Configurando IPSec entre um Microsoft Windows 2000 Server e um dispositivo Cisco

Contents

Introduction

Esse documento demonstra como formar um túnel de IPSec com chaves pré-compartilhadas para unir 2 redes privadas: uma rede privada (192.168.l.X) dentro de um dispositivo Cisco e uma rede privada (10.32.50.X) dentro do Microsoft 2000 Server. Assumimos que o tráfego de dentro do dispositivo Cisco e de dentro do Servidor 2000 para a Internet (representado aqui pelas redes 172.18.124.X) esteja fluindo antes do início da configuração.

Você pode encontrar informações detalhadas sobre como configurar o Microsoft Windows 2000 Server no site da Microsoft na Web: http://support.microsoft.com/support/kb/articles/Q252/7/35.ASP

Antes de Começar

Conventions

Para obter mais informações sobre convenções de documento, consulte as Convenções de dicas técnicas Cisco.

Prerequisites

Não existem requisitos específicos para este documento.

Componentes Utilizados

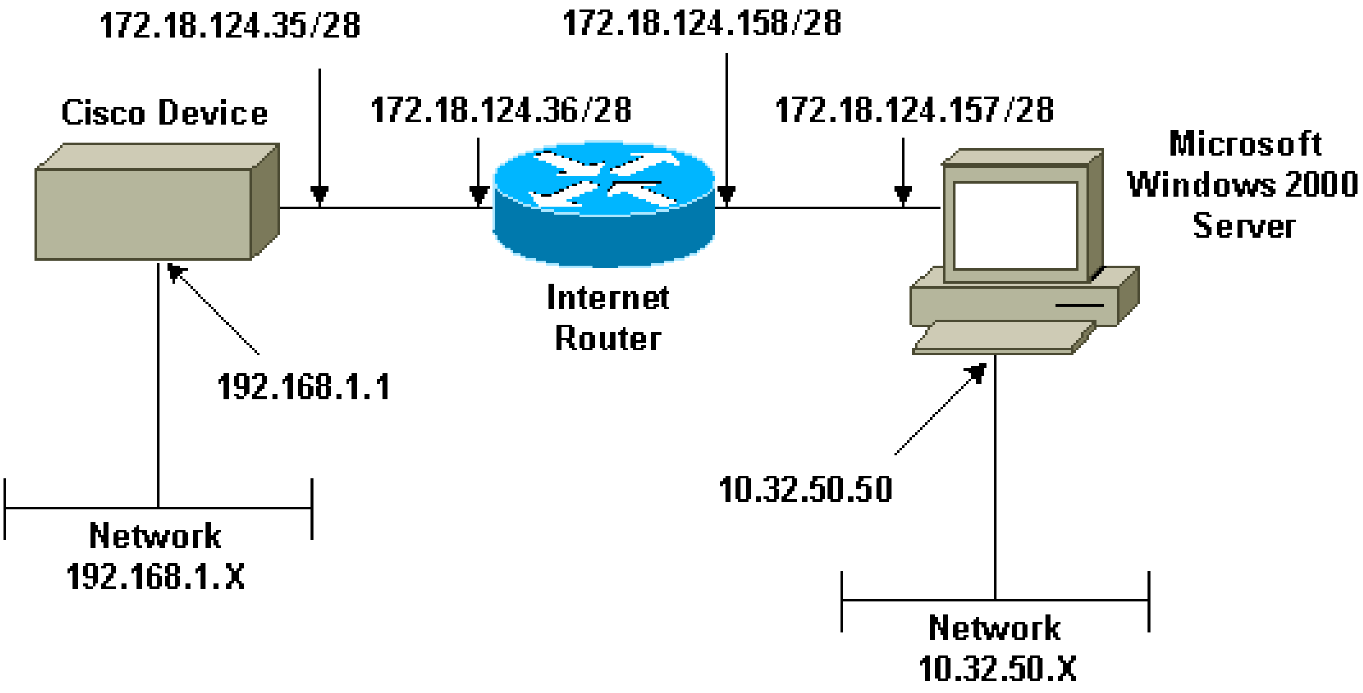
Essas configurações foram desenvolvidas e testadas com as seguintes versões de software e hardware.

- Microsoft Windows 2000 Server 5.00.2195
- Roteador Cisco 3640 com Cisco IOS® Software versão c3640-ik2o3s-mz.121-5.T.bin
- Cisco Secure PIX Firewall com software PIX versão 5.2.1
- Concentrador Cisco VPN 3000 com respectivo software versão 2.5.2.F
- Cisco VPN 5000 Concentrator com software do Cisco VPN 5000 Concentrator versão 5.2.19

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. All of the devices used in this document started with a cleared (default) configuration. Se você estiver trabalhando em uma rede ativa, certifique-se de que entende o impacto potencial de qualquer comando antes de utilizá-lo.

Diagrama de Rede

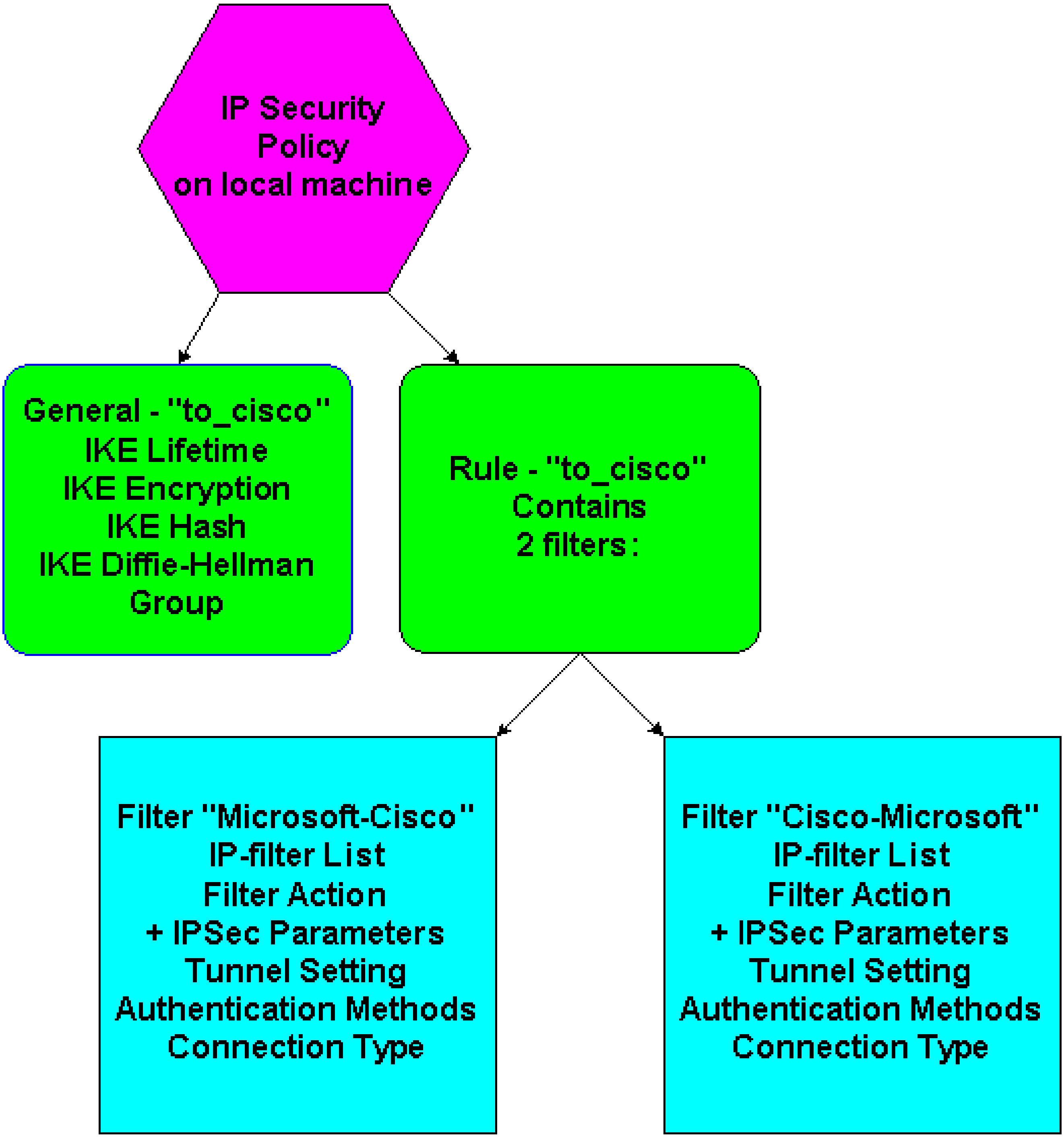
Este documento utiliza a instalação de rede mostrada no diagrama abaixo.



