

Configuring IPsec Between Two PIXes With VPN Client 4.x Access

Document ID: 14092

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

Configure

- Network Diagram
- Configuring the PIXes
- Configuring the VPN Client

Verify

- Verify Crypto Map Sequence Numbers

Troubleshoot

- Troubleshooting Commands

NetPro Discussion Forums – Featured Conversations

Related Information

Introduction

This document illustrates two Cisco Secure PIX Firewall devices that run a simple VPN tunnel from PIX 1 to PIX 2 over a public network using IPsec. A Cisco VPN Client 4.x connects to PIX 1. The configuration uses pre-shared keys (wild-cards for the clients' IPs), and mode configuration for the clients.

Note: The VPN Client can access the LAN behind PIX 1, but not the LAN behind PIX 2. The PIX does not redirect traffic.

Prerequisites

Requirements

For IPsec to work, you must have established connectivity from tunnel endpoint to tunnel endpoint *before* you start this configuration.

Components Used

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

- PIX Firewall Version 6.3 (1)

Note: The **show version** command must show that encryption is enabled.

- VPN Client Version 4.0.2 (A)

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.

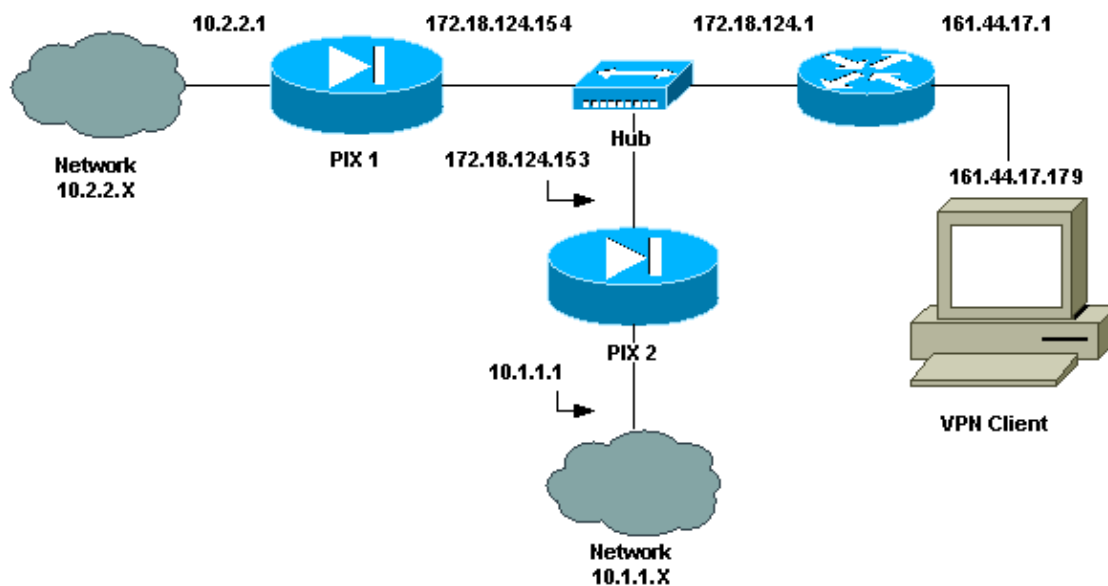
Configure

This section explains how to configure PIX to PIX and VPN Client 4.x.

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:



Configuring the PIXes

This document uses these configurations:

- PIX 1 Configuration
- PIX 2 Configuration

PIX 1 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 pix-1
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
```

```
!--- Except traffic from the Network Address Translation (NAT) process.
```

```
access-list 100 permit ip 10.2.2.0 255.255.255.0 10.1.1.0 255.255.255.0
access-list 100 permit ip 10.2.2.0 255.255.255.0 192.168.1.0 255.255.255.0
```

```
!--- Include traffic in the encryption process.
```

```
access-list 110 permit ip 10.2.2.0 255.255.255.0 10.1.1.0 255.255.255.0
pager lines 24
mtu outside 1500
mtu inside 1500
ip address outside 172.18.124.154 255.255.255.0
ip address inside 10.2.2.1 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
ip local pool test 192.168.1.1-192.168.1.25
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
```

