

LAN-to-LAN IPsec Tunnel Between the Cisco VPN 3000 Concentrator and PIX Firewall Configuration Example

Document ID: 14100

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

Configure

- Network Diagram
- Configurations

Verify

Troubleshoot

- Troubleshooting Commands on the PIX
- Troubleshooting on the VPN Concentrator

NetPro Discussion Forums – Featured Conversations

Related Information

Introduction

The goal of this sample configuration is to connect a private network behind a Cisco PIX Firewall to a private network behind the Cisco VPN 3000 Concentrator. The devices on the networks know each other by their private addresses.

Refer to [IPsec: Router-to-PIX Security Appliance 7.x and Later or ASA Configuration Example](#) for more information about the LAN-to-LAN tunnel configuration between a router and Cisco PIX/ASA Security Appliances.

Refer to [IPsec Tunnel Between PIX 7.x and VPN 3000 Concentrator Configuration Example](#) for more information when the PIX has software version 7.x.

Refer to [LAN-to-LAN IPsec Tunnel Between a Cisco VPN 3000 Concentrator and Router with AES Configuration Example](#) for more information about the L2L IPsec tunnel configuration between a Cisco VPN 3000 Concentrator and router with Advance Encryption Standard (AES).

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 6.3(1)

- VPN 3000 Concentrator with 4.0.1

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

Refer to Cisco Technical Tips Conventions for more information on document conventions.

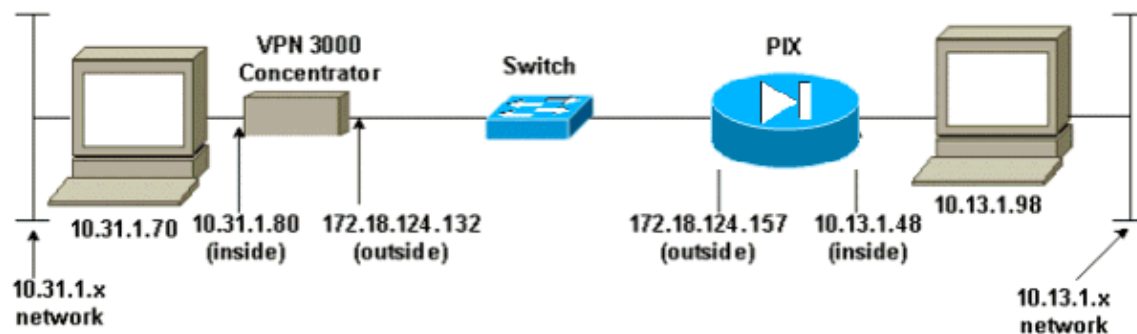
Configure

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

Note: Use the Command Lookup Tool (registered customers only) to obtain more information on the commands used in this section.

Network Diagram

This document uses this network setup:



Configurations

Configure the PIX

PIX Firewall Configuration

```
PIX Version 6.3(1)
interface ethernet0 auto
interface ethernet1 auto
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname sv2-11
fixup protocol ftp 21
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol http 80
fixup protocol ils 389
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol sip 5060
fixup protocol sip udp 5060
fixup protocol skinny 2000
```

```
fixup protocol smtp 25
fixup protocol sqlnet 1521
names

!--- Access control list (ACL) for interesting traffic
!--- to be encrypted over the tunnel.

access-list 101 permit ip 10.13.1.0 255.255.255.0 10.31.1.0 255.255.255.0
pager lines 24
mtu outside 1500
mtu inside 1500

!--- IP addresses on the interfaces.

ip address outside 172.18.124.157 255.255.255.0
ip address inside 10.13.1.48 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
no failover
failover timeout 0:00:00
failover poll 15
no failover ip address outside
no failover ip address inside
pdm history enable
arp timeout 14400
global (outside) 1 interface

!--- Binding ACL 101 to the Network Address Translation (NAT) statement
!--- to avoid NAT on the IPsec packet.

nat (inside) 0 access-list 101
nat (inside) 1 0.0.0.0 0.0.0.0 0 0

!--- Default route to the Internet.

route outside 0.0.0.0 0.0.0.0 172.16.124.132 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h225 1:00:00
timeout h323 0:05:00 mgcp 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
aaa-server LOCAL protocol local
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable

!--- The sysopt command avoids conduit on
!--- the IPsec-encrypted traffic.

sysopt connection permit-ipsec

!---- IPsec policies

crypto ipsec transform-set aptset esp-3des esp-md5-hmac

!--- Setting up the tunnel peer, encryption ACL, and transform set.

crypto map aptmap 10 ipsec-isakmp
crypto map aptmap 10 match address 101
crypto map aptmap 10 set peer 172.18.124.132
crypto map aptmap 10 set transform-set aptset

!--- Applying the crypto map on the interface.
```

```
crypto map aptmap interface outside
isakmp enable outside

!--- Pre-shared key for the tunnel peer.

isakmp key ***** address 172.18.124.132 netmask 255.255.255.255

!--- IKE policies

isakmp policy 10 authentication pre-share
isakmp policy 10 encryption 3des
isakmp policy 10 hash md5
isakmp policy 10 group 2
isakmp policy 10 lifetime 86400
telnet timeout 5
ssh timeout 5
console timeout 0
terminal width 80
Cryptochecksum:1209dc5ffed40ad7c999d655509260f5
: end
[OK]
```

