Table of Contents

Enhanced Spoke−to−Client VPN Configuration Example for PIX Security Appliance Version 7.0

Document ID: 64693

Introduction

This document describes how to configure LAN−to−LAN sessions between PIX Security Appliances, and also allows for a VPN Client to access the spoke network (PIX3) through the hub (PIX1). In addition, this document demonstrates the configuration for a static LAN−to−LAN tunnel with VPN Client to spoke connectivity through the hub PIX Security Appliance. PIX version 7.0 improves support for spoke−to−spoke VPN communications. PIX 7.0 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 used 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 Security Appliance needs to run version 7.0 or later.

Note: For more information on how to upgrade PIX Appliance to 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)

- VPN Client version 4.6.02.0011
- 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.

Caveats

- Cisco bug ID CSCeh29328 (registered customers only) VPN Client mode configuration attributes are not enforced when you disable XAUTH.
- Cisco bug ID CSCeh69389 (registered customers only) Split−tunnel ACLs are not converted to Standard ACLs when you upgrade to PIX 7.0.

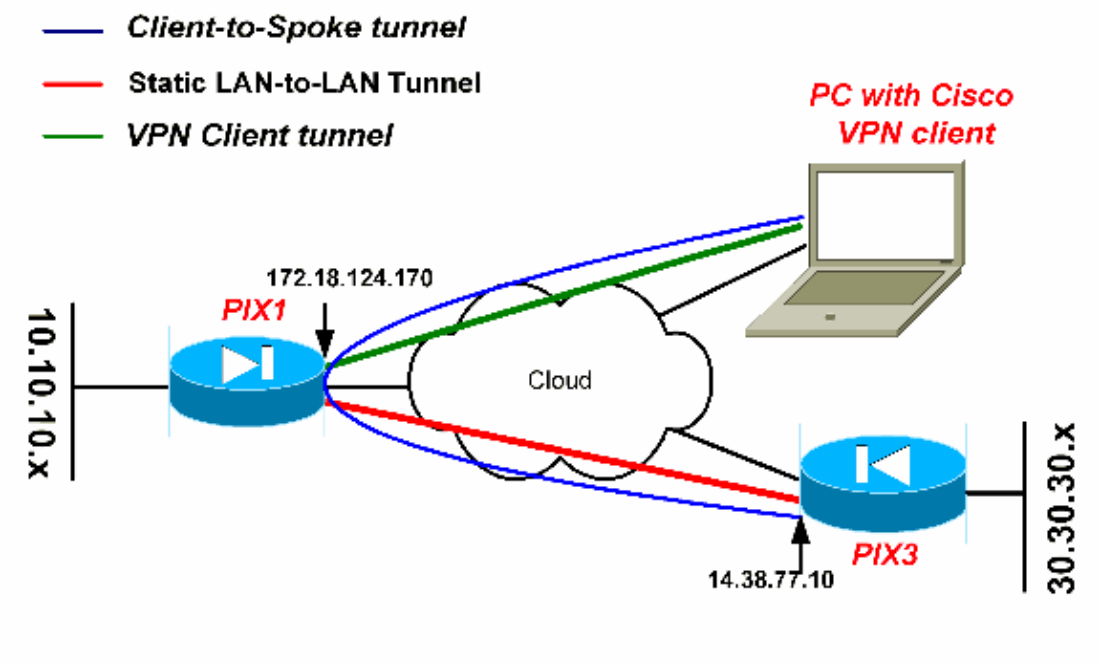
Configure

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
- PIX3
- VPN Client

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

!−−− Command to permit IPSec traffic to enter and exit the same interface.

same−security−traffic permit intra−interface


!−−− Access−list for interesting traffic to be encrypted between
!−−− the hub (PIX1) 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 the VPN Client networks and spoke (PIX3) networks.

access-list 100 extended permit ip 192.168.10.0 255.255.255.0 30.30.30.0 255.255.255.0


!--- Access-list for interesting 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 10.10.10.0 255.255.255.0 192.168.10.0 255.255.255.0


!--- Standard access-list to allow split-tunnel for the VPN Clients.

access-list splittunnel standard permit 10.10.10.0 255.255.255.0
access-list splittunnel standard permit 30.30.30.0 255.255.255.0
pager lines 24
mtu outside 1500
mtu inside 1500
mtu intf2 1500
mtu intf3 1500
mtu intf4 1500
mtu intf5 1500


!--- Address pool for the VPN Clients.

ip local pool vpnpool 192.168.10.1-192.168.10.254
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 NAT process for IPSec traffic.