```
!--- Except traffic from the NAT process.
```

```
nat (inside) 0 access-list 100
route outside 0.0.0.0 0.0.0.0 172.18.124.1 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
aaa-server LOCAL protocol local
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
sysopt connection permit-ipsec
crypto ipsec transform-set myset esp-3des esp-md5-hmac
crypto dynamic-map dynmap 30 set transform-set myset
```

```
!--- Use the crypto-map sequence 10 command for PIX to PIX.
```

```
crypto map newmap 10 ipsec-isakmp
crypto map newmap 10 match address 110
crypto map newmap 10 set peer 172.18.124.153
crypto map newmap 10 set transform-set myset
```

```
!--- Use the crypto-map sequence 65000 command for PIX to VPN Client.
```

```
crypto map newmap 65000 ipsec-isakmp dynamic dynmap
crypto map newmap interface outside
isakmp enable outside
isakmp key ***** address 172.18.124.153 netmask 255.255.255.255
no-xauth no-config-mode
```

```

isakmp identity address
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption 3des
isakmp policy 10 hash md5

!--- Internet Security Association and Key Management Protocol (ISAKMP) policy
!--- for a VPN Client running 3.x code and later needs to be Diffie-Hellman (DH)
!--- group 2 or above (group 1 is default).

isakmp policy 10 group 2
isakmp policy 10 lifetime 86400

!--- IPSec group configuration for VPN Client.

vpngroup vpn3000 address-pool test
vpngroup vpn3000 dns-server 10.2.2.2
vpngroup vpn3000 wins-server 10.2.2.2
vpngroup vpn3000 default-domain cisco.com
vpngroup vpn3000 idle-time 1800
vpngroup vpn3000 password *****
telnet timeout 5
ssh timeout 5
terminal width 80
Cryptochecksum:0527568558f8f0a4017a2db377a36cc2
: end
[OK]

```

PIX 2 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 pix-2
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

!--- Except traffic from the NAT process.

access-list 100 permit ip 10.1.1.0 255.255.255.0 10.2.2.0 255.255.255.0
pager lines 24
interface ethernet0 10baset
interface ethernet1 10full
mtu outside 1500
mtu inside 1500
ip address outside 172.18.124.153 255.255.255.0
ip address inside 10.1.1.1 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
pdm history enable
arp timeout 14400