Configure the VPN Concentrator

Complete these steps in order to configure the VPN Concentrator.

Note: This example was performed in a lab environment by accessing the VPN Concentrator through the console port and adding a minimal configuration (see steps 1 and 2) so that the additional configuration is done through the graphical user interface (GUI).

1. Go to **Administration > System Reboot > Schedule reboot > Reboot with Factory/Default Configuration** and reboot.
2. When the VPN Concentrator comes up in Quick Configuration mode after you reboot, configure basic device information:
 - ◆ Time/Date
 - ◆ Interfaces/Masks in **Configuration > Interfaces** (public=172.18.124.132/24, private=10.31.1.80/24)
 - ◆ Default Gateway in **Configuration > System > IP routing > Default_Gateway > 172.18.124.157**

The VPN Concentrator is now accessible through the GUI from the inside network.

Note: You can also manage the VPN Concentrator from the outside. Refer to How to Manage the VPN 3000 Concentrator from the Public Network for more information.

3. Launch the GUI and go to **Configuration > Interfaces** in order to confirm the interfaces.

Note: The interface that terminates the tunnel should have a filter applied to it. In this case, the public interface has the public (default) filter applied. Rules are automatically added later to the applied filter on the IPSec interface.

Configuration | Interfaces Tuesday, 08
Save Ne...

This section lets you configure the VPN 3000 Concentrator's network interfaces and power supplies.

In the table below, or in the picture, select and click the interface you want to configure:

| Interface | Status | IP Address | Subnet Mask | MAC Address | Default Gateway |
|---------------------------------------|---------------------------|----------------|---------------|-------------------|-----------------|
| Ethernet 1 (Private) | UP | 10.31.1.80 | 255.255.255.0 | 00.03.A0.88.5A.5A | |
| Ethernet 2 (Public) | UP | 172.18.124.132 | 255.255.255.0 | 00.03.A0.88.5A.5B | |
| Ethernet 3 (External) | Not Configured | 0.0.0.0 | 0.0.0.0 | | |
| DNS Server(s) | DNS Server Not Configured | | | | |
| DNS Domain Name | | | | | |

• [Power Supplies](#)

- Go to **Configuration > System > Tunneling Protocols > IPSec LAN-to-LAN > Modify or Add** in order to configure the IPSec LAN-to-LAN tunnel. Click **Apply** when you are finished.

In this example, the necessary information for the outside interface of the PIX is populated.

Configuration | System | Tunneling Protocols | IPSec | LAN-to-LAN | Add

Add a new IPSec LAN-to-LAN connection.

