Table of Contents

Enhanced Spoke−to−Spoke VPN with PIX Security Appliance 7.0 Configuration Example

Document ID: 64692

Introduction

This document describes how to configure LAN−to−LAN sessions between PIX firewalls. It demonstrates a configuration for static and dynamic LAN−to−LAN tunnels with spoke−to−spoke connectivity through the hub PIX firewall. PIX version 7.0 improves support for spoke−to−spoke VPN communications as it provides the ability for encrypted traffic to enter and leave the same interface.

The **same−security−traffic** command permits traffic to enter and exit the same interface when you use it with the ***intra−interface*** keyword which enables spoke−to−spoke VPN support. For more information, refer to the "Permitting Intra−Interface Traffic" section in the Cisco Security Appliance Command Line Configuration Guide.

Prerequisites

Requirements

The hub PIX firewall needs to run code version 7.0 or later.

Note: For more information on how to upgrade to PIX firewall version 7.0, refer to the Guide for Cisco PIX 6.2 and 6.3 Users Upgrading to Cisco PIX Software Version 7.0.

Components Used

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

- PIX − 515 version 7.0.1 (PIX1)
- PIX − 501 version 6.3.4 (PIX2)
- PIX − 515 version 6.3.4 (PIX3)

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.

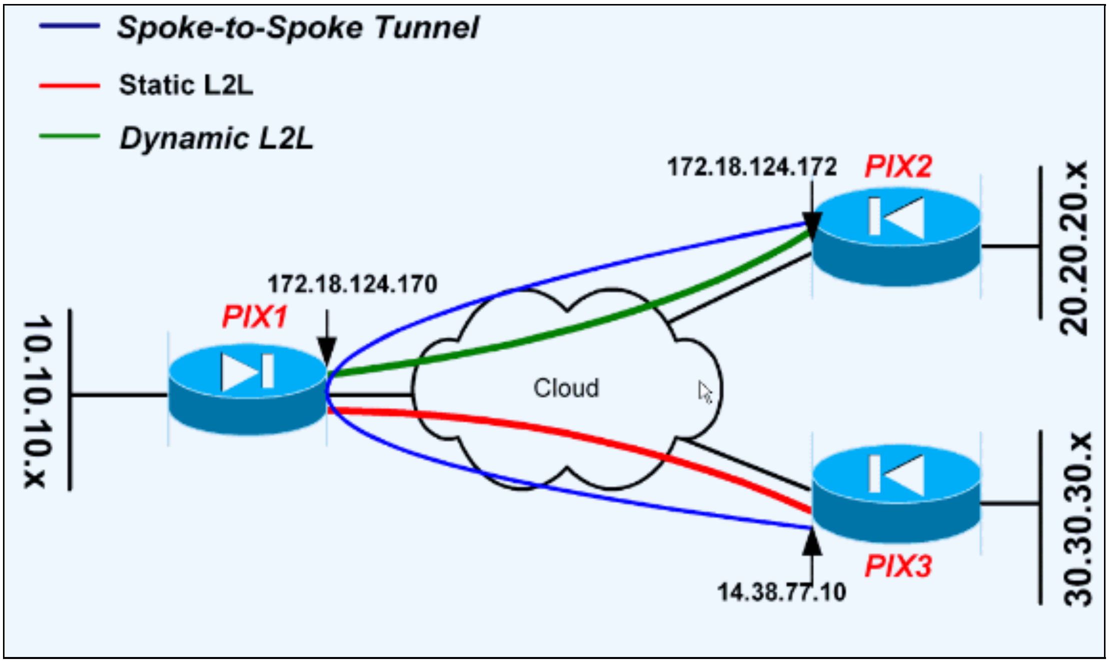
Configure

This section presents you with the information you can use in order to configure the features this document describes.

Note: In order to find additional information on the commands this document uses, use the Command Lookup Tool (registered customers only) .

