

PIX-to-PIX 6.x: Easy VPN (NEM) Configuration Example

Document ID: 40820

Contents

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

Configure

- Network Diagram
- Configurations

Verify

- PIX Easy VPN Server show Commands and Sample Output
- PIX Easy VPN Remote Hardware Client show Commands and Sample Output

Troubleshoot

- Easy VPN Server Commands
- Easy VPN Remote Hardware Client Commands

Related Information

Introduction

This document provides a sample configuration for IPsec between the PIX Easy VPN Remote Hardware Client and the PIX Easy VPN Server. The Easy VPN Remote feature for the PIX was introduced in PIX version 6.2 and is also referred to as hardware client/EzVPN client. Cisco Easy VPN Server is supported in PIX Software version 6.0 and later.

Refer to PIX/ASA 7.x Easy VPN with an ASA 5500 as the Server and PIX 506E as the Client (NEM) Configuration Example in order to learn more about the same scenario where the security appliance runs with software version 7.x.

Refer to PIX/ASA 7.x Easy VPN with an ASA 5500 as the Server and Cisco 871 as the Easy VPN Remote Configuration Example for more information on a similar scenario where the Cisco 871 Router acts as the Easy VPN Remote.

Refer to VPN Hardware Client on a PIX 501/506 Series Security Appliance with VPN 3000 Concentrator Configuration Example for more information on a similar scenario where the Cisco VPN 3000 Concentrator acts as the Easy VPN Server.

Refer to PIX 501/506 Easy VPN Remote to an IOS Router in Network Extension Mode with Extended Authentication Configuration Example for more information on a similar scenario where the Cisco IOS® Router acts as the Easy VPN Server.

Prerequisites

Requirements

Ensure that you meet these requirements before you attempt this configuration:

- Ensure that your PIX Easy VPN Remote Hardware Client is a PIX 501 or PIX 506/506E that runs PIX Software version 6.2 or later.
- Ensure that your Easy VPN Server is a PIX Firewall that runs PIX Software version 6.0 or later.

Components Used

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

- PIX Easy VPN Remote Hardware Client is a PIX 501 that runs PIX Software version 6.3(1).
- Easy VPN Server is a PIX 515 that runs PIX Software version 6.3(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 the Cisco Technical Tips Conventions for more information on document conventions.

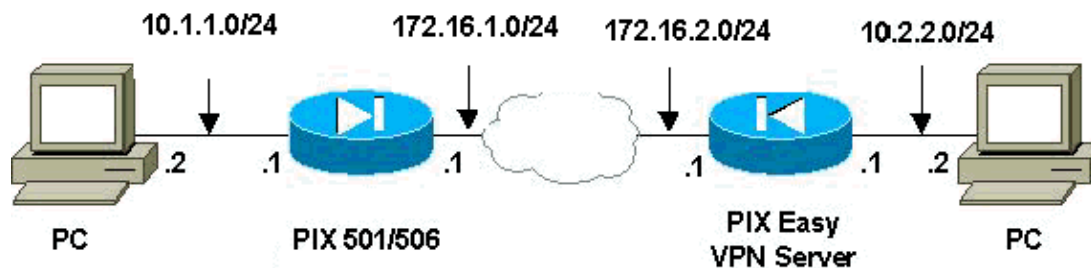
Configure

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 Easy VPN Server
- PIX Easy VPN Remote Hardware Client

PIX Easy VPN Server

```
pix515#write terminal
Building configuration...
: Saved
:
PIX Version 6.3(1)

!--- Specify speed and duplex settings.

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 pix515
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

!--- Specify split tunnelling access list and "nonat" access list.

access-list 101 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
mtu intf2 1500
mtu intf3 1500
mtu intf4 1500
mtu intf5 1500

!--- Define IP address for the PIX's inside and outside interfaces.

ip address outside 172.16.2.1 255.255.255.0
ip address inside 10.2.2.1 255.255.255.0
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
ip local pool ippool 10.3.3.1-10.3.3.254
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

!--- Configure Network Address Translation (NAT)/
!--- Port Address Translation (PAT) for regular traffic,
!--- as well as NAT for IPsec traffic.

global (outside) 1 interface
nat (inside) 0 access-list 101
nat (inside) 1 0.0.0.0 0.0.0.0 0 0

!--- Define the outside router as the default gateway.
!--- Typically this is the IP address of your
!--- Internet service provider's (ISP) router.

route outside 0.0.0.0 0.0.0.0 172.16.2.2 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
sysopt connection permit-ipsec

!--- Configure IPsec transform set and dynamic crypto map.

crypto ipsec transform-set myset esp-aes esp-md5-hmac
crypto dynamic-map dynmap 10 set transform-set myset
crypto map mymap 10 ipsec-isakmp dynamic dynmap

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

crypto map mymap interface outside

!--- Configure Phase 1 Internet Security Association
!--- and Key Management Protocol (ISAKMP) parameters.

isakmp enable outside
isakmp identity address
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption aes
isakmp policy 10 hash md5
isakmp policy 10 group 2
isakmp policy 10 lifetime 86400

!--- Configure VPNGroup parameters, to be sent down to the client.

vpngroup mygroup address-pool ippool
vpngroup mygroup dns-server 10.2.2.2
vpngroup mygroup wins-server 10.2.2.2
vpngroup mygroup default-domain cisco.com
vpngroup mygroup split-tunnel 101
vpngroup mygroup idle-time 1800
vpngroup mygroup password *****
vpngroup idle-time idle-time 1800
telnet timeout 5
ssh timeout 5

```

```
console timeout 0
terminal width 80
Cryptochecksum:67106d7a5a3aa3da0caaeaa93b9fc8d6
: end
[OK]
pix515#
```

