

# Configuring an IPSec LAN-to-LAN Tunnel for Cisco VPN 5000 Concentrator to Cisco Secure PIX Firewall

Document ID: 14094

---

**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**

### **Prerequisites**

- Requirements
- Components Used
- Conventions

### **Configure**

- Network Diagram
- Configurations

### **Verify**

- Verify the VPN 5000 Concentrator
- Verify the PIX

### **Troubleshoot**

- VPN 5000 Concentrator Troubleshooting Commands
- PIX Troubleshooting Commands

### **NetPro Discussion Forums – Featured Conversations**

### **Related Information**

---

## **Introduction**

This document gives an overview of the configuration required to allow a Cisco Secure PIX Firewall and a Cisco VPN 500x Concentrator to open an IPSec LAN-to-LAN tunnel. For information about how to establish basic connectivity, or for reference on configuration syntax, consult the VPN 5000 Concentrator documentation and the PIX documentation.

## **Prerequisites**

### **Requirements**

There are no specific requirements for this document.

### **Components Used**

The information in this document is based on these software and hardware versions:

- PIX Software release 5.1(2)
- VPN 5002 Concentrator with the 5.2.15US and 6.0.20US software releases

**Note:** The configuration for the 6.0.20US software release is differentiated by two asterisks (\*\*).

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

## Conventions

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

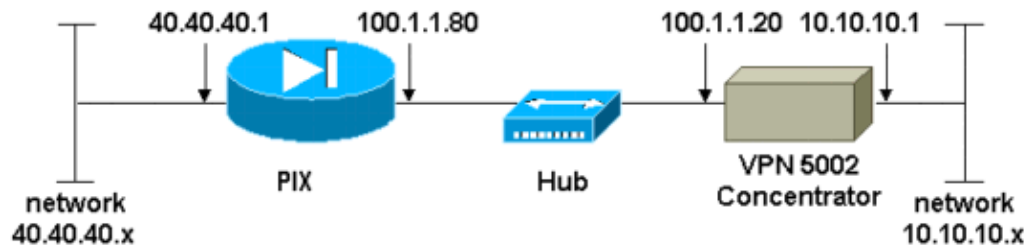
## Configure

In this section, you are presented with the information to configure the features described in this document.

**Note:** To find additional information on the commands used in this document, use the Command Lookup Tool (registered customers only).

## Network Diagram

This document uses this network setup:



## Configurations

This document uses these configurations:

- PIX Configuration
- VPN 5000 Concentrator Configuration

### PIX Configuration

```
:
PIX Version 5.1(2)
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
names

!--- Create crypto access list to specify interesting IPsec traffic
!--- for packets from PIX inside network to VPN 5002.

access-list 100 permit ip 40.40.40.0 255.255.255.0 10.10.10.0 255.255.255.0
```

```
!--- Exempt IPSec traffic from using NAT from PIX to VPN 5002.
```

```
access-list 101 permit ip 40.40.40.0 255.255.255.0 10.10.10.0 255.255.255.0  
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 10baset  
interface ethernet1 10baset  
mtu outside 1500  
mtu inside 1500  
ip address outside 100.1.1.80 255.255.255.0  
ip address inside 40.40.40.1 255.255.255.0  
arp timeout 14400
```

```
!--- Exempt IPSec traffic from using NAT from PIX to  
!--- VPN 5002 (access list 101).
```

```
nat (inside) 0 access-list 101  
conduit permit icmp any any  
route outside 0.0.0.0 0.0.0.0 100.1.1.20 1  
timeout xlate 3:00:00 conn 1:00:00 half-closed 0:10:00 udp 0:02:00  
timeout rpc 0:10:00 h323 0:05:00  
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
```

```
!--- Create an IPSec transform set named "myset". Use DES for ESP  
!--- and ESP with the MD5 (HMAC variant) authentication algorithm  
!--- with transport mode. Note that Authentication Header is not used.
```

```
crypto ipsec transform-set myset esp-des esp-md5-hmac
```

```
!--- Create a crypto map "newmap" and assign sequence number 10. This is used  
!--- to rank multiple entries within one crypto map set (the lower the sequence  
!--- number, the higher the priority). Use IKE to establish Security Associations and  
!--- use IPSec for traffic specified in access list 100. Specify VPN 5002 as the remote  
!--- IPSec peer, and assign transform set "myset" for policy information.
```

```
crypto map newmap 10 ipsec-isakmp  
crypto map newmap 10 match address 100  
crypto map newmap 10 set peer 100.1.1.20  
crypto map newmap 10 set transform-set myset
```

```
!--- Evaluate traffic that goes through the outside  
!--- interface against the crypto map  
!--- "newmap" to determine whether it needs to be protected.
```

```
crypto map newmap interface outside
```

```
!--- Enable IPSec IKE on the outside interface.
```

```
isakmp enable outside
```

```

!--- Specify the pre-shared key and remote peer (VPN 5002) for SA negotiation.

isakmp key cisco123 address 100.1.1.20 netmask 255.255.255.255

!--- Use IP address for ISAKMP identity during IKE negotiation.

isakmp identity address

!--- Use pre-shared key for IKE, DES encryption, MD5, Diffie Hellman Group type 1
!--- (768 bit) and SA lifetime of 1000 seconds.

isakmp policy 10 authentication pre-share
isakmp policy 10 encryption des
isakmp policy 10 hash md5
isakmp policy 10 group 1
isakmp policy 10 lifetime 1000
telnet timeout 5
terminal width 80
Cryptochecksum:21e462e1e749c3138288bfe7ede24ed4
: end
[OK]