Network Diagram

This document uses this network setup:



Configurations

This document uses these configurations:

- PIX1
- PIX2
- PIX3

PIX1

```
PIX Version 7.0(1)
no names
```

```
!
interface Ethernet0
nameif outside
security-level 0
ip address 172.18.124.170 255.255.255.0
!
interface Ethernet1
nameif inside
security-level 100
ip address 10.10.10.1 255.255.255.0
!
interface Ethernet2
shutdown
nameif intf2
security-level 4
no ip address
!
interface Ethernet3
shutdown
nameif intf3
security-level 6
no ip address
!
interface Ethernet4
shutdown
nameif intf4
security-level 8
no ip address
!
interface Ethernet5
shutdown
nameif intf5
security-level 10
no ip address
!
enable password 9jNfZuG3TC5tCVH0 encrypted
passwd OnTrBUG1Tp0edmkr encrypted
hostname PIX1
domain-name cisco.com
boot system flash:/image.bin
ftp mode passive

!--- Use this command in order to permit traffic to enter and exit the
!--- same interface for IPSec traffic.

same-security-traffic permit intra-interface

!--- Access-list for interesting traffic to be
!--- encrypted between hub and spoke (PIX3) networks.

access-list 100 extended permit ip 10.10.10.0 255.255.255.0 30.30.30.0 255.255.255.0

!--- Access-list for interesting traffic to be
!--- encrypted between spoke (PIX2) and spoke (PIX3) networks.

access-list 100 extended permit ip 20.20.20.0 255.255.255.0 30.30.30.0 255.255.255.0

!--- Access-list for traffic to bypass the network address translation (NAT) process.

access-list nonat extended permit ip 10.10.10.0 255.255.255.0 30.30.30.0 255.255.255.0
access-list nonat extended permit ip 10.10.10.0 255.255.255.0 20.20.20.0 255.255.255.0
pager lines 24
mtu outside 1500
mtu inside 1500
mtu intf2 1500
mtu intf3 1500
mtu intf4 1500
mtu intf5 1500
no failover
monitor-interface outside
monitor-interface inside
monitor-interface intf2
monitor-interface intf3
monitor-interface intf4
monitor-interface intf5
asdm history enable
arp timeout 14400
nat-control
global (outside) 1 interface

!--- Bypass the NAT process for IPSec traffic.

nat (inside) 0 access-list nonat
nat (inside) 1 10.10.10.0 255.255.255.0

!--- The default gateway to the Internet.

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 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00
timeout mgcp-pat 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 snmp

!--- Configuration of IPSec Phase 2.

crypto ipsec transform-set myset esp-3des esp-sha-hmac

!--- IPSec configuration for the Dynamic LAN-to-LAN tunnel.

crypto dynamic-map cisco 20 set transform-set myset

!--- IPSec configuration for the Static LAN-to-LAN tunnel.

crypto map mymap 10 match address 100
crypto map mymap 10 set peer 14.38.77.10
crypto map mymap 10 set transform-set myset

!--- IPSec configuration that binds dynamic map to crypto map.

crypto map mymap 20 ipsec-isakmp dynamic cisco

!--- Crypto map applied to the outside interface of the PIX.

crypto map mymap interface outside
isakmp identity address

!--- Configuration of IPSec Phase 1.

isakmp enable outside

!--- Configuration of ISAKMP policy.
```

```
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
isakmp policy 65535 authentication pre-share
isakmp policy 65535 encryption 3des
isakmp policy 65535 hash sha
isakmp policy 65535 group 2
isakmp policy 65535 lifetime 86400
telnet timeout 5
ssh 0.0.0.0 0.0.0.0 outside
ssh timeout 60
ssh version 1
console timeout 0

!--- Configuration of the tunnel-group policy for Remote
!--- access tunnels (dynamic tunnels).

tunnel-group DefaultRAGroup type ipsec-ra
tunnel-group DefaultRAGroup general-attributes

!--- Disables group authentication for Dynamic remote-access tunnels.

authentication-server-group none
tunnel-group DefaultRAGroup ipsec-attributes

!--- Defines the pre-shared secret used for
!--- IKE authentication for the dynamic tunnel.

pre-shared-key *

!--- Configuration of the tunnel-group for the Static LAN-to-LAN tunnel.

tunnel-group 14.38.77.10 type ipsec-l2l
tunnel-group 14.38.77.10 ipsec-attributes

!--- Defines the pre-shared secret used for
!--- IKE authentication for the static tunnel.

pre-shared-key *
!
class-map inspection_default
match default-inspection-traffic
!
!
policy-map global_policy
class inspection_default
inspect dns maximum-length 512
inspect ftp
inspect h323 h225
inspect h323 ras
inspect http
inspect netbios
inspect rsh
inspect rtsp
inspect skinny
inspect esmtp
inspect sqlnet
inspect sunrpc
inspect tftp
inspect sip
inspect xdmcp
```

```
!
service−policy global_policy global
Cryptochecksum:7167c0647778b77f8d1d2400d943b825
```

