Configuring PIX to PIX to PIX IPSec Fully Meshed

Document ID: 5109

Contents

Introduction

This configuration allows private networks behind three Cisco Secure PIX Firewall boxes to be connected by VPN tunnels over the Internet or any public network that uses IPsec. Each of the three networks has connectivity to the other two networks. In this scenario, Network Address Translation (NAT) is required for connections to the public Internet. However, NAT is not required for traffic between the three intranets, which can be transmitted using a VPN tunnel over the public Internet.

Prerequisites

Requirements

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

Components Used

This configuration was developed and tested with PIX Firewall version 6.1(2).

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

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 the Cisco Technical Tips Conventions for more information on document conventions.
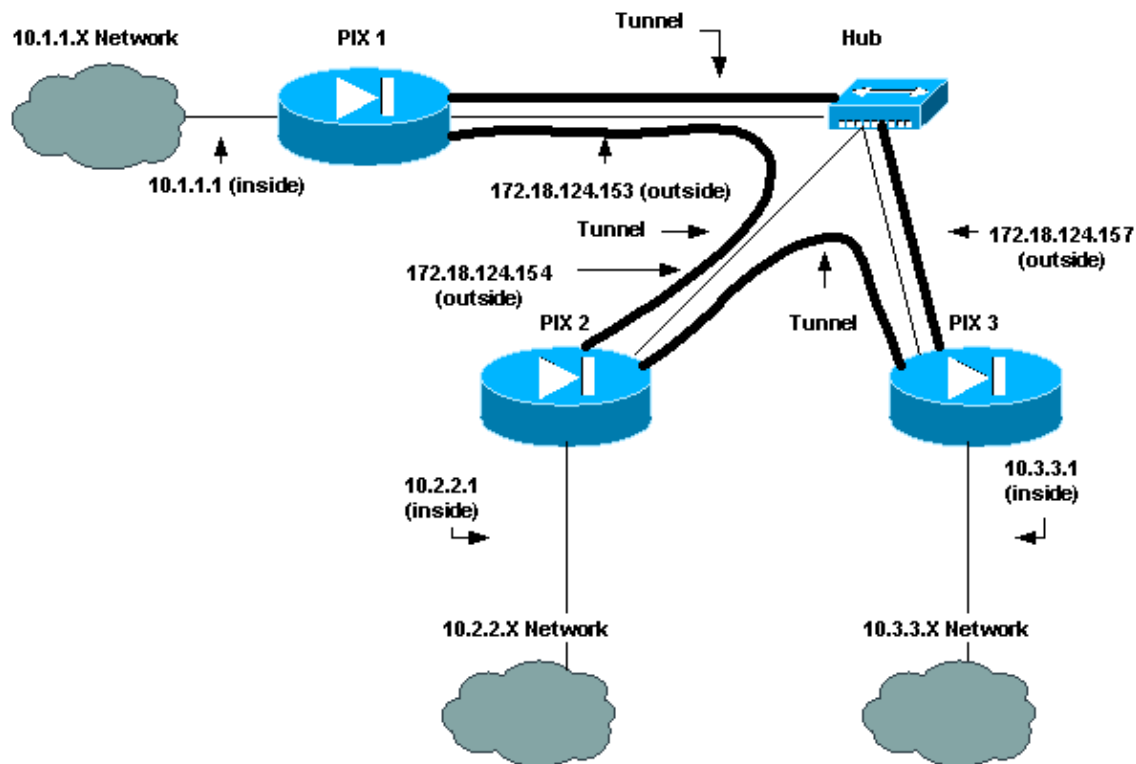
Configure

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

This document uses these configurations:

- PIX 1
- PIX 2
- PIX 3

PIX 1 Configuration

```
PIX Version 6.1(2)
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 http 80
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol smtp 25
```

```
fixup protocol sqlnet 1521
fixup protocol sip 5060
names
```

```
access-list 120 permit ip 10.1.1.0 255.255.255.0 10.2.2.0 255.255.255.0
```

```
access-list 130 permit ip 10.1.1.0 255.255.255.0 10.3.3.0 255.255.255.0
```

```
access-list 100 permit ip 10.1.1.0 255.255.255.0 10.2.2.0 255.255.255.0
access-list 100 permit ip 10.1.1.0 255.255.255.0 10.3.3.0 255.255.255.0
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 auto
interface ethernet1 auto
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
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
```

```
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
no snmp-server location
no snmp-server contact
snmp-server community public
snmp-server enable traps
floodguard enable
sysopt connection permit-ipsec
no sysopt route dnat
crypto ipsec transform-set myset esp-des esp-md5-hmac
```

```
crypto map newmap 20 ipsec-isakmp
crypto map newmap 20 match address 120
```

```
crypto map newmap 20 set peer 172.18.124.154
crypto map newmap 20 set transform-set myset
```