| | |
|---|---|
| Enable <input checked="" type="checkbox"/> | Check to enable this LAN-to-LAN connection. |
| Name <input type="text" value="to_pix"/> | Enter the name for this LAN-to-LAN connection. |
| Interface <input type="text" value="Ethernet 2 (Public) (172.18.124.132)"/> | Select the interface for this LAN-to-LAN connection. |
| Connection Type <input type="text" value="Bi-directional"/> | Choose the type of LAN-to-LAN connection. An <i>Originate-Only</i> connection may have multiple peers specified below. |
| Peers <input type="text" value="172.18.124.157"/> | Enter the remote peer IP addresses for this LAN-to-LAN connection. <i>Originate-Only</i> connection may specify up to ten peer IP addresses. Enter one IP address per line. |
| Digital Certificate <input type="text" value="None (Use Preshared Keys)"/> | Select the digital certificate to use. |
| Certificate Transmission <input type="radio"/> Entire certificate chain <input checked="" type="radio"/> Identity certificate only | Choose how to send the digital certificate to the IKE peer. |
| Preshared Key <input type="text" value="cisco123"/> | Enter the preshared key for this LAN-to-LAN connection. |
| Authentication <input type="text" value="ESP/MD5/HMAC-128"/> | Specify the packet authentication mechanism to use. |
| Encryption <input type="text" value="3DES-168"/> | Specify the encryption mechanism to use. |
| IKE Proposal <input type="text" value="IKE-3DES-MD5"/> | Select the IKE Proposal to use for this LAN-to-LAN connection. |
| Filter <input type="text" value="-None-"/> | Choose the filter to apply to the traffic that is tunneled through this LAN-to-LAN connection. |
| IPSec NAT-T <input type="checkbox"/> | Check to let NAT-T compatible IPSec peers establish this LAN-to-LAN connection through a NAT device. You must also enable IPSec over NAT-T under NAT Transparency. |
| Bandwidth Policy <input type="text" value="-None-"/> | Choose the bandwidth policy to apply to this LAN-to-LAN connection. |
| Routing <input type="text" value="None"/> | Choose the routing mechanism to use. Parameters below are ignored if Network Autodiscovery is chosen. |

Local Network: If a LAN-to-LAN NAT rule is used, this is the Translated Network address.

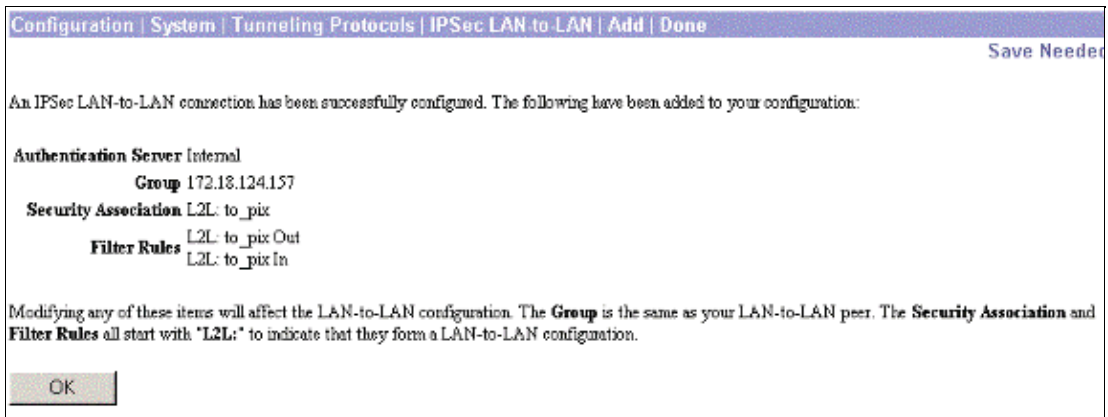
| | |
|---|---|
| Network List <input type="text" value="Use IP Address/Wildcard-mask below"/> | Specify the local network address list or the IP address and wildcard mask for this LAN-to-LAN connection. |
| IP Address <input type="text" value="10.31.1.0"/> | Note: Enter a <i>wildcard mask</i> , which is the reverse of a subnet mask. A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.n.m addresses. |
| Wildcard Mask <input type="text" value="0.0.0.255"/> | |

Remote Network: If a LAN-to-LAN NAT rule is used, this is the Remote Network address.

| | |
|---|---|
| Network List <input type="text" value="Use IP Address/Wildcard-mask below"/> | Specify the remote network address list or the IP address and wildcard mask for this LAN-to-LAN connection. |
| IP Address <input type="text" value="10.13.1.0"/> | Note: Enter a <i>wildcard mask</i> , which is the reverse of a subnet mask. A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.n.m addresses. |
| Wildcard Mask <input type="text" value="0.0.0.255"/> | |