Configurando o Microsoft Windows 2000 Server para funcionar com dispositivos Cisco

Tarefas executadas

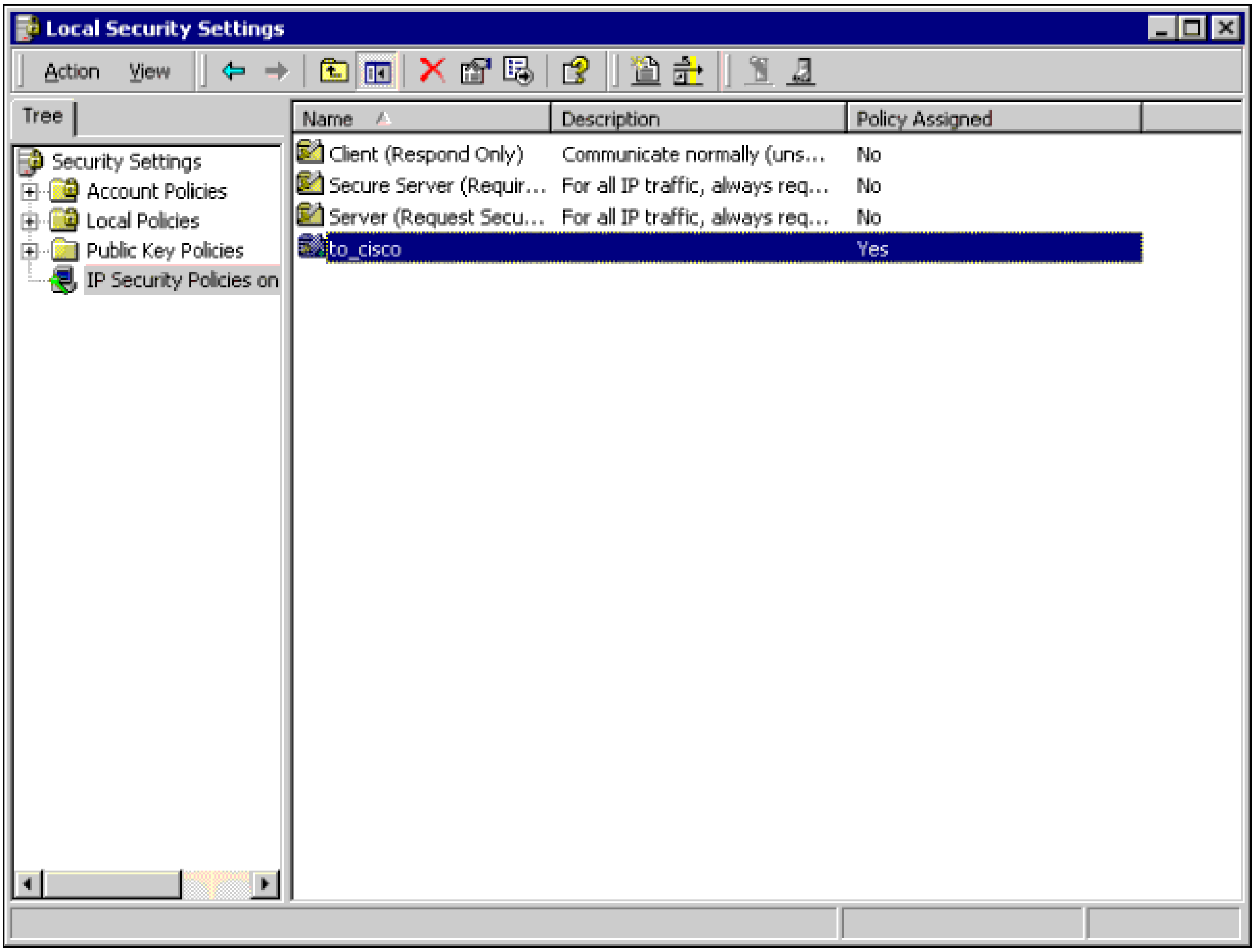
Este diagrama mostra as tarefas executadas na configuração do servidor Microsoft Windows 2000:



Step-by-Step Instructions

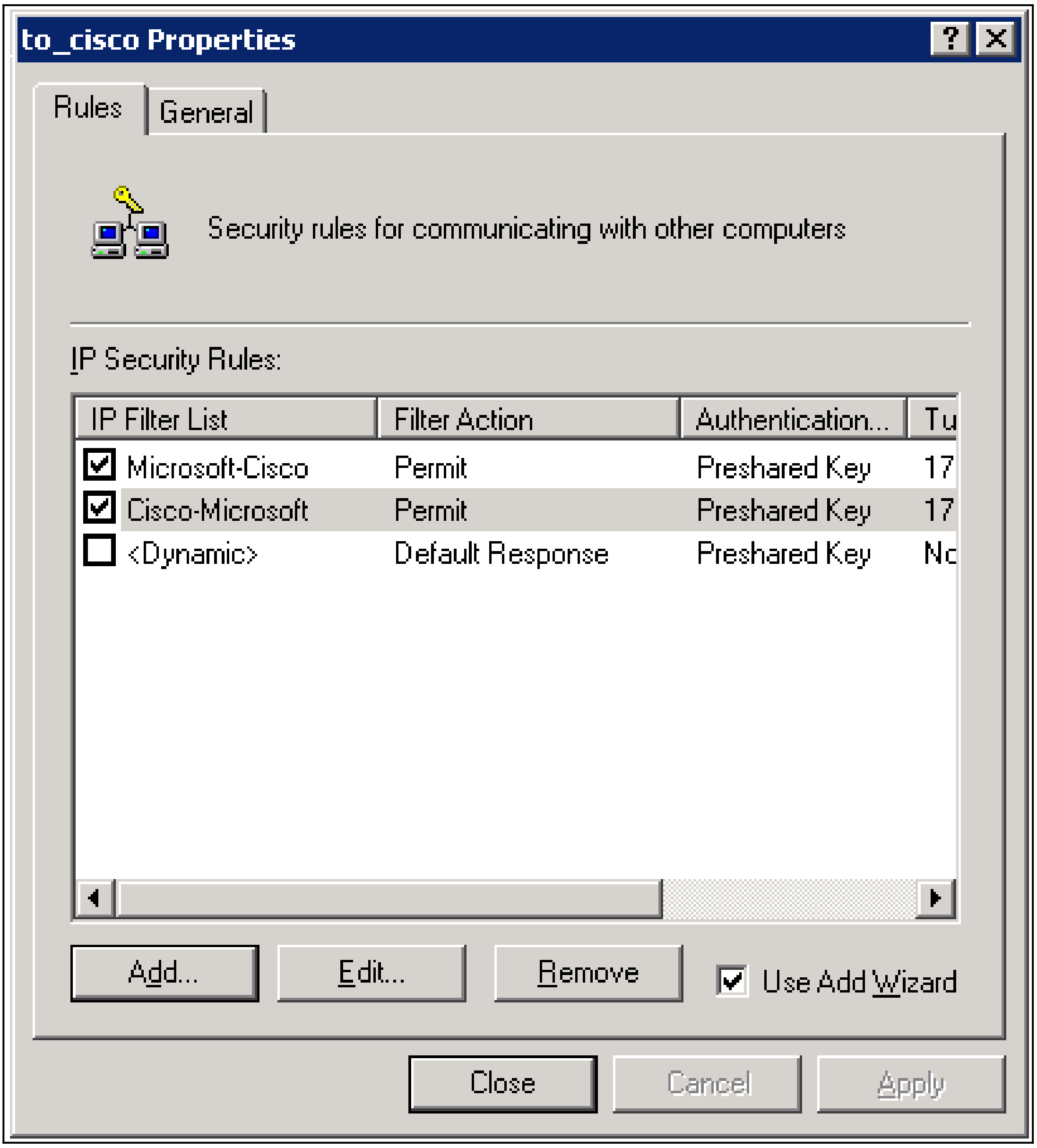
Depois de seguir as instruções de configuração no site da Microsoft, use as seguintes etapas para verificar se sua configuração pode funcionar com dispositivos Cisco. Comentários e alterações são anotados com capturas de tela.

1. Clique em Start (Iniciar) > Run (Executar) > secpol.msc no Microsoft Windows 2000 Server e verifique as informações nas seguintes telas.Depois que as instruções no site da Microsoft foram usadas para configurar um servidor 2000, as seguintes informações de túnel foram exibidas.**Observação:** a regra de exemplo é chamada
"to_cisco".



