IOS Easy VPN Remote Hardware Client to a PIX Easy VPN Server Configuration Example

Document ID: 27124

Introduction

This document provides a sample configuration for IPSec between the Cisco IOS® Easy VPN Remote Hardware Client and the PIX Easy VPN Server.

Note: The Easy VPN Remote feature is also referred to as Hardware Client and EzVPN Client.

Refer to Configuring the Cisco EzVPN Client on Cisco IOS with the VPN 3000 Concentrator for information on how to configure a Cisco IOS router as an EzVPN in Network Extension Mode (NEM) in order to connect to a Cisco VPN 3000 Concentrator.

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 information on how to configure IPSec between a Cisco PIX/ASA 7.x and a Cisco 871 router using Easy VPN.

Refer to 7200 Easy VPN Server to 871 Easy VPN Remote Configuration Example for information on how to configure a Cisco 7200 Router as an EzVPN and the Cisco 871 Router as the Easy VPN Remote client.

Prerequisites

Requirements

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

- Ensure that your Cisco IOS and hardware supports the Easy VPN Remote feature. Refer to the Software Advisor (registered customers only) .
- Ensure that your Easy VPN Server is a PIX Firewall that runs PIX Software Version 6.2 or later.
- Ensure that you have a 3DES license installed on your PIX. Refer to *Free* Register for a 3DES/AES IPSec Software Feature Key (registered customers only) and Upgrade the Activation Key.

Components Used

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

- Cisco IOS Easy VPN Remote Hardware Client is an 831 router that runs Cisco IOS Software Release 12.3(8)T.
- Easy VPN Server is a PIX 525 that runs PIX Software Version 6.3(3).

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

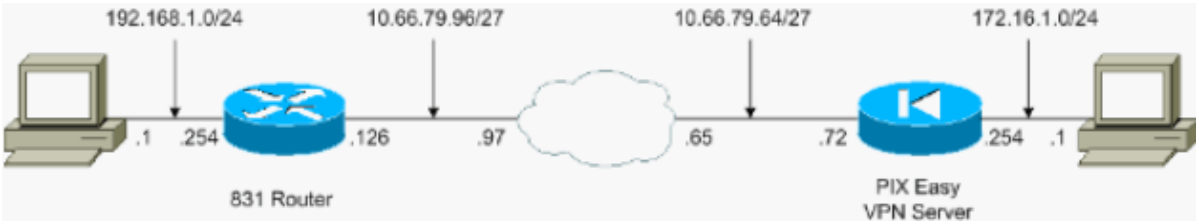
Configure

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
- Cisco IOS Easy VPN Remote Hardware Client

PIX Easy VPN Server

```
pix525#show running-config
: Saved
:
PIX Version 6.3(3)
interface ethernet0 auto
interface ethernet1 auto
interface ethernet2 auto shutdown
interface ethernet3 auto shutdown
interface ethernet4 auto shutdown
interface ethernet5 auto shutdown
interface ethernet6 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
nameif ethernet6 intf6 security12
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pix525
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


!--- Specify the access list to bypass
!--- Network Address Translation (NAT) for VPN traffic.


access-list nonat permit ip 172.16.1.0 255.255.255.0 192.168.1.0 255.255.255.0


!--- Specify the split tunneling access list.


access-list 110 permit ip 172.16.1.0 255.255.255.0 192.168.1.0 255.255.255.0
pager lines 24
mtu outside 1500
mtu inside 1500
mtu intf2 1500
mtu intf3 1500
mtu intf4 1500
mtu intf5 1500
mtu intf6 1500
ip address outside 10.66.79.72 255.255.255.224
ip address inside 172.16.1.254 255.255.255.0
no ip address intf2
no ip address intf3
no ip address intf4
no ip address intf5
no ip address intf6
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
no failover ip address intf6
pdm history enable
arp timeout 14400
```

```
!--- Configure NAT/Port Address Translation (PAT)
 !--- for non-encrypted traffic, as well as NAT for IPSec traffic.


global (outside) 1 interface
nat (inside) 0 access-list nonat
nat (inside) 1 172.16.1.0 255.255.255.0 0 0
route outside 0.0.0.0 0.0.0.0 10.66.79.65 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 tripledes esp-3des esp-sha-hmac
crypto dynamic-map dynmap 10 set transform-set tripledes
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 3des
isakmp policy 10 hash sha
isakmp policy 10 group 2
isakmp policy 10 lifetime 86400


!--- Configure VPN Group parameters that are sent down to the client.


vpngroup vpn-hw-client-group dns-server 172.16.1.1
vpngroup vpn-hw-client-group wins-server 172.16.1.1
vpngroup vpn-hw-client-group default-domain cisco.com
vpngroup vpn-hw-client-group split-tunnel 110
vpngroup vpn-hw-client-group idle-time 1800
vpngroup vpn-hw-client-group password ********
telnet timeout 5
ssh timeout 5
console timeout 0
terminal width 80
Cryptochecksum:700fe4d4e7fcdc6750953e64046930c0
: end
```

Cisco IOS Easy VPN Remote Hardware Client

```
831#show running-config
831#show run
Building configuration...

Current configuration : 1226 bytes
!
version 12.3
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname 831
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
ip subnet-zero
!
!
!
!
ip name-server 172.16.1.1
ip ips po max-events 100
no ftp-server write-enable
!
!
!
!
!
!
!
!
!
crypto ipsec client ezvpn vpn-hw-client
 connect auto
 group vpn-hw-client-group key password
 mode network-extension
 peer 10.66.79.72
!
!
!
!
interface Ethernet0
 ip address 192.168.1.254 255.255.255.0
 crypto ipsec client ezvpn vpn-hw-client inside
!
interface Ethernet1
 ip address 10.66.79.126 255.255.255.224
 duplex auto
 crypto ipsec client ezvpn vpn-hw-client
!
interface FastEthernet1
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet2
 no ip address
 duplex auto
 speed auto
!
```

```
interface FastEthernet3
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet4
 no ip address
 duplex auto
 speed auto
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.66.79.97
!
ip http server
no ip http secure-server
!
!
no cdp run
!
control-plane
!
!
line con 0
 no modem enable
 transport preferred all
 transport output all
line aux 0
line vty 0 4
!
scheduler max-task-time 5000
end
```

Verify

Use these sections to confirm that your configuration works properly.

