

Configuring IPSec Between a Microsoft Windows 2000 Server and a Cisco Device

Document ID: 14121

Cisco has announced the end of sales for the Cisco VPN 5000 Series Concentrators. For more information, please see the End-of-Sales Announcement.

Introduction

Before You Begin

- Conventions

- Prerequisites

- Components Used

- Network Diagram

Configuring the Microsoft Windows 2000 Server to Work with Cisco Devices

- Tasks Performed

- Step-by-Step Instructions

Configuring the Cisco Devices

- Configuring the Cisco 3640 Router

- Configuring PIX

- Configuring the VPN 3000 Concentrator

- Configuring the VPN 5000 Concentrator

Verify

Troubleshoot

- Troubleshooting Commands

Related Information

Introduction

This document demonstrates how to form an IPSec tunnel with pre-shared keys to join 2 private networks: a private network (192.168.1.X) inside a Cisco device and a private network (10.32.50.X) inside the Microsoft 2000 Server. We assume that traffic from inside the Cisco device and inside the 2000 Server to the Internet (represented here by the 172.18.124.X networks) is flowing prior to beginning this configuration.

You can find detailed information on configuring the Microsoft Windows 2000 server at the Microsoft web site: <http://support.microsoft.com/support/kb/articles/Q252/7/35.ASP>

Before You Begin

Conventions

For more information on document conventions, see the Cisco Technical Tips Conventions.

Prerequisites

There are no specific prerequisites for this document.

Components Used

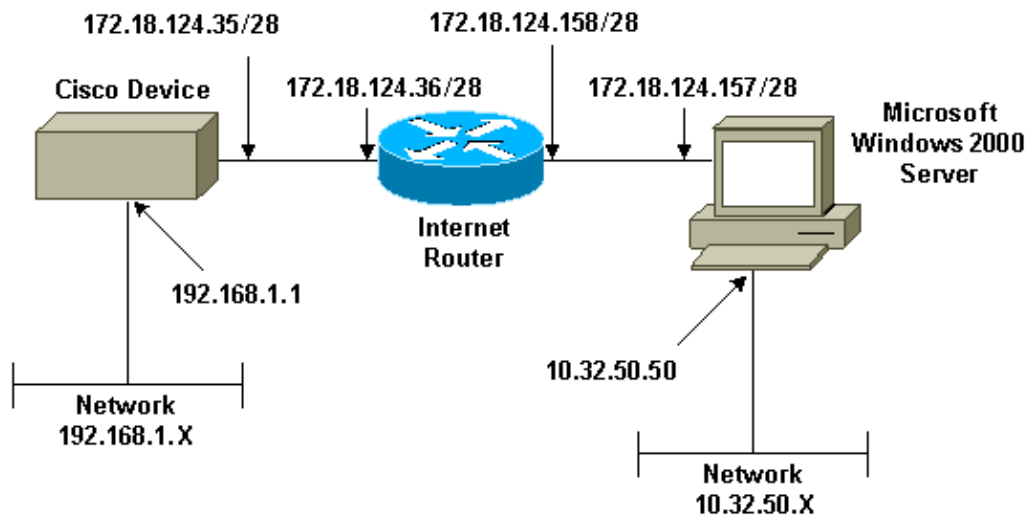
These configurations were developed and tested using the software and hardware versions below.

- Microsoft Windows 2000 Server 5.00.2195
- Cisco 3640 Router with Cisco IOS® Software release c3640-ik2o3s-mz.121-5.T.bin
- Cisco Secure PIX Firewall with PIX Software Release 5.2.1
- Cisco VPN 3000 Concentrator with VPN 3000 Concentrator Software Version 2.5.2.F
- Cisco VPN 5000 Concentrator with VPN 5000 Concentrator Software Version 5.2.19

The information presented in this document was created from devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If you are working in a live network, ensure that you understand the potential impact of any command before using it.

