VPN 3002 Hardware Client to PIX 6.x Configuration Example

Document ID: 6421

Contents

Introduction

The Cisco VPN 3002 Hardware Client is used when you do not want to install the software−based client on your PCs or when the operating system on the desktop does not support the Cisco VPN Client. The VPN 3002 Hardware Client can connect only to a Unity Aware VPN device, such as the VPN 3000 Concentrator 3.x or the PIX 6.x.

Refer to the Cisco Hardware and VPN Clients Supporting IPSec/PPTP/L2TP matrix for more information on support for the VPN 3002 Hardware Client.

Note: Since the PIX does not allow VPN packets to come into an interface and go back out the same interface, Cisco recommends that you use the split−tunnel feature. This feature allows clients behind the VPN 3002 Hardware Client to access the Internet via the Port Address Translation (PAT) address of the VPN 3002 Hardware Client outside interface with an encrypted tunnel back to the main site.

Note: If you decide not to use the split−tunnel feature, devices behind the VPN 3002 Hardware Client can access the Internet only through a proxy server behind the PIX Firewall or through another route to the Internet.

Refer to Configuring a Connection Between the VPN 3002 Hardware Client and a VPN 3000 Concentrator in Network Extension Mode in order to learn more about the same scenario where the VPN server is the Cisco VPN 3000 series concentrator.

Refer to Configuring Cisco VPN 3002 Hardware Client to Cisco IOS Router with EzVPN in Network Extension Mode in order to learn more about the same scenario where the VPN server is Cisco IOS router.

Refer to PIX/ASA 7.x to Support IPsec over TCP on any Port Configuration Example in order to learn more about the same scenario where the PIX Security appliance runs software version 7.x.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

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

- PIX 6.x
- VPN 3002 Hardware Client version 3.x in Client Mode or Network Extension Mode
- Cisco Secure UNIX 2.3.6 (External RADIUS authentication is optional.)

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.

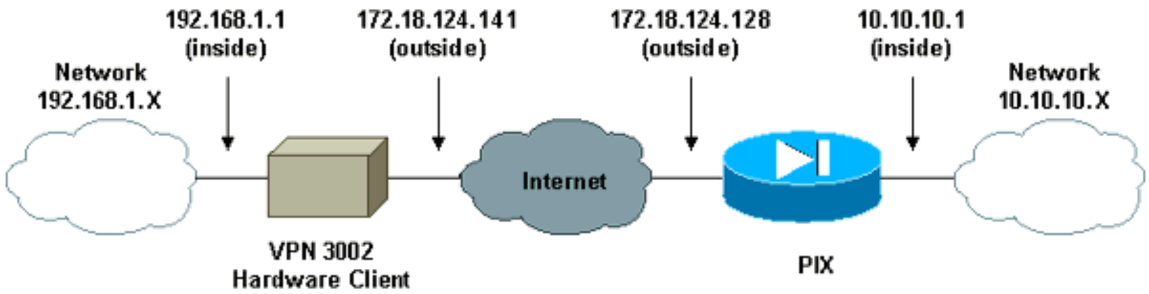
Configure

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) in order to obtain more information on the commands used in this section.

Network Diagram

This document uses this network setup:



Note: Since this setup was created in a lab, the 172.18.124.0 space refers to a private address. Use routable addresses when you set up an actual configuration.

Configurations

Cisco Secure UNIX Radius Profile

```
# ./ViewProfile -p 9900 -u 3002
User Profile Information
user = 3002{
profile_id = 77
set server current-failed-logins = 6
profile_cycle = 7
password = pap "********"
}
```

