoft Windows 2000 Server para que funcione con dispositivos Cisco
Tareas realizadas
Step-by-Step Instructions
Configuración de los dispositivos de Cisco
Configuración del router Cisco 3640
Configuración de PIX
Configuración del concentrador VPN 3000
Configuración del concentrador VPN 5000
Verificación
Troubleshoot
Comandos para resolución de problemas
Información Relacionada

Introducción

Este documento muestra cómo formar un túnel IPSec con claves previamente compartidas para incorporar dos redes privadas: una red privada (192.168.I.X) dentro de un dispositivo Cisco y una red privada (10.32.50.X) dentro de Microsoft 2000 Server. Suponemos que el tráfico desde dentro del dispositivo Cisco y dentro del servidor 2000 a Internet (representado aquí por las redes 172.18.124.X) se encuentra fluyendo desde antes de comenzar esta configuración.

Puede encontrar información detallada sobre la configuración del servidor de Microsoft Windows 2000 en el sitio Web de Microsoft: http://support.microsoft.com/support/kb/articles/Q252/7/35.ASP

Antes de comenzar

Convenciones

Para obtener más información sobre las convenciones del documento, consulte Convenciones de Consejos Técnicos de Cisco.

Prerequisites

No hay requisitos previos específicos para este documento.

Componentes Utilizados

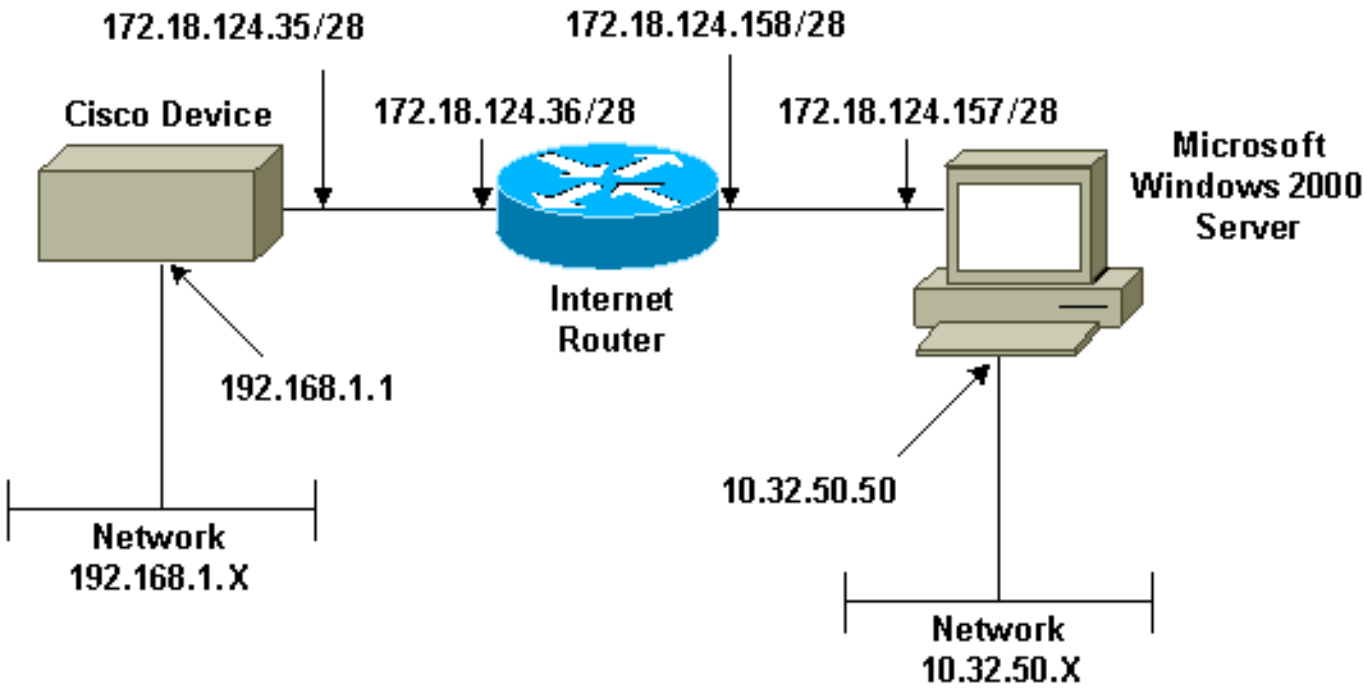
Estas configuraciones fueron desarrolladas y probadas mediante las versiones de software y hardware indicadas a continuación.

- Microsoft Windows 2000 Server 5.00.2195
- Router 3640 de Cisco con la versión c3640-ik2o3s-mz.121-5.T.bin de software del IOS de Cisco.
- Secure PIX Firewall de Cisco con software PIX versión 5.2.1
- Concentrador Cisco VPN 3000 con versión 2.5.2F del software del concentrador VPN 3000
- Concentrador VPN 5000 de Cisco con la Versión 5.2.19 del software del concentrador VPN 5000

La información que se presenta en este documento se originó a partir de dispositivos dentro de un ambiente de laboratorio específico. All of the devices used in this document started with a cleared (default) configuration. Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener un comando antes de ejecutarlo.

Diagrama de la red

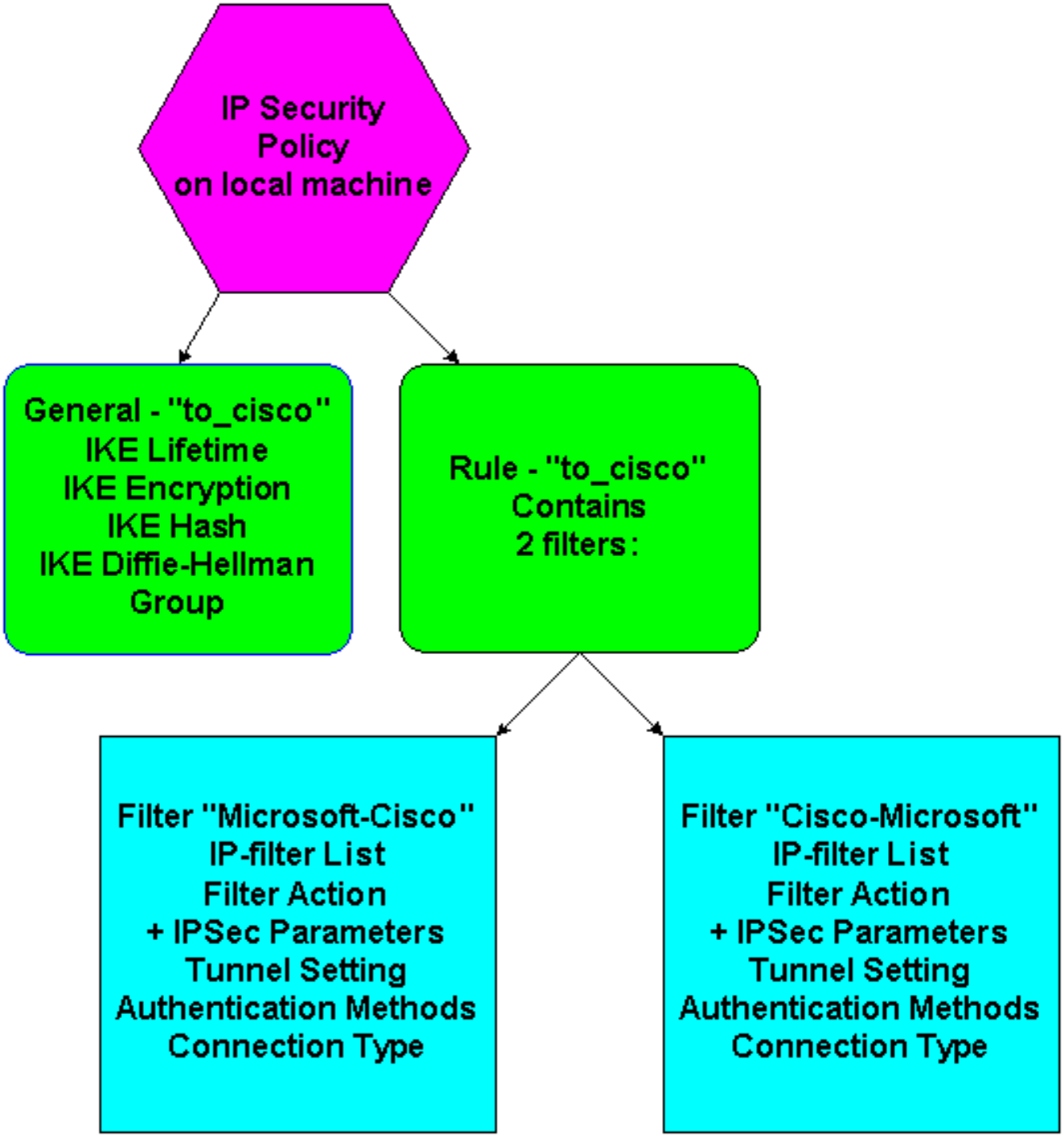
Este documento utiliza la instalación de red que se muestra en el siguiente diagrama.