PIX Easy VPN Remote Hardware Client

```
pix501#write terminal
Building configuration...
: Saved
:
PIX Version 6.3(1)

!--- Specify speed and duplex settings.

interface ethernet0 auto
interface ethernet1 100full
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pix501
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
pager lines 24
mtu outside 1500
mtu inside 1500

!--- Define IP address for the PIX's inside and outside interfaces.

ip address outside 172.16.1.1 255.255.255.0
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

!--- Configure NAT for traffic that is not encrypted.

global (outside) 1 interface
nat (inside) 1 0.0.0.0 0.0.0.0 0 0

!--- Define the outside router as the default gateway.
!--- Typically this is the IP address of your ISP's router.

route outside 0.0.0.0 0.0.0.0 172.16.1.2 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
telnet timeout 5
ssh timeout 5
console timeout 0

!--- Define Easy VPN Remote parameters.

vpnclient server 172.16.2.1
vpnclient mode network-extension-mode
vpnclient vpngroup mygroup password *****

!--- Enable the VPN Client.
!--- (This automatically initiates the IPsec tunnel to the server.)

vpnclient enable
terminal width 80
Cryptochecksum:b8242b410ad8e3b372018cd1cff77f91
: end
[OK]

```

Verify

Use this section to confirm that your configuration works properly.

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

PIX Easy VPN Server show Commands and Sample Output

- **show crypto isakmp sa** Displays all current Internet Key Exchange (IKE) security associations (SA) at a peer.

```

pix515#show crypto isakmp sa
Total      : 1
Embryonic  : 0
           dst          src          state      pending    created
           172.16.2.1   172.16.1.1  QM_IDLE    0          2
pix515#

```

- **show crypto ipsec sa** Displays IPsec SAs built between peers.

```

pix515#show crypto ipsec sa

!--- This command was issued after a ping
!--- was attempted from the PC behind the
!--- Easy VPN Client to the PC
!--- behind the server.

interface: outside
  Crypto map tag: mymap, local addr. 172.16.2.1

  local  ident (addr/mask/prot/port): (10.2.2.0/255.255.255.0/0/0)
  remote ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0)
  current_peer: 172.16.1.1:500
  dynamic allocated peer ip: 0.0.0.0

```

```
PERMIT, flags={}
#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 0, #recv errors 0
```

```
!--- Ping packets
!--- were successfully exchanged between the
!--- Easy VPN Remote Hardware Client
!--- and the Easy VPN Server.
```

```
local crypto endpt.: 172.16.2.1, remote crypto endpt.: 172.16.1.1
path mtu 1500, ipsec overhead 64, media mtu 1500
current outbound spi: 3a5a28e4
```

```
inbound esp sas:
spi: 0x505c96c6(1348245190)
transform: esp-aes esp-md5-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 2, crypto map: mymap
sa timing: remaining key lifetime (k/sec): (4607999/28471)
IV size: 16 bytes
replay detection support: Y
```

```
inbound ah sas:
```

```
inbound pcp sas:
```

```
outbound esp sas:
spi: 0x3a5a28e4(978987236)
transform: esp-aes esp-md5-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 1, crypto map: mymap
sa timing: remaining key lifetime (k/sec): (4607999/28471)
IV size: 16 bytes
replay detection support: Y
```

```
outbound ah sas:
```

```
outbound pcp sas:
```

```
local ident (addr/mask/prot/port): (10.2.2.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (172.16.1.1/255.255.255.255/0/0)
current_peer: 172.16.1.1:500
dynamic allocated peer ip: 0.0.0.0
```

```
PERMIT, flags={}
#pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0,
#pkts decompress failed: 0
#send errors 0, #recv errors 0
```

```
local crypto endpt.: 172.16.2.1, remote crypto endpt.: 172.16.1.1
path mtu 1500, ipsec overhead 64, media mtu 1500
current outbound spi: 27f378f9
```

```
inbound esp sas:
 spi: 0xf2bb4f00(4072361728)
 transform: esp-aes esp-md5-hmac ,
 in use settings = {Tunnel, }
 slot: 0, conn id: 3, crypto map: mymap
 sa timing: remaining key lifetime (k/sec): (4608000/27796)
 IV size: 16 bytes
 replay detection support: Y
```

```
inbound ah sas:
```

```
inbound pcp sas:
```

```
outbound esp sas:
 spi: 0x27f378f9(670267641)
 transform: esp-aes esp-md5-hmac ,
 in use settings = {Tunnel, }
 slot: 0, conn id: 4, crypto map: mymap
 sa timing: remaining key lifetime (k/sec): (4608000/27787)
 IV size: 16 bytes
 replay detection support: Y
```

```
outbound ah sas:
```

```
outbound pcp sas:
```

```
pix515#
```

PIX Easy VPN Remote Hardware Client show Commands and Sample Output

- **vpnclient enable** Enables an Easy VPN Remote connection. (In Network Extension Mode (NEM), the tunnel is up even when there is no interesting traffic to be exchanged with the headend Easy VPN Server.)

```
pix501(config)#vpnclient enable
```

- **show crypto isakmp policy** Displays the parameters for each IKE policy.

```
pix501#show crypto isakmp policy
```

```
Default protection suite
 encryption algorithm:  DES - Data Encryption Standard (56 bit keys).
 hash algorithm:        Secure Hash Standard
 authentication method: Rivest-Shamir-Adleman Signature
 Diffie-Hellman group:  #1 (768 bit)
 lifetime:              86400 seconds, no volume limit
```

Output from the **show crypto isakmp policy** command after the hardware client is enabled is shown here.

```
pix501(config)#show crypto isakmp policy
```

```
Protection suite of priority 65001
 encryption algorithm:  AES - Advanced Encryption Standard (256 bit keys).
 hash algorithm:        Secure Hash Standard
 authentication method:  Pre-Shared Key with XAUTH
```