PIX Configuration

PIX

```
PIX Version 6.0(1)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password OnTrBUG1Tp0edmkr encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pix60
domain-name cisco.com
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
fixup protocol skinny 2000
names

!--- Bypass Network Address Translation (NAT) for VPN connections.

access-list nonat permit ip 10.10.10.0 255.255.255.0 10.10.11.0 255.255.255.0

!--- Split tunnel on the 3002.

access-list ipsectraffic permit ip 10.10.10.0 255.255.255.0
   10.10.11.0 255.255.255.0
no pager
interface ethernet0 auto
interface ethernet1 auto
mtu outside 1500
mtu inside 1500
ip address outside 172.18.124.128 255.255.255.0
ip address inside 10.10.10.1 255.255.255.0
ip audit info action alarm
ip audit attack action alarm

!--- IP addresses that will be assigned to the VPN users.

ip local pool swim 10.10.11.1-10.10.11.254
no failover
failover timeout 0:00:00
failover poll 15
failover ip address outside 0.0.0.0
failover ip address inside 0.0.0.0
pdm history enable
arp timeout 14400

!--- Bypass NAT for VPN connections.
```

```
nat (inside) 0 access-list nonat
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h323
   0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute

!--- Authenticate the VPN 3002 and other VPN Client connections.
!--- Note that the RADIUS server would not normally be on the outside;
!--- the example shown here was generated in a lab.

aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server authme protocol radius
aaa-server authme (outside) host 172.18.124.113 cisco123 timeout 10
http server enable
http 172.18.124.104 255.255.255.255 inside
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable

!--- To allow VPN traffic through the PIX when not using access lists.

sysopt connection permit-ipsec
no sysopt route dnat

!--- IPSec configuration.

crypto ipsec transform-set strong esp-des esp-md5-hmac
crypto dynamic-map dyna 1 set transform-set strong
crypto map vpn 1 ipsec-isakmp dynamic dyna

!--- Authentication is highly recommended for security reasons.

crypto map vpn client authentication authme
crypto map vpn interface outside

!--- IKE configuration.

isakmp enable outside
isakmp policy 1 authentication pre-share
isakmp policy 1 encryption des
isakmp policy 1 hash md5

!--- Group 2 must be used; the VPN 3002 Hardware Client
!--- does not support Diffie-Hellman (DH) group 1.

isakmp policy 1 group 2
isakmp policy 1 lifetime 86400

!--- 3002 group information; group can be used with software clients also.

vpngroup rtpvpn address-pool swim
vpngroup rtpvpn dns-server 10.10.10.10
vpngroup rtpvpn wins-server 10.10.10.20
vpngroup rtpvpn default-domain cisco.com
vpngroup rtpvpn split-tunnel ipsectraffic
vpngroup rtpvpn idle-time 1800
vpngroup rtpvpn password ******** (letmein)
telnet 172.18.124.104 255.255.255.255 inside
telnet timeout 5
ssh timeout 5
terminal width 80
Cryptochecksum:070be42d8f4aded1bb617048763495b9
```

```
: end
```

VPN 3002 Hardware Client Configuration

Note: This example assumes that no initial configuration exists on the client.