- PIX Easy VPN Server
- Cisco IOS Easy VPN Remote Hardware Client

PIX Easy VPN Server

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

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

```
pix525(config)#show crypto isakmp sa
Total     : 1
Embryonic : 0
        dst               src        state     pending     created
     10.66.79.72     10.66.79.126    QM_IDLE         0           1
```

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

```
pix525(config)#show crypto ipsec sa


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

```
interface: outside
    Crypto map tag: mymap, local addr. 10.66.79.72

   local  ident (addr/mask/prot/port): (172.16.1.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
   current_peer: 10.66.79.126:500
   dynamic allocated peer ip: 0.0.0.0

     PERMIT, flags={}
    #pkts encaps: 5, #pkts encrypt: 5, #pkts digest 5
    #pkts decaps: 5, #pkts decrypt: 5, #pkts verify 5
    #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
 !--- are successfully exchanged between the
 !--- Easy VPN Remote Hardware Client
 !--- and the Easy VPN Server.


     local crypto endpt.: 10.66.79.72, remote crypto endpt.: 10.66.79.126
     path mtu 1500, ipsec overhead 56, media mtu 1500
     current outbound spi: 13f1aa83

     inbound esp sas:
      spi: 0xf4dd4178(4108140920)
        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): (4607999/28567)
        IV size: 8 bytes
        replay detection support: Y


     inbound ah sas:


     inbound pcp sas:


     outbound esp sas:
      spi: 0x13f1aa83(334604931)
        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): (4607999/28567)
        IV size: 8 bytes
        replay detection support: Y


     outbound ah sas:


     outbound pcp sas:
```

Cisco IOS Easy VPN Remote Hardware Client

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

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

```
831#show crypto isakmp sa
dst             src             state          conn-id slot
10.66.79.72     10.66.79.126    QM_IDLE              1    0
```

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

```
831#show crypto ipsec sa


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


interface: Ethernet1
    Crypto map tag: Ethernet1-head-0, local addr. 10.66.79.126

   protected vrf:
   local  ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (172.16.1.0/255.255.255.0/0/0)
   current_peer: 10.66.79.72:500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5
    #pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0


!--- ping packets
 !--- are successfully exchanged between
 !--- the Easy VPN Remote Hardware Client
 !--- and the Easy VPN Server.


     local crypto endpt.: 10.66.79.126, remote crypto endpt.: 10.66.79.72
     path mtu 1500, media mtu 1500
     current outbound spi: F4DD4178

     inbound esp sas:
      spi: 0x13F1AA83(334604931)
        transform: esp-3des esp-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 20, flow_id: 1, crypto map: Ethernet1-head-0
        crypto engine type: Hardware, engine_id: 2
        sa timing: remaining key lifetime (k/sec): (4444258/28648)
        ike_cookies: A12E6D0D 2C8D9B92 41AB02FB A00A5B03
        IV size: 8 bytes
        replay detection support: Y

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0xF4DD4178(4108140920)
        transform: esp-3des esp-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 21, flow_id: 2, crypto map: Ethernet1-head-0
        crypto engine type: Hardware, engine_id: 2
        sa timing: remaining key lifetime (k/sec): (4444258/28647)
        ike_cookies: A12E6D0D 2C8D9B92 41AB02FB A00A5B03
```

```
            IV size: 8 bytes
            replay detection support: Y

        outbound ah sas:

        outbound pcp sas:
```

- **show crypto ipsec client ezvpn** Displays VPN Client or Easy VPN Remote device configuration information.

```
831#show crypto ipsec client ezvpn
Easy VPN Remote Phase: 2

Tunnel name : vpn-hw-client
Inside interface list: Ethernet0,
Outside interface: Ethernet1
Current State: IPSEC_ACTIVE
Last Event: SOCKET_UP
DNS Primary: 172.16.1.1
DNS Secondary: 172.16.1.1
NBMS/WINS Primary: 172.16.1.1
NBMS/WINS Secondary: 172.16.1.1
Default Domain: cisco.com
Split Tunnel List: 1
       Address    : 172.16.1.0
       Mask       : 255.255.255.0
       Protocol   : 0x0
       Source Port: 0
       Dest Port  : 0
```

Troubleshoot

These sections provide information you can use to troubleshoot your configuration.

- PIX Easy VPN Server
- Cisco IOS Easy VPN Remote Hardware Client

If you have set up the Easy VPN Remote Hardware Client and Easy VPN Server as described in this document and you still experience problems, gather the **debug** output from each device and the output from the **show** commands for analysis by the Cisco Technical Assistance Center (TAC).

Refer to IP Security Troubleshooting − Understanding and Using debug Commands and Troubleshooting the PIX to Pass Data Traffic on an Established IPSec Tunnel for additional information on troubleshooting.

PIX Easy VPN Server

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

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

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

Sample output is shown here:

```
pix525(config)#


 !--- As soon as the crypto ipsec client ezvpn vpn-hw-client command
```

```
 !--- is issued on the outside interface of the Cisco IOS Easy VPN Remote
 !--- Hardware Client, the server receives an IKE negotiation request.


crypto_isakmp_process_block:src:10.66.79.126, dest:10.66.79.72 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 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 0x20 0xc4 0x9b
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 2 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 0x20 0xc4 0x9b
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 3 against priority 10 policy
ISAKMP:      encryption DES-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 0x20 0xc4 0x9b
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 4 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 0x20 0xc4 0x9b
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 5 against priority 10 policy
ISAKMP:      encryption 3DES-CBC
ISAKMP:      hash SHA
ISAKMP:      default group 2
ISAKMP:      auth pre-share
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x20 0xc4 0x9b
ISAKMP (0): atts are acceptable. Next payload is 3
ISAKMP (0): processing vendor id payload