Name	Description	Policy Assigned
Client (Respond Only)	Communicate normally (uns...	No
Secure Server (Requir...	For all IP traffic, always req...	No
Server (Request Secu...	For all IP traffic, always req...	No
to_cisco		Yes

2. Esta regra de exemplo contém dois filtros: Microsoft-Cisco e Cisco-

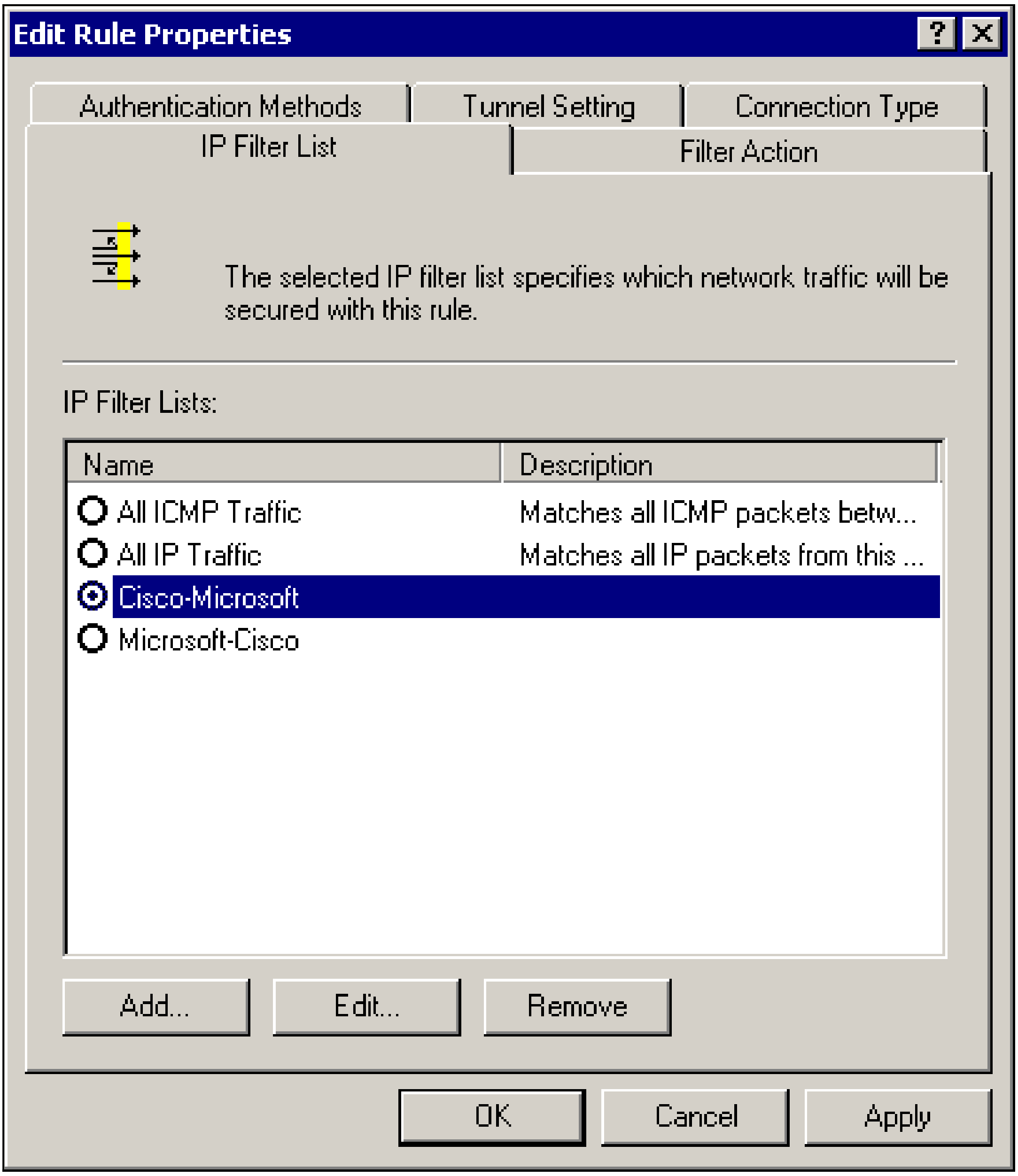


IP Filter List	Filter Action	Authentication...	Tu
☑ Microsoft-Cisco	Permit	Preshared Key	17
☑ Cisco-Microsoft	Permit	Preshared Key	17
□ <Dynamic>	Default Response	Preshared Key	Nc

Microsoft.

3. Selecione a regra de segurança IP Cisco-Microsoft e clique em **Editar** para exibir/adicionar/editar as listas de filtros

IP.



Edit Rule Properties

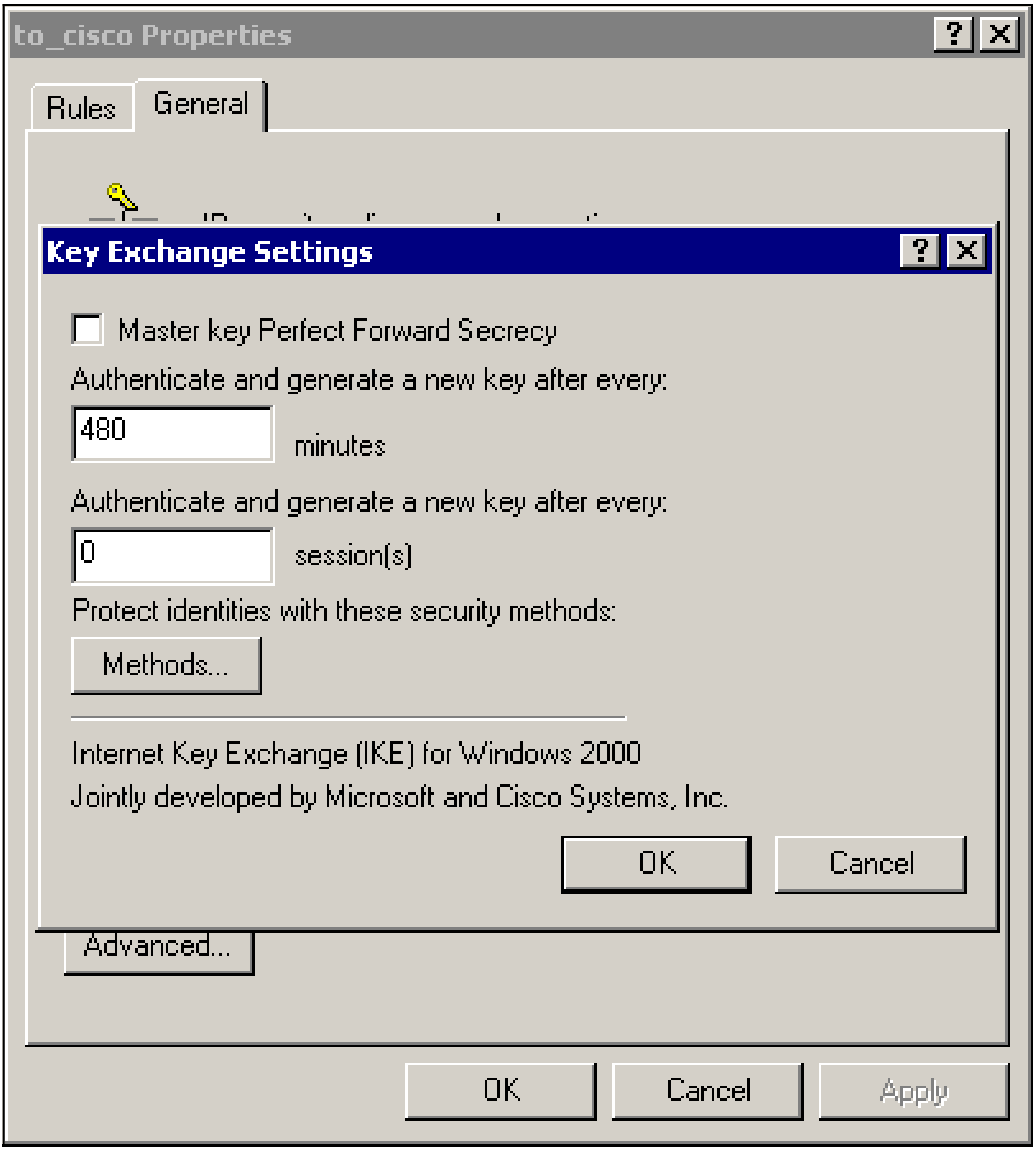
The selected IP filter list specifies which network traffic will be secured with this rule.