Configuración de Microsoft Windows 2000 Server para que funcione con dispositivos Cisco

Tareas realizadas

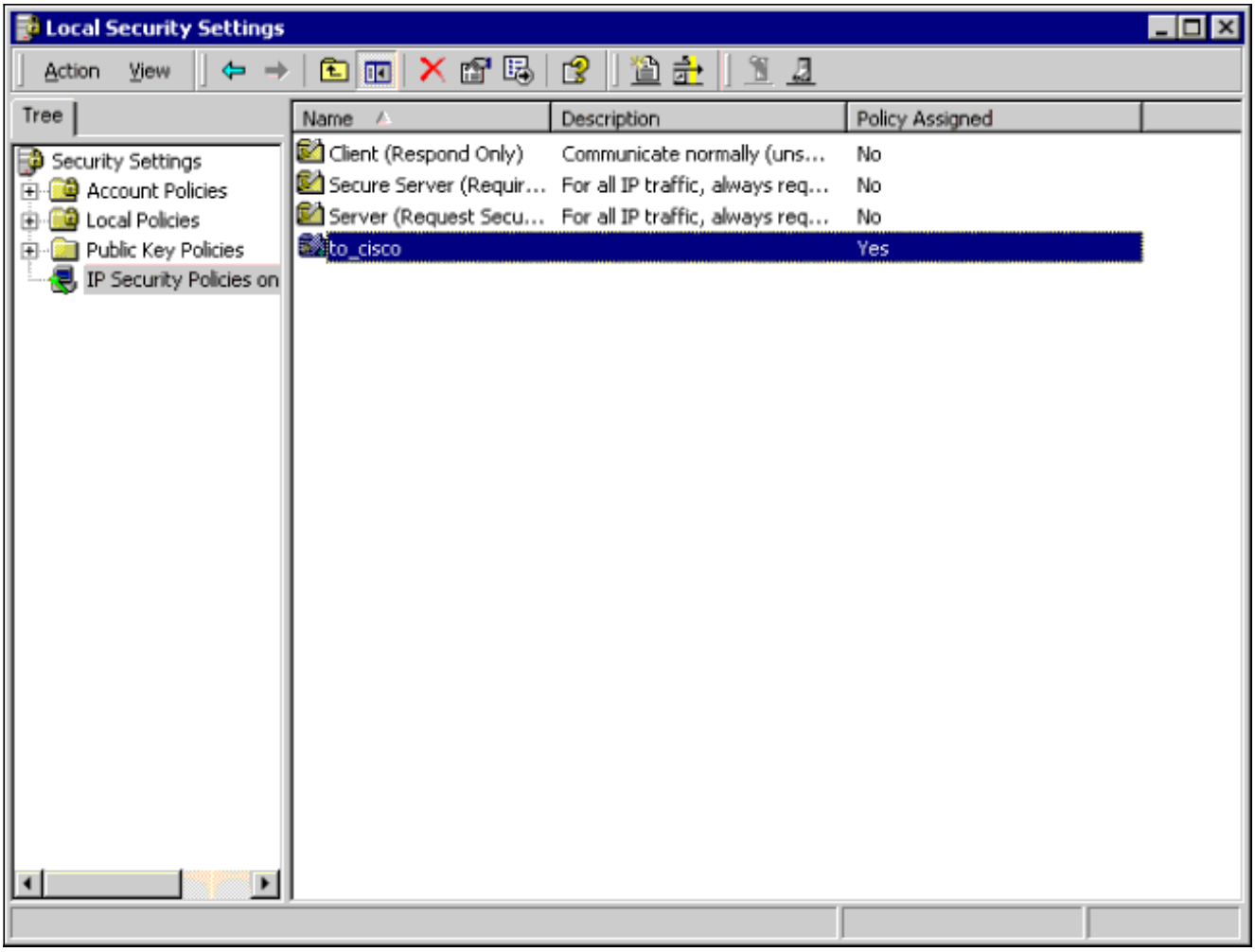
Este diagrama muestra las tareas realizadas en la configuración de Microsoft Windows 2000 Server:



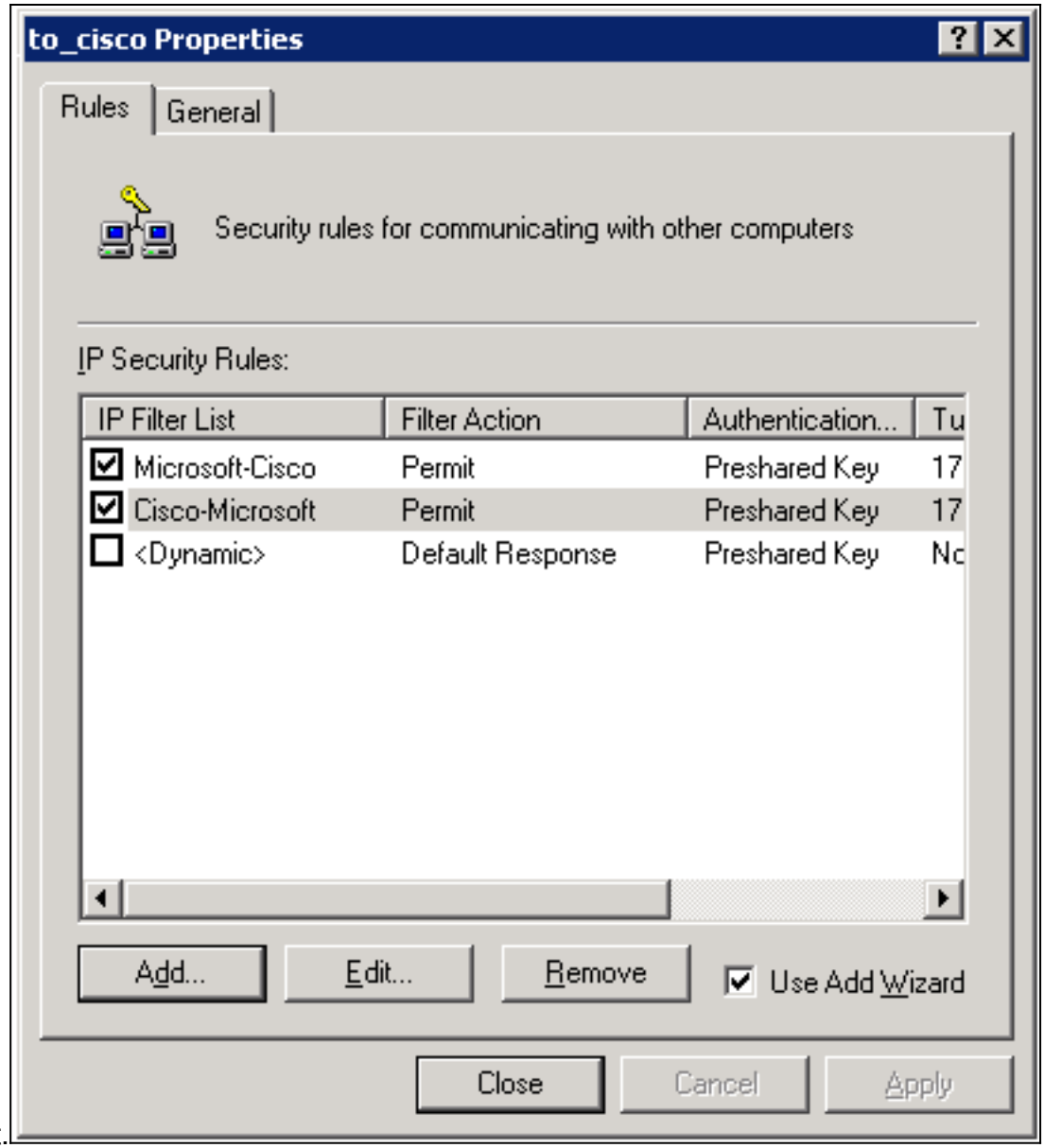
Step-by-Step Instructions

Una vez que haya seguido las instrucciones de configuración en el sitio Web de Microsoft, siga estos pasos para verificar que su configuración pueda funcionar con los dispositivos de Cisco. Los comentarios y cambios se anotan junto a las capturas de pantalla.