```

```

!--- Except traffic from the NAT process.

nat (inside) 0 access-list 100
route outside 0.0.0.0 0.0.0.0 172.18.124.1 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
aaa-server LOCAL protocol local
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
sysopt connection permit-ipsec
crypto ipsec transform-set myset esp-3des esp-md5-hmac
crypto map newmap 10 ipsec-isakmp

!--- Include traffic in the encryption process.

crypto map newmap 10 match address 100
crypto map newmap 10 set peer 172.18.124.154
crypto map newmap 10 set transform-set myset
crypto map newmap interface outside
isakmp enable outside
isakmp key ***** address 172.18.124.154 netmask 255.255.255.255
no-xauth no-config-mode
isakmp identity address
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
terminal width 80
Cryptochecksum:6d2f51a85d4f8a7991b62183fcc2836c
: end
[OK]

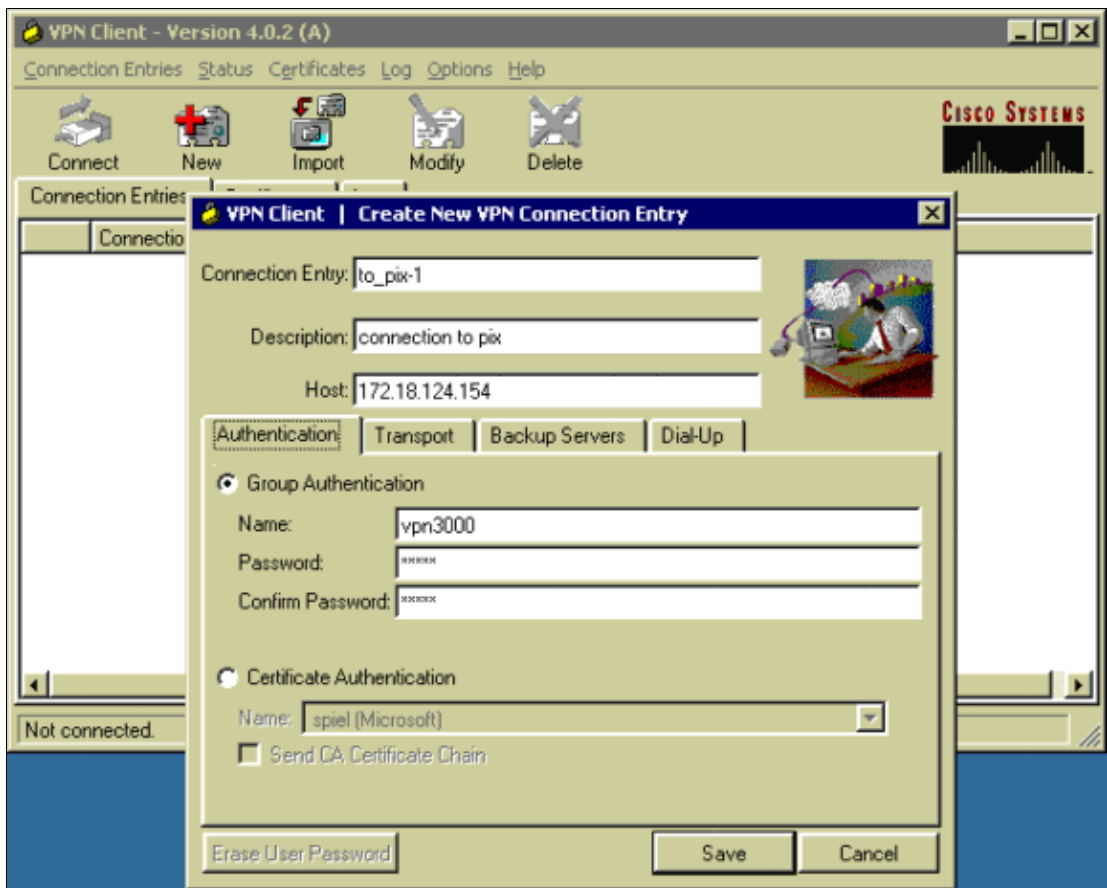
```