IP Filter Lists:

Name	Description
○ All ICMP Traffic	Matches all ICMP packets betw...
○ All IP Traffic	Matches all IP packets from this ...
● Cisco-Microsoft	
○ Microsoft-Cisco	

4. A guia Geral > Avançado da regra tem a duração IKE (480 minutos = 28800

segundos):



☐ Master key Perfect Forward Secrecy

Authenticate and generate a new key after every:

480 minutes

Authenticate and generate a new key after every:

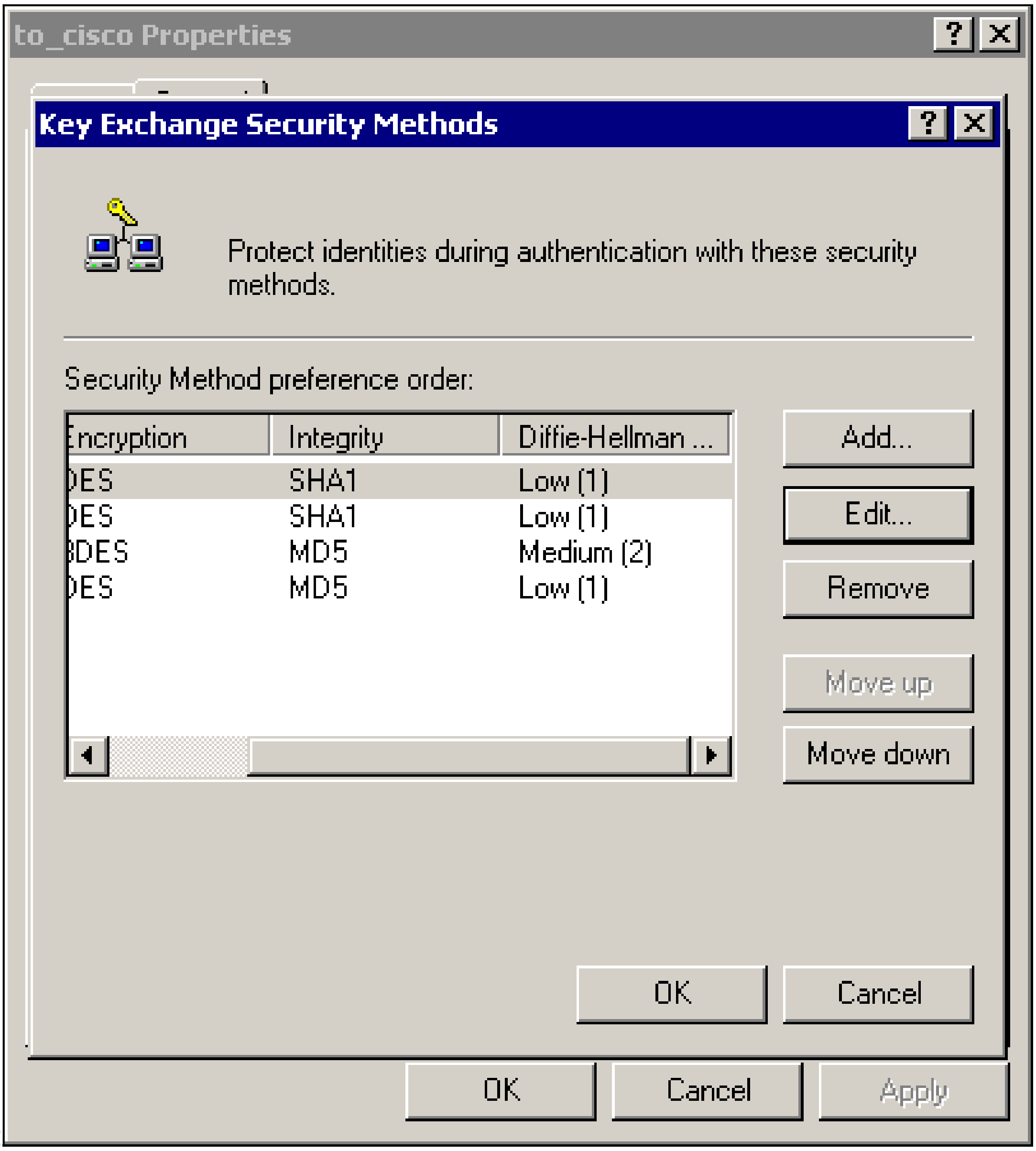
0 session(s)

Protect identities with these security methods:

Internet Key Exchange (IKE) for Windows 2000

Jointly developed by Microsoft and Cisco Systems, Inc.

5. A guia General > Advanced > Methods da regra tem o método de criptografia IKE (DES), hashing de IKE (SHA1) e o Diffie-Helman group



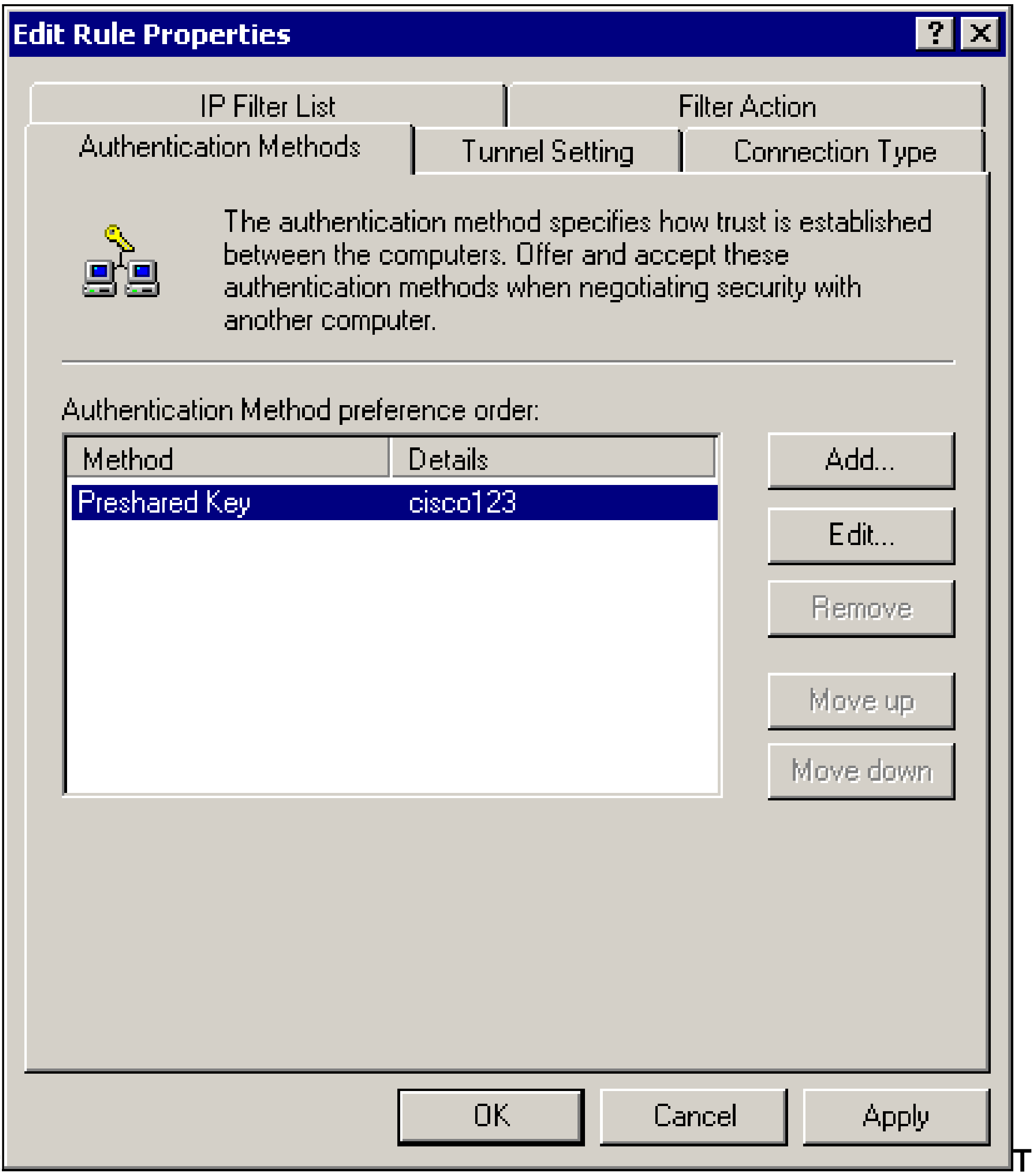
Protect identities during authentication with these security methods.