```

### VPN 5000 Concentrator Configuration

```

[ IP Ethernet 0:0 ]
Mode = Routed
SubnetMask = 255.255.255.0
IPAddress = 10.10.10.1

[ IP Ethernet 1:0 ]
Mode = Routed
SubnetMask = 255.255.255.0
IPAddress = 100.1.1.20

[ General ]
DeviceName = "rtp5002"
IPSecGateway(**VPNGateway)= 100.1.1.80
EthernetAddress = 00:00:a5:e9:c8:00
DeviceType = VPN 5002/8 Concentrator
ConfiguredOn = Timeserver not configured
ConfiguredFrom = Command Line, from Console

[ IP Static ]
40.40.40.0 255.255.255.0 vpn 1 1

[ Tunnel Partner VPN 1 ]
LocalAccess = "10.10.10.0/24"
Peer = "40.40.40.0/24"
Mode = Main
Transform = esp(md5,des)
KeyManage = Auto (**Reliable)
SharedKey = "cisco123"
BindTo = "ethernet 1:0"
Partner = 100.1.1.80
**InactivityTimeout = 120
**TunnelType = IPSec
**KeepaliveInterval = 120
**KeyLifeSecs = 3500
**Certificates = Off

[ IP VPN 1 ]
Numbered = Off
Mode = Routed

[ IKE Policy ]

```

```
Protection                = MD5_DES_G1

[ VPN Group "rtp" ]
DNSPrimaryServer          = 100.100.100.100
BindTo                    = "ethernet 1:0"
StartIPAddress            = 10.10.10.50
IPNet                     = 10.10.10.0/24
Transform                 = esp(md5,des)
MaxConnections            = 10

[ VPN Users ]
omar config="rtp" sharedkey="letmein"

Configuration size is 1388 out of 65500 bytes.
```

## Verify

### Verify the VPN 5000 Concentrator

This section provides information you can use to confirm your configuration is working properly.

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

- **show vpn partners** Displays this information:
  - ◆ The VPN port number to which the peer is connected.
  - ◆ The tunnel peer's IP address.
  - ◆ The UDP port for the connection.
  - ◆ Whether the tunnel peer is connected to this VPN Concentrator's Tunnel Partner Default section instead of a specific Tunnel Partner section.
  - ◆ The IP address used as the local endpoint of the tunnel.
  - ◆ How long the partners have been connected.
- **show vpn statistics** Displays this information for Users and Partners, and the total for both:
  - ◆ Current active connections.
  - ◆ Currently negotiating connections.
  - ◆ The highest number of concurrent active connections since the last reboot.
  - ◆ The total number of successful connections since the last reboot.
  - ◆ The number of tunnel starts.
  - ◆ The number of tunnels for which there were no errors.
  - ◆ The number of tunnels with errors.

### Verify the PIX

This section provides information you can use to confirm your configuration is working properly.

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

- **show crypto ipsec sa** Displays Phase 2 security associations.
- **show crypto isakmp sa** Displays Phase 1 security associations.
- **show crypto engine** Displays information regarding encrypted and decrypted packets.

# Troubleshoot

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

## VPN 5000 Concentrator 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, refer to Important Information on Debug Commands.

- **show sys log buffer** Displays previously buffered events.
- **vpn trace dump all** Displays information about all matching VPN connections. This includes 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.

## PIX 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, refer to Important Information on Debug Commands.

- **debug crypto ipsec** Displays errors during Phase 2.
- **debug crypto isakmp** Displays errors during Phase 1.
- **debug crypto engine** Displays information from the crypto engine.

## NetPro Discussion Forums – Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

NetPro Discussion Forums – Featured Conversations for VPN
Service Providers: VPN Service Architectures
Service Providers: Network Management
Virtual Private Networks: General

## Related Information

- [Cisco VPN 5000 Concentrator Support Page](#)
- [Cisco VPN 5000 Client Support Page](#)
- [IPSec Support Page](#)
- [PIX Support Page](#)
- [Documentation for PIX Firewall](#)
- [PIX Command References](#)
- [Requests for Comments \(RFCs\)](#)
- [Technical Support – Cisco Systems](#)

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

© 2007 – 2008 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

---

Updated: May 02, 2008

Document ID: 14094

---