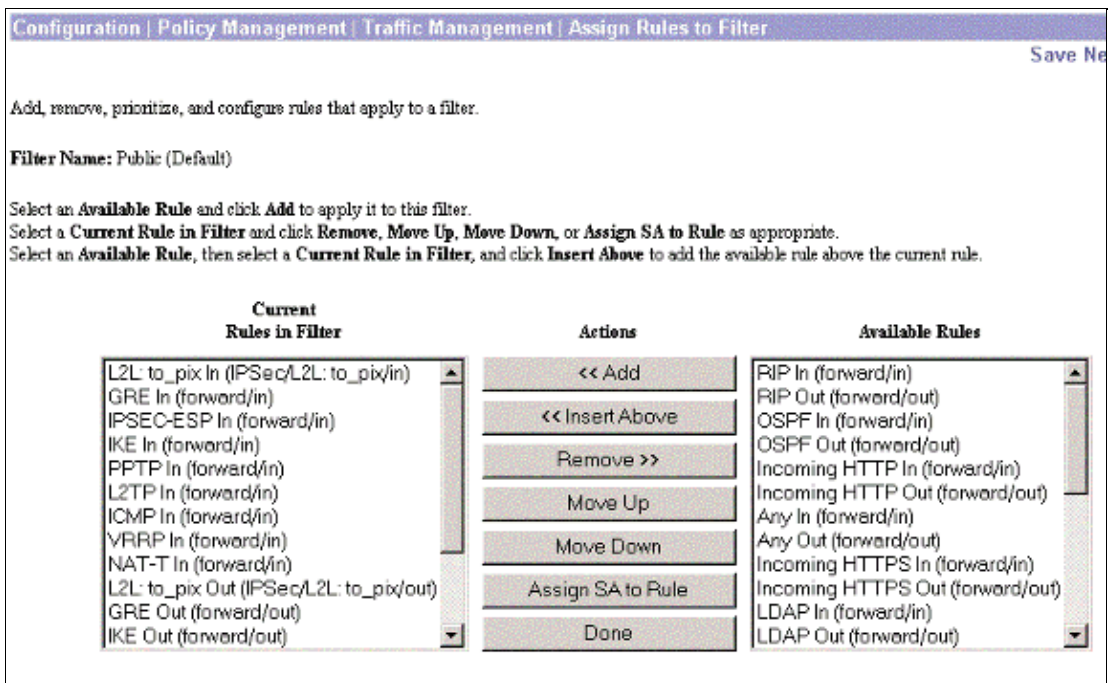
- On the confirmation page that displays the automatically configured parameters, click **OK** in order to accept the configuration.

Note: Do not modify these LAN-to-LAN settings.



- Go to **Configuration > Policy Management > Traffic Management > Assign Rules to Filter** in order to confirm that the rules have been created and applied correctly.

Rules are automatically created and added to the filter applied to the IPsec interface. In this case, the public (default) filter that is applied to the public interface has new rules added to it by the configuration.



- On the confirmation page that displays the automatically configured group information, click **Apply** in order to accept the group settings.

Note: Do not modify these group settings.

Configuration | User Management | Groups | Modify 172.18.124.157

Check the **Inherit?** box to set a field that you want to default to the base group value. Uncheck the **Inherit?** box and enter a new value to override base group values.

Identity | General | IPsec | Client Config | Client FW | HW Client | PPTP/L2TP

| Identity Parameters | | |
|---------------------|----------------|---|
| Attribute | Value | Description |
| Group Name | 172.18.124.157 | Enter a unique name for the group. |
| Password | XXXXXXXXXX | Enter the password for the group. |
| Verify | XXXXXXXXXX | Verify the group's password. |
| Type | Internal | External groups are configured on an external authentication server (e.g. RADIUS). Internal groups are configured on the VPN 3000 Concentrator's Internal Database. |

Apply Cancel

- On the confirmation page that displays the automatically created security association (SA), confirm that the SA appears in the list of IPsec SAs.

Configuration | Policy Management | Traffic Management | Security Associations Save Needed

This section lets you add, configure, modify, and delete IPsec Security Associations (SAs). Security Associations use [IKE Proposals](#) to negotiate IKE parameters.

Click **Add** to add an SA, or select an SA and click **Modify** or **Delete**.

| IPsec SAs | Actions |
|--------------------|-------------------------|
| ESP-3DES-MD5 | Add Modify Delete |
| ESP-3DES-MD5-DH5 | |
| ESP-3DES-MD5-DH7 | |
| ESP-3DES-NONE | |
| ESP-AES128-SHA | |
| ESP-DES-MD5 | |
| ESP-L2TP-TRANSPORT | |
| ESP/IKE-3DES-MD5 | |
| L2L:to_pix | |

- Go to **Configuration > System > Tunneling Protocols > IPsec > IKE Proposals** in order to confirm that the IKE proposals are shown as active.

Configuration | System | Tunneling Protocols | IPsec | IKE Proposals Save

Add, delete, prioritize, and configure IKE Proposals.