1. Haga clic en Start (Inicio) > Run (Ejecutar) > secpol.msc en Microsoft Windows 2000 Server y verifique la información de las siguientes pantallas.Después de utilizar las instrucciones del sitio Web de Microsoft para configurar un servidor 2000, se mostró la siguiente información de túnel.**Nota:** La regla de ejemplo se denomina "to_cisco".

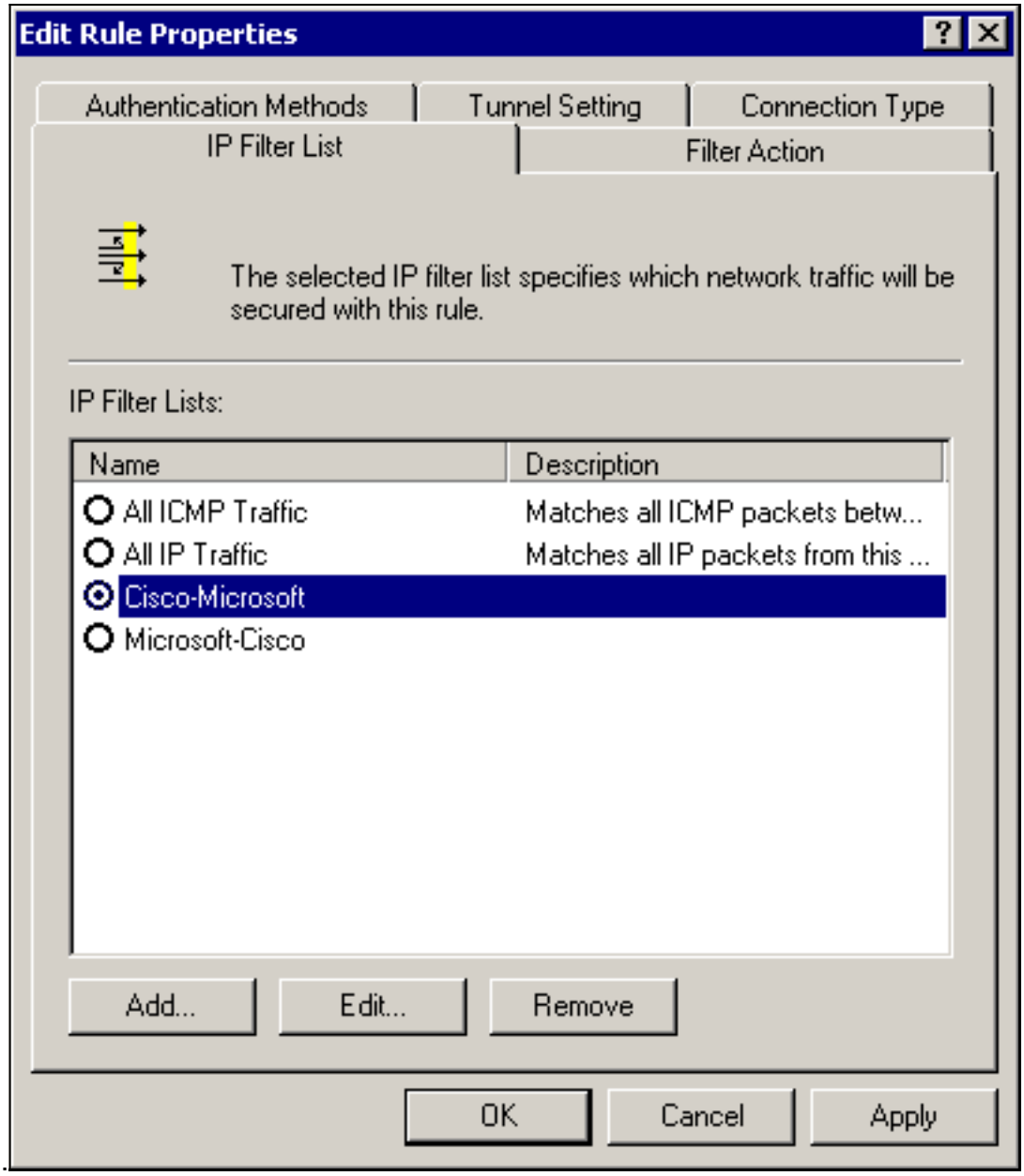


2. Esta regla de ejemplo contiene dos filtros: Microsoft-Cisco y Cisco-



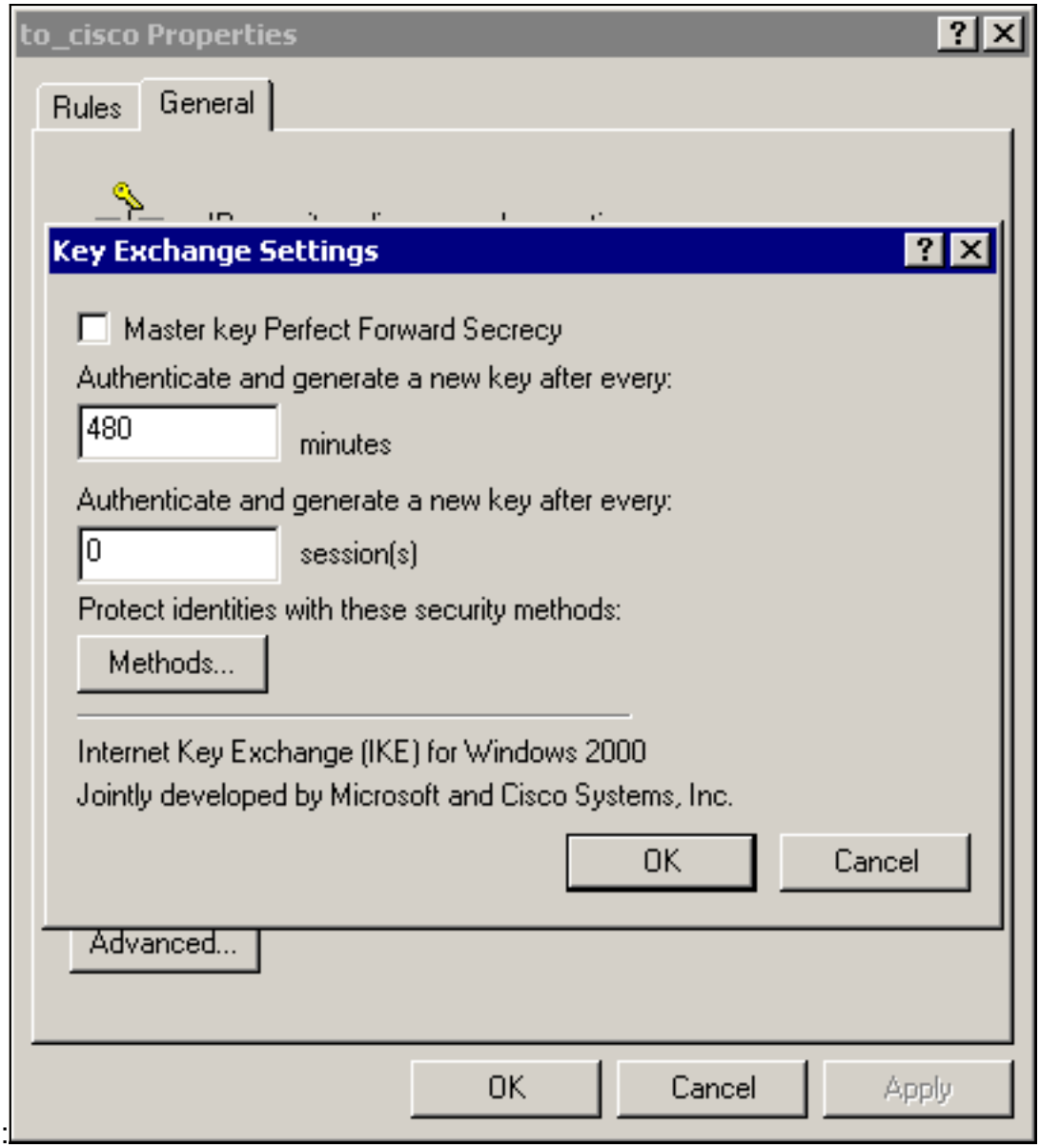
Microsoft.