Network Diagram

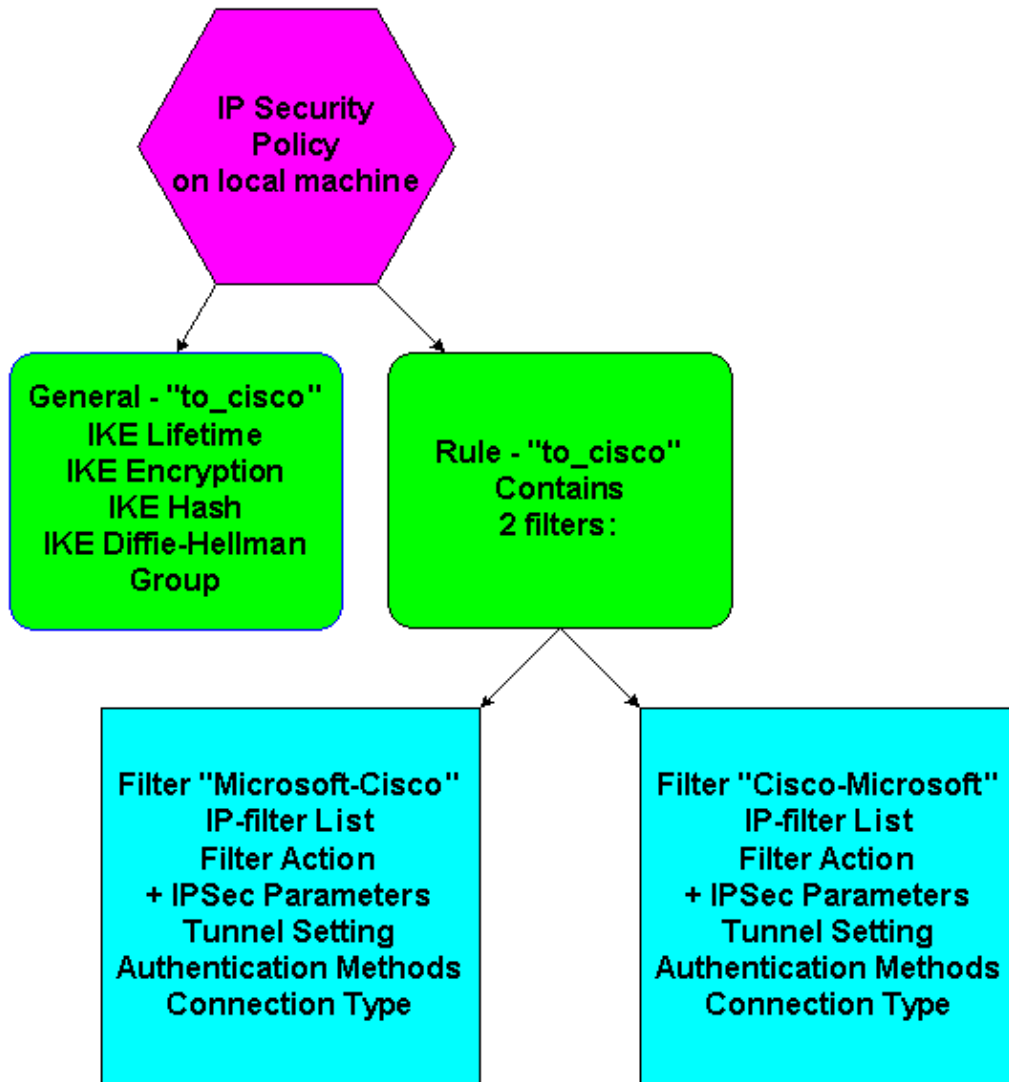
This document uses the network setup shown in the diagram below.



Configuring the Microsoft Windows 2000 Server to Work with Cisco Devices

Tasks Performed

This diagram shows the tasks performed in the Microsoft Windows 2000 server configuration:



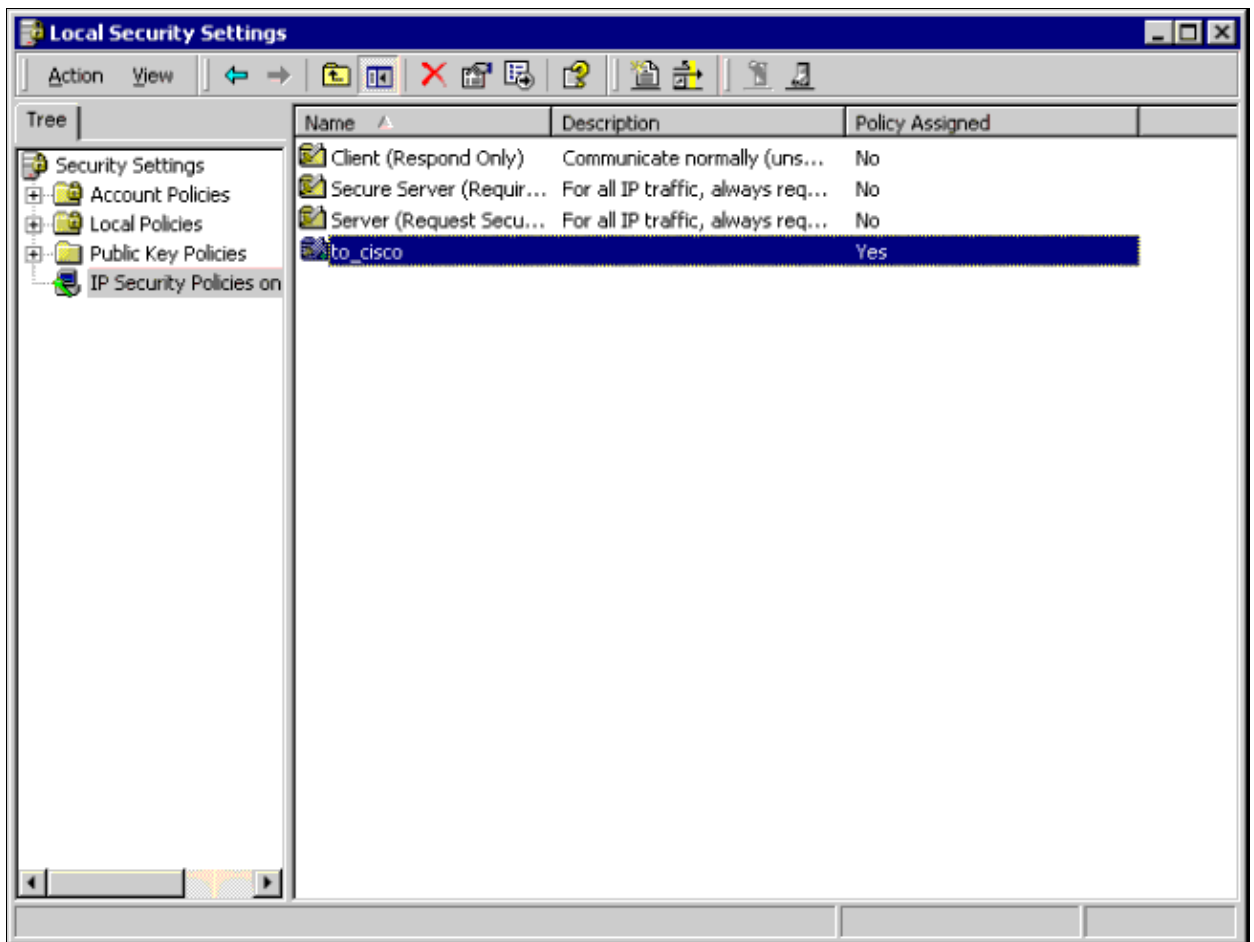
Step-by-Step Instructions

Once you have followed the configuration instructions on the Microsoft web site, use the following steps to verify that your configuration can work with Cisco devices. Comments and changes are noted with the screen captures.