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


!--- Configuration of group-policy for VPN Clients.

group-policy clientgroup internal
group-policy clientgroup attributes
vpn-idle-timeout 20
```

```
!--- See Note 2.



!--- Enable and bind split-tunnel parameters to the group-policy.

split-tunnel-policy tunnelspecified
split-tunnel-network-list value splittunnel
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


!--- Crypto map configuration for VPN Clients that connect to this PIX.

crypto dynamic-map rtpdynmap 20 set transform-set myset


!--- crypto map configuration for a 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


!--- Binding the dynamic map to the crypto map process.

crypto map mymap 20 ipsec-isakmp dynamic rtpdynmap


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

crypto map mymap interface outside
isakmp identity address
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
isakmp disconnect-notify
telnet timeout 5
ssh 0.0.0.0 0.0.0.0 outside
ssh timeout 60
ssh version 1
console timeout 0
tunnel-group DefaultRAGroup type ipsec-ra
tunnel-group DefaultRAGroup general-attributes
```

```
authentication-server-group none
tunnel-group DefaultRAGroup ipsec-attributes
pre-shared-key *


!--- Configuration of 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


!--- Configuraiton of a pre-shared key for the static LAN-to-LAN tunnel.

pre-shared-key *


!--- Configuration of tunnel-group with group information for VPN Clients.

tunnel-group rtptacvpn type ipsec-ra


!--Configuration of group parameters for the VPN clients

tunnel-group rtptacvpn general-attributes
address-pool vpnpool


!--- Disable user authentication.

authentication-server-group none
authorization-server-group LOCAL


!--- Bind group-policy parameters to the tunnel-group for VPN Clients.

default-group-policy clientgroup
tunnel-group rtptacvpn ipsec-attributes
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:646541da0da9a4c764effd2e05633018
: end
```

Note 1: The **sysopt connection permit−ipsec** command needs to be configured to permit all inbound IPSec authenticated cipher sessions. In PIX 7.0, the **sysopt** commands do not show up in the running configuration. In order to verify if the **sysopt connection permit−ipsec** command is enabled, execute the command **show running−config sysopt**.

Note 2: In order for VPN Clients to connect via IPSec over UDP, configure this output in the **group−policy** section of the PIX Appliance.

```
group−policy clientgroup attributes
vpn−idle−timeout 20
ipsec−udp enable
ipsec−udp−port 10000
split−tunnel−policy tunnelspecified
split−tunnel−network−list value splittunnel
```

Note 3: In order for VPN Clients to connect via IPSec over TCP, configure this command in the **global configuration** of the PIX Appliance.

```
isakmp ipsec−over−tcp port 10000
```

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 for the encryption of  traffic
!−−− between PIX3 and PIX1 networks.
```