3. Seleccione la regla de seguridad IP de Cisco-Microsoft y, a continuación, haga clic en **Editar** para ver/agregar/editar las listas de filtros



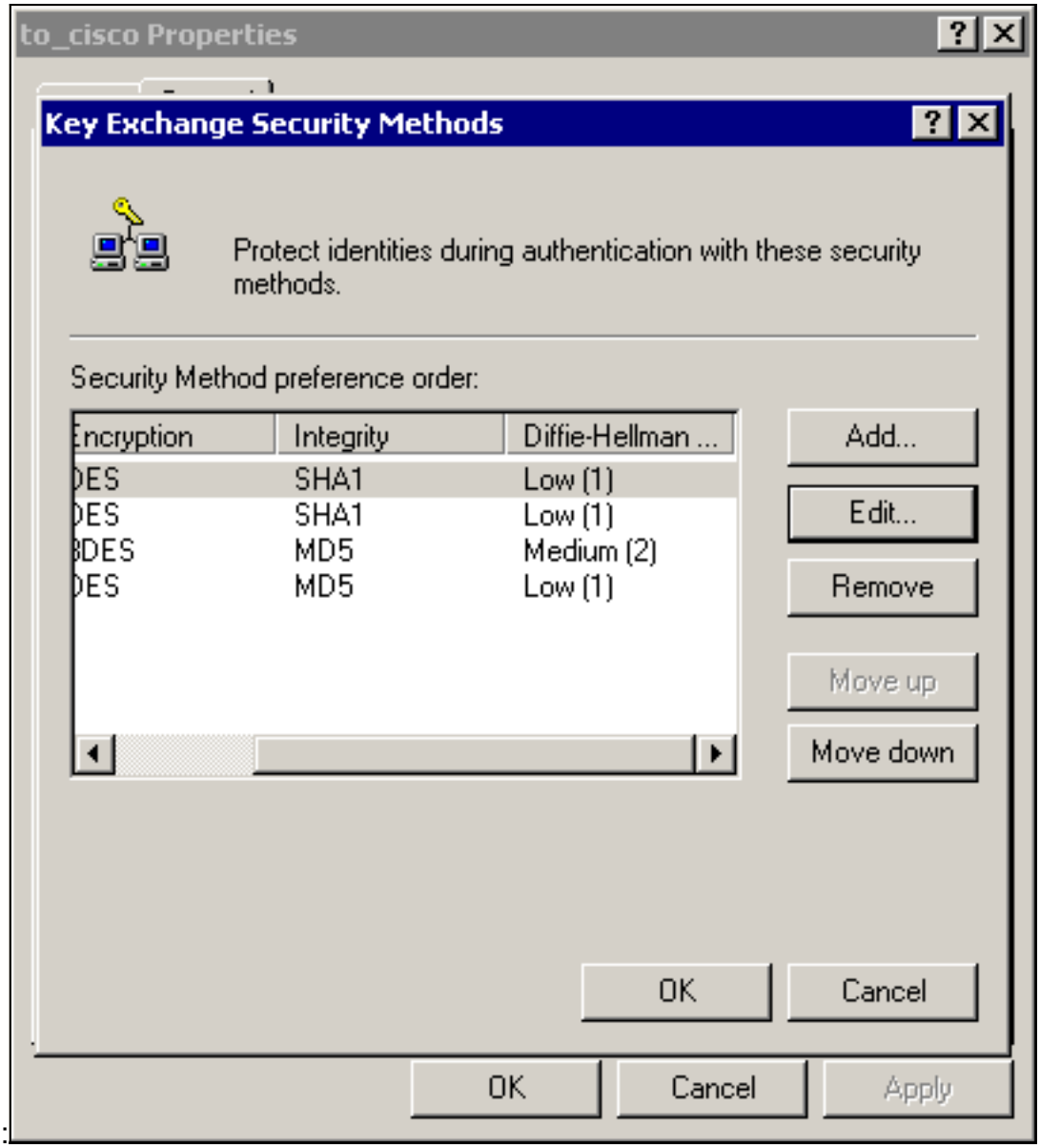
IP.

4. En la regla General > Advanced (Opciones avanzadas) se encuentra la vida útil de IKE (480 minutos = 28800



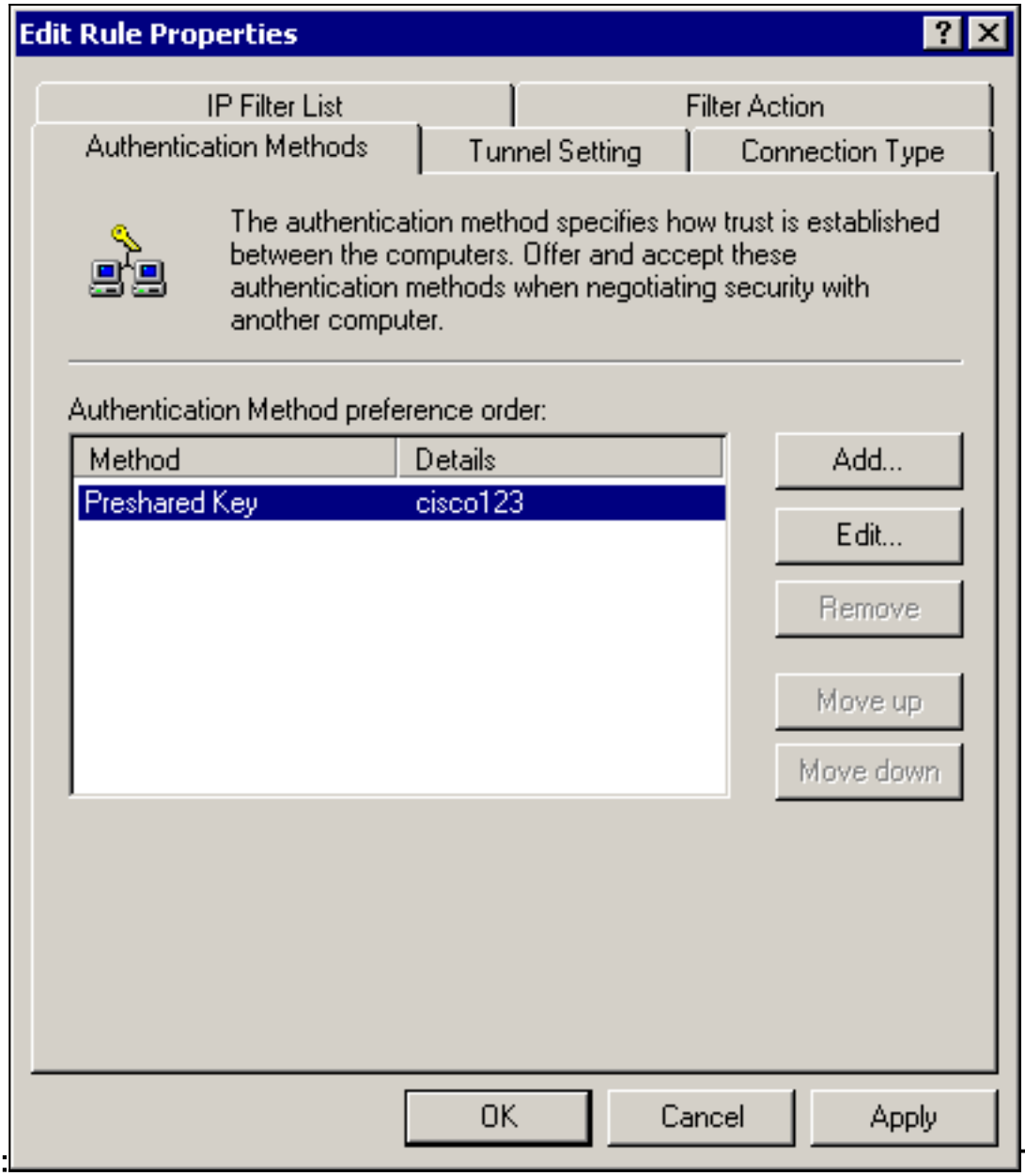
segundos):

5. La ficha General > Advanced (Opciones avanzadas) > Method (Método) de la regla contiene el método de encripción IKE (DES), resumen IKE (SHA1) y el grupo Diffie-Helman