Security Method preference order:

Encryption	Integrity	Diffie-Hellman ...
DES	SHA1	Low (1)
DES	SHA1	Low (1)
3DES	MD5	Medium (2)
DES	MD5	Low (1)

(Low1)):

6. Cada filtro tem 5 guias:**Métodos de autenticação (Chaves pré-compartilhadas para Internet Key Exchange**



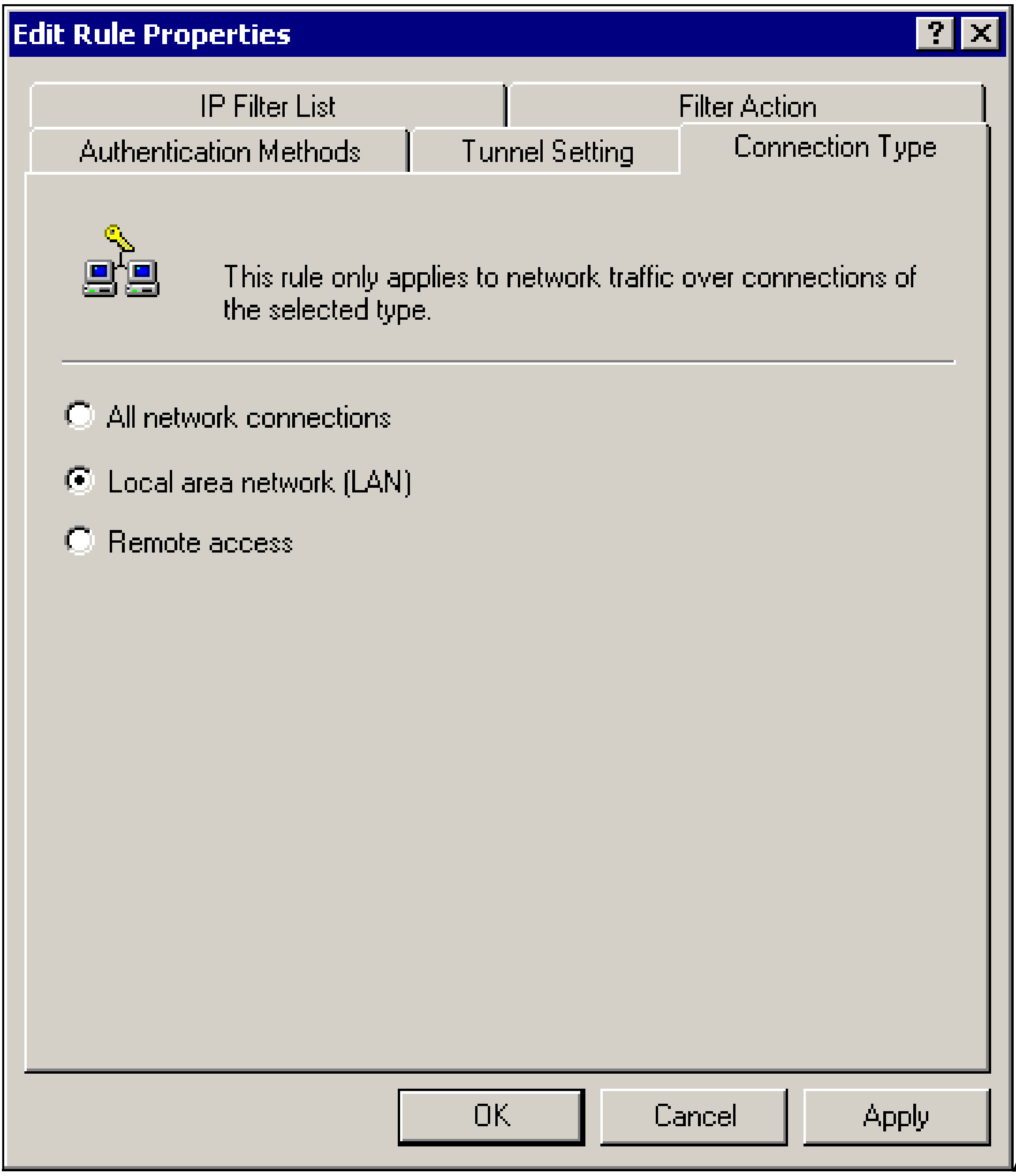
Edit Rule Properties

The authentication method specifies how trust is established between the computers. Offer and accept these authentication methods when negotiating security with another computer.

Authentication Method preference order:

Method	Details
Preshared Key	cisco123

[IKE]): Tipo de conexão



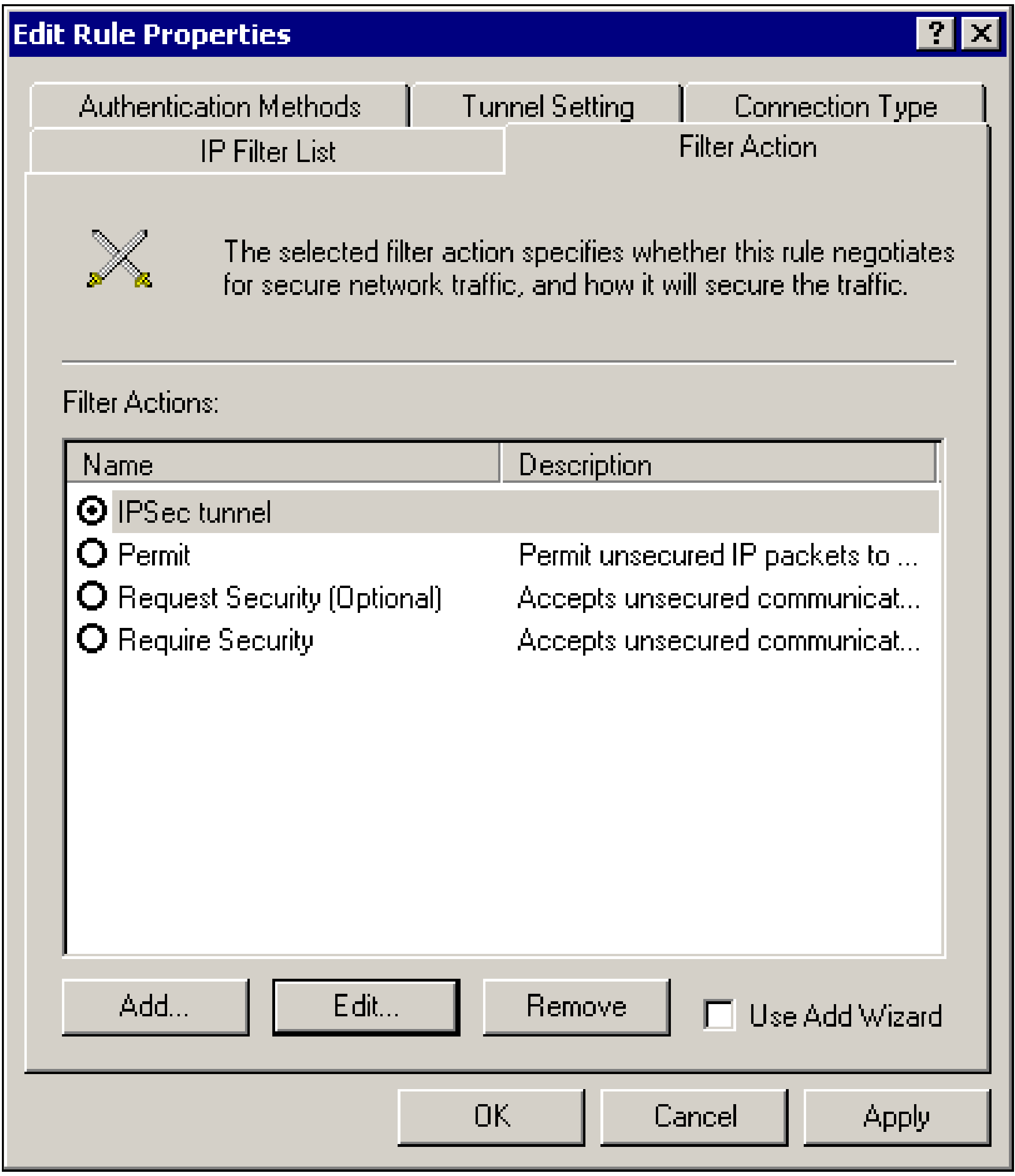
This rule only applies to network traffic over connections of the selected type.

○ All network connections

● Local area network (LAN)