Diffie-Hellman group: #2 (1024 bit)
lifetime: 86400 seconds, no volume limit
Protection suite of priority 65002
encryption algorithm: AES - Advanced Encryption Standard (256 bit keys).
hash algorithm: Message Digest 5
authentication method: Pre-Shared Key with XAUTH
Diffie-Hellman group: #2 (1024 bit)
lifetime: 86400 seconds, no volume limit
Protection suite of priority 65003
encryption algorithm: AES - Advanced Encryption Standard (192 bit keys).
hash algorithm: Secure Hash Standard
authentication method: Pre-Shared Key with XAUTH
Diffie-Hellman group: #2 (1024 bit)
lifetime: 86400 seconds, no volume limit
Protection suite of priority 65004
encryption algorithm: AES - Advanced Encryption Standard (192 bit keys).
hash algorithm: Message Digest 5
authentication method: Pre-Shared Key with XAUTH
Diffie-Hellman group: #2 (1024 bit)
lifetime: 86400 seconds, no volume limit
Protection suite of priority 65005
encryption algorithm: AES - Advanced Encryption Standard (128 bit keys).
hash algorithm: Secure Hash Standard
authentication method: Pre-Shared Key with XAUTH
Diffie-Hellman group: #2 (1024 bit)
lifetime: 86400 seconds, no volume limit
Protection suite of priority 65006
encryption algorithm: AES - Advanced Encryption Standard (128 bit keys).
hash algorithm: Message Digest 5
authentication method: Pre-Shared Key with XAUTH
Diffie-Hellman group: #2 (1024 bit)
lifetime: 86400 seconds, no volume limit
Protection suite of priority 65007
encryption algorithm: Three key triple DES
hash algorithm: Secure Hash Standard
authentication method: Pre-Shared Key with XAUTH
Diffie-Hellman group: #2 (1024 bit)
lifetime: 86400 seconds, no volume limit
Protection suite of priority 65008
encryption algorithm: Three key triple DES
hash algorithm: Message Digest 5
authentication method: Pre-Shared Key with XAUTH
Diffie-Hellman group: #2 (1024 bit)
lifetime: 86400 seconds, no volume limit
Protection suite of priority 65009
encryption algorithm: DES - Data Encryption Standard (56 bit keys).
hash algorithm: Message Digest 5
authentication method: Pre-Shared Key with XAUTH
Diffie-Hellman group: #2 (1024 bit)
lifetime: 86400 seconds, no volume limit
Protection suite of priority 65010
encryption algorithm: AES - Advanced Encryption Standard (256 bit keys).
hash algorithm: Secure Hash Standard
authentication method: Pre-Shared Key
Diffie-Hellman group: #2 (1024 bit)
lifetime: 86400 seconds, no volume limit
Protection suite of priority 65011
encryption algorithm: AES - Advanced Encryption Standard (256 bit keys).
hash algorithm: Message Digest 5
authentication method: Pre-Shared Key
Diffie-Hellman group: #2 (1024 bit)
lifetime: 86400 seconds, no volume limit
Protection suite of priority 65012
encryption algorithm: AES - Advanced Encryption Standard (192 bit keys).
hash algorithm: Secure Hash Standard
authentication method: Pre-Shared Key

```

    Diffie-Hellman group:    #2 (1024 bit)
    lifetime:                86400 seconds, no volume limit
Protection suite of priority 65013
    encryption algorithm:   AES - Advanced Encryption Standard (192 bit keys).
    hash algorithm:        Message Digest 5
    authentication method: Pre-Shared Key
    Diffie-Hellman group:   #2 (1024 bit)
    lifetime:              86400 seconds, no volume limit
Protection suite of priority 65014
    encryption algorithm:   AES - Advanced Encryption Standard (128 bit keys).
    hash algorithm:        Secure Hash Standard
    authentication method: Pre-Shared Key
    Diffie-Hellman group:   #2 (1024 bit)
    lifetime:              86400 seconds, no volume limit
Protection suite of priority 65015
    encryption algorithm:   AES - Advanced Encryption Standard (128 bit keys).
    hash algorithm:        Message Digest 5
    authentication method: Pre-Shared Key
    Diffie-Hellman group:   #2 (1024 bit)
    lifetime:              86400 seconds, no volume limit
Protection suite of priority 65016
    encryption algorithm:   Three key triple DES
    hash algorithm:        Secure Hash Standard
    authentication method: Pre-Shared Key
    Diffie-Hellman group:   #2 (1024 bit)
    lifetime:              86400 seconds, no volume limit
Protection suite of priority 65017
    encryption algorithm:   Three key triple DES
    hash algorithm:        Message Digest 5
    authentication method: Pre-Shared Key
    Diffie-Hellman group:   #2 (1024 bit)
    lifetime:              86400 seconds, no volume limit
Protection suite of priority 65018
    encryption algorithm:   DES - Data Encryption Standard (56 bit keys).
    hash algorithm:        Message Digest 5
    authentication method: Pre-Shared Key
    Diffie-Hellman group:   #2 (1024 bit)
    lifetime:              86400 seconds, no volume limit

```

- **show crypto isakmp sa** Displays all current IKE SAs at a peer.

```

pix501(config)#show crypto isakmp sa
Total      : 1
Embryonic  : 0
           dst          src          state      pending   created
           172.16.2.1   172.16.1.1   QM_IDLE    0         1