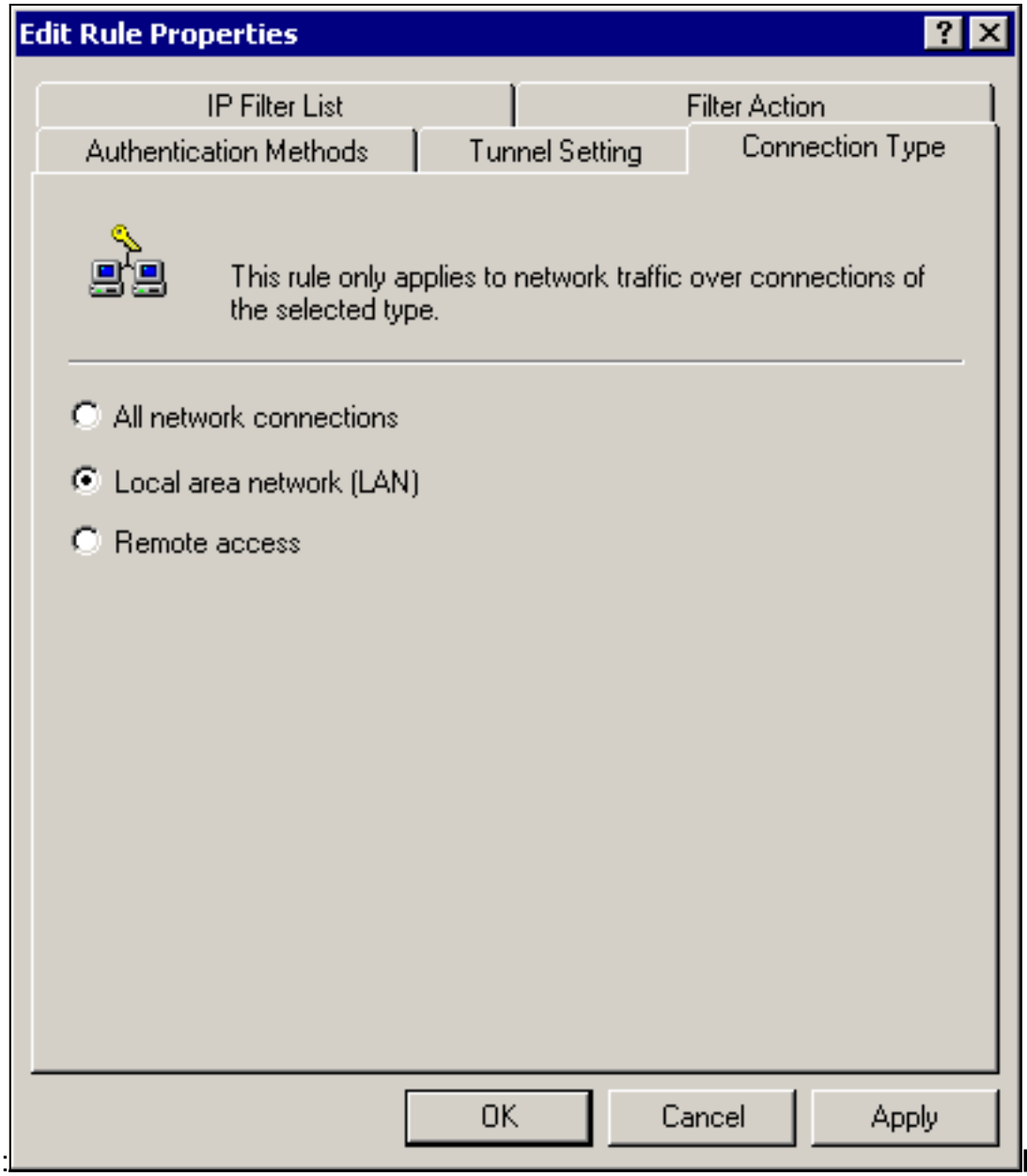


(Bajo(1)):

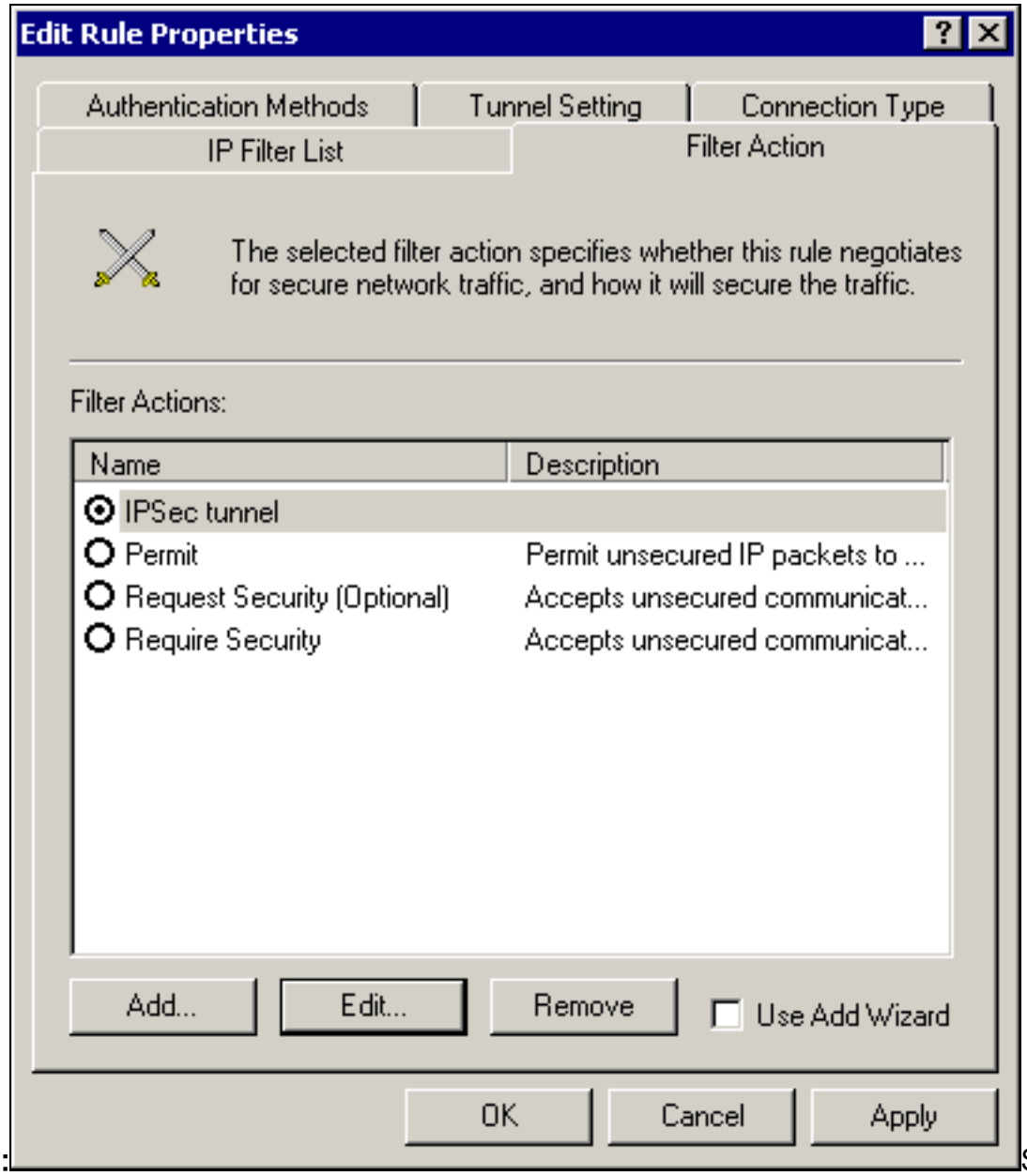
6. Cada filtro tiene 5 fichas:**Métodos de autenticación (claves precompartidas para Internet Key Exchange**