Select an **Inactive Proposal** and click **Activate** to make it **Active**, or click **Modify**, **Copy** or **Delete** as appropriate.
 Select an **Active Proposal** and click **Deactivate** to make it **Inactive**, or click **Move Up** or **Move Down** to change its priority.
 Click **Add** or **Copy** to add a new **Inactive Proposal**. IKE Proposals are used by [Security Associations](#) to specify IKE parameters.

| Active Proposals | Actions | Inactive Proposals |
|--|---|--|
| CiscoVPNClient-3DES-MD5 IKE-3DES-MD5 IKE-3DES-MD5-DH1 IKE-DES-MD5 IKE-3DES-MD5-DH7 IKE-3DES-MD5-RSA CiscoVPNClient-3DES-MD5-DH5 CiscoVPNClient-AES128-SHA IKE-AES128-SHA | << Activate Deactivate >> Move Up Move Down Add Modify Copy Delete | IKE-3DES-SHA-DSA IKE-3DES-MD5-RSA-DH1 IKE-DES-MD5-DH7 CiscoVPNClient-3DES-MD5-RSA CiscoVPNClient-3DES-SHA-DSA CiscoVPNClient-3DES-MD5-RSA-DH5 CiscoVPNClient-3DES-SHA-DSA-DH5 CiscoVPNClient-AES256-SHA IKE-AES256-SHA |

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

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

Troubleshooting Commands on the PIX

Note: Refer to Important Information on Debug Commands before you use **debug** commands.

- **debug crypto engine** Shows the traffic that is encrypted.
- **debug crypto ipsec** Use to see the IPSec negotiations of phase 2.
- **debug crypto isakmp** Use to see the Internet Security Association and Key Management Protocol (ISAKMP) negotiations of phase 1.

Troubleshooting on the VPN Concentrator

These debug options are individually available if you go to **Configuration > System > Events > Classes > Add**.

- IKE
- IKEDBG
- IKEDECODE
- IPSEC
- IPSECDBG
- IPSECDECODE

Go to **Monitoring > Event Log** and click **Get Log** in order to see the actual debug.

Monitoring | Filterable Event Log

Select Filter Options

Event Class: All Classes, AUTH, AUTHDBG, AUTHDECODE

Severities: ALL, 1, 2, 3

Client IP Address: 0.0.0.0

Events/Page: 100

Group: -All-

Direction: Oldest to Newest

Get Log, Save Log, Clear Log

Navigation buttons: [Left Arrow], [Double Left Arrow], [Double Right Arrow], [Right Arrow]

Go to **Monitoring > Statistics > IPSec** in order to see IPSec status.

| IKE (Phase 1) Statistics | | IPSec (Phase 2) Statistics | |
|-------------------------------------|----|--|-----|
| Active Tunnels | 0 | Active Tunnels | 0 |
| Total Tunnels | 0 | Total Tunnels | 0 |
| Received Bytes | 84 | Received Bytes | 256 |
| Sent Bytes | 84 | Sent Bytes | 256 |
| Received Packets | 1 | Received Packets | 4 |
| Sent Packets | 1 | Sent Packets | 4 |
| Received Packets Dropped | 0 | Received Packets Dropped | 0 |
| Sent Packets Dropped | 0 | Received Packets Dropped (Anti-Replay) | 0 |
| Received Notifies | 1 | Sent Packets Dropped | 0 |
| Sent Notifies | 2 | Inbound Authentications | 4 |
| Received Phase-2 Exchanges | 0 | Failed Inbound Authentications | 0 |
| Sent Phase-2 Exchanges | 0 | Outbound Authentications | 4 |
| Invalid Phase-2 Exchanges Received | 0 | Failed Outbound Authentications | 0 |
| Invalid Phase-2 Exchanges Sent | 0 | Decryptions | 4 |
| Rejected Received Phase-2 Exchanges | 0 | Failed Decryptions | 0 |
| Rejected Sent Phase-2 Exchanges | 0 | Encryptions | 4 |
| Phase-2 SA Delete Requests Received | 0 | Failed Encryptions | 0 |
| Phase-2 SA Delete Requests Sent | 0 | System Capability Failures | 0 |
| Initiated Tunnels | 0 | No-SA Failures | 0 |
| Failed Initiated Tunnels | 0 | Protocol Use Failures | 0 |

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 3000 Series Concentrators Support Page](#)
- [Cisco VPN 3000 Client Support Page](#)
- [PIX 500 Series Firewalls Support Page](#)
- [Cisco Secure PIX Firewall Command References](#)
- [IP Security Protocol \(IPSec\) Support Page](#)
- [Configuring IPSec Network Security](#)
- [Request for Comments \(RFCs\)](#)
- [Technical Support and Documentation – 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: Oct 14, 2009

Document ID: 14100