VPN 3002 Hardware Client

```
Login: admin
Password:
Welcome to
Cisco Systems
VPN 3002 Hardware Client
Command Line Interface
Copyright (C) 1998−2001 Cisco Systems, Inc.
1) Configuration
2) Administration
3) Monitoring
4) Save changes to Config file
5) Help Information
6) Exit

Main −> 1
1) Quick Configuration
2) Interface Configuration
3) System Management
4) Policy Management
5) Back

Config −> 1
−− : Set the time on your device. The correct time is very important,
−− : so that logging and accounting entries are accurate.
−− : Enter the system time in the following format:
−− : HH:MM:SS. Example 21:30:00 for 9:30 PM

> Time
Quick −> [ 13:54:34 ] 7:30:00
−− : Enter the date in the following format.
−− : MM/DD/YYYY Example 06/12/1999 for June 12th 1999.
> Date
Quick −> [ 05/23/2001 ]
−− : Set the time zone on your device. The correct time zone is very
−− : important so that logging and accounting entries are accurate.
−− : Enter the time zone using the hour offset from GMT:
−− : −12 : Kwajalein −11 : Samoa −10 : Hawaii −9 : Alaska
−− : −8 : PST −7 : MST −6 : CST −5 : EST
−− : −4 : Atlantic −3 : Brasilia −2 : Mid−Atlantic −1 : Azores
−− : 0 : GMT +1 : Paris +2 : Cairo +3 : Kuwait
−− : +4 : Abu Dhabi +5 : Karachi +6 : Almaty +7 : Bangkok
−− : +8 : Singapore +9 : Tokyo +10 : Sydney +11 : Solomon Is.
−− : +12 : Marshall Is.

> Time Zone
Quick −> [ −5 ]

1) Enable DST Support
2) Disable DST Support

Quick −> [ 1 ]

1) Upload Config File
2) Do Not Upload Config File
3) Back
```

```
Quick -> [ 2 ]
This table shows current IP addresses.
Interface IP Address/Subnet Mask MAC Address
-------------------------------------------------------------------------------
| Private Interface | 192.168.10.1/255.255.255.0 | 00.05.31.98.00.0E
| Public Interface | 0.0.0.0/0.0.0.0 | 00.05.31.98.00.0F
-------------------------------------------------------------------------------

1) Configure the Private Interface
2) Skip the Private Interface Configuration
3) Back

Quick -> [ 2 ] 1
This table shows current IP addresses.
Interface IP Address/Subnet Mask MAC Address

-------------------------------------------------------------------------------
| Private Interface | 192.168.10.1/255.255.255.0 | 00.05.31.98.00.0E
| Public Interface | 0.0.0.0/0.0.0.0 | 00.05.31.98.00.0F
-------------------------------------------------------------------------------

> Enter IP Address
Private Interface -> [ 192.168.10.1 ] 192.168.1.1
> Enter Subnet Mask
Private Interface -> [ 255.255.255.0 ]

DHCP Server: Enabled
Address Pool: 192.168.1.2 - 192.168.1.128

1) Disable DHCP Server
2) Enable and Configure DHCP Server
3) Enable DHCP Server with existing parameter values
4) Back

Quick -> [ 3 ] 2

1) Enable/Disable DHCP
2) Set DHCP Lease Timeout
3) Set DHCP Pool
4) Back
5) Continue

Quick -> 3

> DHCP Pool Start

Quick -> [ 192.168.1.2 ]

> DHCP Pool End

Quick -> [ 192.168.1.128 ]

1) Enable/Disable DHCP
2) Set DHCP Lease Timeout
3) Set DHCP Pool
4) Back
5) Continue

Quick -> 1
1) Enable DHCP
2) Disable DHCP

Quick -> [ 1 ]

1) Enable/Disable DHCP
2) Set DHCP Lease Timeout
```