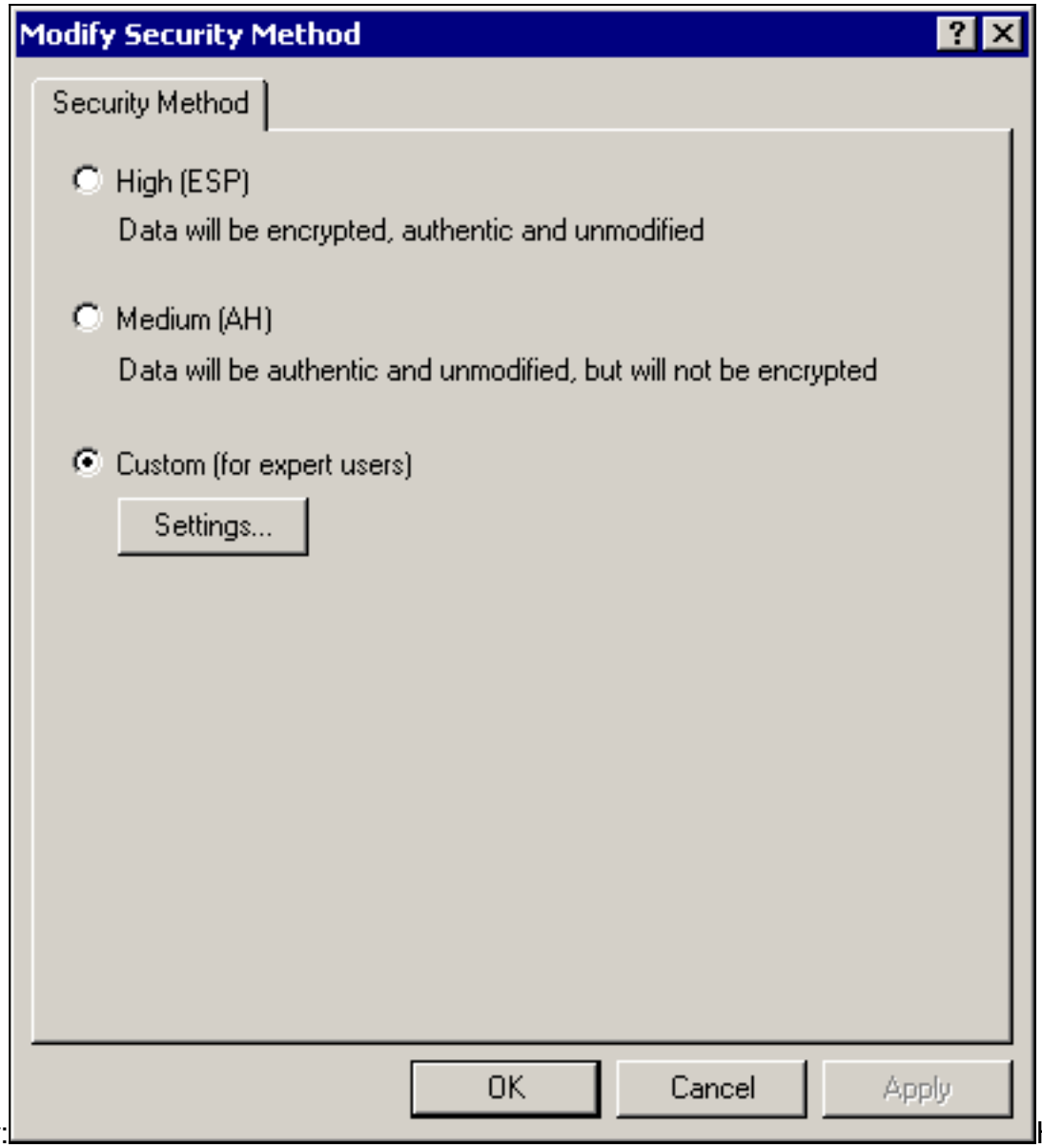
[IKE]): **Tipo de conexión**



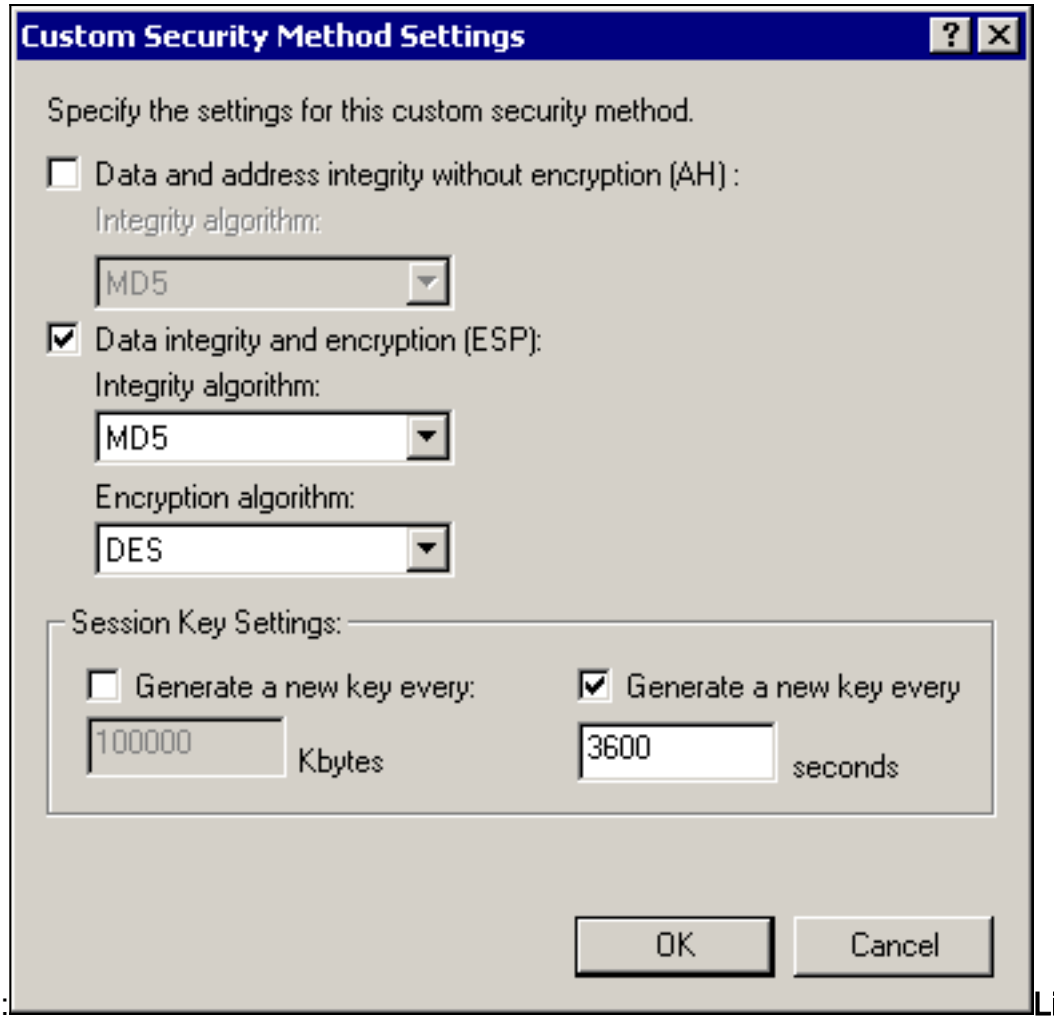
(LAN): **Filtrar acción**



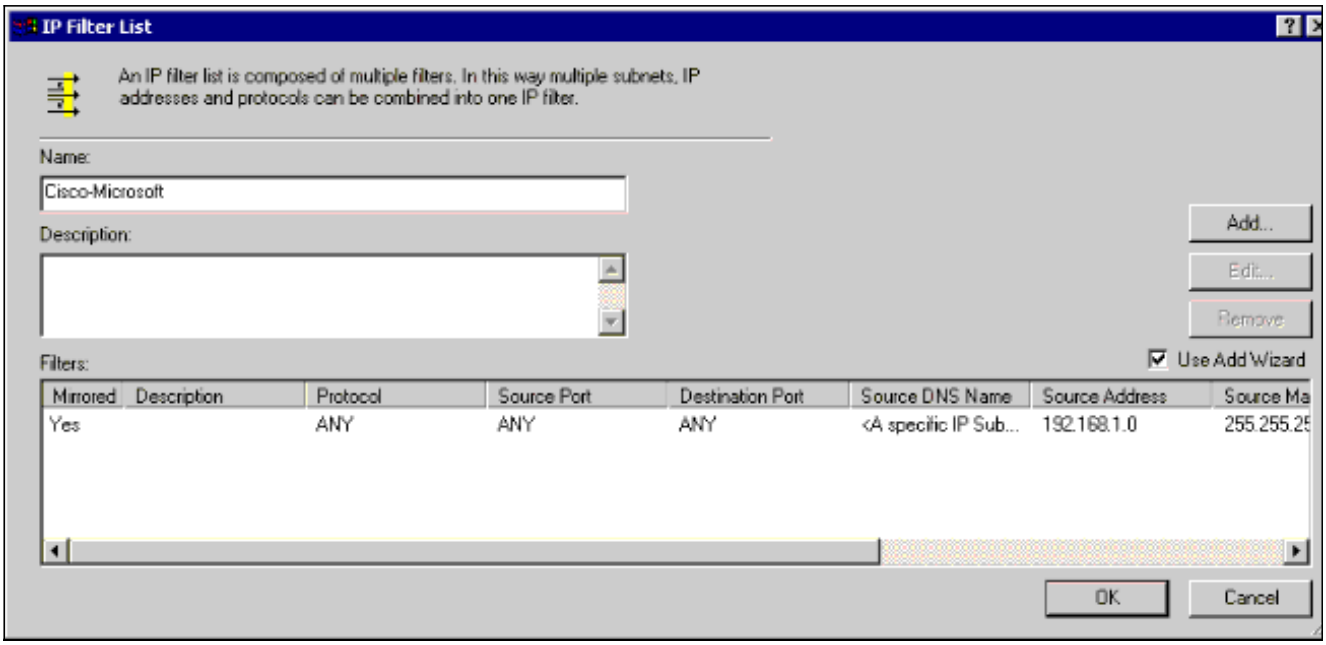
(IPSec): Seleccione Filtrar acción > túnel IPsec > Editar > Editar y haga clic en