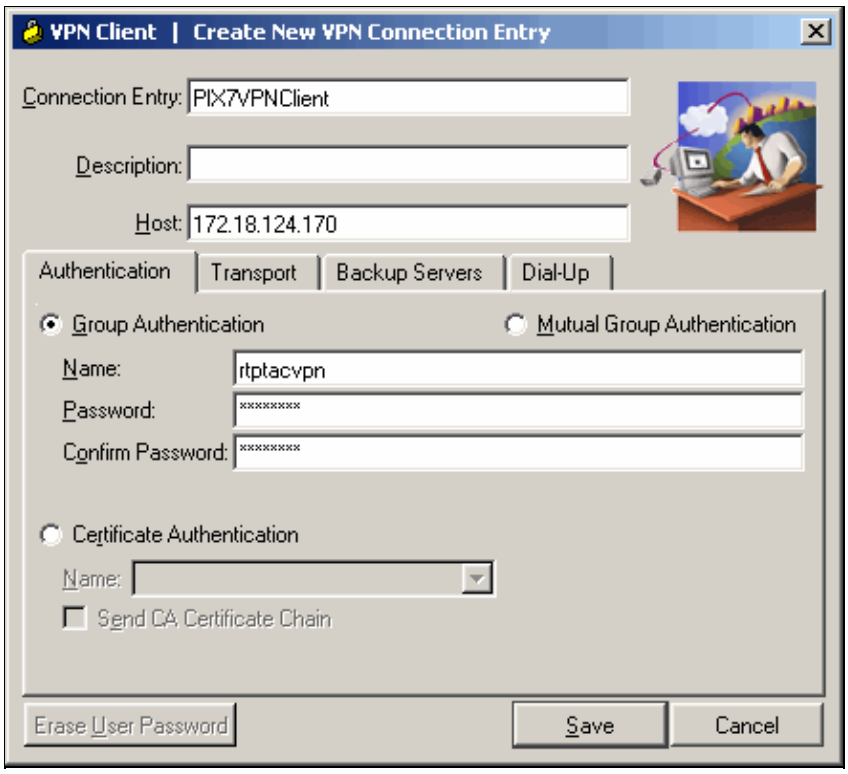
```
access-list 100 permit ip 30.30.30.0 255.255.255.0 10.10.10.0 255.255.255.0


!--- Access-list for the encryption of  traffic
!--- between the PIX3 network and the VPN Client address pool.

access-list 100 permit ip 30.30.30.0 255.255.255.0 192.168.10.0 255.255.255.0


!--- Access-list used 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 30.30.30.0 255.255.255.0 192.168.10.0 255.255.255.0
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


!--- Bind 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
: end
```

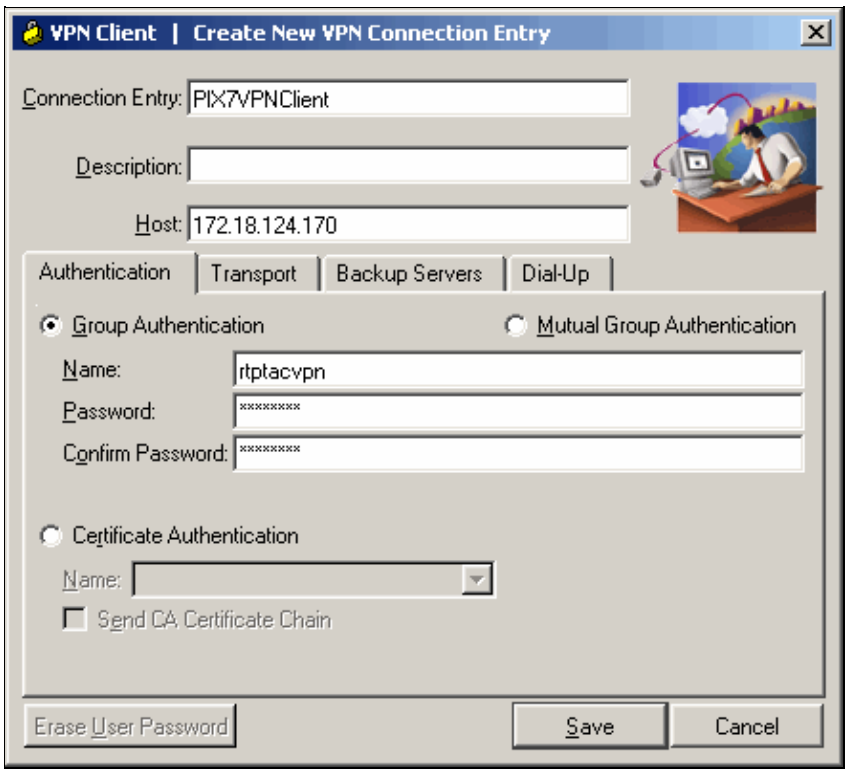
VPN Client Configuration

Complete these steps in order to create a new connection entry on the VPN Client.