!--- IPsec configuration for tunnel to PIX 3:

```
crypto map newmap 30 ipsec-isakmp
crypto map newmap 30 match address 130
crypto map newmap 30 set peer 172.18.124.157
crypto map newmap 30 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 key ******** address 172.18.124.157 netmask 255.255.255.255
   no-xauth no-config-mode
isakmp identity address
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
ssh timeout 5
terminal width 80
Cryptochecksum:436c96500052d0276324b9ef33221b2d
: end
[OK]
```

PIX 2 Configuration

```
PIX Version 6.1(2)
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 http 80
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
names
```

!--- Traffic to PIX 1:

```
access-list 110 permit ip 10.2.2.0 255.255.255.0 10.1.1.0 255.255.255.0
```

!--- Traffic to PIX 3:

```
access-list 130 permit ip 10.2.2.0 255.255.255.0 10.3.3.0 255.255.255.0
```

!--- Do not perform NAT for traffic to other PIX Firewalls:

```
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 10.3.3.0 255.255.255.0
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 auto
interface ethernet1 auto
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
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
```

!--- Do not perform NAT for traffic to other PIX Firewalls:

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

!--- IPsec configuration for tunnel to PIX 1:

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

!--- IPsec configuration for tunnel to PIX 3:

crypto map newmap 30 ipsec-isakmp
crypto map newmap 30 match address 130
crypto map newmap 30 set peer 172.18.124.157
crypto map newmap 30 set transform-set myset
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 key ****** address 172.18.124.157 netmask 255.255.255.255**
  no-xauth no-config-mode
isakmp identity address
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
ssh timeout 5
terminal width 80
Cryptochecksum:aef12453a0ea29b592dd0d395de881f5
```

```
: end
```

PIX 3 Configuration

```
PIX Version 6.1(2)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pix_3
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


!--- IPsec configuration for tunnel to PIX 1:


access-list 110 permit ip 10.3.3.0 255.255.255.0 10.1.1.0 255.255.255.0


!--- IPsec configuration for tunnel to PIX 2:


access-list 120 permit ip 10.3.3.0 255.255.255.0 10.2.2.0 255.255.255.0


!--- Do not perform NAT for traffic to other PIX Firewalls:


access-list 100 permit ip 10.3.3.0 255.255.255.0 10.2.2.0 255.255.255.0
access-list 100 permit ip 10.3.3.0 255.255.255.0 10.1.1.0 255.255.255.0
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 auto
interface ethernet1 auto
mtu outside 1500
mtu inside 1500
ip address outside 172.18.124.157 255.255.255.0
ip address inside 10.3.3.1 255.255.255.0
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


!--- Do not perform NAT for traffic to other PIX Firewalls:


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

!--- IPsec configuration for tunnel to PIX 1:

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

!--- IPsec configuration for tunnel to PIX 2:

crypto map newmap 20 ipsec-isakmp
crypto map newmap 20 match address 120
crypto map newmap 20 set peer 172.18.124.154
crypto map newmap 20 set transform-set myset
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 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 des
isakmp policy 10 hash md5
isakmp policy 10 group 1
isakmp policy 10 lifetime 1000
telnet timeout 5
ssh timeout 5
terminal width 80
Cryptochecksum:e6ad75852dff21efdb2d24cc95ffbe1c
: end
[OK]
```

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

This section provides information you can use to troubleshoot your configuration. Refer to Troubleshooting the PIX to Pass Data Traffic on an Established IPsec Tunnel for more information.

Troubleshooting Commands

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

debug Commands

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 Internet Security Association and Key Management Protocol (ISAKMP) processing.
- **debug crypto engine** Displays debug messages about crypto engines, which perform encryption and decryption.

clear Commands

In order to clear security associations (SAs), use these commands in the config mode of the PIX.

- **clear [crypto] ipsec sa** Deletes the active IPsec SAs. The keyword crypto is optional.
- **clear [crypto] isakmp sa** Deletes the active Internet Key Exchange (IKE) SAs. The keyword crypto is optional.

Note: For IPsec to work, you must have connectivity from tunnel endpoint to tunnel endpoint before you begin this configuration.

Related Information

- **Troubleshooting the PIX to Pass Data Traffic on an Established IPSec Tunnel**
- **Cisco PIX 500 Series Security Appliances**
- **Documentation for PIX Firewall**
- **PIX Command References**
- **IPsec Negotiations/IKE Protocols**
- **Requests for Comments (RFCs)**
- **Technical Support & Documentation – Cisco Systems**

Updated: Sep 30, 2008   Document ID: 5109