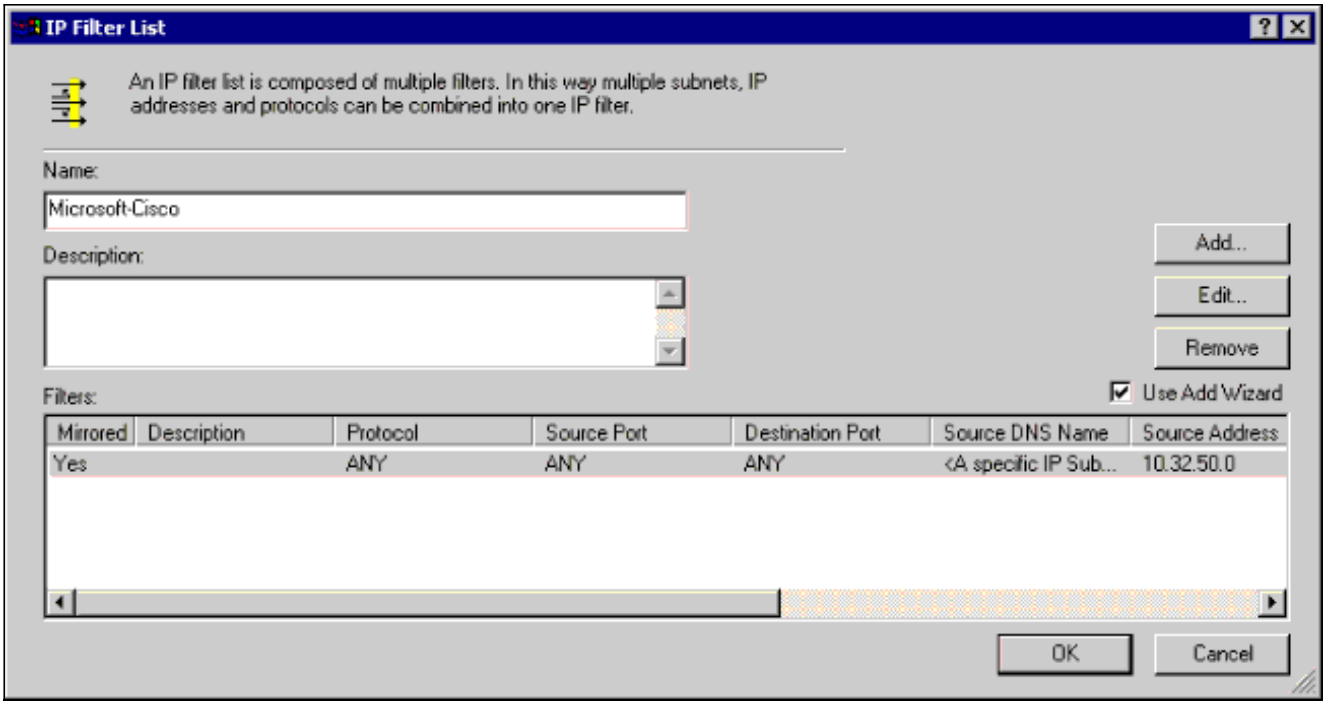
Personalizar: Haga clic en Settings (Configuración) - IPSec transforms (Transformaciones IPSec) e IPSec lifetime (Duración



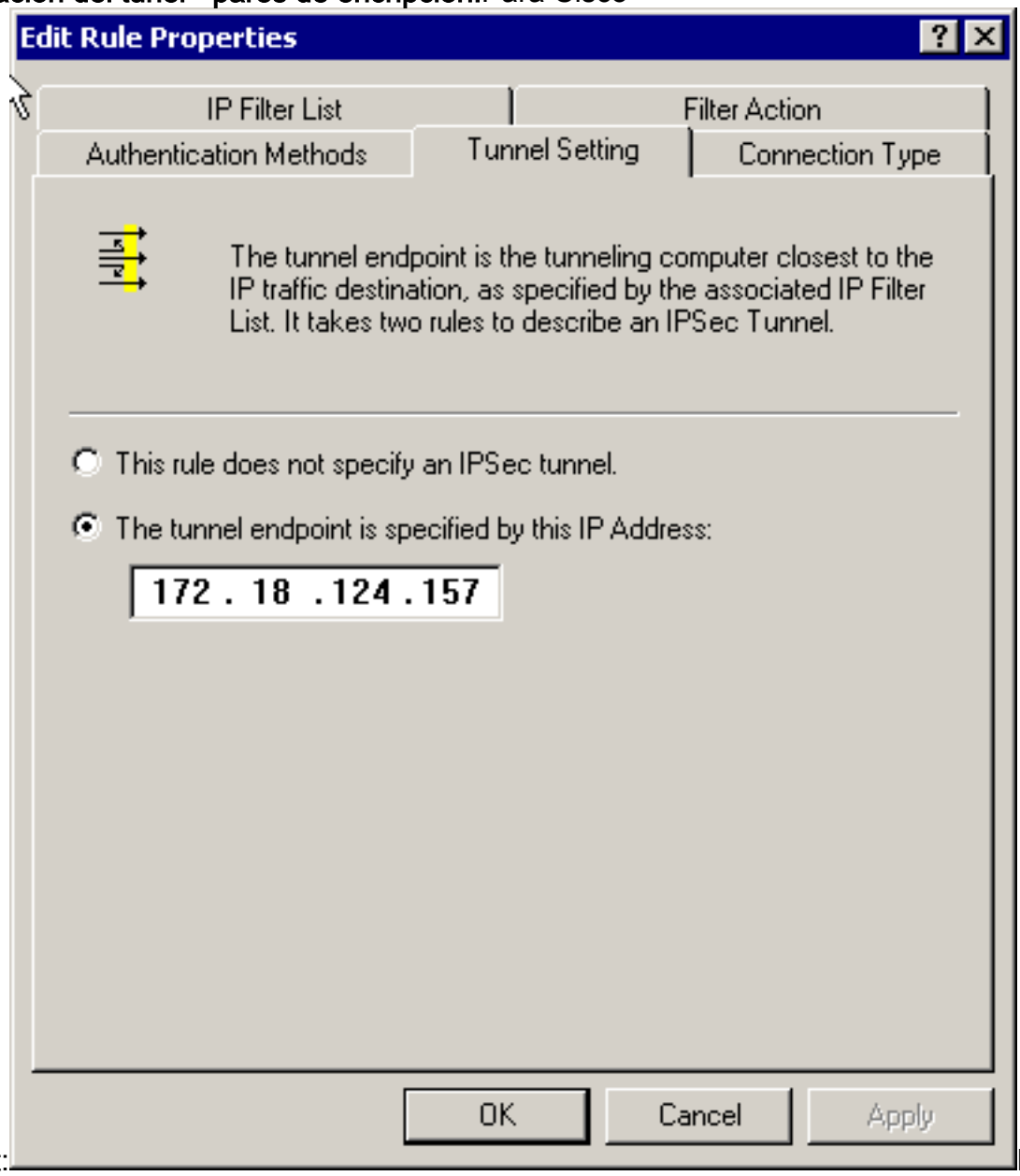
IPSec):**Lista de filtros IP:** redes **de origen** y **destino** que se cifrarán:Para Cisco-Microsoft:



Para Microsoft-Cisco:

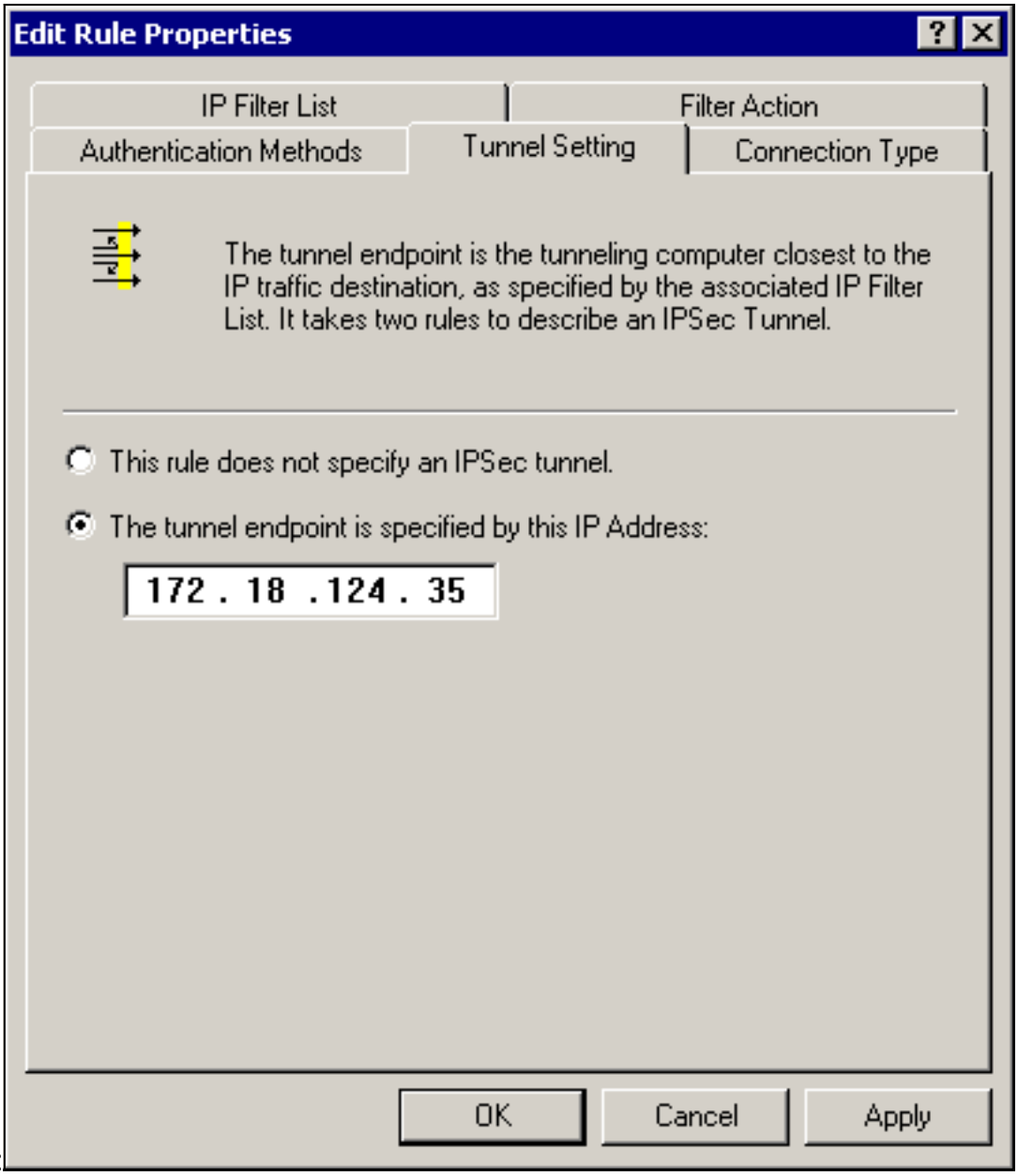


Configuración del túnel - pares de encripción: Para Cisco-



Microsoft:Para

Microsoft-Cisco:



Configuración de los dispositivos de Cisco

Configure el router de Cisco, PIX y los concentradores VPN como se muestra en los siguientes ejemplos.

- Cisco 3640 Router
- PIX
- VPN 3000 Concentrator
- Concentrador VPN 5000

Configuración del router Cisco 3640

Cisco 3640 Router

`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
```

Configuración 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
```

Configuración del concentrador VPN 3000

Utilice las opciones de menú y los parámetros que se muestran a continuación para configurar el concentrador VPN según sea necesario.

- Para agregar una propuesta IKE, seleccione Configuration (Configuración) > System (Sistema) > Tunneling Protocols (Protocolos de tunelización) > IPSec > IKE Proposals (Propuestas IKE) > Add a proposal (Agregar una propuesta).

  ```
  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
  ```

- Para definir el túnel de LAN a LAN, seleccione **Configuration > System > Tunneling Protocols > IPSec LAN a 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
```

- Para modificar la asociación de seguridad, seleccione **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
```

Configuración del concentrador VPN 5000

Concentrador 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.
```

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshoot

Esta sección proporciona información que puede utilizar para resolver problemas de sus

configuraciones.

Comandos para resolución de problemas

La herramienta Output Interpreter (sólo para clientes registrados) permite utilizar algunos comandos “show” y ver un análisis del resultado de estos comandos.

Nota: Antes de ejecutar **comandos debug**, consulte Información Importante sobre Comandos Debug.

Cisco 3640 Router

- **debug crypto engine** - Muestra mensajes de depuración sobre los motores criptográficos, que realizan el cifrado y el descifrado.
- **debug crypto isakmp - Muestra mensajes sobre eventos IKE.**
- **debug crypto ipsec: Muestra eventos de IPSec.**
- **show crypto isakmp sa: muestra todas las asociaciones actuales de seguridad IKE (SA) de un par.**
- **show crypto ipsec sa - Muestra las configuraciones usadas por las asociaciones de seguridad actuales.**
- **clear crypto isakmp** - (del modo de configuración) Borra todas las conexiones IKE activas.
- **clear crypto sa - (en el modo de configuración) Borra todas las asociaciones de seguridad de IPSec.**

PIX

- **debug crypto ipsec - Muestra los IPSec Negotiations de la fase 2.**
- **debug crypto isakmp: muestra las negociaciones de fase 1 del protocolo Asociación de seguridad en Internet y administración de claves (ISAKMP).**
- **debug crypto engine** - Muestra el tráfico cifrado.
- **show crypto ipsec sa - Muestra las asociaciones de seguridad de la fase 2.**
- **show crypto isakmp sa - Muestra las asociaciones de seguridad de la Fase 1.**
- **clear crypto isakmp - (del modo configuración) Limpia las asociaciones de seguridad de Intercambio de clave de Internet (IKE).**
- **clear crypto ipsec sa** - (from configuration mode) Borra las asociaciones de seguridad IPSec.

VPN 3000 Concentrator

- - Inicie la depuración del Concentrador VPN 3000 seleccionando Configuration (Configuración) > System (Sistema) > Events (Eventos) > Classes (Clases) > Modify (Modificar) (Gravedad en el registro=1-13, Gravedad en la consola=1-3): IKE, IKEDBG, IKEDECODE, IPSEC, IPSECDBG, IPSECDECODE
- - El registro de eventos puede borrarse o recuperarse seleccionando Monitoring (Monitoreo) > Event Log (Registro de eventos).
- - El tráfico de túnel de LAN a LAN puede supervisarse en Monitoring (Supervisión) > Sessions (Sesiones).
- - El túnel se puede borrar en **Administración > Administración > Sesiones > Sesiones LAN a**

LAN > Acciones - Cierre de sesión.

Concentrador VPN 5000

- **vpn trace dump all - Muestra información acerca de todas las conexiones de VPN concordantes, incluida la información acerca de la hora, el número VPN, la dirección IP real del par, las secuencias de comandos que se ejecutaron y, en caso de algún error, la rutina y el número de línea del código de software en el que se produjo el error.**
- **show vpn statistics: Muestra la siguiente información para usuarios, socios y el total para ambos.** (En el caso de los modelos modulares, la pantalla incluye una sección para cada ranura del módulo.) Activas actualmente: Las conexiones que están activas actualmente. In Negot – Las conexiones que están siendo negociadas actualmente. Agua alta - Cantidad máxima de conexiones activas al mismo tiempo desde el último reinicio. Total en ejecución - Cantidad total de conexiones correctas desde el último reinicio. Comienzo del túnel - El número de túneles comienza. Túneles correctos – Cantidad de túneles que no presentan errores. Error de túnel – El número de túneles con errores.
- **show vpn statistics verbose – Muestra las estadísticas de negociación ISAKMP y muchas otras estadísticas de conexión activa.**

Información Relacionada

- Anuncio de fin de venta de los concentradores Serie VPN 5000 de Cisco
- Configuración de seguridad de red IPSec
- Configuración del protocolo de seguridad de intercambio de claves de Internet
- Soporte Técnico - Cisco Systems