○ Remote access

(LAN): **Ação de filtro**



Edit Rule Properties

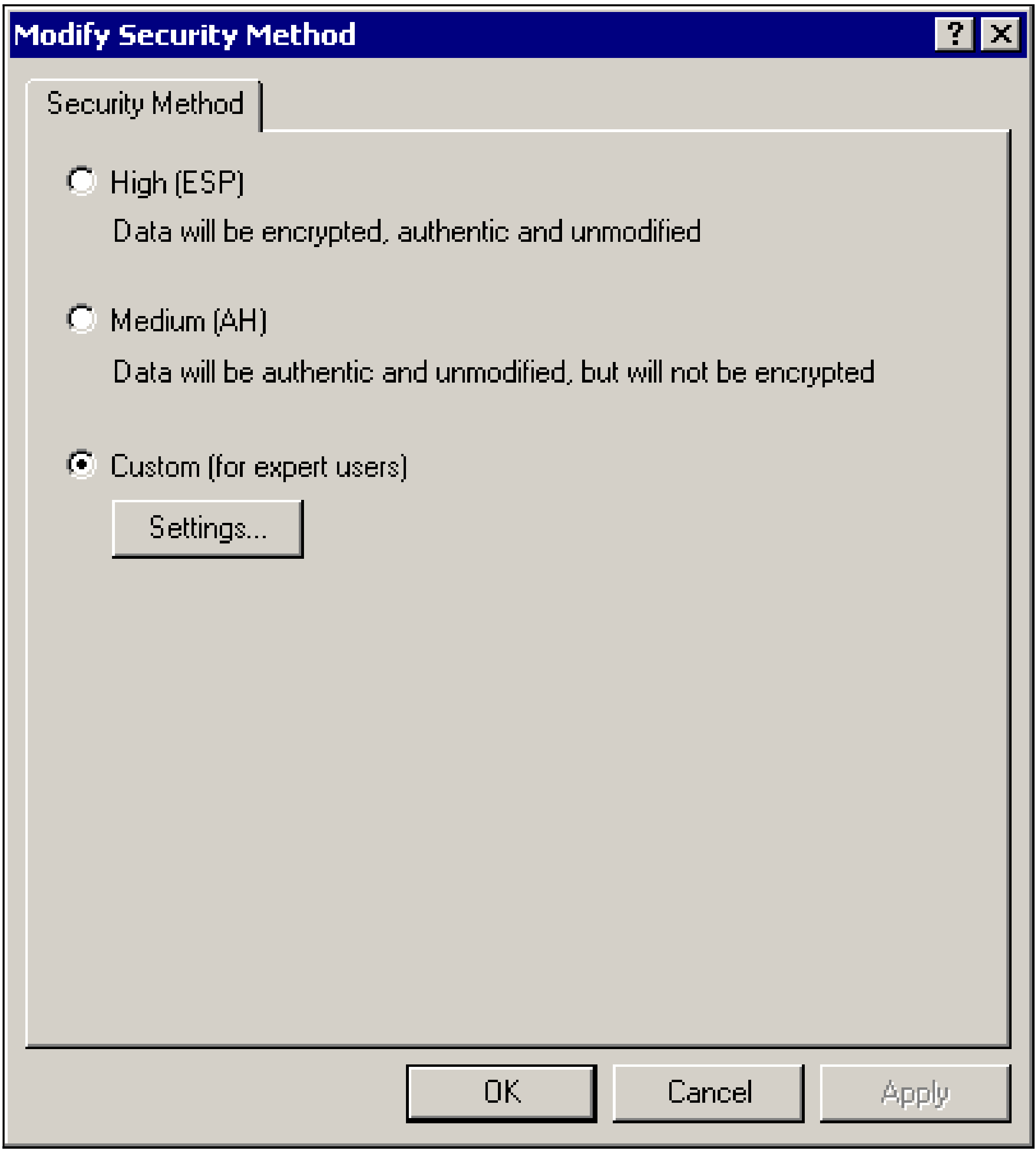
The selected filter action specifies whether this rule negotiates for secure network traffic, and how it will secure the traffic.

Filter Actions:

Name	Description
● IPSec tunnel	
○ Permit	Permit unsecured IP packets to ...
○ Request Security (Optional)	Accepts unsecured communicat...
○ Require Security	Accepts unsecured communicat...

□ Use Add Wizard

(IPSec): Selecione Ação de filtro > Túnel IPSec > Editar > Editar e clique em

Personalizar:Clique em Settings – transformações de IPSec e duração de

Modify Security Method

Security Method

○ High (ESP)

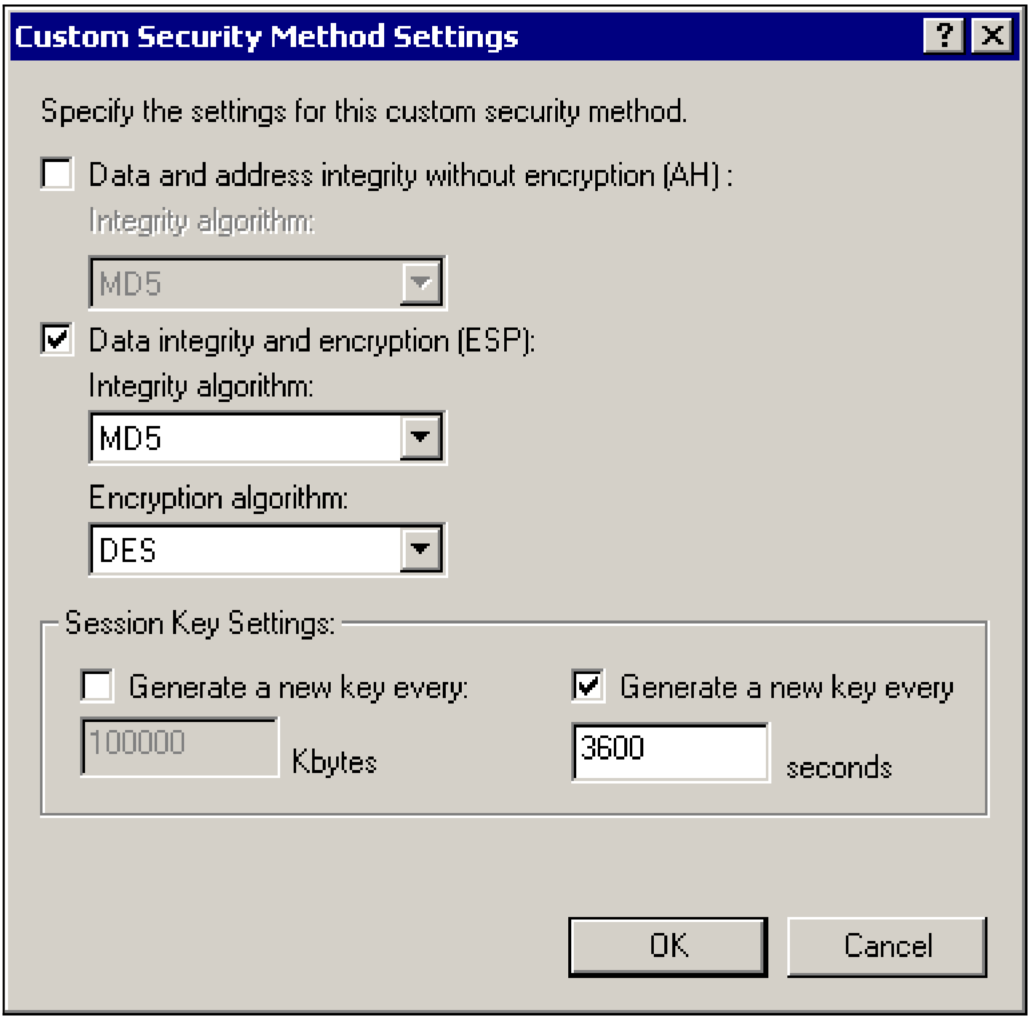
Data will be encrypted, authentic and unmodified

○ Medium (AH)

Data will be authentic and unmodified, but will not be encrypted

● Custom (for expert users)

IPSec:



Custom Security Method Settings

Specify the settings for this custom security method.

☐ Data and address integrity without encryption (AH) :

Integrity algorithm: MD5

☑ Data integrity and encryption (ESP):

Integrity algorithm: MD5

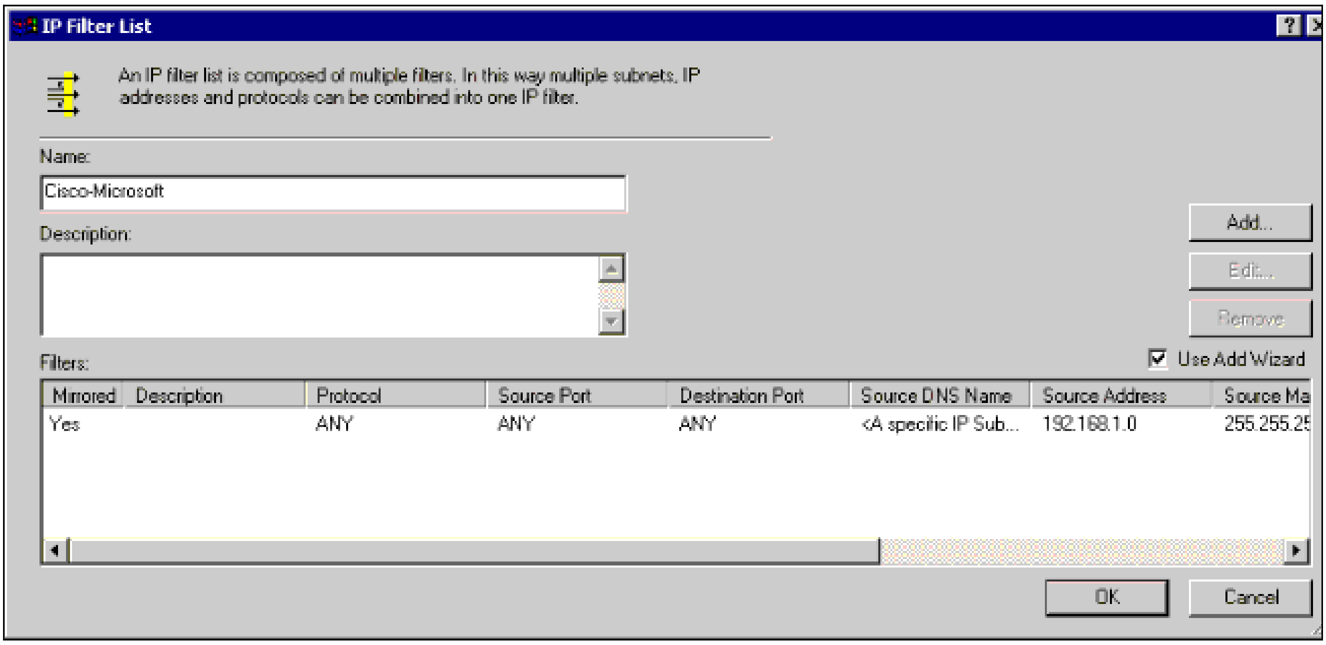
Encryption algorithm: DES

Session Key Settings:

☐ Generate a new key every: 100000 Kbytes

☑ Generate a new key every 3600 seconds

Lista de filtros IP - redes **de origem** e **destino** a serem criptografadas:Para a Cisco-Microsoft:



IP Filter List

An IP filter list is composed of multiple filters. In this way multiple subnets, IP addresses and protocols can be combined into one IP filter.