ISAKMP (0:0): vendor ID is NAT-T
ISAKMP (0): processing vendor id payload

ISAKMP (0:0): vendor ID is NAT-T
ISAKMP (0): processing KE payload. message ID = 0

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

ISAKMP (0): processing ID payload. message ID = 0
ISAKMP (0): processing vendor id payload

ISAKMP (0): remote peer supports dead peer detection

ISAKMP (0): processing vendor id payload

ISAKMP (0): received xauth v6 vendor id
```

```
ISAKMP (0): processing vendor id payload

ISAKMP (0): claimed IOS but failed authentication

ISAKMP (0): processing vendor id payload

ISAKMP (0): speaking to a Unity client

ISAKMP (0): ID payload
        next-payload : 10
        type         : 1
        protocol     : 17
        port         : 500
        length       : 8
ISAKMP (0): Total payload length: 12
return status is IKMP_NO_ERROR
crypto_isakmp_process_block:src:10.66.79.126, dest:10.66.79.72 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    10.66.79.126

ISAKMP (0): SA has been authenticated
ISAKMP: Created a peer struct for 10.66.79.126, peer port 62465
return status is IKMP_NO_ERROR
ISAKMP (0): sending phase 1 RESPONDER_LIFETIME notify
ISAKMP (0): sending NOTIFY message 24576 protocol 1
VPN Peer: ISAKMP: Added new peer: ip:10.66.79.126/500 Total VPN Peers:1
VPN Peer: ISAKMP: Peer ip:10.66.79.126/500 Ref cnt incremented to:1 Total
VPN Peers:1
ISAKMP: peer is a remote access client
crypto_isakmp_process_block:src:10.66.79.126, dest:10.66.79.72 spt:500 dpt:500
ISAKMP_TRANSACTION exchange
ISAKMP (0:0): processing transaction payload from 10.66.79.126.
 message ID = 63324444
ISAKMP: Config payload CFG_REQUEST
ISAKMP (0:0): checking request:
ISAKMP: attribute    IP4_DNS (3)
ISAKMP: attribute    IP4_DNS (3)
ISAKMP: attribute    IP4_NBNS (4)
ISAKMP: attribute    IP4_NBNS (4)
ISAKMP: attribute    ALT_SPLIT_INCLUDE (28676)
ISAKMP: attribute    ALT_SPLITDNS_NAME (28675)
ISAKMP: attribute    ALT_DEF_DOMAIN (28674)
ISAKMP: attribute    UNKNOWN (28673)
        Unsupported Attr: 28673
ISAKMP: attribute    UNKNOWN (28678)
        Unsupported Attr: 28678
ISAKMP: attribute    ALT_PFS (28679)
ISAKMP: attribute    ALT_BACKUP_SERVERS (28681)
ISAKMP: attribute    APPLICATION_VERSION (7)
ISAKMP (0:0): responding to peer config from 10.66.79.126. ID = 2563858956
return status is IKMP_NO_ERROR
crypto_isakmp_process_block:src:10.66.79.126, dest:10.66.79.72 spt:500 dpt:500
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_IDLE
ISAKMP (0): processing SA payload. message ID = 3238088328

ISAKMP : Checking IPSec proposal 1

ISAKMP: transform 1, ESP_3DES
```

```
ISAKMP:   attributes in transform:
ISAKMP:      encaps is 1
ISAKMP:      SA life type in seconds
ISAKMP:      SA life duration (VPI) of  0x0 0x20 0xc4 0x9b
ISAKMP:      SA life type in kilobytes
ISAKMP:      SA life duration (VPI) of  0x0
crypto_isakmp_process_block:src:10.66.79.126, dest:10.66.79.72 spt:500 dpt:500
OAK_QM exchange
ISADB: reaper checking SA 0x3c6420c, conn_id = 0
```

Cisco IOS Easy VPN Remote Hardware Client

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

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

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

Sample output is shown here:

```
831(config)#int eth 1
831(config-if)#crypto ipsec client ezvpn vpn-hw-client
*Mar  1 01:42:18.739: ISAKMP: callback: no SA found for 0.0.0.0/0.0.0.0 [vrf 0]
*Mar  1 01:42:18.739: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
*Mar  1 01:42:18.743: ISAKMP: Looking for a matching key for 10.66.79.72 in default
*Mar  1 01:42:18.743: ISAKMP: received ke message (1/1)
*Mar  1 01:42:18.743: ISAKMP:(0:0:N/A:0): SA request profile is (NULL)
*Mar  1 01:42:18.743: ISAKMP: Created a peer struct for 10.66.79.72, peer port 500
*Mar  1 01:42:18.743: ISAKMP: Locking peer struct 0x81F05E5C, IKE refcount
  1 for isakmp_initiator
*Mar  1 01:42:18.747: ISAKMP:(0:0:N/A:0):Setting client config settings 81C8F564
*Mar  1 01:42:18.747: ISAKMP: local port 500, remote port 500
*Mar  1 01:42:18.747: insert sa successfully sa = 81C8EEB8
*Mar  1 01:42:18.747: ISAKMP:(0:0:N/A:0): client mode configured.
*Mar  1 01:42:18.751: ISAKMP:(0:0:N/A:0): constructed NAT-T vendor-03 ID
*Mar  1 01:42:18.751: ISAKMP:(0:0:N/A:0): constructed NAT-T vendor-02 ID
*Mar  1 01:42:19.203: ISAKMP:(0:1:HW:2):SA is doing pre-shared key authentication
  plus XAUTH using id type ID_KEY_ID
*Mar  1 01:42:19.203: ISAKMP (0:268435457): ID payload
        next-payload : 13
        type         : 11
        group id     : vpn-hw-client-group
        protocol     : 17
        port         : 0
        length       : 27
*Mar  1 01:42:19.203: ISAKMP:(0:1:HW:2):Total payload length: 27
*Mar  1 01:42:19.207: ISAKMP:(0:1:HW:2):Input = IKE_MESG_FROM_IPSEC, IKE_SA_REQ_AM
*Mar  1 01:42:19.207: ISAKMP:(0:1:HW:2):Old State = IKE_READY  New State = IKE_I_AM1