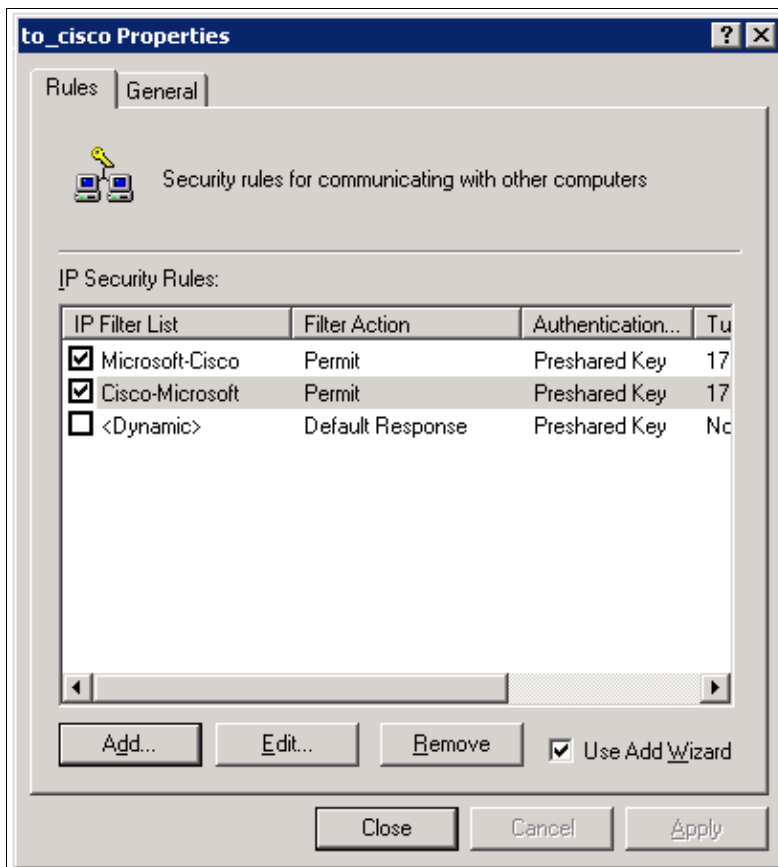
1. Click **Start > Run > secpol.msc** on the Microsoft Windows 2000 Server, and verify the information on the following screens.

After the instructions on the Microsoft web site were used to configure a 2000 server, the following tunnel information was displayed.

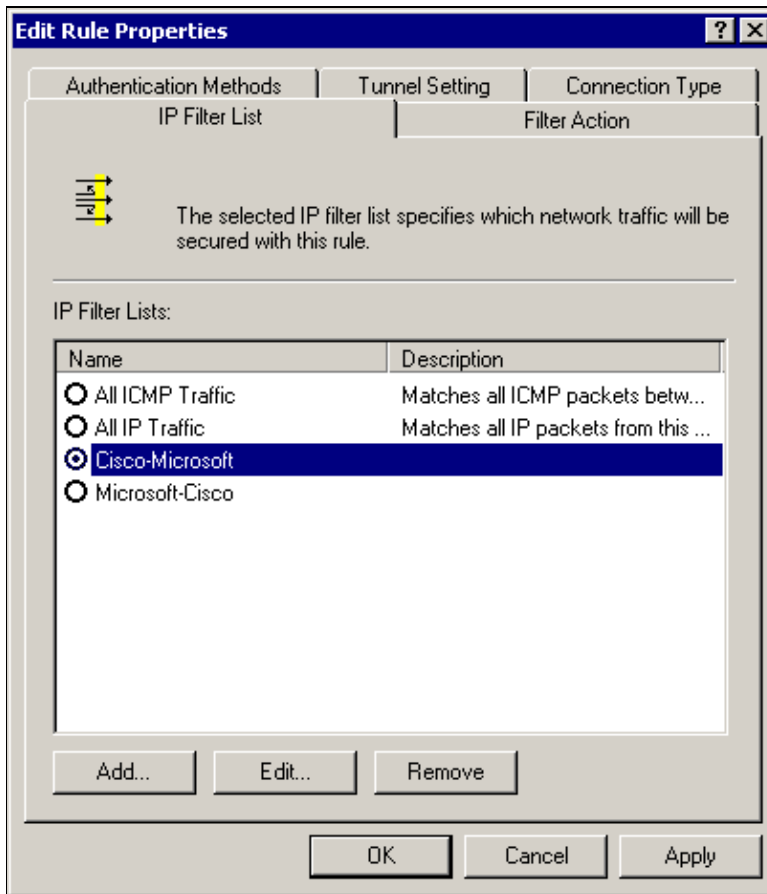
Note: The example rule is called "to_cisco".