Note: You need to configure the **sysopt connection permit−ipsec** command in order to permit all inbound IPSec authenticated cipher sessions. In the PIX 7.0 version of the code the **sysopt** commands do not show up in the running configuration. In order to verify if **sysopt connection permit−ipsec** is enabled, execute the **show running−config sysopt** command.

PIX2

```
PIX Version 6.3(4)
interface ethernet0 auto
interface ethernet1 100full
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname PIX2
domain−name cisco.com
fixup protocol dns maximum−length 512
fixup protocol ftp 21
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718−1719
fixup protocol http 80
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
fixup protocol tftp 69
names

!−−− Access−list to encrypt traffic between PIX2 and PIX1 networks.

access−list 100 permit ip 20.20.20.0 255.255.255.0 10.10.10.0 255.255.255.0

!−−− Access−list to encrypt traffic between PIX2 and PIX1 networks.

access−list 100 permit ip 20.20.20.0 255.255.255.0 30.30.30.0 255.255.255.0

!−−− Access−list to bypass the NAT process.

access−list nonat permit ip 20.20.20.0 255.255.255.0 10.10.10.0 255.255.255.0
access−list nonat permit ip 20.20.20.0 255.255.255.0 30.30.30.0 255.255.255.0
pager lines 24
mtu outside 1500
mtu inside 1500
ip address outside 172.18.124.172 255.255.255.0
ip address inside 20.20.20.1 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
pdm history enable
arp timeout 14400
global (outside) 1 interface

!−−− Bypass the NAT process for IPSec traffic.

nat (inside) 0 access−list nonat
nat (inside) 1 20.20.20.0 255.255.255.0 0 0
```

```
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 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 TACACS+ max-failed-attempts 3
aaa-server TACACS+ deadtime 10
aaa-server RADIUS protocol radius
aaa-server RADIUS max-failed-attempts 3
aaa-server RADIUS deadtime 10
aaa-server LOCAL protocol local
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable

!--- Permit all inbound IPSec authenticated cipher sessions.

sysopt connection permit-ipsec

!--- Defines IPSec encryption and authentication alogrithms.

crypto ipsec transform-set myset esp-3des esp-sha-hmac

!--- Defines crypto map.

crypto map mymap 10 ipsec-isakmp
crypto map mymap 10 match address 100
crypto map mymap 10 set peer 172.18.124.170
crypto map mymap 10 set transform-set myset

!--- Apply crypto map on the outside interface.

crypto map mymap interface outside
isakmp enable outside

!--- Defines the pre-shared secret used for IKE authentication.

isakmp key ******** address 172.18.124.170 netmask 255.255.255.255 no-xauth
isakmp identity address

!--- The ISAKMP policy configuration.

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:fb2e89ab9da0ae93d69e345a4675ff38
```

