Contenido

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.

prerrequisitos

No hay requisitos previos específicos para este documento.

Componentes Utilizados

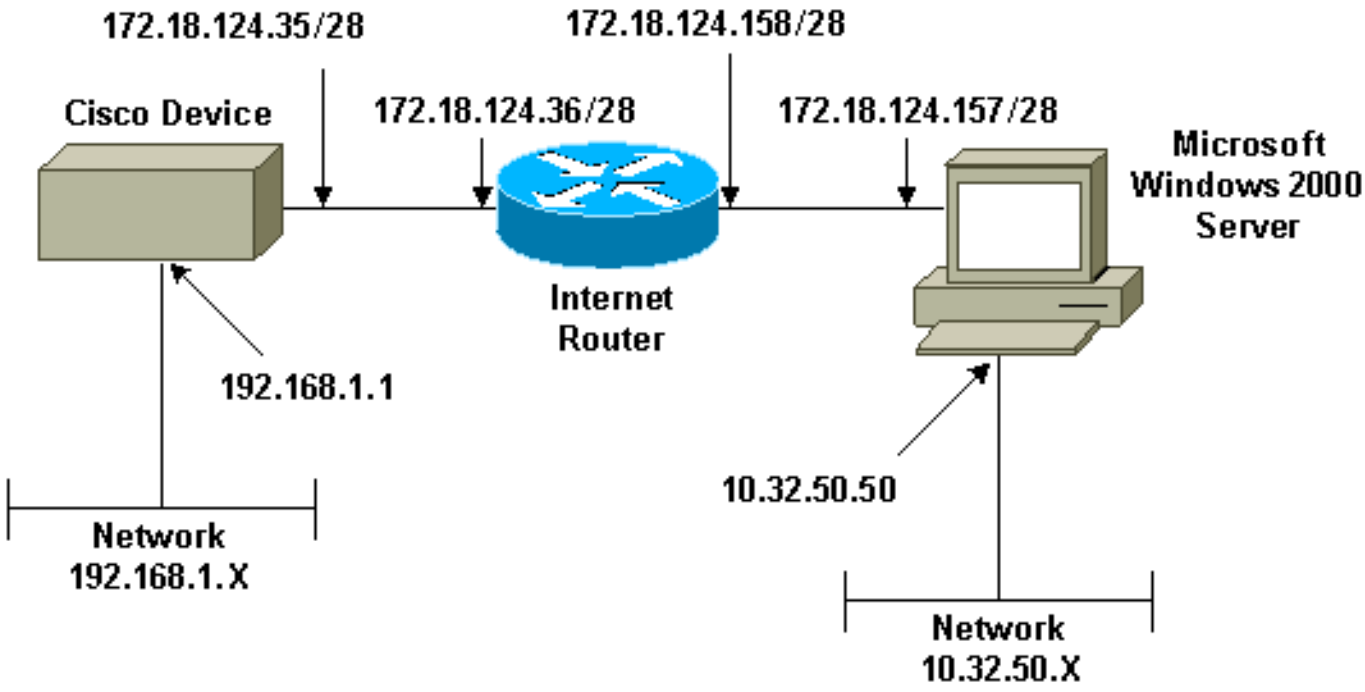
Estas configuraciones fueron desarrolladas y probadas mediante las versiones de software y hardware indicadas a continuación.

- 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. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). 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