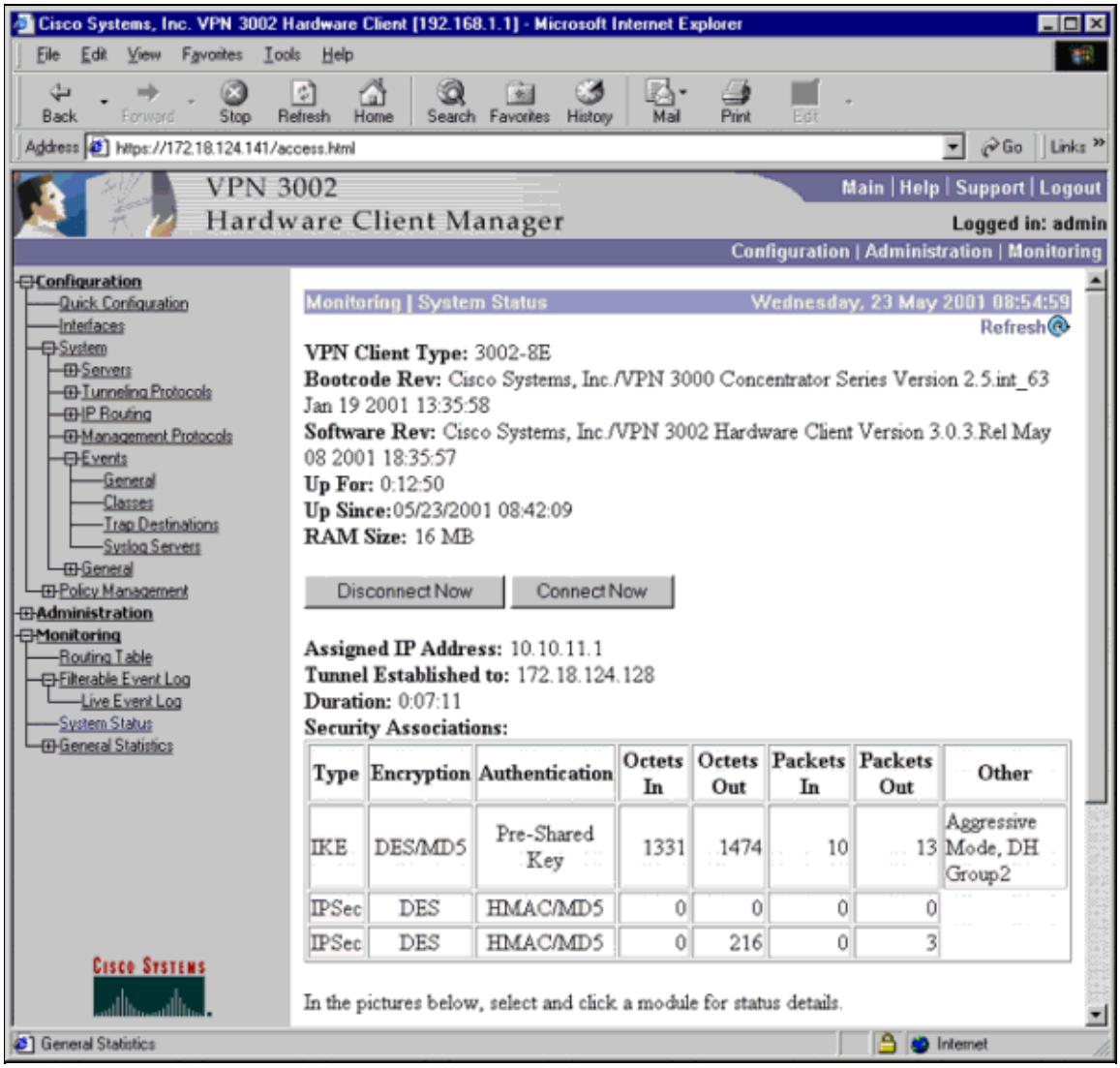
```
3) Set DHCP Pool
4) Back
5) Continue

Quick -> 5

This table shows current IP addresses.

Interface IP Address/Subnet Mask MAC Address

-------------------------------------------------------------------------------
| Private Interface | 192.168.1.1/255.255.255.0 | 00.05.31.98.00.0E
| Public Interface | 0.0.0.0/0.0.0.0 | 00.05.31.98.00.0F
-------------------------------------------------------------------------------

1) Configure System Name (hostname)
2) Obtain address via DHCP for the Public Interface
3) Configure the Public Interface
4) Back
Quick -> [ 2 ] 3

This table shows current IP addresses.
Interface IP Address/Subnet Mask MAC Address
-------------------------------------------------------------------------------
| Private Interface | 192.168.1.1/255.255.255.0 | 00.05.31.98.00.0E
| Public Interface | 0.0.0.0/0.0.0.0 | 00.05.31.98.00.0F
-------------------------------------------------------------------------------

> Enter IP Address
Quick Public Interface -> [ 0.0.0.0 ] 172.18.124.141
> Enter Subnet Mask
Quick Public Interface -> [ 255.255.0.0 ] 255.255.255.0
> Default Gateway
Quick -> 172.18.124.1
> IPSec Peer Address
Quick -> 172.18.124.128
> IPSec Group Name
Quick -> rtpvpn
> IPSec Group Password
Quick -> ******* (letmein : should match the vpngroup on the PIX)
Verify -> ******* (letmein)
> IPSec User Name
Quick -> 3002
> IPSec User Password
Quick -> *******
Verify -> *******

!--- Please choose 1 when you want to use Client mode.

1) Enable PAT over the IPSec Tunnel

!--- Please choose 2 when you want to use Network Extension Mode.

2) Disable PAT over the IPSec Tunnel (Network Extension)

Quick -> [ 1 ]
-- : Specify a local DNS server, which lets you enter hostnames
-- : rather than IP addresses while configuring.

> DNS Server
Quick -> [ 0.0.0.0 ] 10.10.10.10
-- : Enter your ISP's domain name; e.g., ispdomain.com
> Domain
Quick -> cisco.com

Static Routes
```

```
-------------
Destination Mask Metric Destination
------------------------------------------------------------
0.0.0.0 0.0.0.0 1 172.18.124.1

1) Add Static Route
2) Delete Static Route
3) Back
4) Continue

Quick -> [ 4 ]
-- : We strongly recommend that you change the password for user admin.
> Reset Admin Password
Quick -> [ ***** ] *****
Verify -> *****

1) Goto Main Configuration Menu
2) Exit

Quick -> 1
```