PIX3

```
PIX Version 6.3(4)
interface ethernet0 auto
interface ethernet1 auto
interface ethernet2 auto shutdown
interface ethernet3 auto shutdown
interface ethernet4 auto shutdown
interface ethernet5 auto shutdown
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 intf2 security4
nameif ethernet3 intf3 security6
nameif ethernet4 intf4 security8
nameif ethernet5 intf5 security10
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname PIX3
domain−name cisco.com
fixup protocol dns maximum−length 512
fixup protocol ftp 21
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718−1719
fixup protocol http 80
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
fixup protocol tftp 69
names

!−−− Access−list to encrypt traffic between PIX3 and PIX1 networks.

access−list 100 permit ip 30.30.30.0 255.255.255.0 10.10.10.0 255.255.255.0

!−−− Access−list to encrypt traffic between PIX3 and PIX2 networks.

access−list 100 permit ip 30.30.30.0 255.255.255.0 20.20.20.0 255.255.255.0

!−−− Access−list to bypass the NAT process.

access−list nonat permit ip 30.30.30.0 255.255.255.0 10.10.10.0 255.255.255.0
access−list nonat permit ip 30.30.30.0 255.255.255.0 20.20.20.0 255.255.255.0
pager lines 24
mtu outside 1500
mtu inside 1500
mtu intf2 1500
mtu intf3 1500
mtu intf4 1500
mtu intf5 1500
ip address outside 14.38.77.10 255.255.0.0
ip address inside 30.30.30.1 255.255.255.0
no ip address intf2
no ip address intf3
no ip address intf4
no ip address intf5
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
no failover ip address intf2
no failover ip address intf3
no failover ip address intf4
no failover ip address intf5
pdm history enable
```

```
arp timeout 14400
global (outside) 1 interface

!--- Binds ACL nonat to the NAT statement in order to
!--- avoid NAT on the IPSec packets.

nat (inside) 0 access-list nonat
nat (inside) 1 30.30.30.0 255.255.255.0 0 0
route outside 0.0.0.0 0.0.0.0 14.38.1.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 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 TACACS+ max-failed-attempts 3
aaa-server TACACS+ deadtime 10
aaa-server RADIUS protocol radius
aaa-server RADIUS max-failed-attempts 3
aaa-server RADIUS deadtime 10
aaa-server LOCAL protocol local
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable

!--- Permits all inbound IPSec authenticated cipher sessions.

sysopt connection permit-ipsec

!--- Defines IPSec encryption and authentication algorithms.

crypto ipsec transform-set myset esp-3des esp-sha-hmac

!--- Defines crypto map
.
crypto map mymap 10 ipsec-isakmp
crypto map mymap 10 match address 100
crypto map mymap 10 set peer 172.18.124.170
crypto map mymap 10 set transform-set myset

!--- Apply crypto map on the outside interface.

crypto map mymap interface outside
isakmp enable outside

!--- Defines the pre-shared secret key used for IKE authentication.

isakmp key ******** address 172.18.124.170 netmask 255.255.255.0 no-xauth
isakmp identity address

!--- Defines the ISAKMP policy.

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 0.0.0.0 0.0.0.0 outside
ssh timeout 5
console timeout 0
terminal width 80
Cryptochecksum:cb5c245112db607e3a9a85328d1295db
```

Verify

This section provides information you can use in order to confirm your configuration works 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.

In order to test communication between the two private networks between PIX3 and PIX1, you can initiate a **ping** from one of the private networks.

In this configuration:

- For static LAN−to−LAN, the ping is sent from behind the PIX3 network (30.30.30.x) to the PIX1 network (10.10.10.x).
- For the dynamic LAN−to−LAN tunnel, a ping is sent from the PIX2 network (20.20.20.x) to the PIX1 network (10.10.10.x).

- **show crypto isakmp sa** Displays all current IKE security associations (SAs) at a peer.
- **show crypto ipsec sa** Displays all current SAs.