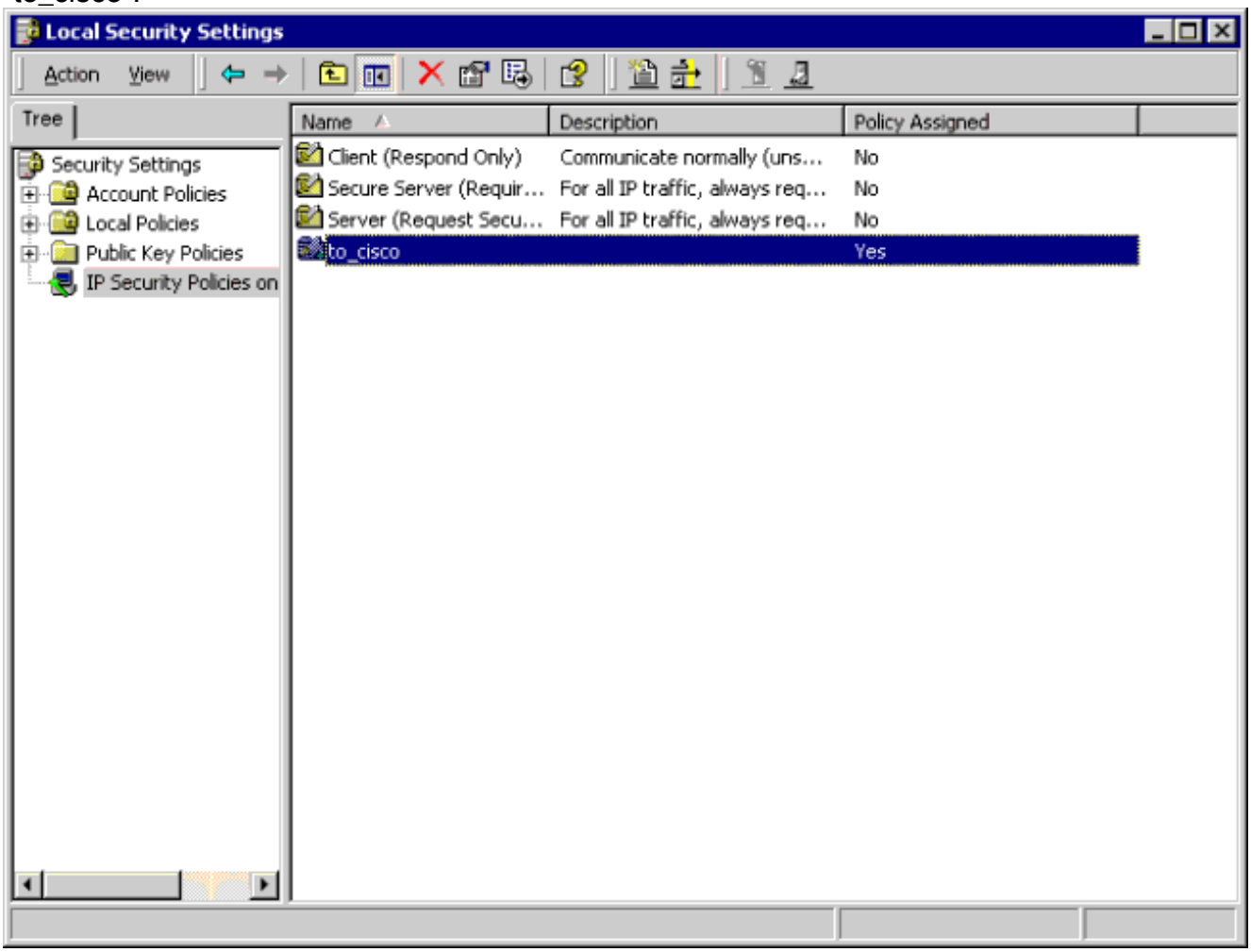
Tareas realizadas

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

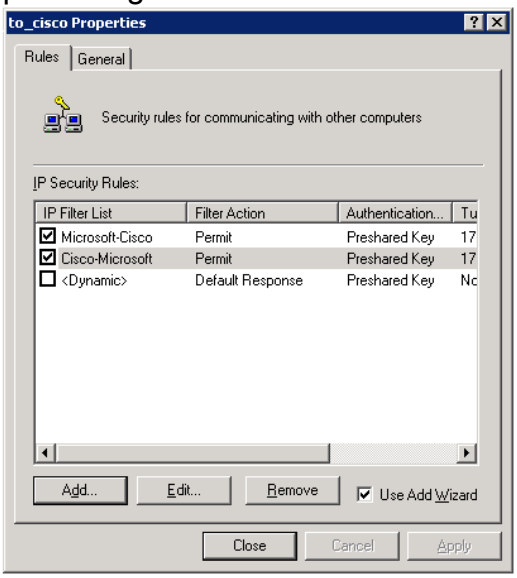
Instrucciones Paso a Paso

Una vez que usted ha seguido Los comentarios y cambios se anotan junto a las capturas de pantalla.

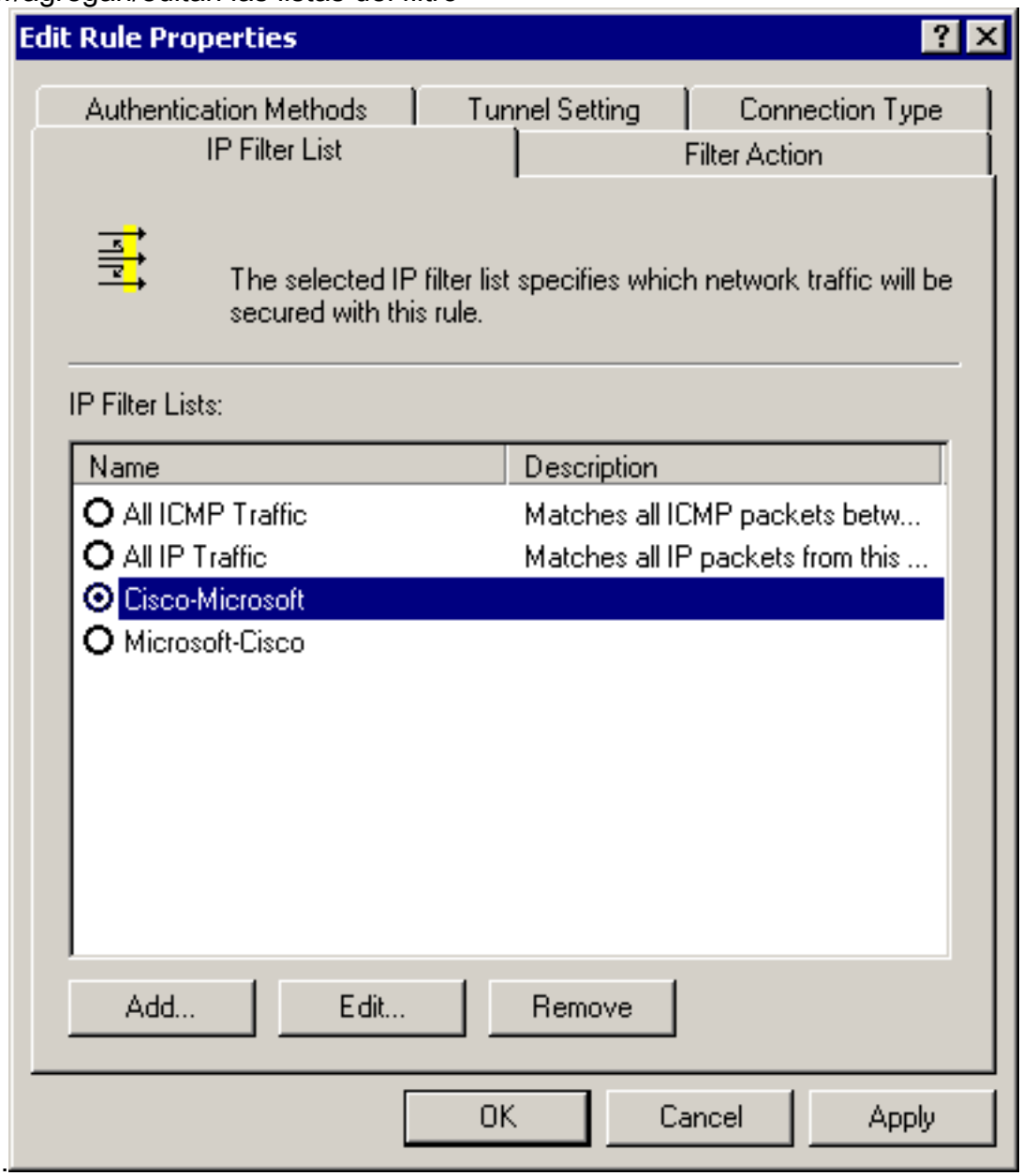
1. Haga clic en Start (Inicio) > Run (Ejecutar) > secpol.msc en Microsoft Windows 2000 Server y verifique la información de las siguientes pantallas.Después de que las instrucciones en el sitio Web de Microsoft fueran utilizadas para configurar los 2000 servidores, la información del túnel siguiente fue visualizada.**Nota:** El ejemplo de regla se llama "to_cisco".