*Mar  1 01:42:19.207: ISAKMP:(0:1:HW:2): beginning Aggressive Mode exchange
*Mar  1 01:42:19.207: ISAKMP:(0:1:HW:2): sending packet to 10.66.79.72
  my_port 500 peer_port 500 (I) AG_INIT_EXCH
*Mar  1 01:42:19.267: ISAKMP (0:268435457): received packet from 10.66.79.72
  dport 500 sport 500 Global (I) AG_INIT_EXCH
*Mar  1 01:42:19.271: ISAKMP:(0:1:HW:2): processing SA payload. message ID = 0
*Mar  1 01:42:19.271: ISAKMP:(0:1:HW:2): processing ID payload. message ID = 0
*Mar  1 01:42:19.271: ISAKMP (0:268435457): ID payload
        next-payload : 10
        type         : 1
        address      : 10.66.79.72
        protocol     : 17
```

```
        port         : 500
        length       : 12
*Mar  1 01:42:19.271: ISAKMP:(0:1:HW:2): processing vendor id payload
*Mar  1 01:42:19.271: ISAKMP:(0:1:HW:2): vendor ID seems Unity/DPD but major
  215 mismatch
*Mar  1 01:42:19.275: ISAKMP:(0:1:HW:2): vendor ID is XAUTH
*Mar  1 01:42:19.275: ISAKMP:(0:1:HW:2): processing vendor id payload
*Mar  1 01:42:19.275: ISAKMP:(0:1:HW:2): vendor ID is DPD
*Mar  1 01:42:19.275: ISAKMP:(0:1:HW:2): processing vendor id payload
*Mar  1 01:42:19.275: ISAKMP:(0:1:HW:2): vendor ID is Unity
*Mar  1 01:42:19.275: ISAKMP:(0:1:HW:2): local preshared key found
*Mar  1 01:42:19.275: ISAKMP : Scanning profiles for xauth ...
*Mar  1 01:42:19.279: ISAKMP:(0:1:HW:2): Authentication by xauth preshared
*Mar  1 01:42:19.279: ISAKMP:(0:1:HW:2):Checking ISAKMP transform 1 against
  priority 65527 policy
*Mar  1 01:42:19.279: ISAKMP:      encryption 3DES-CBC
*Mar  1 01:42:19.279: ISAKMP:      hash SHA
*Mar  1 01:42:19.279: ISAKMP:      default group 2
*Mar  1 01:42:19.279: ISAKMP:      auth pre-share
*Mar  1 01:42:19.279: ISAKMP:      life type in seconds
*Mar  1 01:42:19.279: ISAKMP:      life duration (VPI) of  0x0 0x20 0xC4 0x9B
*Mar  1 01:42:19.279: ISAKMP:(0:1:HW:2):Authentication method offered does
  not match policy!
*Mar  1 01:42:19.283: ISAKMP:(0:1:HW:2):atts are not acceptable.
  Next payload is 0
*Mar  1 01:42:19.283: ISAKMP:(0:1:HW:2):Checking ISAKMP transform 1
  against priority 65528 policy
*Mar  1 01:42:19.283: ISAKMP:      encryption 3DES-CBC
*Mar  1 01:42:19.283: ISAKMP:      hash SHA
*Mar  1 01:42:19.283: ISAKMP:      default group 2
*Mar  1 01:42:19.283: ISAKMP:      auth pre-share
*Mar  1 01:42:19.283: ISAKMP:      life type in seconds
*Mar  1 01:42:19.283: ISAKMP:      life duration (VPI) of  0x0 0x20 0xC4 0x9B
*Mar  1 01:42:19.283: ISAKMP:(0:1:HW:2):Hash algorithm offered does not
  match policy!
*Mar  1 01:42:19.283: ISAKMP:(0:1:HW:2):atts are not acceptable. Next
 payload is 0
*Mar  1 01:42:19.287: ISAKMP:(0:1:HW:2):Checking ISAKMP transform 1
  against priority 65529 policy
*Mar  1 01:42:19.287: ISAKMP:      encryption 3DES-CBC
*Mar  1 01:42:19.287: ISAKMP:      hash SHA
*Mar  1 01:42:19.287: ISAKMP:      default group 2
*Mar  1 01:42:19.287: ISAKMP:      auth pre-share
*Mar  1 01:42:19.287: ISAKMP:      life type in seconds
*Mar  1 01:42:19.287: ISAKMP:      life duration (VPI) of  0x0 0x20 0xC4 0x9B
*Mar  1 01:42:19.287: ISAKMP:(0:1:HW:2):Encryption algorithm offered does
  not match policy!
*Mar  1 01:42:19.287: ISAKMP:(0:1:HW:2):atts are not acceptable.
  Next payload is 0
*Mar  1 01:42:19.291: ISAKMP:(0:1:HW:2):Checking ISAKMP transform
  1 against priority 65530 policy
*Mar  1 01:42:19.291: ISAKMP:      encryption 3DES-CBC
*Mar  1 01:42:19.291: ISAKMP:      hash SHA
*Mar  1 01:42:19.291: ISAKMP:      default group 2
*Mar  1 01:42:19.291: ISAKMP:      auth pre-share
*Mar  1 01:42:19.291: ISAKMP:      life type in seconds
*Mar  1 01:42:19.291: ISAKMP:      life duration (VPI) of  0x0 0x20 0xC4 0x9B
*Mar  1 01:42:19.291: ISAKMP:(0:1:HW:2):Encryption algorithm offered
  does not match policy!
*Mar  1 01:42:19.291: ISAKMP:(0:1:HW:2):atts are not acceptable. Next
  payload is 0
*Mar  1 01:42:19.295: ISAKMP:(0:1:HW:2):Checking ISAKMP transform 1
  against priority 65531 policy
*Mar  1 01:42:19.295: ISAKMP:      encryption 3DES-CBC
*Mar  1 01:42:19.295: ISAKMP:      hash SHA
*Mar  1 01:42:19.295: ISAKMP:      default group 2
```