```

- **show crypto ipsec sa** Displays IPsec SAs built between peers.

```

pix501(config)#show crypto ipsec sa

!--- This command was issued after a ping
!--- was attempted from the PC behind the
!--- Easy VPN client to the PC
!--- behind the server.

interface: outside
    Crypto map tag: _vpnc_cm, local addr. 172.16.1.1

    local ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0)
    remote ident (addr/mask/prot/port): (10.2.2.0/255.255.255.0/0/0)
    current_peer: 172.16.2.1:500
        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
```

```
!--- Ping packets
!--- were successfully exchanged between
!--- the Easy VPN Remote Hardware Client
!--- and the Easy VPN Server.
```

```
local crypto endpt.: 172.16.1.1, remote crypto endpt.: 172.16.2.1
path mtu 1500, ipsec overhead 64, media mtu 1500
current outbound spi: 505c96c6
```

```
inbound esp sas:
spi: 0x3a5a28e4(978987236)
transform: esp-aes esp-md5-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 4, crypto map: _vpnc_cm
sa timing: remaining key lifetime (k/sec): (4607999/28745)
IV size: 16 bytes
replay detection support: Y
```

```
inbound ah sas:
```

```
inbound pcp sas:
```

```
outbound esp sas:
spi: 0x505c96c6(1348245190)
transform: esp-aes esp-md5-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 3, crypto map: _vpnc_cm
sa timing: remaining key lifetime (k/sec): (4607999/28745)
IV size: 16 bytes
replay detection support: Y
```

```
outbound ah sas:
```

```
outbound pcp sas:
```

```
local ident (addr/mask/prot/port): (172.16.1.1/255.255.255.255/0/0)
remote ident (addr/mask/prot/port): (10.2.2.0/255.255.255.0/0/0)
current_peer: 172.16.2.1:500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0,
#pkts decompress failed: 0
#send errors 0, #recv errors 0
```

```
local crypto endpt.: 172.16.1.1, remote crypto endpt.: 172.16.2.1
path mtu 1500, ipsec overhead 64, media mtu 1500
current outbound spi: f2bb4f00
```

```
inbound esp sas:
spi: 0x27f378f9(670267641)
transform: esp-aes esp-md5-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 1, crypto map: _vpnc_cm
sa timing: remaining key lifetime (k/sec): (4608000/28125)
```

```
IV size: 16 bytes
replay detection support: Y
```

```
inbound ah sas:
```

```
inbound pcp sas:
```

```
outbound esp sas:
spi: 0xf2bb4f00(4072361728)
transform: esp-aes esp-md5-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 2, crypto map: _vpnc_cm
sa timing: remaining key lifetime (k/sec): (4608000/28125)
IV size: 16 bytes
replay detection support: Y
```

```
outbound ah sas:
```

```
outbound pcp sas:
```

```
pix501(config)#
```

- **show vpnclient** Displays VPN Client or Easy VPN Remote device configuration information.

```
pix501(config)#show vpnclient
LOCAL CONFIGURATION
vpnclient server 172.16.2.1
vpnclient mode network-extension-mode
vpnclient vpngroup mygroup password *****
vpnclient enable

DOWNLOADED DYNAMIC POLICY
Current Server                : 172.16.2.1
Primary DNS                   : 10.2.2.2
Primary WINS                   : 10.2.2.2
Default Domain                 : cisco.com
PFS Enabled                   : No
Secure Unit Authentication Enabled : No
User Authentication Enabled    : No
Split Networks                 : 10.2.2.0/255.255.255.0
Backup Servers                 : None

pix501(config)#
```

Troubleshoot

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

If you have set up the Easy VPN Remote Hardware Client and Easy VPN Server as described in this document and still experience problems, gather the debug output from each PIX and the output from the **show** commands for analysis by the Cisco Technical Assistance Center (TAC). Also refer to Troubleshooting the PIX to Pass Data Traffic on an Established IPsec Tunnel or IP Security Troubleshooting – Understanding and Using debug Commands. Enable IPsec debugging on the PIX.

PIX **debug** commands and sample output are shown here.

- Easy VPN Server Commands

- Easy VPN Remote Hardware Client Commands

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

Easy VPN Server Commands

- **debug crypto ipsec** Displays the IPsec negotiations of Phase 2.
- **debug crypto isakmp** Displays the ISAKMP negotiations of Phase 1.

This is sample output.

```

pix515(config)#

!--- As soon as the vpnclient enable command
!--- is issued on the remote client PIX,
!--- the server receives an IKE negotiation request.

crypto_isakmp_process_block:src:172.16.1.1,
  dest:172.16.2.1 spt:500 dpt:500
OAK_AG exchange
ISAKMP (0): processing SA payload. message ID = 0

ISAKMP (0): Checking ISAKMP transform 1 against priority 10 policy
ISAKMP:      encryption AES-CBC
ISAKMP:      keylength of 256
ISAKMP:      hash SHA
ISAKMP:      default group 2
ISAKMP:      extended auth pre-share (init)
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x1 0x51 0x80
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 2 against priority 10 policy
ISAKMP:      encryption AES-CBC
ISAKMP:      keylength of 256
ISAKMP:      hash MD5
ISAKMP:      default group 2
ISAKMP:      extended auth pre-share (init)
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x1 0x51 0x80
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 3 against priority 10 policy
ISAKMP:      encryption AES-CBC
ISAKMP:      keylength of 192
ISAKMP:      hash SHA
ISAKMP:      default group 2
ISAKMP:      extended auth pre-share (init)
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x1 0x51 0x80
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 4 against priority 10 policy
ISAKMP:      encryption AES-CBC
ISAKMP:      keylength of 192
ISAKMP:      hash MD5
ISAKMP:      default group 2
ISAKMP:      extended auth pre-share (init)
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x1 0x51 0x80
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 5 against priority 10 policy
ISAKMP:      encryption AES-CBC
ISAKMP:      keylength of 128
ISAKMP:      hash SHA
ISAKMP:      default group 2
ISAKMP:      extended auth pre-share (init)