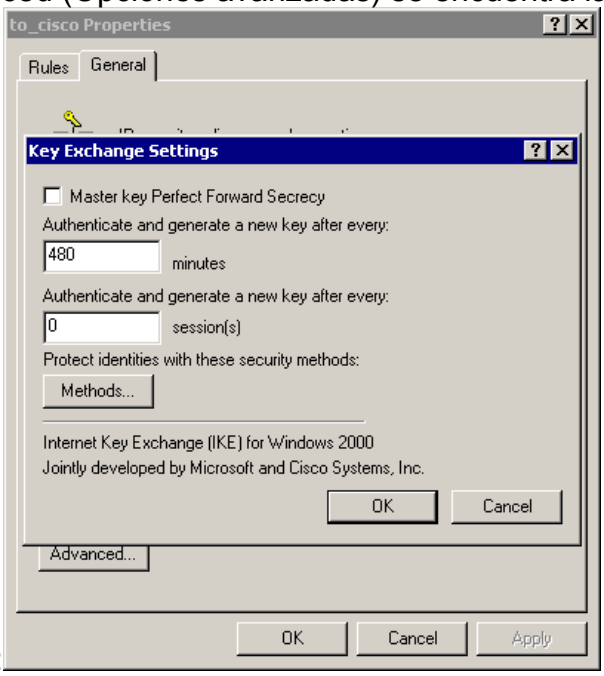
2. Este ejemplo de regla contiene dos filtros: Microsoft-Cisco y Cisco-Microsoft.



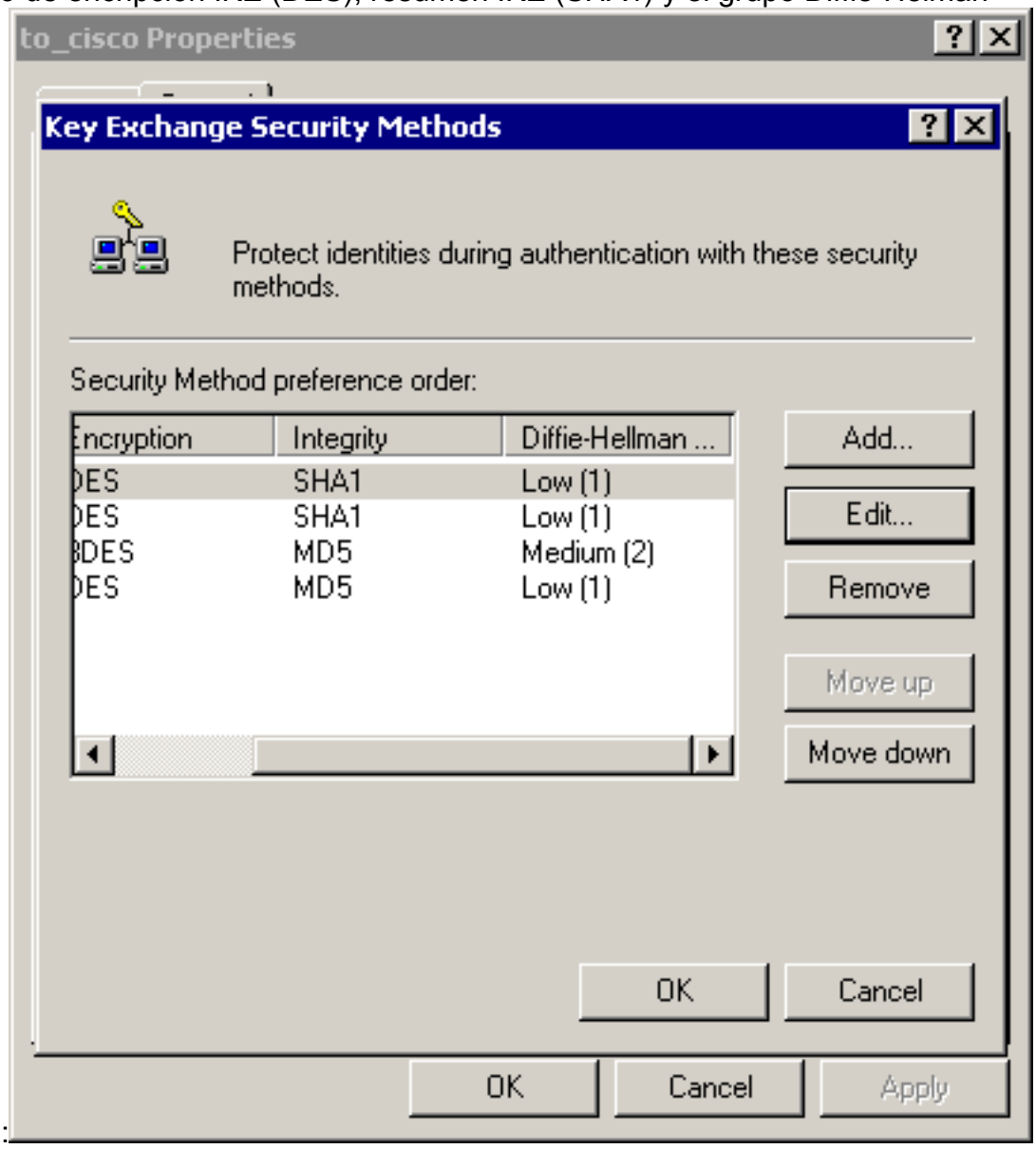
3. Seleccione la regla de seguridad IP de Cisco-Microsoft, después haga clic **editan** para ver/agregan/editan las listas del filtro IP.