```
*Mar  1 01:42:19.295: ISAKMP:      auth pre-share
*Mar  1 01:42:19.295: ISAKMP:      life type in seconds
*Mar  1 01:42:19.295: ISAKMP:      life duration (VPI) of  0x0 0x20 0xC4 0x9B
*Mar  1 01:42:19.295: ISAKMP:(0:1:HW:2):atts are acceptable. Next payload is 0
*Mar  1 01:42:19.295: ISAKMP:(0:1:HW:2): processing KE payload. message ID = 0
*Mar  1 01:42:19.747: ISAKMP:(0:1:HW:2): processing NONCE payload. message ID = 0
*Mar  1 01:42:19.747: ISAKMP:(0:1:HW:2):SKEYID state generated
*Mar  1 01:42:19.747: ISAKMP:(0:1:HW:2): processing HASH payload. message ID = 0
*Mar  1 01:42:19.751: ISAKMP:(0:1:HW:2):SA authentication status:
       authenticated
*Mar  1 01:42:19.751: ISAKMP:(0:1:HW:2):SA has been authenticated with 10.66.79.72
*Mar  1 01:42:19.751: ISAKMP: Trying to insert a peer
  10.66.79.126/10.66.79.72/500/,  and inserted successfully.
*Mar  1 01:42:19.751: ISAKMP:(0:1:HW:2):Send initial contact
*Mar  1 01:42:19.759: ISAKMP:(0:1:HW:2): sending packet to 10.66.79.72
  my_port 500 peer_port 500 (I) AG_INIT_EXCH
*Mar  1 01:42:19.759: ISAKMP:(0:1:HW:2):Input = IKE_MESG_FROM_PEER, IKE_AM_EXCH
*Mar  1 01:42:19.759: ISAKMP:(0:1:HW:2):Old State = IKE_I_AM1
  New State = IKE_P1_COMPLETE

*Mar  1 01:42:19.763: ISAKMP:(0:1:HW:2):Need config/address
*Mar  1 01:42:19.763: ISAKMP:(0:1:HW:2):Need config/address
*Mar  1 01:42:19.763: ISAKMP: set new node -1731108340 to CONF_ADDR
*Mar  1 01:42:19.763: ISAKMP: Sending APPLICATION_VERSION string:
  Cisco IOS Software, C831 Software (C831-K9O3SY6-M), Version 12.3(8)T,
 RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2004 by Cisco Systems, Inc.
Compiled Fri 14-May-04 01:40 by eaarmas
*Mar  1 01:42:19.775: ISAKMP:(0:1:HW:2): initiating peer config to
  10.66.79.72. ID = -1731108340
*Mar  1 01:42:19.775: ISAKMP:(0:1:HW:2): sending packet to 10.66.79.72
  my_port 500 peer_port 500 (I) CONF_ADDR
*Mar  1 01:42:19.775: ISAKMP:(0:1:HW:2):Input = IKE_MESG_INTERNAL,
  IKE_PHASE1_COMPLETE
*Mar  1 01:42:19.775: ISAKMP:(0:1:HW:2):Old State = IKE_P1_COMPLETE
  New State = IKE_CONFIG_MODE_REQ_SENT

*Mar  1 01:42:19.775: ISAKMP (0:268435457): received packet from 10.66.79.72
  dport 500 sport 500 Global (I) CONF_ADDR
*Mar  1 01:42:19.779: ISAKMP: set new node -531260300 to CONF_ADDR
*Mar  1 01:42:19.783: ISAKMP:(0:1:HW:2): processing HASH payload.
  message ID = -531260300
*Mar  1 01:42:19.783: ISAKMP:(0:1:HW:2): processing NOTIFY
  RESPONDER_LIFETIME protocol 1
        spi 0, message ID = -531260300, sa = 81C8EEB8
*Mar  1 01:42:19.783: ISAKMP:(0:1:HW:2):SA authentication status:
       authenticated
*Mar  1 01:42:19.787: ISAKMP:(0:1:HW:2): processing responder lifetime
*Mar  1 01:42:19.787: ISAKMP:(0:1:HW:2): start processing isakmp
  responder lifetime
*Mar  1 01:42:19.787: ISAKMP:(0:1:HW:2): restart ike sa timer to 86400 secs
*Mar  1 01:42:19.787: ISAKMP:(0:1:HW:2):deleting node -531260300 error
  FALSE reason "Informational (in) state 1"
*Mar  1 01:42:19.787: ISAKMP:(0:1:HW:2):Input = IKE_MESG_FROM_PEER,
  IKE_INFO_NOTIFY
*Mar  1 01:42:19.787: ISAKMP:(0:1:HW:2):Old State = IKE_CONFIG_MODE_REQ_SENT
  New State = IKE_CONFIG_MODE_REQ_SENT

*Mar  1 01:42:19.791: ISAKMP (0:268435457): received packet from 10.66.79.72
  dport 500 sport 500 Global (I) CONF_ADDR
*Mar  1 01:42:19.795: ISAKMP:(0:1:HW:2):processing transaction payload from
  10.66.79.72. message ID = -1731108340
*Mar  1 01:42:19.795: ISAKMP: Config payload REPLY
*Mar  1 01:42:19.799: ISAKMP(0:268435457) process config reply
*Mar  1 01:42:19.799: ISAKMP:(0:1:HW:2):deleting node -1731108340 error
```