Configuring the VPN Client

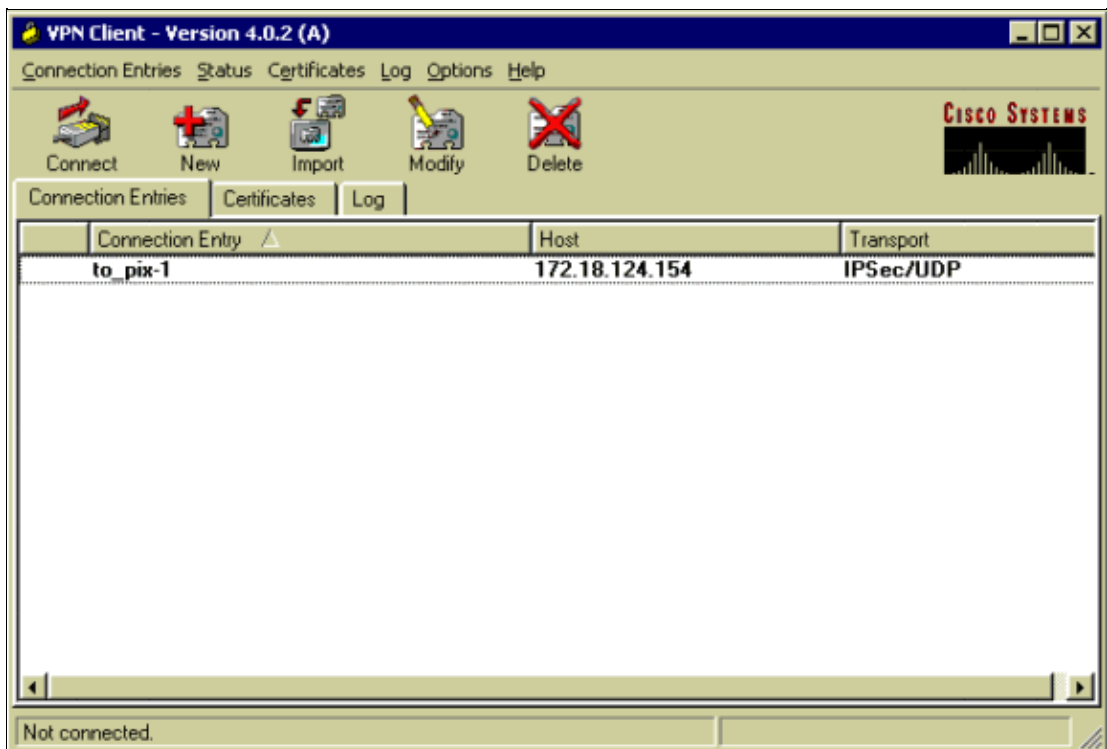
Complete these steps in order to configure the VPN Client:

1. Launch the VPN Client, and then click **New** in order to create a new connection.
2. Enter the initial information for the entry, such as name, host, and password.
 - ◆ In the Connection Entry field, assign a name to your entry.
 - ◆ In the Host field, enter the IP address of the public interface of the PIX for connections.
 - ◆ Under Group Authentication, enter the group name and group password, and then enter the password again to confirm it.

Click **Save** when you are finished.



3. Select the connection entry that you created, and then click **Connect** in order to connect to the PIX.



Verify

Use this section to confirm that your configuration works properly.

Verify Crypto Map Sequence Numbers

If static and dynamic peers are configured on the same crypto map, the order of the crypto map entries is very important. The sequence number of the dynamic crypto map entry must be higher than all of the other static crypto map entries. If the static entries are numbered higher than the dynamic entry, connections with those peers fail.

This is an example of a properly numbered crypto map that contains a static entry and a dynamic entry. Note that the dynamic entry has the highest sequence number and room has been left to add additional static entries:

```
crypto dynamic-map dynmap 30 set transform-set myset
crypto map newmap 10 ipsec-isakmp
crypto map newmap 10 match address 110
crypto map newmap 10 set peer 172.18.124.153
crypto map newmap 10 set transform-set myset
crypto map newmap 65000 ipsec-isakmp dynamic dynmap
```

Troubleshoot

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

Troubleshooting Commands

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

You can use these commands on the PIX with the **logging monitor debugging** or **logging console debugging** commands running:

- **debug crypto ipsec** Debugs IPsec processing.
- **debug crypto isakmp** Debugs ISAKMP processing.

On the VPN Client, bring up the log window in the lower left window.

Clearing Security Associations (SAs)

In the configuration mode of the PIX, use these commands:

- **clear [crypto] ipsec sa** Deletes the active IPsec security associations. The keyword **crypto** is optional.
- **clear [crypto] isakmp sa** Deletes the active IKE security associations. The keyword **crypto** is optional.

On the VPN Client, you can select the Log tab to view the log entries.

Note: For IPsec to work, tunnel endpoint to tunnel endpoint connectivity is *required* before you start this configuration.

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 Security

Security: Intrusion Detection [Systems]

Security: AAA

Security: General

Security: Firewalling

Related Information

- [PIX Support Page](#)
- [Documentation for PIX Firewall](#)
- [PIX Command References](#)
- [Cisco VPN Client Support Page](#)
- [IPSec Support Page](#)
- [Request for Comments \(RFCs\)](#)
- [Technical Support & Documentation – 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: Feb 02, 2006

Document ID: 14092