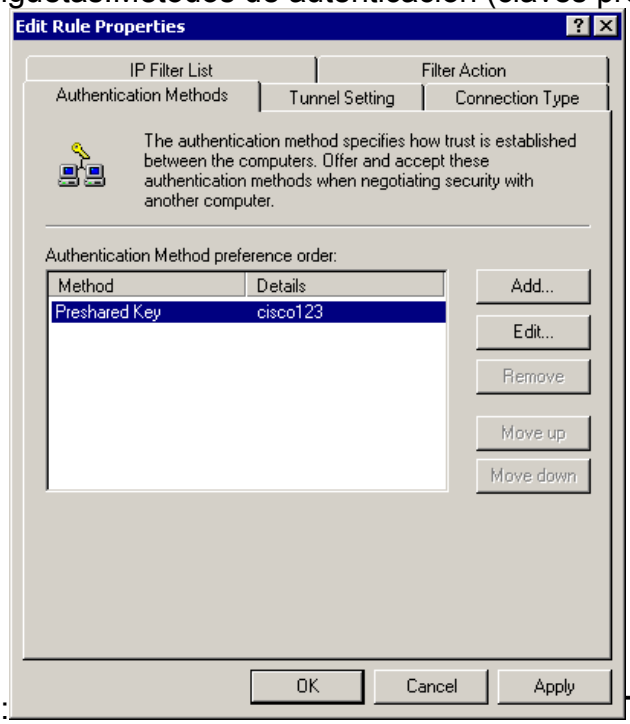
4. En la regla General > Advanced (Opciones avanzadas) se encuentra la vida útil de IKE (480 minutos = 28800 segundos):



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)):