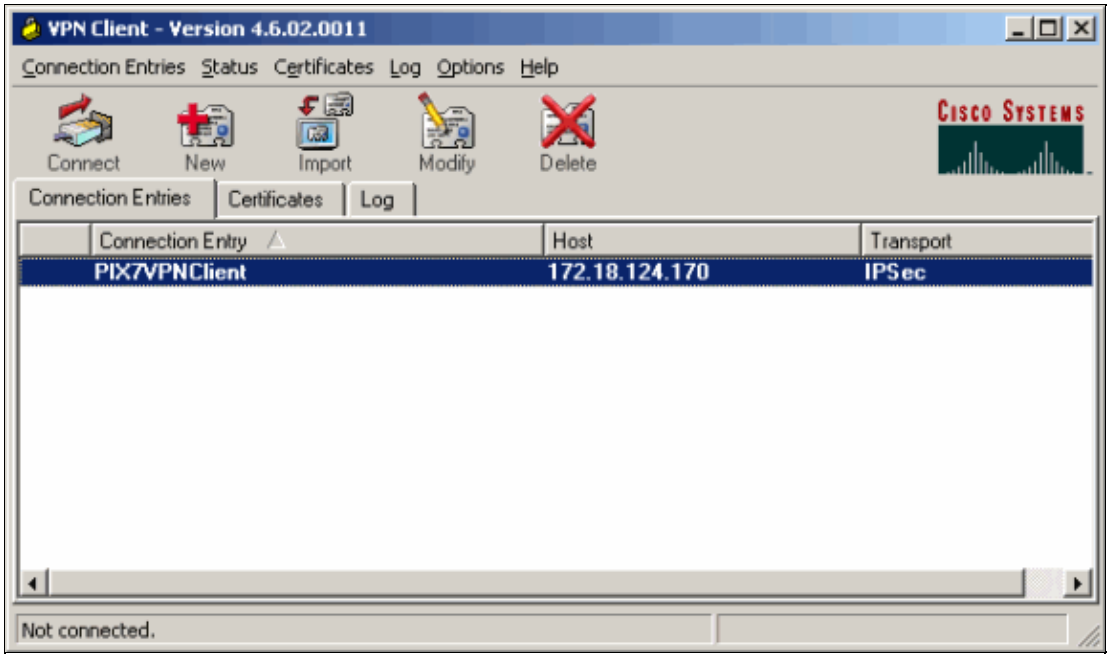
1. Enter the host IP address (PIX1 external IP address).
2. Under the authentication tab, enter the group attributes (group name and password as configured on the PIX Appliance).



3. Under the Transport tab choose the method of tunneling which you want to use for the VPN Clients connection. In this configuration, **Enable Transport Tunneling** is disabled for straight IPSec connectivity.



4. Click **Save** in order to save the connection profile configured on the VPN Client.



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.

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

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, a ping is sent from behind the PIX3 network (30.30.30.x) to the PIX1 network (10.10.10.x).
- In order for the VPN Clients to access the networks behind PIX3, a security association needs to be built from the PIX3 to PIX1 for VPN Client networks.

PIX1 Verification
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 1 IKE Peer: 172.18.173.77 **Type : user Role : responder** Rekey : no State : **AM_ACTIVE** **2 IKE Peer: 14.38.77.10** **Type : L2L Role : responder** Rekey : no State : **MM_ACTIVE**

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

!--- IPSec SA for the connection between VPN Clients and the PIX1 network.

local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (192.168.10.1/255.255.255.255/0/0)
current_peer: 172.18.173.77
dynamic allocated peer ip: 192.168.10.1

#pkts encaps: 12, #pkts encrypt: 12, #pkts digest: 12
#pkts decaps: 12, #pkts decrypt: 12, #pkts verify: 12
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 12, #pkts comp failed: 0, #pkts decomp failed: 0
#send errors: 0, #recv errors: 0

local crypto endpt.: 172.18.124.170, remote crypto endpt.: 172.18.173.77

path mtu 1500, ipsec overhead 60, media mtu 1500
current outbound spi: 1ECCB41D

inbound esp sas:
spi: 0x6C1615A7 (1813386663)
transform: esp-3des esp-sha-hmac
in use settings ={RA, Tunnel, }
slot: 0, conn_id: 5, crypto-map: rtpdynmap
sa timing: remaining key lifetime (sec): 28761
IV size: 8 bytes
replay detection support: Y


outbound esp sas:
spi: 0x1ECCB41D (516731933)
transform: esp-3des esp-sha-hmac
in use settings ={RA, Tunnel, }
slot: 0, conn_id: 5, crypto-map: rtpdynmap
sa timing: remaining key lifetime (sec): 28760
IV size: 8 bytes
replay detection support: Y