```

```
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x1 0x51 0x80
ISAKMP (0):  atts are not acceptable. Next payload is 3
ISAKMP (0):  Checking ISAKMP transform 6 against priority 10 policy
ISAKMP:      encryption AES-CBC
ISAKMP:      keylength of 128
ISAKMP:      hash MD5
ISAKMP:      default group 2
ISAKMP:      extended auth pre-share (init)
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x1 0x51 0x80
ISAKMP (0):  atts are not acceptable. Next payload is 3
ISAKMP (0):  Checking ISAKMP transform 7 against priority 10 policy
ISAKMP:      encryption 3DES-CBC
ISAKMP:      hash SHA
ISAKMP:      default group 2
ISAKMP:      extended auth pre-share (init)
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x1 0x51 0x80
ISAKMP (0):  atts are not acceptable. Next payload is 3
ISAKMP (0):  Checking ISAKMP transform 8 against priority 10 policy
ISAKMP:      encryption 3DES-CBC
ISAKMP:      hash MD5
ISAKMP:      default group 2
ISAKMP:      extended auth pre-share (init)
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x1 0x51 0x80
ISAKMP (0):  atts are not acceptable. Next payload is 3
ISAKMP (0):  Checking ISAKMP transform 9 against priority 10 policy
ISAKMP:      encryption DES-CBC
ISAKMP:      hash MD5
ISAKMP:      default group 2
ISAKMP:      extended auth pre-share (init)
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x1 0x51 0x80
ISAKMP (0):  atts are not acceptable. Next payload is 3
ISAKMP (0):  Checking ISAKMP transform 10 against priority 10 policy
crypto_isakmp_process_block:src:172.16.1.1,
  dest:172.16.2.1 spt:500 dpt:500
OAK_AG exchange
ISAKMP (0):  processing HASH payload. message ID = 0
ISAKMP (0):  processing NOTIFY payload 24578 protocol 1
             spi 0, message ID = 0
ISAKMP (0):  processing notify INITIAL_CONTACTIPSEC(key_engine):
             got a queue event...
IPSEC(key_engine_delete_sas): rec'd delete notify from ISAKMP
IPSEC(key_engine_delete_sas): delete all SAs shared with 172.16.1.1

ISAKMP (0):  processing vendor id payload

ISAKMP (0):  received xauth v6 vendor id

ISAKMP (0):  processing vendor id payload

ISAKMP (0):  remote peer supports dead peer detection

ISAKMP (0):  processing vendor id payload

ISAKMP (0):  speaking to another IOS box!

ISAKMP (0):  processing vendor id payload

crypto_isakmp_process_block:src:172.16.1.1,
  dest:172.16.2.1 spt:500 dpt:500
ISAKMP_TRANSACTION exchange
crypto_isakmp_process_block:src:172.16.1.1,
```

```
    dest:172.16.2.1 spt:500 dpt:500
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_IDLE
ISAKMP (0): processing SA payload. message ID = 4788683

ISAKMP : Checking IPsec proposal 1

ISAKMP: transform 1, ESP_AES
ISAKMP:   attributes in transform:
ISAKMP:     encaps is 1
ISAKMP:     SA life type in seconds
ISAKMP:     SA life duration (basic) of 28800
ISAKMP:     SA life type in kilobytes
ISAKMP:     SA life duration (VPI) of  0x0 0x46 0x50 0x0
ISAKMP:     authenticator is HMAC-SHA
ISAKMP:     key length is 256IPSEC(validate_proposal):
      transform proposal (prot 3, trans 12, hmac_alg 2) not supported

ISAKMP (0): atts not acceptable. Next payload is 0
ISAKMP : Checking IPsec proposal 2

ISAKMP: transform 1, ESP_AES
ISAKMP:   attributes in transform:
ISAKMP:     encaps is 1
ISAKMP:     SA life type in seconds
ISAKMP:     SA life duration (basic) of 28800
ISAKMP:     SA life type in kilobytes
ISAKMP:     SA life duration (VPI) of  0x0 0x46 0x50 0x0
ISAKMP:     authenticator is HMAC-MD5
ISAKMP:     key length is 256IPSEC(validate_proposal):
      transform proposal (prot 3, trans 12, hmac_alg 1) not supported

ISAKMP (0): atts not acceptable. Next payload is 0
ISAKMP : Checking IPsec proposal 3

ISAKMP: transform 1, ESP_AES
ISAKMP:   attributes in transform:
ISAKMP:     encaps is 1
ISAKMP:     SA life type in seconds
ISAKMP:     SA life duration (basic) of 28800
ISAKMP:     SA life type in kilobytes
ISAKMP:     SA life duration (VPI) of  0x0 0x46 0x50 0x0
ISAKMP:     authenticator is HMAC-SHA
ISAKMP:     key length is 192IPSEC(validate_proposal):
      transform proposal (prot 3, trans 12, hmac_alg 2) not supported

ISAKMP (0): atts not acceptable. Next payload is 0
ISAKMP : Checking IPsec proposal 4

ISAKMP: transform 1, ESP_AES
ISAKMP:   attributes in transform:
ISAKMP:     encaps is 1
ISAKMP:     SA life type in seconds
ISAKMP:     SA life duration (basic) of 28800
ISAKMP:     SA life type in kilobytes
ISAKMP:     SA life duration (VPI) of  0x0 0x46 0x50 0x0
ISAKMP:     authenticator is HMAC-MD5
ISAKMP:     key length is 192IPSEC(validate_proposal):
      transform proposal (prot 3, trans 12, hmac_alg 1) not supported

ISAKMP (0): atts not acceptable. Next payload is 0
ISAKMP : Checking IPsec proposal 5

ISAKMP: transform 1, ESP_AES
ISAKMP:   attributes in transform:
```

```
ISAKMP:         encaps is 1
ISAKMP:         SA life type in seconds
ISAKMP:         SA life duration (basic) of 28800
ISAKMP:         SA life type in kilobytes
ISAKMP:         SA life duration (VPI) of  0x0 0x46 0x50 0x0
ISAKMP:         authenticator is HMAC-SHA
ISAKMP:         key length is 128IPSEC(validate_proposal):
    transform proposal (prot 3, trans 12, hmac_alg 2) not supported
```

```
ISAKMP (0): atts not acceptable. Next payload is 0
ISAKMP : Checking IPsec proposal 6
```

```
ISAKMP: transform 1, ESP_AES
ISAKMP:   attributes in transform:
ISAKMP:     encaps is 1
ISAKMP:     SA life type in seconds
ISAKMP:     SA life duration (basic) of 28800
ISAKMP:     SA life type in kilobytes
ISAKMP:     SA life duration (VPI) of  0x0 0x46 0x50 0x0
ISAKMP:     authenticator is HMAC-MD5
ISAKMP:     key length is 128
ISAKMP (0): atts are acceptable.IPSEC(validate_proposal_request):
    proposal part #1,
    (key eng. msg.) dest= 172.16.2.1, src= 172.16.1.1,
    dest_proxy= 10.2.2.0/255.255.255.0/0/0 (type=4),
    src_proxy= 172.16.1.1/255.255.255.255/0/0 (type=1),
    protocol= ESP, transform= esp-aes esp-md5-hmac ,
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 128, flags= 0x4
```