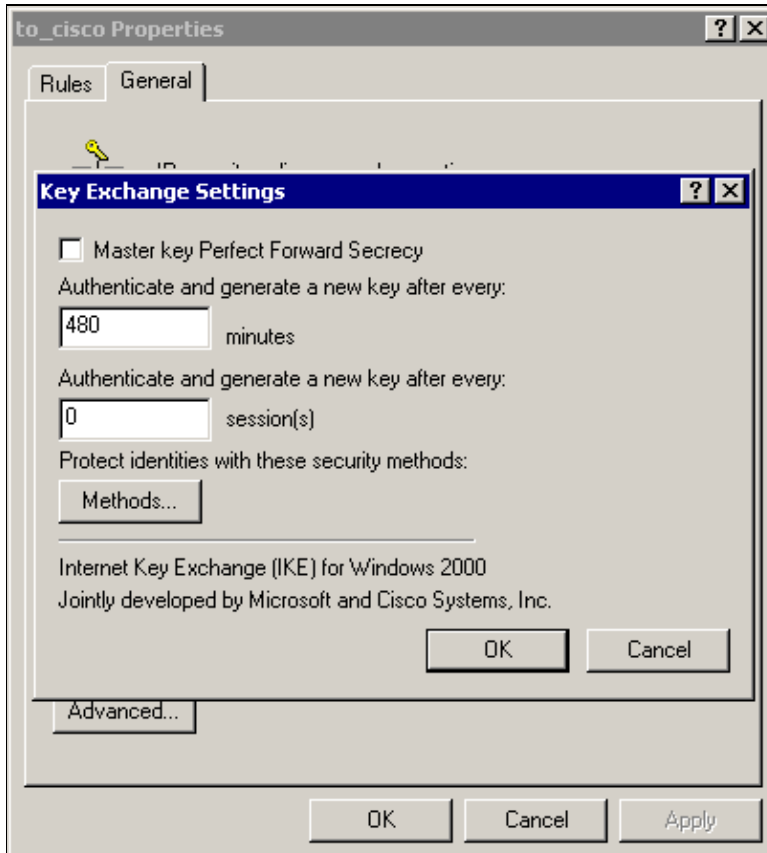
2. This example rule contains two filters: Microsoft–Cisco and Cisco–Microsoft.



3. Select the Cisco–Microsoft IP Security Rule, then click **Edit** to view/add/edit the IP Filter Lists.



4. The rule's **General > Advanced** tab has the **IKE lifetime** (480 minutes = 28800 seconds):

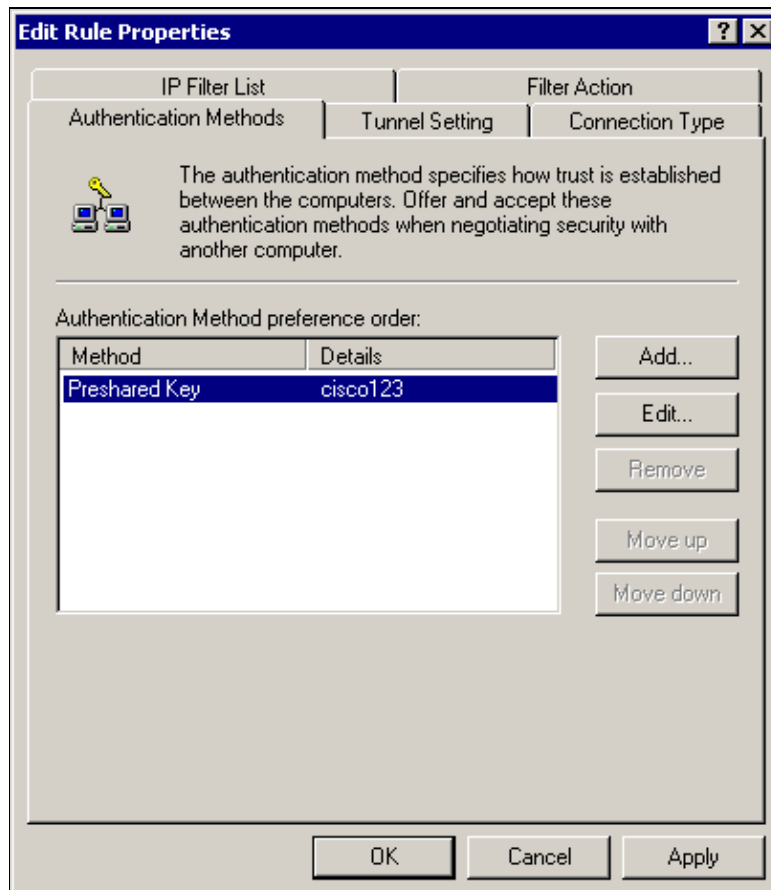


5. The rule's **General > Advanced > Methods** tab has the **IKE encryption method** (DES), **IKE hashing** (SHA1), and the **Diffie-Helman group** (Low(1)):