Crypto map tag: mymap, local addr: 172.18.124.170

!-- IPSec SA for connection between the VPN Clients network and PIX3 network.

local ident (addr/mask/prot/port): (192.168.10.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (30.30.30.0/255.255.255.0/0/0)
current_peer: 14.38.77.10

#pkts encaps: 8, #pkts encrypt: 8, #pkts digest: 8
#pkts decaps: 8, #pkts decrypt: 8, #pkts verify: 8
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 8, #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: 9EF2885C

inbound esp sas:
spi: 0x82E9BF07 (2196356871)
```

```
transform: esp-3des esp-sha-hmac
in use settings ={L2L, Tunnel, }
slot: 0, conn_id: 4, crypto-map: mymap
sa timing: remaining key lifetime (kB/sec): (4274999/28786)
IV size: 8 bytes
replay detection support: Y


outbound esp sas:
spi: 0x9EF2885C (2666694748)
transform: esp-3des esp-sha-hmac
in use settings ={L2L, Tunnel, }
slot: 0, conn_id: 4, crypto-map: mymap
sa timing: remaining key lifetime (kB/sec): (4274999/28786)
IV size: 8 bytes
replay detection support: Y

Crypto map tag: mymap, local addr: 172.18.124.170

!--- IPSec security association for a connection between
!--- the PIX1 and PIX3 networks.

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: C86585AB

inbound esp sas:
spi: 0x95604966 (2506115430)
transform: esp-3des esp-sha-hmac
in use settings ={L2L, Tunnel, }
slot: 0, conn_id: 4, crypto-map: mymap
sa timing: remaining key lifetime (kB/sec): (4274999/28653)
IV size: 8 bytes
replay detection support: Y


outbound esp sas:
spi: 0xC86585AB (3362096555)
transform: esp-3des esp-sha-hmac
in use settings ={L2L, Tunnel, }
slot: 0, conn_id: 4, crypto-map: mymap
sa timing: remaining key lifetime (kB/sec): (4274999/28652)
IV size: 8 bytes
replay detection support: Y
```

PIX3 Verification

```
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 security association for connection between
!--- the PIX3 and PIX1 networks.

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: 95604966

inbound esp sas:
spi: 0xc86585ab(3362096555)
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): (4607999/28213)
IV size: 8 bytes
replay detection support: Y


inbound ah sas:


inbound pcp sas:


outbound esp sas:
spi: 0x95604966(2506115430)
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): (4607999/28213)
IV size: 8 bytes
replay detection support: Y


outbound ah sas:


outbound pcp sas:



!--- IPSec security association for the connection between the VPN Client
!--- network and PIX3 networks.