!--- Both PIXes accept the policy for IPsec.

```
ISAKMP (0): processing NONCE payload. message ID = 4788683
```

```
ISAKMP (0): processing ID payload. message ID = 4788683
ISAKMP (0): ID_IPV4_ADDR src 172.16.1.1 prot 0 port 0
ISAKMP (0): processing ID payload. message ID = 4788683
ISAKMP (0): ID_IPV4_ADDR_SUBNET dst 10.2.2.0/255.255.255.0 prot 0
    port 0IPSEC(key_engine): got a queue event...
IPSEC(spi_response): getting spi 0xf5720496(4117890198) for SA
    from      172.16.1.1 to      172.16.2.1 for prot 3
```

```
return status is IKMP_NO_ERROR
crypto_isakmp_process_block:src:172.16.1.1,
    dest:172.16.2.1 spt:500 dpt:500
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_AUTH_AWAIT
ISAKMP (0): Creating IPsec SAs
    inbound SA from 172.16.1.1 to 172.16.2.1
    (proxy 172.16.1.1 to 10.2.2.0)
    has spi 4117890198 and conn_id 3 and flags 4
    lifetime of 28800 seconds
crypto_isakmp_process_block:src:172.16.1.1,
    dest:172.16.2.1 spt:500 dpt:500
ISAKMP (0): processing NOTIFY payload 36136 protocol 1
    spi 0, message ID = 843197376
ISAKMP (0): received DPD_R_U_THERE from peer 172.16.1.1
ISAKMP (0): sending NOTIFY message 36137 protocol 1
return status is IKMP_NO_ERR_NO_TRANS
crypto_isakmp_process_block:src:172.16.1.1,
    dest:172.16.2.1 spt:500 dpt:500
ISAKMP (0): processing NOTIFY payload 36136 protocol 1
    spi 0, message ID = 1985282089
ISAKMP (0): received DPD_R_U_THERE from peer 172.16.1.1
ISAKMP (0): sending NOTIFY message 36137 protocol 1
```

```

return status is IKMP_NO_ERR_NO_TRANS
crypto_isakmp_process_block:src:172.16.1.1,
  dest:172.16.2.1 spt:500 dpt:500
ISAKMP (0): processing NOTIFY payload 36136 protocol 1
  spi 0, message ID = 1510977390
ISAKMP (0): received DPD_R_U_THERE from peer 172.16.1.1
ISAKMP (0): sending NOTIFY message 36137 protocol 1
return status is IKMP_NO_ERR_NO_TRANS

```

Easy VPN Remote Hardware Client Commands

- **debug crypto ipsec** Displays the IPsec negotiations of Phase 2.
- **debug crypto isakmp** Displays the ISAKMP negotiations of Phase 1.

```

pix501(config)#vpnclient enable
(cIoSnAfKigM)P# (0): ID payload
  next-payload : 13
  type         : 11
  protocol     : 17
  port         : 0
  length      : 11
ISAKMP (0): Total payload length: 15
ISAKMP (0:0): sending NAT-T vendor ID - rev 2 & 3
ISAKMP (0): beginning Aggressive Mode exchange
crypto_isakmp_process_block:src:172.16.2.1,
  dest:172.16.1.1 spt:500 dpt:500
OAK_AG exchange
ISAKMP (0): processing SA payload. message ID = 0

ISAKMP (0): Checking ISAKMP transform 1 against priority 65001 policy
ISAKMP:   encryption AES-CBC
ISAKMP:   keylength of 128
ISAKMP:   hash MD5
ISAKMP:   default group 2
ISAKMP:   auth pre-share
ISAKMP:   life type in seconds
ISAKMP:   life duration (VPI) of 0x0 0x1 0x51 0x80
ISAKMP (0): atts are not acceptable. Next payload is 0
ISAKMP (0): Checking ISAKMP transform 1 against priority 65002 policy
ISAKMP:   encryption AES-CBC
ISAKMP:   keylength of 128
ISAKMP:   hash MD5
ISAKMP:   default group 2
ISAKMP:   auth pre-share
ISAKMP:   life type in seconds
ISAKMP:   life duration (VPI) of 0x0 0x1 0x51 0x80
ISAKMP (0): atts are not acceptable. Next payload is 0
ISAKMP (0): Checking ISAKMP transform 1 against priority 65003 policy
ISAKMP:   encryption AES-CBC
ISAKMP:   keylength of 128
ISAKMP:   hash MD5
ISAKMP:   default group 2
ISAKMP:   auth pre-share
ISAKMP:   life type in seconds
ISAKMP:   life duration (VPI) of 0x0 0x1 0x51 0x80
ISAKMP (0): atts are not acceptable. Next payload is 0
ISAKMP (0): Checking ISAKMP transform 1 against priority 65004 policy
ISAKMP:   encryption AES-CBC
ISAKMP:   keylength of 128
ISAKMP:   hash MD5
ISAKMP:   default group 2
ISAKMP:   auth pre-share
ISAKMP:   life type in seconds
ISAKMP:   life duration (VPI) of 0x0 0x1 0x51 0x80
ISAKMP (0): atts are not acceptable. Next payload is 0