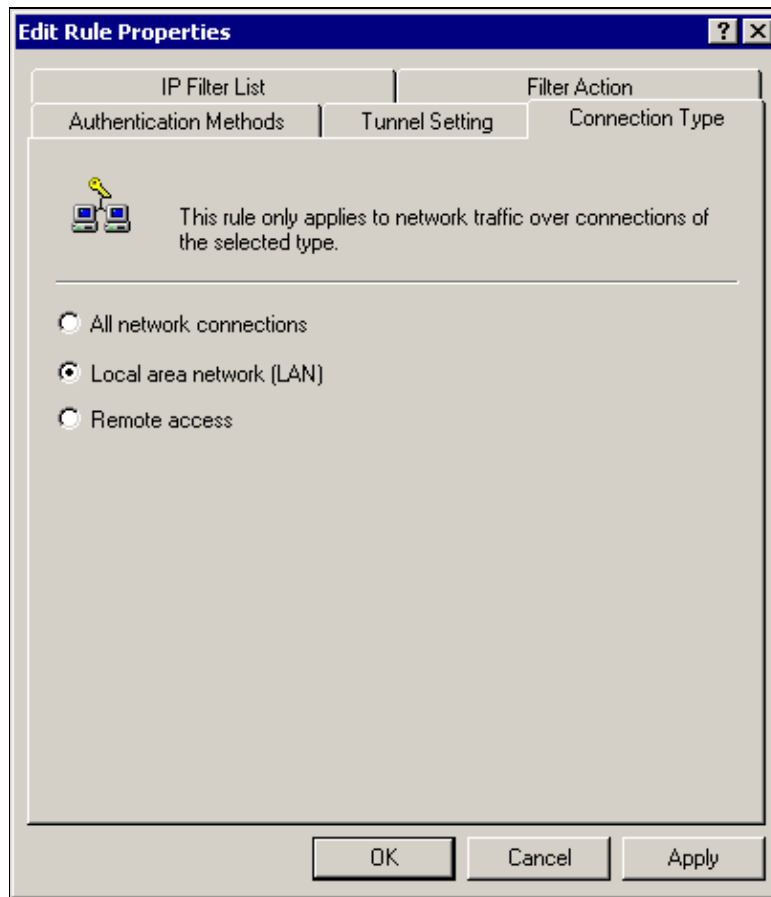


6. Each filter has 5 tabs:

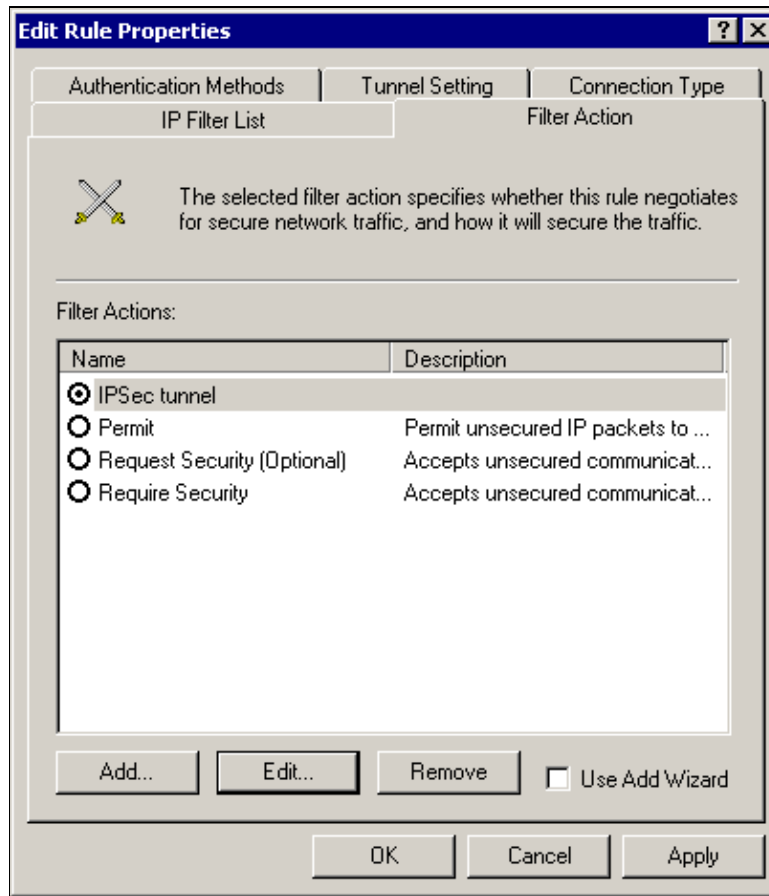
a. **Authentication Methods** (Preshared keys for Internet Key Exchange [IKE]):