```
  FALSE reason "Transaction mode done"
*Mar  1 01:42:19.799: ISAKMP:(0:1:HW:2):Input = IKE_MESG_FROM_PEER,
  IKE_CFG_REPLY
*Mar  1 01:42:19.799: ISAKMP:(0:1:HW:2):Old State = IKE_CONFIG_MODE_REQ_SENT
  New State = IKE_P1_COMPLETE

*Mar  1 01:42:19.807: ISAKMP:(0:1:HW:2):Input = IKE_MESG_INTERNAL,
  IKE_PHASE1_COMPLETE
*Mar  1 01:42:19.807: ISAKMP:(0:1:HW:2):Old State = IKE_P1_COMPLETE
  New State = IKE_P1_COMPLETE

*Mar  1 01:42:19.815: IPSEC(sa_request): ,
  (key eng. msg.) OUTBOUND local= 10.66.79.126, remote= 10.66.79.72,
    local_proxy= 192.168.1.0/255.255.255.0/0/0 (type=4),
    remote_proxy= 172.16.1.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-3des esp-sha-hmac  (Tunnel),
    lifedur= 2147483s and 4608000kb,
    spi= 0x13F1AA83(334604931), conn_id= 0, keysize= 0, flags= 0x400A
*Mar  1 01:42:19.815: IPSEC(sa_request): ,
  (key eng. msg.) OUTBOUND local= 10.66.79.126, remote= 10.66.79.72,
    local_proxy= 192.168.1.0/255.255.255.0/0/0 (type=4),
    remote_proxy= 172.16.1.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-3des esp-md5-hmac  (Tunnel),
    lifedur= 2147483s and 4608000kb,
    spi= 0xAD8C95C7(2911671751), conn_id= 0, keysize= 0, flags= 0x400A
*Mar  1 01:42:19.819: IPSEC(sa_request): ,
  (key eng. msg.) OUTBOUND local= 10.66.79.126, remote= 10.66.79.72,
    local_proxy= 192.168.1.0/255.255.255.0/0/0 (type=4),
    remote_proxy= 172.16.1.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-des esp-sha-hmac  (Tunnel),
    lifedur= 2147483s and 4608000kb,
    spi= 0x7B5EBFA(129362938), conn_id= 0, keysize= 0, flags= 0x400A
*Mar  1 01:42:19.819: IPSEC(sa_request): ,
  (key eng. msg.) OUTBOUND local= 10.66.79.126, remote= 10.66.79.72,
    local_proxy= 192.168.1.0/255.255.255.0/0/0 (type=4),
    remote_proxy= 172.16.1.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-des esp-md5-hmac  (Tunnel),
    lifedur= 2147483s and 4608000kb,
    spi= 0x702568AE(1881499822), conn_id= 0, keysize= 0, flags= 0x400A
*Mar  1 01:42:19.823: ISAKMP: received ke message (1/4)
*Mar  1 01:42:19.823: ISAKMP: set new node 0 to QM_IDLE
*Mar  1 01:42:19.823: ISAKMP:(0:1:HW:2): sitting IDLE. Starting QM
  immediately (QM_IDLE      )
*Mar  1 01:42:19.823: ISAKMP:(0:1:HW:2):beginning Quick Mode exchange,
  M-ID of -1056878968
*Mar  1 01:42:19.835: ISAKMP:(0:1:HW:2): sending packet to 10.66.79.72
  my_port 500 peer_port 500 (I) QM_IDLE
*Mar  1 01:42:19.835: ISAKMP:(0:1:HW:2):Node -1056878968, Input =
  IKE_MESG_INTERNAL, IKE_INIT_QM
*Mar  1 01:42:19.843: ISAKMP:(0:1:HW:2):Old State = IKE_QM_READY
  New State = IKE_QM_I_QM1
*Mar  1 01:42:19.859: ISAKMP (0:268435457): received packet from
  10.66.79.72 dport 500 sport 500 Global (I) QM_IDLE
*Mar  1 01:42:19.863: ISAKMP:(0:1:HW:2): processing HASH payload.
  message ID = -1056878968
*Mar  1 01:42:19.863: ISAKMP:(0:1:HW:2): processing SA payload.
  message ID = -1056878968
*Mar  1 01:42:19.863: ISAKMP:(0:1:HW:2):Checking IPSec proposal 1
*Mar  1 01:42:19.863: ISAKMP: transform 1, ESP_3DES
*Mar  1 01:42:19.863: ISAKMP:   attributes in transform:
*Mar  1 01:42:19.863: ISAKMP:      encaps is 1 (Tunnel)
*Mar  1 01:42:19.867: ISAKMP:      SA life type in seconds
*Mar  1 01:42:19.867: ISAKMP:      SA life duration (VPI) of  0x0 0x20 0xC4 0x9B
*Mar  1 01:42:19.867: ISAKMP:      SA life type in kilobytes
*Mar  1 01:42:19.867: ISAKMP:      SA life duration (VPI) of  0x0 0x46 0x50 0x0
*Mar  1 01:42:19.867: ISAKMP:      authenticator is HMAC-SHA
```