```

```
ISAKMP (0): Checking ISAKMP transform 1 against priority 65005 policy
ISAKMP: encryption AES-CBC
ISAKMP: keylength of 128
ISAKMP: hash MD5
ISAKMP: default group 2
ISAKMP: auth pre-share
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x0 0x1 0x51 0x80
ISAKMP (0): atts are not acceptable. Next payload is 0
ISAKMP (0): Checking ISAKMP transform 1 against priority 65006 policy
ISAKMP: encryption AES-CBC
ISAKMP: keylength of 128
ISAKMP: hash MD5
ISAKMP: default group 2
ISAKMP: auth pre-share
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x0 0x1 0x51 0x80
ISAKMP (0): atts are not acceptable. Next payload is 0
ISAKMP (0): Checking ISAKMP transform 1 against priority 65007 policy
ISAKMP: encryption AES-CBC
ISAKMP: keylength of 128
ISAKMP: hash MD5
ISAKMP: default group 2
ISAKMP: auth pre-share
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x0 0x1 0x51 0x80
ISAKMP (0): atts are not acceptable. Next payload is 0
ISAKMP (0): Checking ISAKMP transform 1 against priority 65008 policy
ISAKMP: encryption AES-CBC
ISAKMP: keylength of 128
ISAKMP: hash MD5
ISAKMP: default group 2
ISAKMP: auth pre-share
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x0 0x1 0x51 0x80
ISAKMP (0): atts are not acceptable. Next payload is 0
ISAKMP (0): Checking ISAKMP transform 1 against priority 65009 policy
ISAKMP: encryption AES-CBC
ISAKMP: keylength of 128
ISAKMP: hash MD5
ISAKMP: default group 2
ISAKMP: auth pre-share
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x0 0x1 0x51 0x80
ISAKMP : attributes being requested
```

```
crypto_isakmp_process_block:src:172.16.2.1,
  dest:172.16.1.1 spt:500 dpt:500
ISAKMP (0): beginning Quick Mode exchange,
  M-ID of 1112046058:424879eaIPSEC(key_engine): got a queue event...
IPSEC(spi_response): getting spi 0x274d3063(659370083) for SA
  from 172.16.2.1 to 172.16.1.1 for prot 3
```

```
crypto_isakmp_process_block:src:172.16.2.1,
  dest:172.16.1.1 spt:500 dpt:500
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_IDLE
ISAKMP (0): processing SA payload. message ID = 1112046058
```

```
ISAKMP : Checking IPsec proposal 1
```

```
ISAKMP: transform 1, ESP_AES
ISAKMP: attributes in transform:
ISAKMP: encaps is 1
ISAKMP: SA life type in seconds
```

```

ISAKMP:      SA life duration (basic) of 28800
ISAKMP:      SA life type in kilobytes
ISAKMP:      SA life duration (VPI) of 0x0 0x46 0x50 0x0
ISAKMP:      authenticator is HMAC-MD5
ISAKMP:      key length is 128
ISAKMP (0): atts are acceptable.IPSEC(validate_proposal_request):
  proposal part #1,
  (key eng. msg.) dest= 172.16.2.1, src= 172.16.1.1,
  dest_proxy= 10.2.2.0/255.255.255.0/0/0 (type=4),
  src_proxy= 172.16.1.1/255.255.255.255/0/0 (type=1),
  protocol= ESP, transform= esp-aes esp-md5-hmac ,
  lifedur= 0s and 0kb,
  spi= 0x0(0), conn_id= 0, keysize= 128, flags= 0x4

ISAKMP (0):  processing NONCE payload. message ID = 1112046058

ISAKMP (0):  processing ID payload. message ID = 1112046058
ISAKMP (0):  processing ID payload. message ID = 1112046058
ISAKMP (0):  Creating IPsec SAs
  inbound SA from 172.16.2.1 to 172.16.1.1
  (proxy 10.2.2.0 to 172.16.1.1)
  has spi 659370083 and conn_id 2 and flags 4
  lifetime of 28800 seconds
  lifetime of 4608000 kilobytes
  outbound SA from 172.16.1.1 to 172.16.2.1
  (proxy 172.16.1.1 to 10.2.2.0)
  has spi 264316759 and conn_id 1 and flags 4
  lifetime of 28800 seconds
  lifetime of 4608000 kilobytesIPSEC(key_engine):
  got a queue event...
IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 172.16.1.1, src= 172.16.2.1,
  dest_proxy= 172.16.1.1/255.255.255.255/0/0 (type=1),
  src_proxy= 10.2.2.0/255.255.255.0/0/0 (type=4),
  protocol= ESP, transform= esp-aes esp-md5-hmac ,
  lifedur= 28800s and 4608000kb,
  spi= 0x274d3063(659370083), conn_id= 2, keysize= 128, flags= 0x4
IPSEC(initialize_sas): ,
  (key eng. msg.) src= 172.16.1.1, dest= 172.16.2.1,
  src_proxy= 172.16.1.1/255.255.255.255/0/0 (type=1),
  dest_proxy= 10.2.2.0/255.255.255.0/0/0 (type=4),
  protocol= ESP, transform= esp-aes esp-md5-hmac ,
  lifedur= 28800s and 4608000kb,
  spi= 0xf1c12757(264316759), conn_id= 1, keysize= 128, flags= 0x4

VPN Peer: IPSEC: Peer ip:172.16.2.1/500 Ref cnt incremented to:2
  Total VPN Peers:1
VPN Peer: IPSEC: Peer ip:172.16.2.1/500 Ref cnt incremented to:3
  Total VPN Peers:1
return status is IKMP_NO_ERROR
pix501(config)#
pix501(config)#
ISAKMP (0):  sending NOTIFY message 36136 protocol 1
crypto_isakmp_process_block:src:172.16.2.1,
  dest:172.16.1.1 spt:500 dpt:500
ISAKMP (0):  processing NOTIFY payload 36137 protocol 1
  spi 0, message ID = 136860646n
ISAKMP (0):  received DPD_R_U_THERE_ACK from peer 172.16.2.1