This section shows example verification configurations for:

- PIX1
- PIX2
- PIX3

PIX1

```
show crypto isakmp sa

Active SA: 2
Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 2

!--- Static LAN-to-LAN tunnel establishment.

1 IKE Peer: 14.38.77.10
Type: L2L Role : responder
Rekey : no State: MM_ACTIVE

!--- Dynamic LAN-to-LAN tunnel establishment.

2 IKE Peer: 172.18.124.172
Type: user Role: responder
Rekey : no State: MM_ACTIVE




PIX1(config)# show crypto ipsec sa
interface: outside
Crypto map tag: cisco, local addr: 172.18.124.170

!--- IPSec SA for networks between PIX2 and PIX1.

local ident (addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (20.20.20.0/255.255.255.0/0/0)
current_peer: 172.18.124.172
```

```
dynamic allocated peer ip: 0.0.0.0

#pkts encaps: 9, #pkts encrypt: 9, #pkts digest: 9
#pkts decaps: 9, #pkts decrypt: 9, #pkts verify: 9
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 9, #pkts comp failed: 0, #pkts decomp failed: 0
#send errors: 0, #recv errors: 0

local crypto endpt.: 172.18.124.170, remote crypto endpt.: 172.18.124.172

path mtu 1500, ipsec overhead 60, media mtu 1500
current outbound spi: 2C4400C7

inbound esp sas:
spi: 0x6D29993F (1831442751)
transform: esp-3des esp-sha-hmac
in use settings ={RA, Tunnel, }
slot: 0, conn_id: 7, crypto-map: cisco
sa timing: remaining key lifetime (sec): 28413
IV size: 8 bytes
replay detection support: Y


outbound esp sas:
spi: 0x2C4400C7 (742654151)
transform: esp-3des esp-sha-hmac
in use settings ={RA, Tunnel, }
slot: 0, conn_id: 7, crypto-map: cisco
sa timing: remaining key lifetime (sec): 28411
IV size: 8 bytes
replay detection support: Y


!--- IPSec SA for networks between PIX2 and PIX3.

Crypto map tag: cisco, local addr: 172.18.124.170

local ident (addr/mask/prot/port): (30.30.30.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (20.20.20.0/255.255.255.0/0/0)
current_peer: 172.18.124.172
dynamic allocated peer ip: 0.0.0.0

#pkts encaps: 9, #pkts encrypt: 9, #pkts digest: 9
#pkts decaps: 13, #pkts decrypt: 13, #pkts verify: 13
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 9, #pkts comp failed: 0, #pkts decomp failed: 0
#send errors: 0, #recv errors: 0

local crypto endpt.: 172.18.124.170, remote crypto endpt.: 172.18.124.172

path mtu 1500, ipsec overhead 60, media mtu 1500
current outbound spi: 9D40B1DC

inbound esp sas:
spi: 0xEE6F6479 (4000277625)
transform: esp-3des esp-sha-hmac
in use settings ={RA, Tunnel, }
slot: 0, conn_id: 7, crypto-map: cisco
sa timing: remaining key lifetime (sec): 28777
IV size: 8 bytes
replay detection support: Y


outbound esp sas:
```

```
spi: 0x9D40B1DC (2638262748)
transform: esp-3des esp-sha-hmac
in use settings ={RA, Tunnel, }
slot: 0, conn_id: 7, crypto-map: cisco
sa timing: remaining key lifetime (sec): 28777
IV size: 8 bytes
replay detection support: Y

Crypto map tag: mymap, local addr: 172.18.124.170

!--- IPSec SA for networks between PIX3 and PIX1.

local ident (addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (30.30.30.0/255.255.255.0/0/0)
current_peer: 14.38.77.10

#pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
#pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 4, #pkts comp failed: 0, #pkts decomp failed: 0
#send errors: 0, #recv errors: 0

local crypto endpt.: 172.18.124.170, remote crypto endpt.: 14.38.77.10

path mtu 1500, ipsec overhead 60, media mtu 1500
current outbound spi: BE57D878

inbound esp sas:
spi: 0xAF25D7DB (2938492891)
transform: esp-3des esp-sha-hmac
in use settings ={L2L, Tunnel, }
slot: 0, conn_id: 6, crypto-map: mymap
sa timing: remaining key lifetime (kB/sec): (4274999/27145)
IV size: 8 bytes
replay detection support: Y


outbound esp sas:
spi: 0xBE57D878 (3193428088)
transform: esp-3des esp-sha-hmac
in use settings ={L2L, Tunnel, }
slot: 0, conn_id: 6, crypto-map: mymap
sa timing: remaining key lifetime (kB/sec): (4274999/27144)
IV size: 8 bytes
replay detection support: Y

Crypto map tag: cisco, local addr: 172.18.124.170

!--- IPSec SA for networks between PIX2 and PIX3.

local ident (addr/mask/prot/port): (20.20.20.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (30.30.30.0/255.255.255.0/0/0)
current_peer: 14.38.77.10

#pkts encaps: 9, #pkts encrypt: 9, #pkts digest: 9
#pkts decaps: 9, #pkts decrypt: 9, #pkts verify: 9
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 9, #pkts comp failed: 0, #pkts decomp failed: 0
#send errors: 0, #recv errors: 0

local crypto endpt.: 172.18.124.170, remote crypto endpt.: 14.38.77.10

path mtu 1500, ipsec overhead 60, media mtu 1500
current outbound spi: 963766A1
```

```

inbound esp sas:
spi: 0x1CD1B5B7 (483505591)
transform: esp-3des esp-sha-hmac
in use settings ={L2L, Tunnel, }
slot: 0, conn_id: 6, crypto-map: cisco
sa timing: remaining key lifetime (kB/sec): (4274999/28780)
IV size: 8 bytes
replay detection support: Y


outbound esp sas:
spi: 0x963766A1 (2520213153)
transform: esp-3des esp-sha-hmac
in use settings ={L2L, Tunnel, }
slot: 0, conn_id: 6, crypto-map: cisco
sa timing: remaining key lifetime (kB/sec): (4274999/28780)
IV size: 8 bytes
replay detection support: Y
```