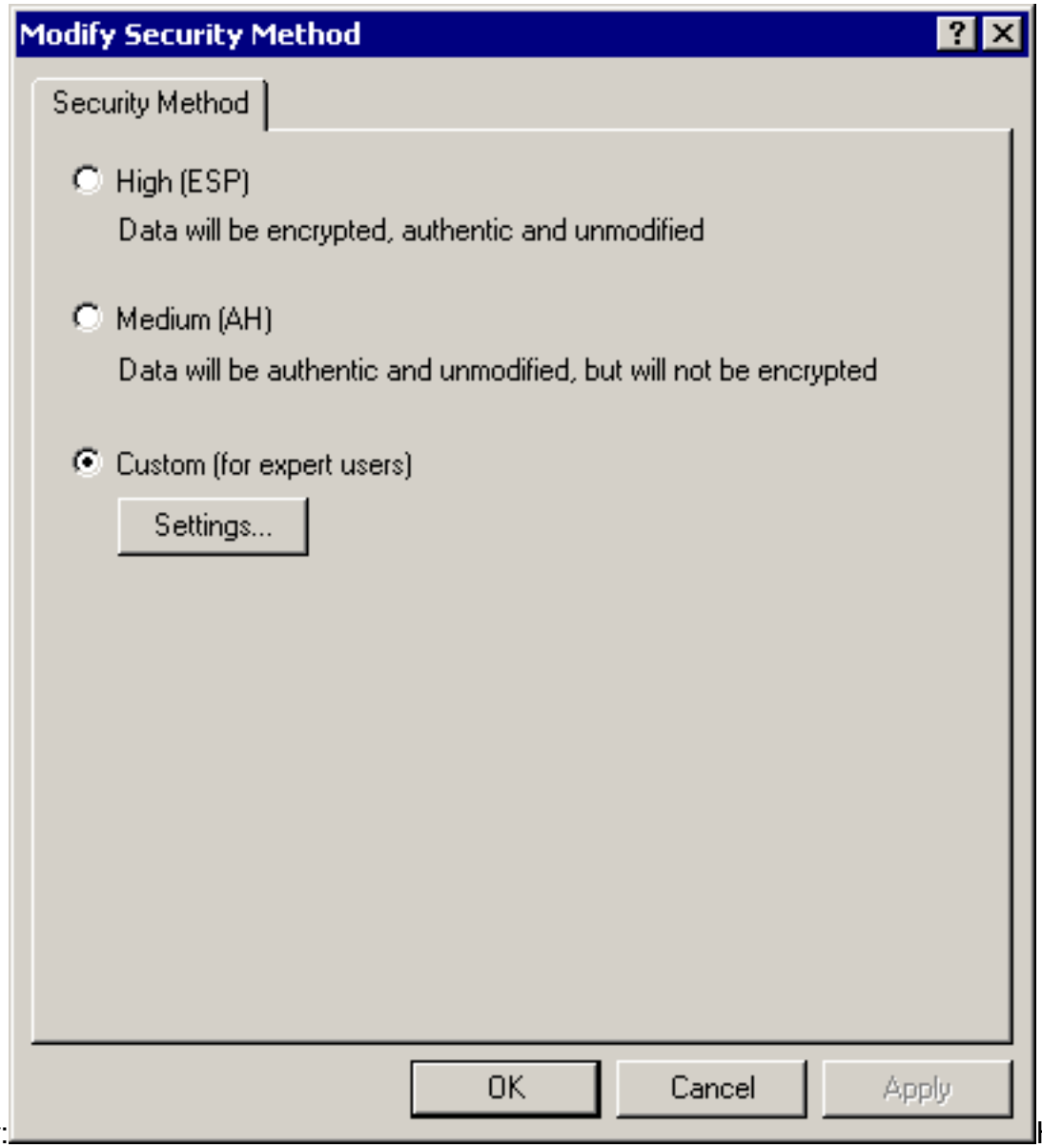


6. Cada filtro tiene 5 lenguetas:Métodos de autenticación (claves precompartidas para Internet Key Exchange [IKE]):

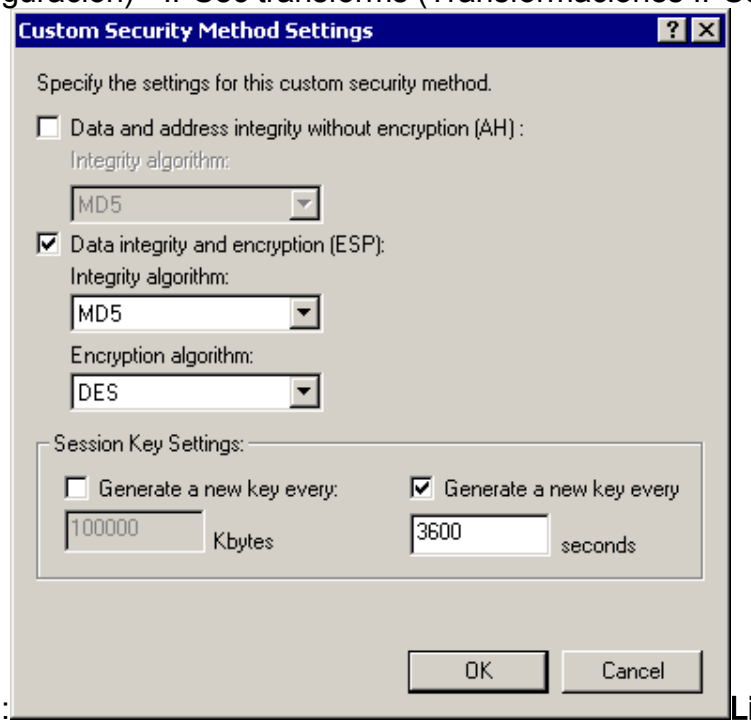


Tipo de conexión

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

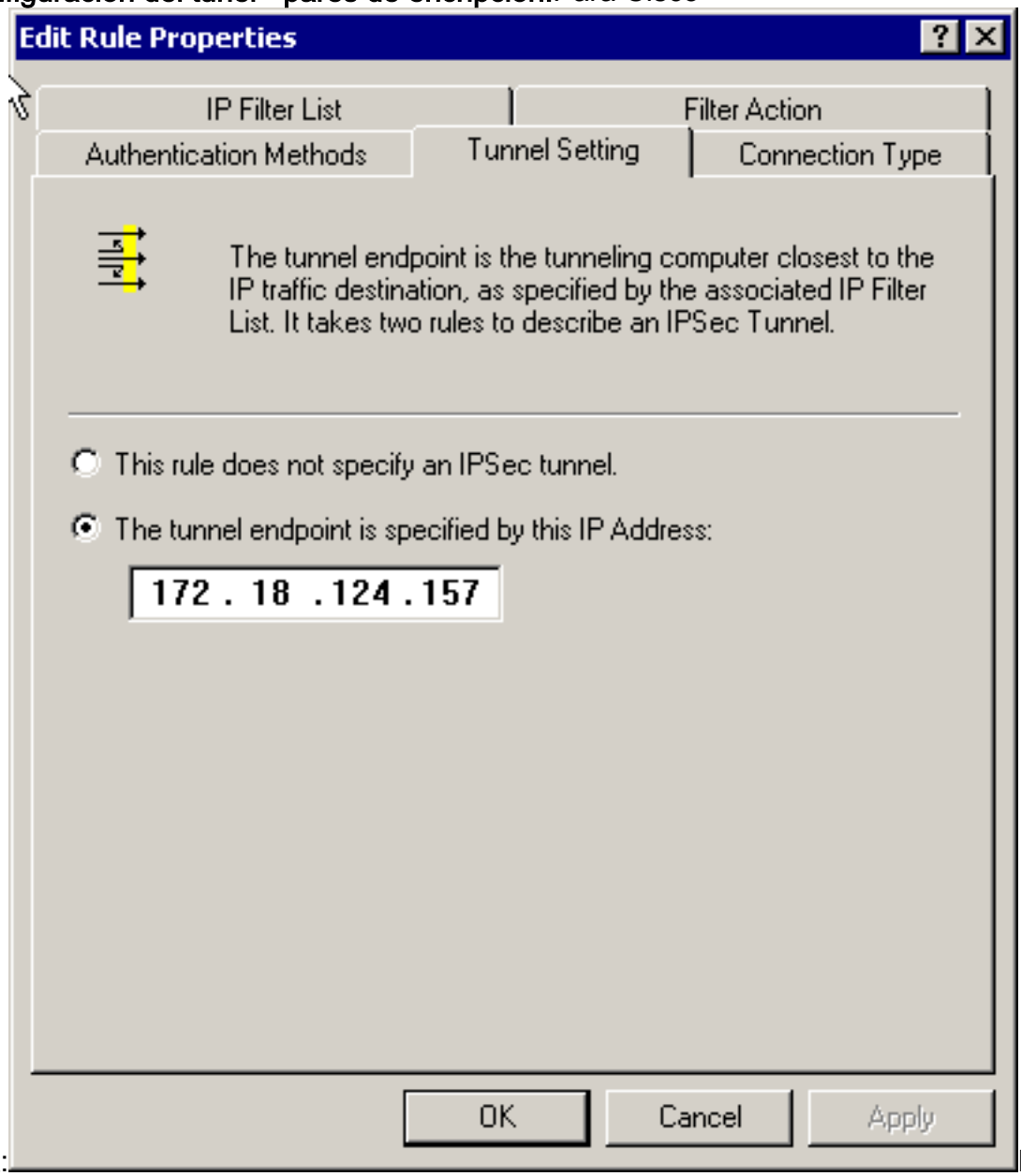


Personalizar:Haga clic en Settings (Configuración) - IPSec transforms (Transformaciones IPSec) e IPSec

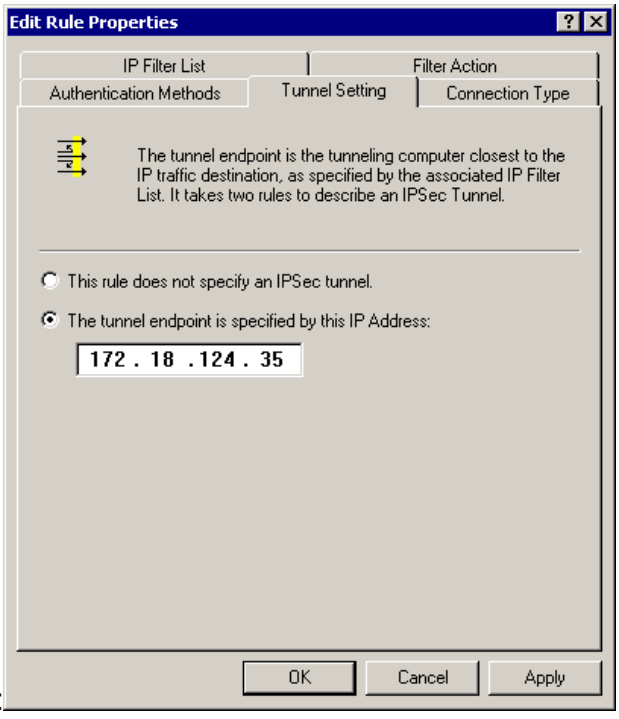


lifetime (Duración IPSec):**Lista del filtro IP**

- fuente y **redes de destino** que se cifrarán:Para Cisco-MicrosoftPara Microsoft-Cisco**Configuración del túnel - pares de encripción:**Para Cisco-Microsoft:



Para Microsoft-Cisco:



Configuración de los dispositivos de Cisco

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

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

Configuración del router Cisco 3640

Cisco 3640 Router

```
Current configuration : 1840 bytes!version 12.1no
service single-slot-reload-enableservice timestamps
debug uptimeservice timestamps log uptimeno service
password-encryption!hostname moss!logging rate-limit
console 10 except errors!ip subnet-zero!no ip finger!ip
audit notify logip audit po max-events 100!crypto isakmp
policy 1!--- The following are IOS defaults so they do
not appear: !--- IKE encryption methodencryption des!---
IKE hashinghash sha!--- Diffie-Hellman groupgroup 1!---
Authentication methodauthentication pre-share!--- IKE
lifetimelifetime 28800!--- encryption peercrypto isakmp
key cisco123 address 172.18.124.157!!--- The following
is the IOS default so it does not appear: !--- IPSec
lifetimecrypto ipsec security-association lifetime
seconds 3600!--- IPSec transformscrypto ipsec
transform-set rtpset esp-des esp-md5-hmac !crypto map
rtp 1 ipsec-isakmp !--- Encryption peerset peer
172.18.124.157set transform-set rtpset !---
Source/Destination networks definedmatch address
115!call rsvp-sync!interface Ethernet0/0ip address
192.168.1.1 255.255.255.0ip nat insidehalf-
duplex!interface Ethernet0/1ip address 172.18.124.35
255.255.255.240ip nat outsidehalf-duplexcrypto map
rtp!ip nat pool INTERNET 172.18.124.35 172.18.124.35
netmask 255.255.255.240ip nat inside source route-map
nonat pool INTERNETip classlessip route 0.0.0.0 0.0.0.0
172.18.124.36no ip http server!access-list 101 deny ip
192.168.1.0 0.0.0.255 10.32.50.0 0.0.0.255access-list
101 permit ip 192.168.1.0 0.0.0.255 any!---
Source/Destination networks definedaccess-list 115
permit ip 192.168.1.0 0.0.0.255 10.32.50.0
0.0.0.255access-list 115 deny ip 192.168.1.0 0.0.0.255
anyroute-map nonat permit 10match ip address 101!line
con 0transport input noneline 65 94line aux 0line vty 0
4!end
```

Configuración de PIX

PIX

```
PIX Version 5.2(1)nameif ethernet0 outside
security0nameif ethernet1 inside security100enable
password 8Ry2YjIyt7RRXU24 encryptedpasswd
2KFQnbNIdI.2KYOU encryptedhostname pixfirewallfixup
```

```
protocol ftp 21fixup protocol http 80fixup protocol h323
1720fixup protocol rsh 514fixup protocol smtp 25fixup
protocol sqlnet 1521fixup protocol sip 5060names!---
Source/Destination networks definedaccess-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 24logging onno logging
timestampno logging standbyno logging consoleno logging
monitorno logging bufferedno logging trapno logging
historylogging facility 20logging queue 512interface
ethernet0 autointerface ethernet1 10basetmtu outside
1500mtu inside 1500ip address outside 172.18.124.35
255.255.255.240ip address inside 192.168.1.1
255.255.255.0ip audit info action alarmip audit attack
action alarmno failoverfailover timeout 0:00:00failover
poll 15failover ip address outside 0.0.0.0failover ip
address inside 0.0.0.0arp timeout 14400!--- Except
Source/Destination from Network Address Translation
(NAT):nat (inside) 0 access-list 115route outside
0.0.0.0 0.0.0.0 172.18.124.36 1timeout xlate
3:00:00timeout conn 1:00:00 half-closed 0:10:00 udp
0:02:00 rpc 0:10:00 h323 0:05:00sip 0:30:00 sip_media
0:02:00timeout uauth 0:05:00 absoluteaaa-server TACACS+
protocol tacacs+ aaa-server RADIUS protocol radius no
snmp-server locationno snmp-server contactsnmp-server
community publicno snmp-server enable trapsfloodguard
enablesysopt connection permit-ipsecno sysopt route
dnat!--- IPSec transformscrypto ipsec transform-set
myset esp-des esp-md5-hmac !--- IPSec lifetimecrypto
ipsec security-association lifetime seconds 3600crypto
map rtpmap 10 ipsec-isakmp!--- Source/Destination
networkscrypto map rtpmap 10 match address 115!---
Encryption peercrypto map rtpmap 10 set peer
172.18.124.157 crypto map rtpmap 10 set transform-set
mysetcrypto map rtpmap interface outsideisakmp enable
outside!--- Encryption peerisakmp key ******** address
172.18.124.157 netmask 255.255.255.240 isakmp identity
address!--- Authentication methodisakmp policy 10
authentication pre-share!--- IKE encryption methodisakmp
policy 10 encryption des!--- IKE hashingisakmp policy 10
hash sha!--- Diffie-Hellman groupisakmp policy 10 group
1!--- IKE lifetimeisakmp policy 10 lifetime 28800telnet
timeout 5ssh timeout 5terminal width
80Cryptochecksum:c237ed11307abea7b530bbd0c2b2ec08: end
```

Configuración del concentrador VPN 3000

Utilice las opciones de menú y los parámetros mostrados abajo para configurar el concentrador VPN según las necesidades.