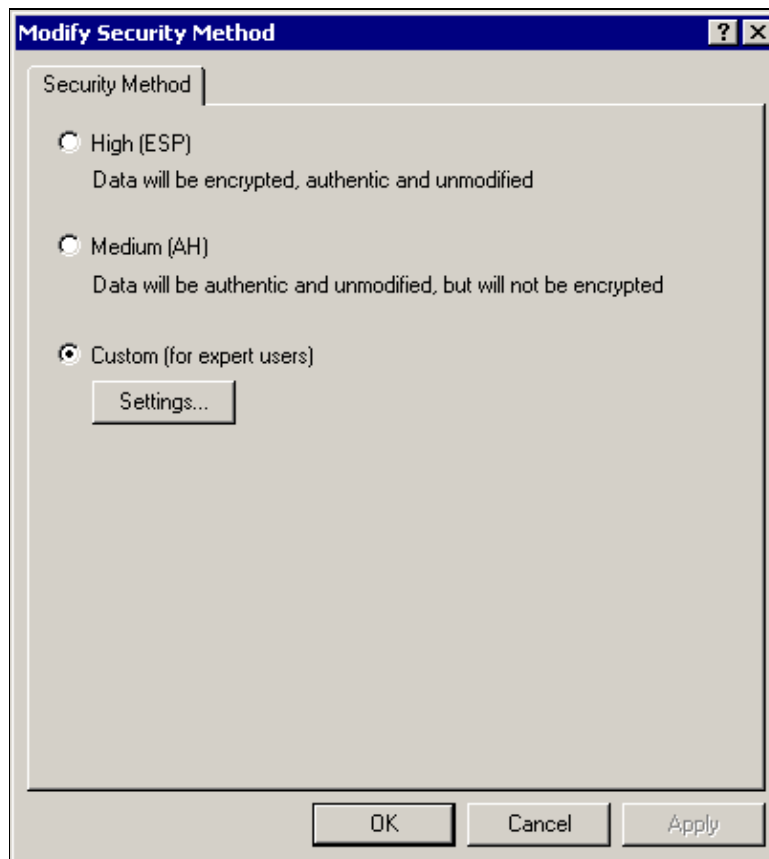
b. **Connection Type (LAN):**



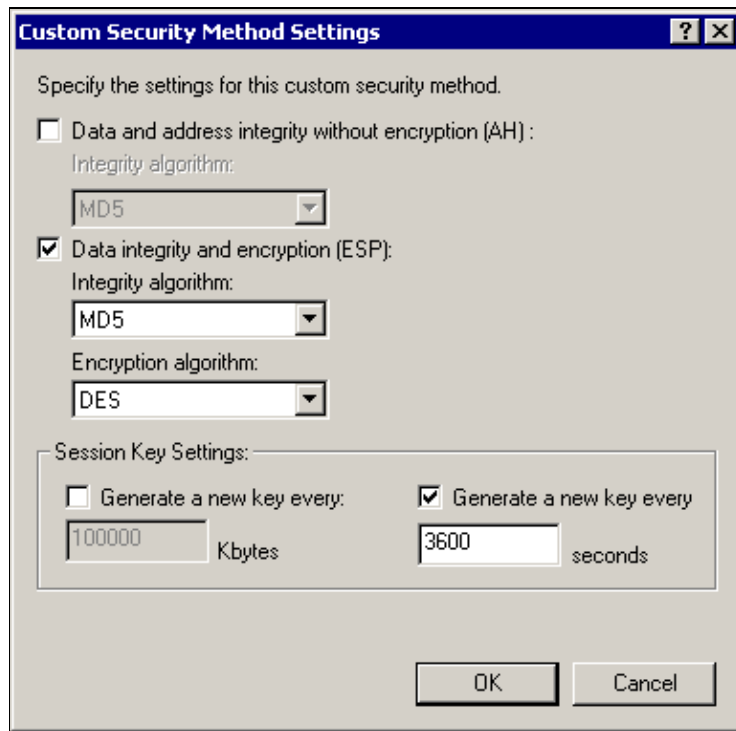
c. **Filter Action (IPSec):**



Select **Filter Action** > **IPSec tunnel** > **Edit** > **Edit**, and click **Custom**:

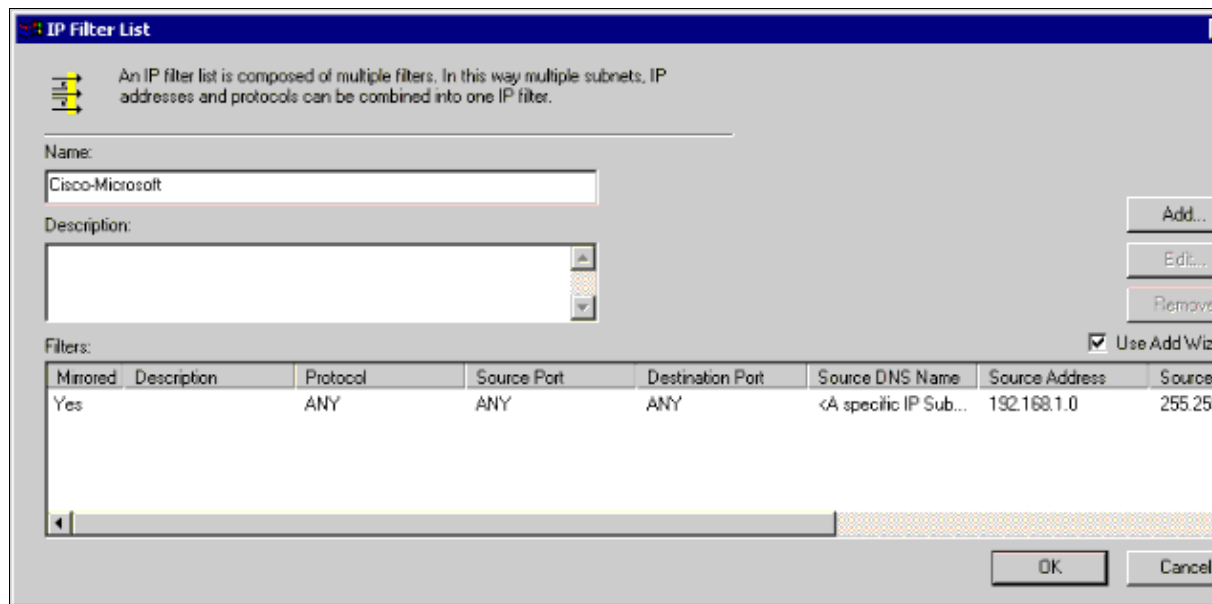


Click **Settings – IPsec transforms** and **IPsec lifetime**:

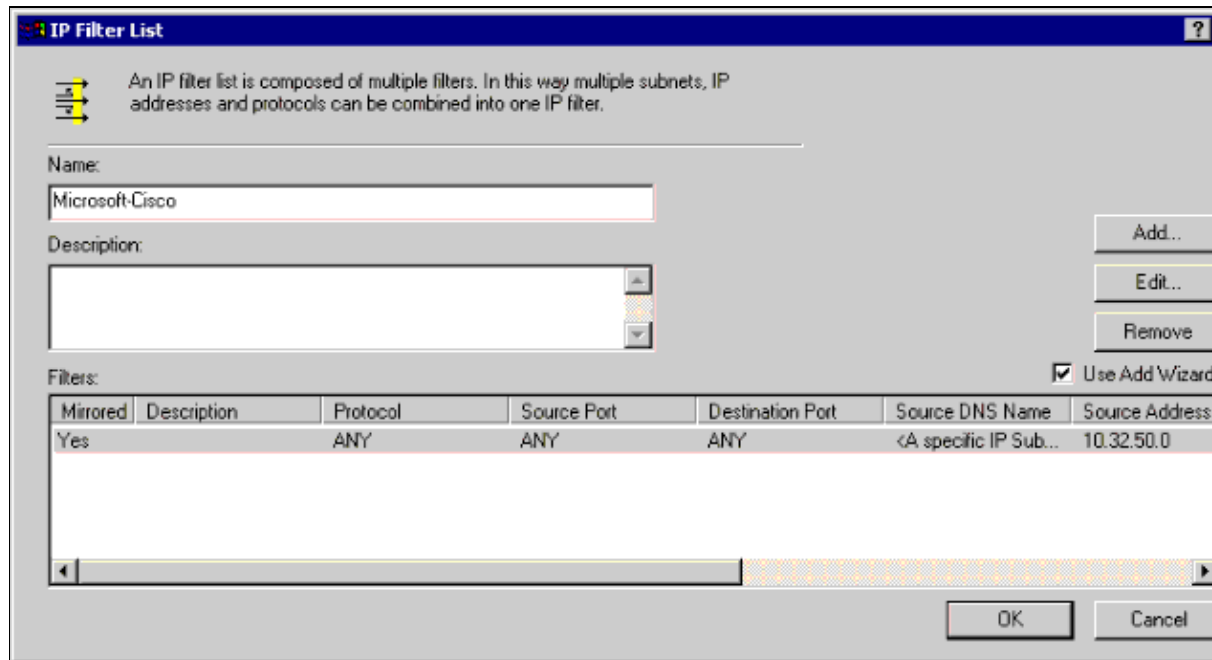


d. **IP Filter List – source & destination** networks to be encrypted:

For Cisco–Microsoft:

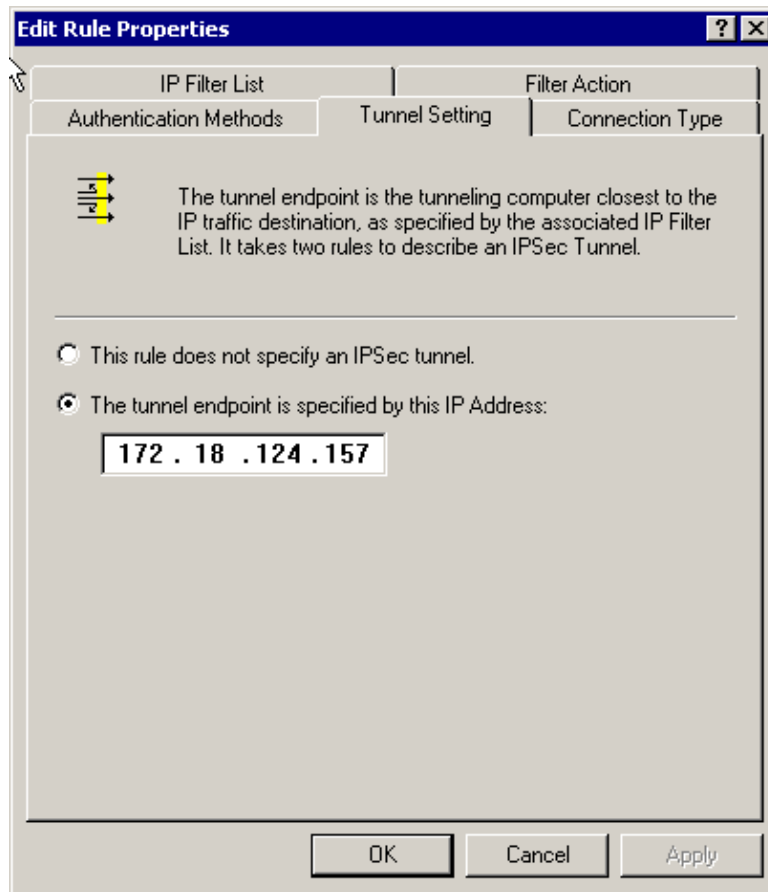


For Microsoft–Cisco:

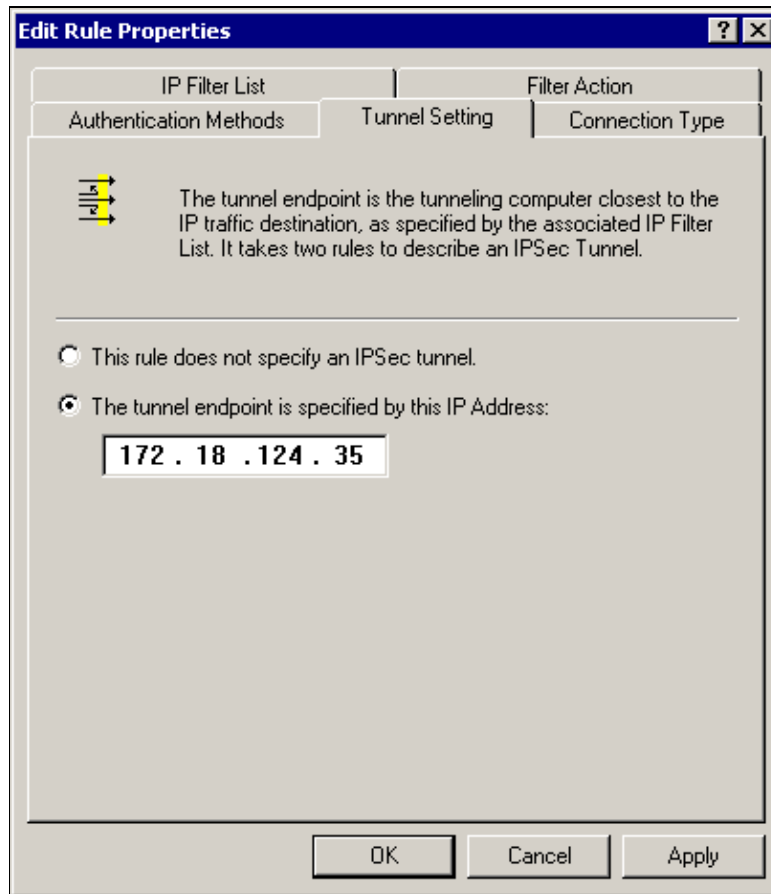


e. Tunnel Setting – encryption peers:

For Cisco–Microsoft:



For Microsoft–Cisco:



Configuring the Cisco Devices

Configure the Cisco router, PIX and VPN Concentrators as shown in the examples below.

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

Configuring the 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

```

Configuring 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
```

Configuring the VPN 3000 Concentrator

Use the menu options and parameters shown below to configure the VPN Concentrator as needed.

- To add an IKE proposal, select **Configuration > System > Tunneling Protocols > IPSec > IKE Proposals > Add a proposal.**

```
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
```

- To define the LAN-to-LAN tunnel, select **Configuration > System > Tunneling Protocols > IPSec LAN-to-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

- To modify the security association, select **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

Configuring the 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.
```

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

This section provides information you can use to troubleshoot your configurations.

Troubleshooting Commands

Certain **show** commands are supported by the Output Interpreter Tool (registered customers only) , which allows you to view an analysis of **show** command output.

Note: Before issuing **debug** commands, please see Important Information on Debug Commands.

Cisco 3640 Router

- **debug crypto engine** – Shows debug messages about crypto engines, which perform encryption and decryption.
- **debug crypto isakmp** – Shows messages about IKE events.
- **debug crypto ipsec** – Shows IPsec events.
- **show crypto isakmp sa** – Shows all current IKE security associations (SAs) at a peer.
- **show crypto ipsec sa** – Shows the settings used by current security associations.
- **clear crypto isakmp** – (from configuration mode) Clears all active IKE connections.
- **clear crypto sa** – (from configuration mode) Deletes all IPsec security associations.

PIX

- **debug crypto ipsec** – Shows the IPsec negotiations of phase 2.
- **debug crypto isakmp** – Shows the Internet Security Association and Key Management Protocol (ISAKMP) negotiations of phase 1.
- **debug crypto engine** – Shows the traffic that is encrypted.
- **show crypto ipsec sa** – Shows the phase 2 security associations.
- **show crypto isakmp sa** – Shows the phase 1 security associations.
- **clear crypto isakmp** – (from configuration mode) Clears Internet Key Exchange (IKE) security associations.
- **clear crypto ipsec sa** – (from configuration mode) Clears IPsec security associations.

VPN 3000 Concentrator

- – Start the VPN 3000 Concentrator debug by selecting **Configuration > System > Events > Classes > Modify** (Severity to Log=1–13, Severity to Console=1–3): IKE, IKEDBG, IKEDCODE, IPSEC, IPSECDBG, IPSECDCODE
- – The event log can be cleared or retrieved by selecting **Monitoring > Event Log**.
- – The LAN-to-LAN tunnel traffic can be monitored in **Monitoring > Sessions**.
- – The tunnel can be cleared in **Administration > Administer Sessions > LAN-to-LAN sessions > Actions – Logout**.

VPN 5000 Concentrator

- **vpn trace dump all** – Shows information about all matching VPN connections, including information about the time, the VPN number, the real IP address of the peer, which scripts have been run, and in the case of an error, the routine and line number of the software code where the error occurred.
- **show vpn statistics** – Shows the following information for Users, Partners, and the Total for both. (For modular models, the display includes a section for each module slot.) Current Active – The current active connections. In Negot – The currently negotiating connections. High Water – The highest number of concurrent active connections since the last reboot. Running Total – The total number of successful connections since the last reboot. Tunnel Starts – The number of tunnel starts. Tunnel OK – The number of tunnels for which there were no errors. Tunnel Error – The number of tunnels with errors.

- **show vpn statistics verbose** – Shows ISAKMP negotiation statistics, and many more active connection statistics.
-

Related Information

- **Cisco VPN 5000 Series Concentrators End-of-Sales Announcement**
 - **Configuring IPSec Network Security**
 - **Configuring Internet Key Exchange Security Protocol**
 - **Technical Support – Cisco Systems**
-

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 – 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Apr 04, 2008

Document ID: 14121