Name: Cisco-Microsoft

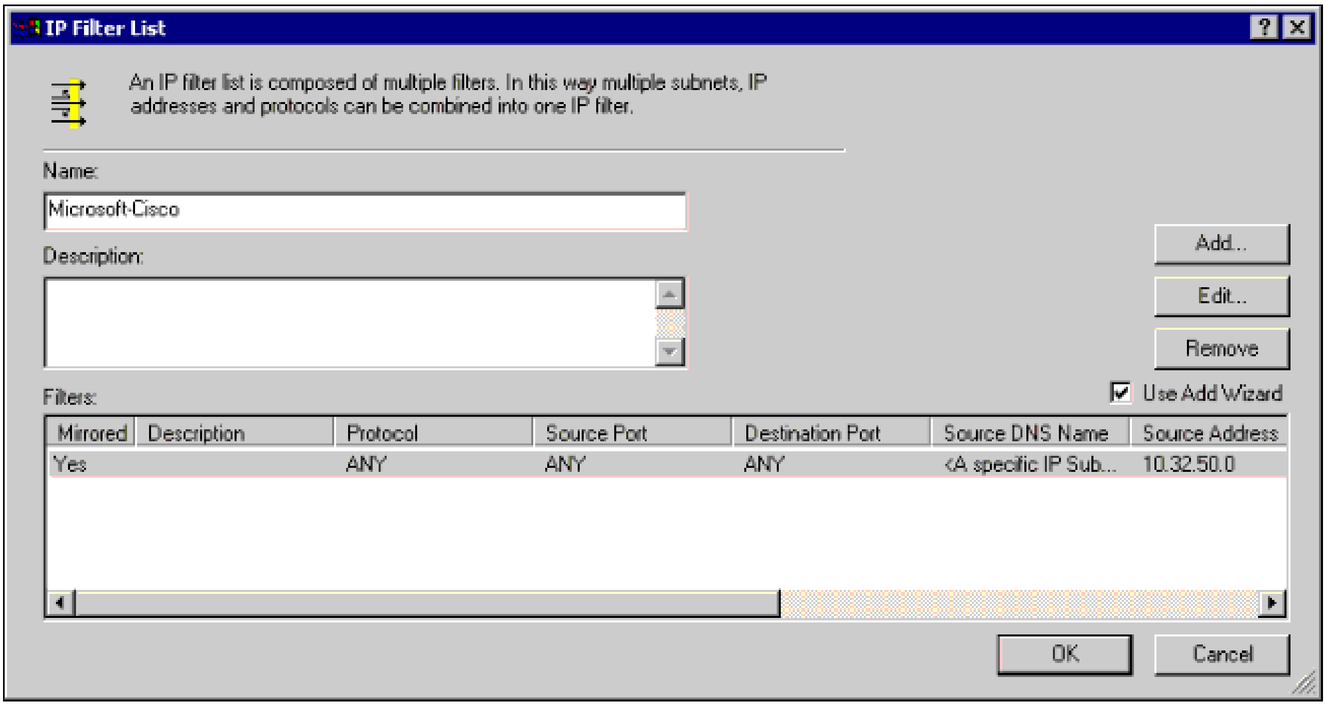
Description:

☑ Use Add Wizard

Filters:

Mirrored	Description	Protocol	Source Port	Destination Port	Source DNS Name	Source Address	Source Ma
Yes		ANY	ANY	ANY	<A specific IP Sub...	192.168.1.0	255.255.25

Para Microsoft-Cisco:



An IP filter list is composed of multiple filters. In this way multiple subnets, IP addresses and protocols can be combined into one IP filter.

Name: Microsoft-Cisco

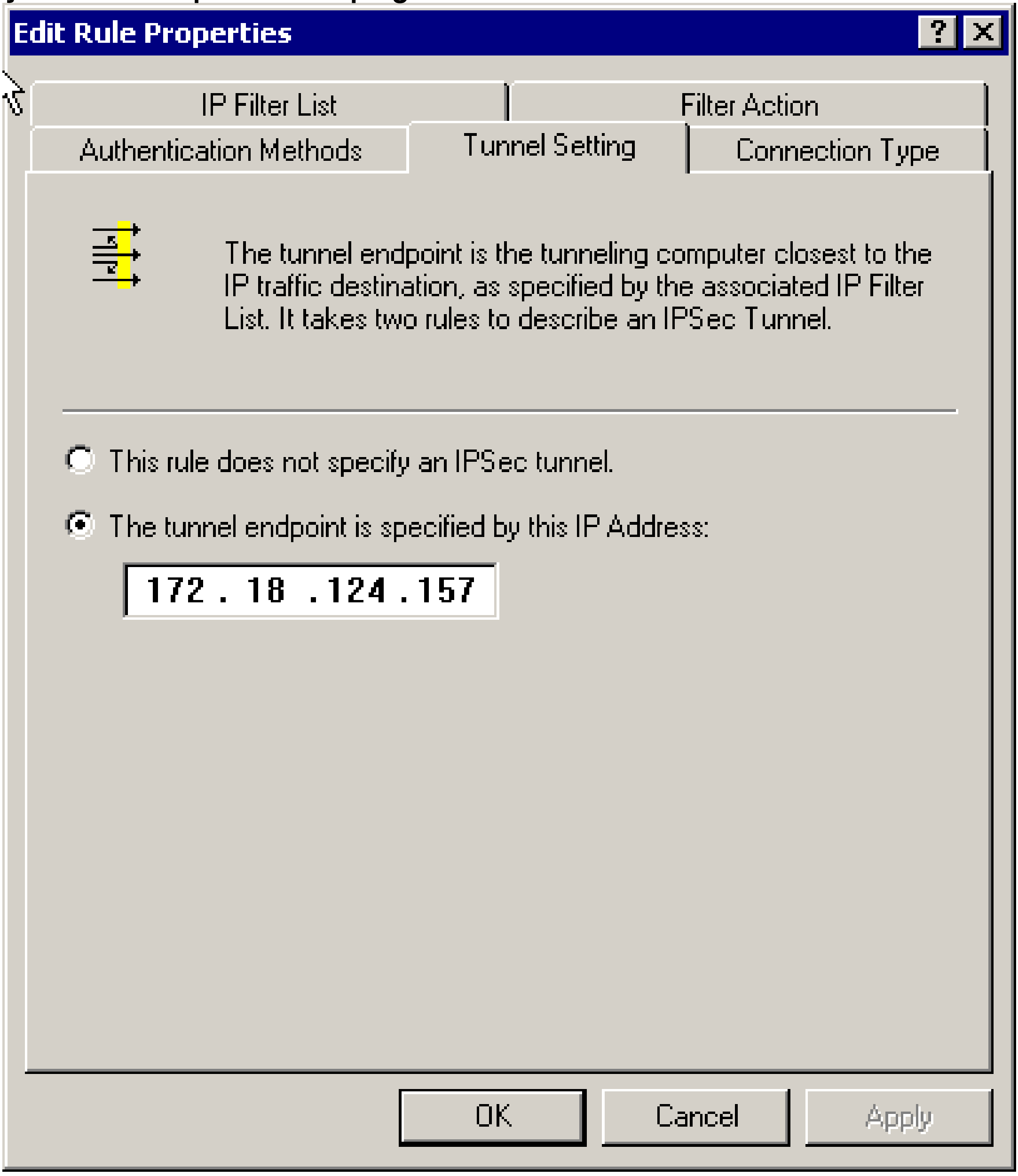
Description:

☑ Use Add Wizard

Filters:

Mirrored	Description	Protocol	Source Port	Destination Port	Source DNS Name	Source Address
Yes		ANY	ANY	ANY	<A specific IP Sub...	10.32.50.0

Configuração de túnel - peers de criptografia: Para a Cisco-Microsoft:



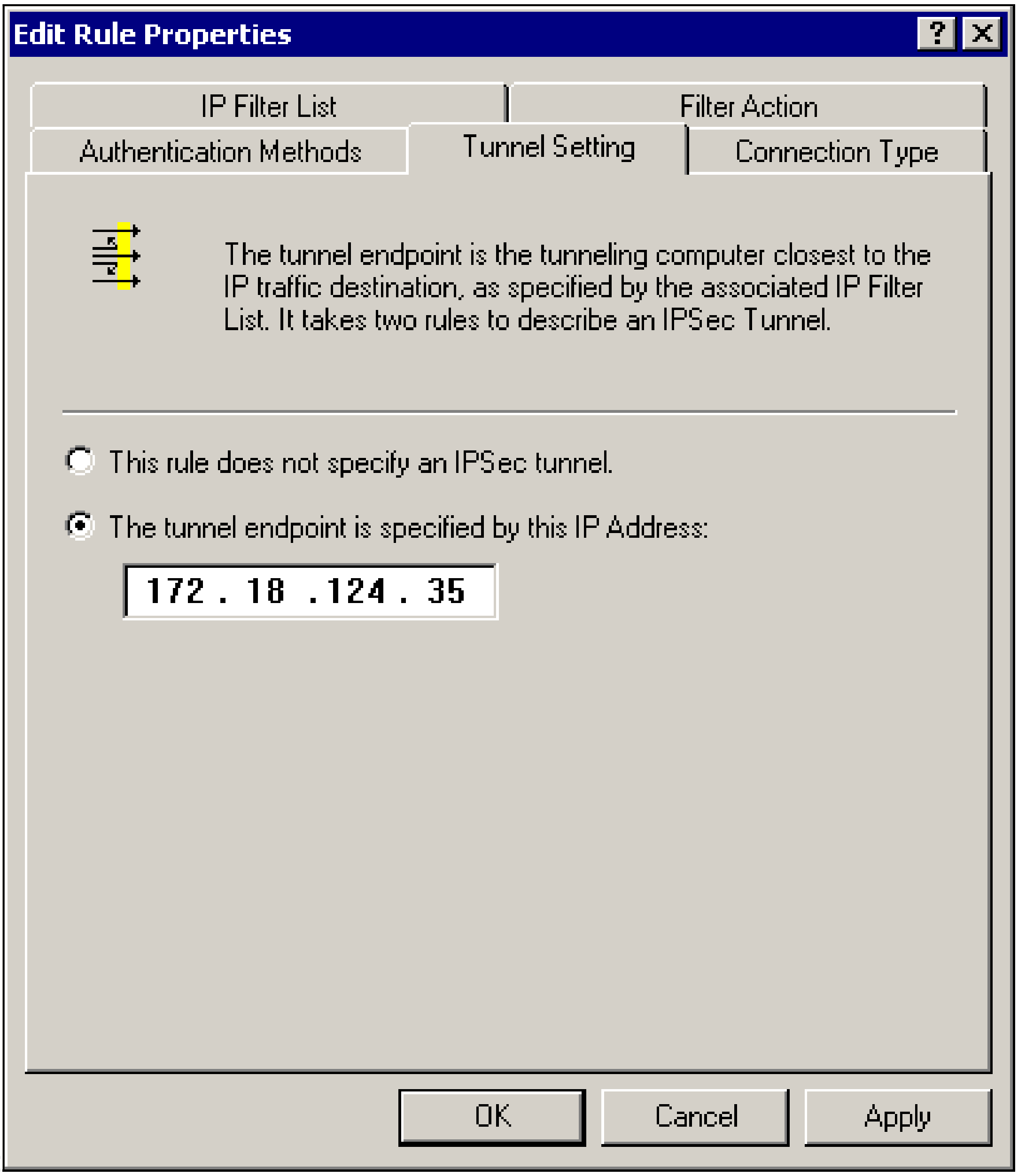
The tunnel endpoint is the tunneling computer closest to the IP traffic destination, as specified by the associated IP Filter List. It takes two rules to describe an IPSec Tunnel.

○ This rule does not specify an IPSec tunnel.

● The tunnel endpoint is specified by this IP Address:

172 . 18 . 124 . 157

Para

Microsoft-Cisco: 

The tunnel endpoint is the tunneling computer closest to the IP traffic destination, as specified by the associated IP Filter List. It takes two rules to describe an IPSec Tunnel.

○ This rule does not specify an IPSec tunnel.

● The tunnel endpoint is specified by this IP Address:

172 . 18 .124 . 35

Configuração dos dispositivos Cisco

Configure o roteador Cisco, PIX e VPN Concentrators conforme mostrado nos exemplos abaixo.

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

Configurando o Cisco 3640 Router

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
```

Configuração 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
```

Configurando o VPN 3000 Concentrator

Use as opções de menu e os parâmetros mostrados abaixo para configurar o VPN Concentrator conforme necessário.

- Para adicionar uma proposta IKE, selecione Configuration (Configuração) > System (Sistema) > Tunneling Protocols (Protocolos de Tunelamento) > IPSec > IKE Proposals (Propostas IKE) > Add a proposal (Adicionar proposta).

```
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 o túnel LAN a LAN, selecione **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 a associação de segurança, selecione **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
```

Configurando o VPN 5000 Concentrator

VPN 5000 Concentrator

```
[ 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.
```

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshoot

Esta seção fornece informações que você pode usar para solucionar problemas de suas configurações.

Comandos para Troubleshooting

A Output Interpreter Tool (somente clientes registrados) oferece suporte a determinados comandos show, o que permite exibir uma análise da saída do comando show.

Observação: antes de emitir comandos **debug**, consulte Informações importantes sobre comandos debug.

Cisco 3640 Router

- **debug crypto engine** - Mostra mensagens de depuração sobre mecanismos de criptografia, que executam criptografia e descriptografia.
- **debug crypto isakmp ? Exibe mensagens sobre eventos IKE.**
- **debug crypto ipsec - Mostra os eventos de IPSec.**
- **show crypto isakmp sa – Mostra todas as associações de segurança (SAs) IKE atuais no correspondente.**
- **show crypto ipsec sa – Mostra as configurações usadas pelas associações segurança atuais.**
- **clear crypto isakmp** - (do modo de configuração) Limpa todas as conexões IKE ativas.
- **clear crypto sa - (do modo de configuração) Exclui todas as associações de segurança de IPSec.**

PIX

- **debug crypto ipsec – Exibe as negociações de IPSec da fase 2.**
- **debug crypto isakmp – Mostra as negociações de Internet Security Association and Key Management Protocol (ISAKMP) da fase 1.**
- **debug crypto engine** - Mostra o tráfego que está criptografado.
- **show crypto ipsec sa – Mostra as associações de segurança da fase 2.**
- **show crypto isakmp sa - Mostra as associações de segurança da fase 1.**
- **clear crypto isakmp - (a partir do modo de configuração) Limpa associações de segurança Internet Key Exchange (IKE).**
- **clear crypto ipsec sa** - (do modo de configuração) Limpa associações de segurança IPSec.

VPN 3000 Concentrator

- - Inicie a depuração do VPN 3000 Concentrator selecionando Configuration (Configuração) > System (Sistema) > Events (Eventos) > Classes (Classes) > Modify (Modificar) (Severity to Log=1-13, Severity to Console=1-3): IKE, IKEDBG, IKEDECODE, IPSEC, IPSECDBG, IPSECDECODE
- O registro de eventos pode ser limpo ou recuperado selecionando Monitoring > Event Log.
- É possível monitorar o tráfego do túnel de LAN para LAN em Monitoring (Monitorando) > Sessions (Sessões).
- - O túnel pode ser limpo em **Administration > Administer Sessions > LAN-to-LAN sessions > Actions - Logout.**

VPN 5000 Concentrator

- **vpn trace dump all - Mostra informações sobre todas as conexões VPN correspondentes, incluindo: informações sobre o horário, o número VPN, o endereço IP real do correspondente, quais scripts foram executadas e, em caso de erro, a rotina e o número da linha do código do software em que ocorrreu o erro.**
- **show vpn statistics Exibe as seguintes informações para Usuários, Parceiros e o Total para ambos.** (Para modelos modulares, a tela inclui uma seção para cada slot de módulo.) Current Active - As conexões ativas no momento. Em negociação - As conexões em negociação no momento. Nível alto – O maior número de conexões ativas desde a última reinicialização. Total em execução – O número total de conexões bem-sucedidas desde a última reinicialização. Inicialização do túnel – O número do túnel é iniciado. Túnel OK – O número de túneis que não apresentaram erros. Tunnel Error – O número de túneis com erros.
- **show vpn statistics verbose - Mostra estatísticas de negociação de ISAKMP e muitas outras estatísticas de conexão.**

Informações Relacionadas

- Anúncio do fim do ciclo de comercialização dos concentradores Cisco VPN 5000 Series
- Configuração da segurança de rede IPSec
- Configurando o protocolo de segurança do intercâmbio chave de Internet
- Suporte Técnico - Cisco Systems