- 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).PIX Version 5.2(1)nameif ethernet0 outside security0nameif ethernet1 inside security100enable password 8Ry2YjIyt7RRXU24 encryptedpasswd 2KFQnbNIdI.2KYOU encryptedhostname pixfirewallfixup protocol ftp 21fixup protocol http 80fixup protocol h323 1720fixup protocol rsh 514fixup protocol smtp 25fixup protocol sqlnet 1521fixup protocol sip 5060names!--- Source/Destination networks definedaccess-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 24logging onno logging timestampno logging standbyno logging consoleno logging monitorno logging bufferedno logging trapno logging historylogging facility 20logging queue

```
512interface ethernet0 autointerface ethernet1 10basetmtu outside 1500mtu inside 1500ip
address outside 172.18.124.35 255.255.255.240ip address inside 192.168.1.1 255.255.255.0ip
audit info action alarmip audit attack action alarmno failoverfailover timeout
0:00:00failover poll 15failover ip address outside 0.0.0.0failover ip address inside
0.0.0.0arp timeout 14400!--- Except Source/Destination from Network Address Translation
(NAT):nat (inside) 0 access-list 115route outside 0.0.0.0 0.0.0.0 172.18.124.36 1timeout
xlate 3:00:00timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h323
0:05:00sip 0:30:00 sip_media 0:02:00timeout uauth 0:05:00 absoluteaaa-server TACACS+
protocol tacacs+ aaa-server RADIUS protocol radius no snmp-server locationno snmp-server
contactsnmp-server community publicno snmp-server enable trapsfloodguard enablesysopt
connection permit-ipsecno sysopt route dnat!--- IPSec transformscrypto ipsec transform-set
myset esp-des esp-md5-hmac !--- IPSec lifetimecrypto ipsec security-association lifetime
seconds 3600crypto map rtpmap 10 ipsec-isakmp!--- Source/Destination networkscrypto map
rtpmap 10 match address 115!--- Encryption peercrypto map rtpmap 10 set peer 172.18.124.157
crypto map rtpmap 10 set transform-set mysetcrypto map rtpmap interface outsideisakmp enable
outside!--- Encryption peerisakmp key ******** address 172.18.124.157 netmask
255.255.255.240 isakmp identity address!--- Authentication methodisakmp policy 10
authentication pre-share!--- IKE encryption methodisakmp policy 10 encryption des!--- IKE
hashingisakmp policy 10 hash sha!--- Diffie-Hellman groupisakmp policy 10 group 1!--- IKE
lifetimeisakmp policy 10 lifetime 28800telnet timeout 5ssh timeout 5terminal width
80Cryptochecksum:c237ed11307abea7b530bbd0c2b2ec08: end
```

- Para definir el túnel de LAN a LAN, seleccione el **Configuration (Configuración) > System (Sistema) > Tunneling Protocols (Protocolos de tunelización) > IPSec LAN-to-LAN (IPSec de LAN a LAN).**

```
PIX Version 5.2(1)nameif ethernet0 outside security0nameif ethernet1 inside
security100enable password 8Ry2YjIyt7RRXU24 encryptedpasswd 2KFQnbNIdI.2KYOU
encryptedhostname pixfirewallfixup protocol ftp 21fixup protocol http 80fixup protocol h323
1720fixup protocol rsh 514fixup protocol smtp 25fixup protocol sqlnet 1521fixup protocol sip
5060names!--- Source/Destination networks definedaccess-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 24logging onno logging timestampno logging standbyno logging consoleno logging
monitorno logging bufferedno logging trapno logging historylogging facility 20logging queue
512interface ethernet0 autointerface ethernet1 10basetmtu outside 1500mtu inside 1500ip
address outside 172.18.124.35 255.255.255.240ip address inside 192.168.1.1 255.255.255.0ip
audit info action alarmip audit attack action alarmno failoverfailover timeout
0:00:00failover poll 15failover ip address outside 0.0.0.0failover ip address inside
0.0.0.0arp timeout 14400!--- Except Source/Destination from Network Address Translation
(NAT):nat (inside) 0 access-list 115route outside 0.0.0.0 0.0.0.0 172.18.124.36 1timeout
xlate 3:00:00timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h323
0:05:00sip 0:30:00 sip_media 0:02:00timeout uauth 0:05:00 absoluteaaa-server TACACS+
protocol tacacs+ aaa-server RADIUS protocol radius no snmp-server locationno snmp-server
contactsnmp-server community publicno snmp-server enable trapsfloodguard enablesysopt
connection permit-ipsecno sysopt route dnat!--- IPSec transformscrypto ipsec transform-set
myset esp-des esp-md5-hmac !--- IPSec lifetimecrypto ipsec security-association lifetime
seconds 3600crypto map rtpmap 10 ipsec-isakmp!--- Source/Destination networkscrypto map
rtpmap 10 match address 115!--- Encryption peercrypto map rtpmap 10 set peer 172.18.124.157
crypto map rtpmap 10 set transform-set mysetcrypto map rtpmap interface outsideisakmp enable
outside!--- Encryption peerisakmp key ******** address 172.18.124.157 netmask
255.255.255.240 isakmp identity address!--- Authentication methodisakmp policy 10
authentication pre-share!--- IKE encryption methodisakmp policy 10 encryption des!--- IKE
hashingisakmp policy 10 hash sha!--- Diffie-Hellman groupisakmp policy 10 group 1!--- IKE
lifetimeisakmp policy 10 lifetime 28800telnet timeout 5ssh timeout 5terminal width
80Cryptochecksum:c237ed11307abea7b530bbd0c2b2ec08: end
```