```

- **debug vpncient** Displays the negotiations specific to the VPN Client.

```

pix501(config)#vpncient enable
pix501(config)# 505: VPNC CFG: transform set unconfig attempt done
506: VPNC CLI: no isakmp keepalive 10
507: VPNC CLI: no isakmp nat-traversal 20
508: VPNC CFG: IKE unconfig successful

```

```
509: VPNC CLI: no crypto map _vpnc_cm
510: VPNC CFG: crypto map deletion attempt done
511: VPNC CFG: crypto unconfig successful
512: VPNC CLI: no global (outside) 65001
513: VPNC CLI: no nat (inside) 0 access-list _vpnc_acl
514: VPNC CFG: nat unconfig attempt failed
515: VPNC CLI: no http 10.1.1.1 255.255.255.0 inside
516: VPNC CLI: no http server enable
517: VPNC CLI: no access-list _vpnc_acl
518: VPNC CFG: ACL deletion attempt failed
519: VPNC CLI: no crypto map _vpnc_cm interface outside
520: VPNC CFG: crypto map de/attach failed
521: VPNC CLI: no sysopt connection permit-ipsec
522: VPNC CLI: sysopt connection permit-ipsec
523: VPNC CFG: transform sets configured
524: VPNC CFG: crypto config successful
525: VPNC CLI: isakmp keepalive 10
526: VPNC CLI: isakmp nat-traversal 20
527: VPNC CFG: IKE config successful
528: VPNC CLI: http 10.1.1.1 255.255.255.0 inside
529: VPNC CLI: http server enable
530: VPNC CLI: no access-list _vpnc_acl
531: VPNC CFG: ACL deletion attempt failed
532: VPNC CLI: access-list _vpnc_acl
    permit ip host 172.16.1.1 host 172.16.2.1
533: VPNC CLI: crypto map _vpnc_cm 10 match address _vpnc_acl
534: VPNC CFG: crypto map acl update successful
535: VPNC CLI: no crypto map _vpnc_cm interface outside
536: VPNC CLI: crypto map _vpnc_cm interface outside
537: VPNC INF: IKE trigger request done
538: VPNC INF: Constructing policy download req
539: VPNC INF: Packing attributes for policy request
540: VPNC INF: Attributes being requested
541: VPNC ATT: ALT_DEF_DOMAIN: cisco.com
542: VPNC ATT: INTERNAL_IP4_NBNS: 10.2.2.2
543: VPNC ATT: INTERNAL_IP4_DNS: 10.2.2.2
544: VPNC ATT: ALT_SPLIT_INCLUDE
545: VPNC INF: 10.2.2.0/255.255.255.0
546: VPNC ATT: ALT_PFS: 0
547: VPNC ATT: ALT_CFG_SEC_UNIT: 0
548: VPNC ATT: ALT_CFG_USER_AUTH: 0
549: VPNC CLI: no access-list _vpnc_acl
550: VPNC CLI: access-list _vpnc_acl
    permit ip 10.1.1.0 255.255.255.0 10.2.2.0 255.255.255.0
551: VPNC CLI: access-list _vpnc_acl
    permit ip host 172.16.1.1 10.2.2.0 255.255.255.0
552: VPNC CFG: _vpnc_acl ST define done
553: VPNC CFG: Split DNS config attempt done
554: VPNC CLI: crypto map _vpnc_cm 10 match address _vpnc_acl
555: VPNC CFG: crypto map acl update successful
556: VPNC CLI: no crypto map _vpnc_cm interface outside
557: VPNC CLI: crypto map _vpnc_cm interface outside
558: VPNC CLI: no global (outside) 65001
559: VPNC CLI: no nat (inside) 0 access-list _vpnc_acl
560: VPNC CFG: nat unconfig attempt failed
561: VPNC CLI: nat (inside) 0 access-list _vpnc_acl
562: VPNC INF: IKE trigger request done
```

Related Information

- [PIX Support Page](#)
- [Documentation for PIX Firewall](#)
- [PIX Command References](#)
- [IPsec Negotiations/IKE Protocols Support Page](#)

- **Requests for Comments (RFCs)**
 - **Technical Support – Cisco Systems**
-

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2010 – 2011 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Sep 26, 2008

Document ID: 40820