PIX2

```
PIX2(config)# show crypto isakmp sa
Total : 1
Embryonic : 0
dst              src            state      pending created
172.18.124.170 172.18.124.172 QM_IDLE      0        2




PIX2(config)# show crypto ipsec sa


interface: outside
Crypto map tag: mymap, local addr. 172.18.124.172

!--- IPSec SA created between networks for PIX2 and PIX3.

local ident (addr/mask/prot/port): (20.20.20.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (30.30.30.0/255.255.255.0/0/0)
current_peer: 172.18.124.170:500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 4, #pkts encrypt: 4, #pkts digest 4
#pkts decaps: 4, #pkts decrypt: 4, #pkts verify 4
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
#send errors 1, #recv errors 0

local crypto endpt.: 172.18.124.172, remote crypto endpt.: 172.18.124.170
path mtu 1500, ipsec overhead 56, media mtu 1500
current outbound spi: 38cf2399

inbound esp sas:
spi: 0xb37404c2(3010725058)
transform: esp-3des esp-sha-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 4, crypto map: mymap
sa timing: remaining key lifetime (k/sec): (4607999/28765)
IV size: 8 bytes
replay detection support: Y
```

```
inbound ah sas:


inbound pcp sas:


outbound esp sas:
spi: 0x38cf2399(953099161)
transform: esp-3des esp-sha-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 3, crypto map: mymap
sa timing: remaining key lifetime (k/sec): (4607999/28765)
IV size: 8 bytes
replay detection support: Y


outbound ah sas:


outbound pcp sas:



!--- IPSec SA created between networks PIX1 and PIX2.

local ident (addr/mask/prot/port): (20.20.20.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0)
current_peer: 172.18.124.170:500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 4, #pkts encrypt: 4, #pkts digest 4
#pkts decaps: 4, #pkts decrypt: 4, #pkts verify 4
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
#send errors 1, #recv errors 0

local crypto endpt.: 172.18.124.172, remote crypto endpt.: 172.18.124.170
path mtu 1500, ipsec overhead 56, media mtu 1500
current outbound spi: fffd0c20

inbound esp sas:
spi: 0x1a2a994b(438999371)
transform: esp-3des esp-sha-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 1, crypto map: mymap
sa timing: remaining key lifetime (k/sec): (4607999/28717)
IV size: 8 bytes
replay detection support: Y


inbound ah sas:


inbound pcp sas:


outbound esp sas:
spi: 0xfffd0c20(4294773792)
transform: esp-3des esp-sha-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 2, crypto map: mymap
sa timing: remaining key lifetime (k/sec): (4607999/28717)
IV size: 8 bytes
replay detection support: Y
```

```
outbound ah sas:


outbound pcp sas:
```