- Para modificar la asociación de seguridad, seleccione el **Configuration (Configuración) > Policy Management (Administración de políticas) > Management Traffic (Tráfico de administración) > Security Associations (Asociaciones de seguridad) > Modify (Modificar).**

```
PIX Version 5.2(1)nameif ethernet0 outside security0nameif ethernet1 inside security100enable
password 8Ry2YjIyt7RRXU24 encryptedpasswd 2KFQnbNIdI.2KYOU encryptedhostname
pixfirewallfixup protocol ftp 21fixup protocol http 80fixup protocol h323 1720fixup protocol
rsh 514fixup protocol smtp 25fixup protocol sqlnet 1521fixup protocol sip 5060names!---
Source/Destination networks definedaccess-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
24logging onno logging timestampno logging standbyno logging consoleno logging monitorno
```

```
logging bufferedno logging trapno logging historylogging facility 20logging queue
512interface ethernet0 autointerface ethernet1 10basetmtu outside 1500mtu inside 1500ip
address outside 172.18.124.35 255.255.255.240ip address inside 192.168.1.1 255.255.255.0ip
audit info action alarmip audit attack action alarmno failoverfailover timeout
0:00:00failover poll 15failover ip address outside 0.0.0.0failover ip address inside
0.0.0.0arp timeout 14400!--- Except Source/Destination from Network Address Translation
(NAT):nat (inside) 0 access-list 115route outside 0.0.0.0 0.0.0.0 172.18.124.36 1timeout
xlate 3:00:00timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h323
0:05:00sip 0:30:00 sip_media 0:02:00timeout uauth 0:05:00 absoluteaaa-server TACACS+
protocol tacacs+ aaa-server RADIUS protocol radius no snmp-server locationno snmp-server
contactsnmp-server community publicno snmp-server enable trapsfloodguard enablesysopt
connection permit-ipsecno sysopt route dnat!--- IPSec transformscrypto ipsec transform-set
myset esp-des esp-md5-hmac !--- IPSec lifetimecrypto ipsec security-association lifetime
seconds 3600crypto map rtpmap 10 ipsec-isakmp!--- Source/Destination networkscrypto map
rtpmap 10 match address 115!--- Encryption peercrypto map rtpmap 10 set peer 172.18.124.157
crypto map rtpmap 10 set transform-set mysetcrypto map rtpmap interface outsideisakmp enable
outside!--- Encryption peerisakmp key ******** address 172.18.124.157 netmask
255.255.255.240 isakmp identity address!--- Authentication methodisakmp policy 10
authentication pre-share!--- IKE encryption methodisakmp policy 10 encryption des!--- IKE
hashingisakmp policy 10 hash sha!--- Diffie-Hellman groupisakmp policy 10 group 1!--- IKE
lifetimeisakmp policy 10 lifetime 28800telnet timeout 5ssh timeout 5terminal width
80Cryptochecksum:c237ed11307abea7b530bbd0c2b2ec08: end
```

Configuración del concentrador VPN 5000

Concentrador VPN 5000

```
PIX Version 5.2(1)nameif ethernet0 outside
security0nameif ethernet1 inside security100enable
password 8Ry2YjIyt7RRXU24 encryptedpasswd
2KFQnbNIdI.2KYOU encryptedhostname pixfirewallfixup
protocol ftp 21fixup protocol http 80fixup protocol h323
1720fixup protocol rsh 514fixup protocol smtp 25fixup
protocol sqlnet 1521fixup protocol sip 5060names!---
Source/Destination networks definedaccess-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 24logging onno logging
timestampno logging standbyno logging consoleno logging
monitorno logging bufferedno logging trapno logging
historylogging facility 20logging queue 512interface
ethernet0 autointerface ethernet1 10basetmtu outside
1500mtu inside 1500ip address outside 172.18.124.35
255.255.255.240ip address inside 192.168.1.1
255.255.255.0ip audit info action alarmip audit attack
action alarmno failoverfailover timeout 0:00:00failover
poll 15failover ip address outside 0.0.0.0failover ip
address inside 0.0.0.0arp timeout 14400!--- Except
Source/Destination from Network Address Translation
(NAT):nat (inside) 0 access-list 115route outside
0.0.0.0 0.0.0.0 172.18.124.36 1timeout xlate
3:00:00timeout conn 1:00:00 half-closed 0:10:00 udp
0:02:00 rpc 0:10:00 h323 0:05:00sip 0:30:00 sip_media
0:02:00timeout uauth 0:05:00 absoluteaaa-server TACACS+
protocol tacacs+ aaa-server RADIUS protocol radius no
snmp-server locationno snmp-server contactsnmp-server
community publicno snmp-server enable trapsfloodguard
enablesysopt connection permit-ipsecno sysopt route
dnat!--- IPSec transformscrypto ipsec transform-set
myset esp-des esp-md5-hmac !--- IPSec lifetimecrypto
ipsec security-association lifetime seconds 3600crypto
map rtpmap 10 ipsec-isakmp!--- Source/Destination
networkscrypto map rtpmap 10 match address 115!---
```

```
Encryption peercrypto map rtpmap 10 set peer
172.18.124.157 crypto map rtpmap 10 set transform-set
mysetcrypto map rtpmap interface outsideisakmp enable
outside!--- Encryption peerisakmp key ******** address
172.18.124.157 netmask 255.255.255.240 isakmp identity
address!--- Authentication methodisakmp policy 10
authentication pre-share!--- IKE encryption methodisakmp
policy 10 encryption des!--- IKE hashingisakmp policy 10
hash sha!--- Diffie-Hellman groupisakmp policy 10 group
1!--- IKE lifetimeisakmp policy 10 lifetime 28800telnet
timeout 5ssh timeout 5terminal width
80Cryptochecksum:c237ed11307abea7b530bbd0c2b2ec08: end
```

Verificación

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

Troubleshooting

Esta sección proporciona la información que usted puede utilizar para resolver problemas 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:

Cisco 3640 Router

- **motor del debug crypto** - Mensajes del debug de las demostraciones sobre los motores de criptografía, que realizan el cifrado y el desciframiento.
- 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.
- **borre el isakmp crypto** - (del modo de configuración) borra todas las conexiones del IKE activo.
- 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).

- **motor del debug crypto** - Muestra el tráfico se cifra que.
- show crypto ipsec sa - Muestra las asociaciones de seguridad de la fase 2.
- **muestre isakmp crypto 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** - (del modo de configuración) 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 el **> Actions - Logout (Acciones – Cierre de sesión) de las Sesiones de LAN a LAN del Administration (Administración) > Administer sessions (Administrar sesiones).**

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. (Para los modelos modulares, la visualización incluye una sección para cada slot 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