local ident (addr/mask/prot/port): (30.30.30.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (192.168.10.0/255.255.255.0/0/0)
current_peer: 172.18.124.170:500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 8, #pkts encrypt: 8, #pkts digest 8
```

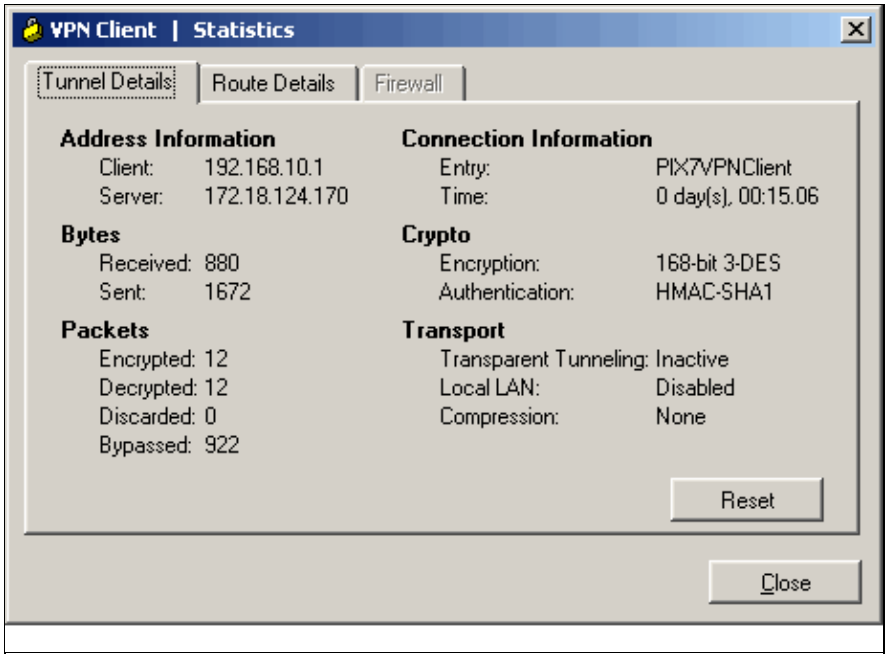
```
#pkts decaps: 8, #pkts decrypt: 8, #pkts verify 8
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
#send errors 1, #recv errors 0

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: 82e9bf07

inbound esp sas:
spi: 0x9ef2885c(2666694748)
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): (4607999/28295)
IV size: 8 bytes
replay detection support: Y


inbound ah sas:


inbound pcp sas:


outbound esp sas:
spi: 0x82e9bf07(2196356871)
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): (4607999/28295)
IV size: 8 bytes
replay detection support: Y


outbound ah sas:


outbound pcp sas:
```

VPN Client Verification

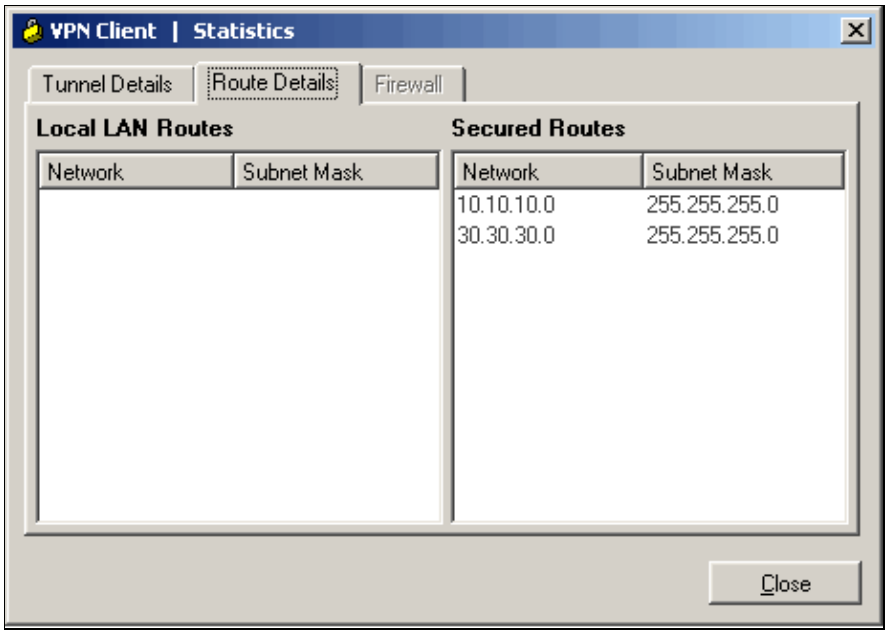
Complete these steps in order to verify the VPN Client.

1. Right−click on the VPN Client lock icon present at the system tray after successful connection and choose the option for **statistics**.

   You can view details about the VPN Client connection and encryption/decryption of packet information.



2. Click on the Route Details tab in order to verify the split−tunnel list passed down from the PIX. Appliance.



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.

- **clear crypto isakmp sa** Clears the phase 1 security associations (SAs).
- **clear crypto ipsec sa** Clears the phase 2 SAs
- **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 References**
- **Requests for Comments (RFCs)**
- **Technical Support − Cisco Systems**

Updated: Jul 03, 2005 Document ID: 64693