PIX3

```
PIX3(config)# show crypto isakmp sa
Total : 1
Embryonic : 0
dst                src       state         pending     created
172.18.124.170 14.38.77.10  QM_IDLE          0             2




PIX3(config)# show crypto ipsec sa


interface: outside
Crypto map tag: mymap, local addr. 14.38.77.10

!--- IPSec SA created between networks PIX3 and PIX2.

local ident (addr/mask/prot/port): (30.30.30.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (20.20.20.0/255.255.255.0/0/0)
current_peer: 172.18.124.170:500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 9, #pkts encrypt: 9, #pkts digest 9
#pkts decaps: 9, #pkts decrypt: 9, #pkts verify 9
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
#send errors 1, #recv errors 0

local crypto endpt.: 14.38.77.10, remote crypto endpt.: 172.18.124.170
path mtu 1500, ipsec overhead 56, media mtu 1500
current outbound spi: 8282748

inbound esp sas:
spi: 0x28c9b70a(684308234)
transform: esp-3des esp-sha-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 1, crypto map: mymap
sa timing: remaining key lifetime (k/sec): (4607998/28775)
IV size: 8 bytes
replay detection support: Y


inbound ah sas:


inbound pcp sas:


outbound esp sas:
spi: 0x8282748(136849224)
transform: esp-3des esp-sha-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 2, crypto map: mymap
sa timing: remaining key lifetime (k/sec): (4607999/28775)
IV size: 8 bytes
replay detection support: Y
```

```
outbound ah sas:


outbound pcp sas:



!--- IPSec SA created between networks PIX3 and PIX1.

local ident (addr/mask/prot/port): (30.30.30.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0)
current_peer: 172.18.124.170:500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 4, #pkts encrypt: 4, #pkts digest 4
#pkts decaps: 4, #pkts decrypt: 4, #pkts verify 4
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
#send errors 1, #recv errors 0

local crypto endpt.: 14.38.77.10, remote crypto endpt.: 172.18.124.170
path mtu 1500, ipsec overhead 56, media mtu 1500
current outbound spi: f415cec9

inbound esp sas:
spi: 0x12c5caf1(314952433)
transform: esp-3des esp-sha-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 3, crypto map: mymap
sa timing: remaining key lifetime (k/sec): (4607999/28763)
IV size: 8 bytes
replay detection support: Y


inbound ah sas:


inbound pcp sas:


outbound esp sas:
spi: 0xf415cec9(4095069897)
transform: esp-3des esp-sha-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 4, crypto map: mymap
sa timing: remaining key lifetime (k/sec): (4607999/28763)
IV size: 8 bytes
replay detection support: Y


outbound ah sas:


outbound pcp sas:
```

Troubleshoot

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

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 you issue **debug** commands, refer to Important Information on Debug Commands.

Perform PIX commands in config mode:

- **clear crypto isakmp sa** Clears the Phase 1 SAs
- **clear crypto ipsec sa** Clears the Phase 2 SAs

The **debug** commands for VPN tunnels:

- **debug crypto isakmp sa** Debugs ISAKMP SA negotiations.
- **debug crypto ipsec sa** Debugs IPSec SA negotiations.

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

- **PIX Support Page**
- **Documentation for PIX Firewall**
- **PIX Command Reference**
- **Requests for Comments (RFCs)**
- **PIX Firewall Frequently Asked Questions**
- **Technical Support − Cisco Systems**

Updated: Jun 25, 2005 Document ID: 64692