```
*Mar  1 01:42:19.867: ISAKMP:(0:1:HW:2):atts are acceptable.
*Mar  1 01:42:19.871: IPSEC(validate_proposal_request): proposal part #1,
  (key eng. msg.) INBOUND local= 10.66.79.126, remote= 10.66.79.72,
    local_proxy= 192.168.1.0/255.255.255.0/0/0 (type=4),
    remote_proxy= 172.16.1.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-3des esp-sha-hmac  (Tunnel),
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2
*Mar  1 01:42:19.871: Crypto mapdb : proxy_match
        src addr     : 192.168.1.0
        dst addr     : 172.16.1.0
        protocol     : 0
        src port     : 0
        dst port     : 0
*Mar  1 01:42:19.871: ISAKMP:(0:1:HW:2): processing NONCE payload.
  message ID = -1056878968
*Mar  1 01:42:19.875: ISAKMP:(0:1:HW:2): processing ID payload.
  message ID = -1056878968
*Mar  1 01:42:19.875: ISAKMP:(0:1:HW:2): processing ID payload.
  message ID = -1056878968
*Mar  1 01:42:19.875: ISAKMP:(0:1:HW:2): processing NOTIFY
  RESPONDER_LIFETIME protocol 3
        spi 4108140920, message ID = -1056878968, sa = 81C8EEB8
*Mar  1 01:42:19.875: ISAKMP:(0:1:HW:2):SA authentication status:
        authenticated
*Mar  1 01:42:19.875: ISAKMP:(0:1:HW:2): processing responder lifetime
*Mar  1 01:42:19.875: ISAKMP (268435457): responder lifetime of 28800s
*Mar  1 01:42:19.879: IPSec: Flow_switching Allocated flow for flow_id 268435457
*Mar  1 01:42:19.879: IPSec: Flow_switching Allocated flow for flow_id 268435458
*Mar  1 01:42:19.887: %CRYPTO-5-SESSION_STATUS: Crypto tunnel is UP  .
  Peer 10.66.79.72:500       Id: 10.66.79.72
*Mar  1 01:42:19.887: ISAKMP: Locking peer struct 0x81F05E5C, IPSEC
  refcount 1 for for stuff_ke
*Mar  1 01:42:19.887: ISAKMP:(0:1:HW:2): Creating IPSec SAs
*Mar  1 01:42:19.895:         inbound SA from 10.66.79.72 to 10.66.79.126
  (f/i)  0/ 0
        (proxy 172.16.1.0 to 192.168.1.0)
*Mar  1 01:42:19.895:         has spi 0x13F1AA83 and conn_id 20 and flags 2
*Mar  1 01:42:19.895:         lifetime of 28790 seconds
*Mar  1 01:42:19.895:         lifetime of 4608000 kilobytes
*Mar  1 01:42:19.895:         has client flags 0x0
*Mar  1 01:42:19.895:         outbound SA from 10.66.79.126 to 10.66.79.72
 (f/i) 0/0
        (proxy 192.168.1.0 to 172.16.1.0)
*Mar  1 01:42:19.895:         has spi -186826376 and conn_id 21 and flags A
*Mar  1 01:42:19.895:         lifetime of 28790 seconds
*Mar  1 01:42:19.895:         lifetime of 4608000 kilobytes
*Mar  1 01:42:19.895:         has client flags 0x0
*Mar  1 01:42:19.899: IPSEC(key_engine): got a queue event with 2 kei messages
*Mar  1 01:42:19.899: IPSEC(initialize_sas): ,
  (key eng. msg.) INBOUND local= 10.66.79.126, remote= 10.66.79.72,
    local_proxy= 192.168.1.0/255.255.255.0/0/0 (type=4),
    remote_proxy= 172.16.1.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-3des esp-sha-hmac  (Tunnel),
    lifedur= 28790s and 4608000kb,
    spi= 0x13F1AA83(334604931), conn_id= 268435476, keysize= 0, flags= 0x2
*Mar  1 01:42:19.899: IPSEC(initialize_sas): ,
  (key eng. msg.) OUTBOUND local= 10.66.79.126, remote= 10.66.79.72,
    local_proxy= 192.168.1.0/255.255.255.0/0/0 (type=4),
    remote_proxy= 172.16.1.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-3des esp-sha-hmac  (Tunnel),
    lifedur= 28790s and 4608000kb,
    spi= 0xF4DD4178(4108140920), conn_id= 268435477, keysize= 0, flags= 0xA
*Mar  1 01:42:19.903: Crypto mapdb : proxy_match
        src addr     : 192.168.1.0
        dst addr     : 172.16.1.0
```

```
        protocol     : 0
        src port     : 0
        dst port     : 0
*Mar  1 01:42:19.903: IPSEC(crypto_ipsec_sa_find_ident_head):
 reconnecting with the same proxies and 10.66.79.72
*Mar  1 01:42:19.903: IPSEC(policy_db_add_ident): src 192.168.1.0,
 dest 172.16.1.0, dest_port 0

*Mar  1 01:42:19.907: IPSEC(create_sa): sa created,
  (sa) sa_dest= 10.66.79.126, sa_prot= 50,
    sa_spi= 0x13F1AA83(334604931),
    sa_trans= esp-3des esp-sha-hmac , sa_conn_id= 268435476
*Mar  1 01:42:19.907: IPSEC(create_sa): sa created,
  (sa) sa_dest= 10.66.79.72, sa_prot= 50,
    sa_spi= 0xF4DD4178(4108140920),
    sa_trans= esp-3des esp-sha-hmac , sa_conn_id= 268435477
*Mar  1 01:42:19.911: ISAKMP:(0:1:HW:2): sending packet to
 10.66.79.72 my_port 500 peer_port 500 (I) QM_IDLE
*Mar  1 01:42:19.911: ISAKMP:(0:1:HW:2):deleting node -1056878968
 error FALSE reason "No Error"
*Mar  1 01:42:19.911: ISAKMP:(0:1:HW:2):Node -1056878968, Input =
 IKE_MESG_FROM_PEER, IKE_QM_EXCH
*Mar  1 01:42:19.911: ISAKMP:(0:1:HW:2):Old State = IKE_QM_I_QM1
 New State = IKE_QM_PHASE2_COMPLETE
*Mar  1 01:43:09.787: ISAKMP:(0:1:HW:2):purging node -531260300
*Mar  1 01:43:09.799: ISAKMP:(0:1:HW:2):purging node -1731108340
*Mar  1 01:43:09.911: ISAKMP:(0:1:HW:2):purging node -1056878968
```

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

Sample output is shown here:

```
831(config)#int eth 1
831(config-if)#crypto ipsec client ezvpn vpn-hw-client
*Mar  1 01:49:26.543: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
*Mar  1 01:49:26.547: EZVPN(vpn-hw-client): Current State: IDLE
*Mar  1 01:49:26.547: EZVPN(vpn-hw-client): Event: VALID_CONFIG_ENTERED
*Mar  1 01:49:26.547: EZVPN(vpn-hw-client): ezvpn_check_tunnel_interface_state
*Mar  1 01:49:26.547: EZVPN(vpn-hw-client): New State: VALID_CFG
*Mar  1 01:49:26.547: EZVPN(vpn-hw-client): Current State: VALID_CFG
*Mar  1 01:49:26.547: EZVPN(vpn-hw-client): Event: VALID_CONFIG_ENTERED
*Mar  1 01:49:26.547: EZVPN(vpn-hw-client): No state change
*Mar  1 01:49:26.547: EZVPN(vpn-hw-client): Current State: VALID_CFG
*Mar  1 01:49:26.551: EZVPN(vpn-hw-client): Event: TUNNEL_INTERFACE_UP
*Mar  1 01:49:26.551: EZVPN(vpn-hw-client): ezvpn_check_tunnel_interface_address
*Mar  1 01:49:26.551: EZVPN(vpn-hw-client): New State: TUNNEL_INT_UP
*Mar  1 01:49:26.551: EZVPN(vpn-hw-client): Current State: TUNNEL_INT_UP
*Mar  1 01:49:26.551: EZVPN(vpn-hw-client): Event: TUNNEL_HAS_PUBLIC_IP_ADD
*Mar  1 01:49:26.551: EZVPN(vpn-hw-client): New State: CONNECT_REQUIRED
*Mar  1 01:49:26.551: EZVPN(vpn-hw-client): Current State: CONNECT_REQUIRED
*Mar  1 01:49:26.551: EZVPN(vpn-hw-client): Event: CONNECT
*Mar  1 01:49:26.555: EZVPN(vpn-hw-client): ezvpn_connect_request
*Mar  1 01:49:26.555: EZVPN(vpn-hw-client): New State: READY
*Mar  1 01:49:27.535: EZVPN(vpn-hw-client): Current State: READY
*Mar  1 01:49:27.535: EZVPN(vpn-hw-client): Event: CONN_UP
*Mar  1 01:49:27.535: EZVPN(vpn-hw-client): ezvpn_conn_up A12E6D0D D9C3B1AE
 41AB02FB 62DD1B01
*Mar  1 01:49:27.539: EZVPN(vpn-hw-client): No state change
*Mar  1 01:49:27.563: EZVPN(vpn-hw-client): Current State: READY
*Mar  1 01:49:27.563: EZVPN(vpn-hw-client): Event: MODE_CONFIG_REPLY
*Mar  1 01:49:27.563: EZVPN(vpn-hw-client): ezvpn_mode_config
*Mar  1 01:49:27.563: EZVPN(vpn-hw-client): ezvpn_parse_mode_config_msg
*Mar  1 01:49:27.563: EZVPN: Attributes sent in message:
*Mar  1 01:49:27.563:         DNS Primary: 172.16.1.1
*Mar  1 01:49:27.567:         DNS Secondary: 172.16.1.1
```

```
*Mar  1 01:49:27.567:         NBMS/WINS Primary: 172.16.1.1
*Mar  1 01:49:27.567:         NBMS/WINS Secondary: 172.16.1.1
*Mar  1 01:49:27.567:         Split Tunnel List: 1
*Mar  1 01:49:27.567:              Address    : 172.16.1.0
*Mar  1 01:49:27.567:              Mask       : 255.255.255.0
*Mar  1 01:49:27.567:              Protocol   : 0x0
*Mar  1 01:49:27.567:              Source Port: 0
*Mar  1 01:49:27.567:              Dest Port  : 0
*Mar  1 01:49:27.567:         Default Domain: cisco.com
*Mar  1 01:49:27.567: EZVPN: Unknown/Unsupported Attr: PFS (0x7007)
*Mar  1 01:49:27.571: EZVPN(vpn-hw-client): ezvpn_nat_config
*Mar  1 01:49:27.571: EZVPN: close old connection, len 0
*Mar  1 01:49:27.575: EZVPN(vpn-hw-client): New State: SS_OPEN
*Mar  1 01:49:27.587: EZVPN(vpn-hw-client): Current State: SS_OPEN
*Mar  1 01:49:27.587: EZVPN(vpn-hw-client): Event: SOCKET_READY
*Mar  1 01:49:27.587: EZVPN(vpn-hw-client): No state change
*Mar  1 01:49:27.619: %CRYPTO-5-SESSION_STATUS: Crypto tunnel is UP  .
 Peer 10.66.79.72:500       Id: 10.66.79.72
*Mar  1 01:49:27.623: EZVPN(vpn-hw-client): Current State: SS_OPEN
*Mar  1 01:49:27.623: EZVPN(vpn-hw-client): Event: MTU_CHANGED
*Mar  1 01:49:27.623: EZVPN(vpn-hw-client): No state change
*Mar  1 01:49:27.627: EZVPN(vpn-hw-client): Current State: SS_OPEN
*Mar  1 01:49:27.627: EZVPN(vpn-hw-client): Event: SOCKET_UP
*Mar  1 01:49:27.631: ezvpn_socket_up
*Mar  1 01:49:27.631: EZVPN(vpn-hw-client): New State: IPSEC_ACTIVE
```

Related Information

- **PIX 500 Series Support Page**
- **Documentation for PIX Firewall**
- **PIX Command References**
- **Request for Comments (RFCs)**
- **IPSec Negotiation/IKE Protocols Support Page**
- **Technical Support & Documentation − Cisco Systems**

Updated: Sep 26, 2008 Document ID: 27124