Verify

VPN 3002 Hardware Client Tunnel Monitoring

In order to see the tunnel on the VPN 3002 Hardware Client, go to **Monitoring** > **System Status**.



PIX show Command and Sample Output

```
pix60#show crypto ipsec sa
interface: outside
Crypto map tag: vpn, local addr. 172.18.124.128
local ident (addr/mask/prot/port): (172.18.124.128/255.255.255.255/0/0)
remote ident (addr/mask/prot/port): (172.18.124.141/255.255.255.255/0/0)
current_peer: 172.18.124.141
dynamic allocated peer ip: 10.10.11.1
PERMIT, flags={}
#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.: 172.18.124.128, remote crypto endpt.: 172.18.124.141
path mtu 1500, ipsec overhead 56, media mtu 1500
current outbound spi: feb3a67
inbound esp sas:
spi: 0x69ae1406(1773016070)
transform: esp-des esp-md5-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 3, crypto map: vpn
sa timing: remaining key lifetime (k/sec): (4608000/28772)
IV size: 8 bytes
replay detection support: Y
inbound ah sas:
```

```
inbound pcp sas:
outbound esp sas:
spi: 0xfeb3a67(267074151)
transform: esp-des esp-md5-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 4, crypto map: vpn
sa timing: remaining key lifetime (k/sec): (4608000/28772)
IV size: 8 bytes
replay detection support: Y
outbound ah sas:
outbound pcp sas:
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (10.10.11.1/255.255.255.255/0/0)
current_peer: 172.18.124.141
dynamic allocated peer ip: 10.10.11.1
PERMIT, flags={}
#pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0
#pkts decaps: 3, #pkts decrypt: 3, #pkts verify 3
#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.: 172.18.124.128, remote crypto endpt.: 172.18.124.141
path mtu 1500, ipsec overhead 56, media mtu 1500
current outbound spi: 34e1e58e
inbound esp sas:
spi: 0xf05a96f1(4032468721)
transform: esp-des esp-md5-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 1, crypto map: vpn
sa timing: remaining key lifetime (k/sec): (4607999/27340)
IV size: 8 bytes
replay detection support: Y
inbound ah sas:
inbound pcp sas:
outbound esp sas:
spi: 0x34e1e58e(887219598)
transform: esp-des esp-md5-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 2, crypto map: vpn
sa timing: remaining key lifetime (k/sec): (4608000/27340)
IV size: 8 bytes
replay detection support: Y
outbound ah sas:
outbound pcp sas:
```

Troubleshoot

PIX debug Commands

Before you use any **debug** commands, refer to Important Information on Debug Commands.

- **debug crypto ipsec 1** Use this command in order to see if a client negotiates the IPSec portion of the VPN connection.
- **debug crypto isakmp 1** Use this command in order to see if the peers negotiate the Internet Security Association and Key Management Protocol (ISAKMP) portion of the VPN connection.
- **debug crypto engine** Use this command in order to display debug messages about crypto engines, which perform encryption and decryption.

This output provides an example of good PIX debug output:

```
crypto_isakmp_process_block: src 172.18.124.141, dest 172.18.124.128
OAK_AG exchange
```

```
ISAKMP (0): processing SA payload. message ID = 0
ISAKMP (0): Checking ISAKMP transform 1 against priority 1 policy
ISAKMP: default group 2
ISAKMP: encryption 3DES-CBC
ISAKMP: hash SHA
ISAKMP: extended auth pre-share
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x7f 0xff 0xff 0xff
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 2 against priority 1 policy
ISAKMP: default group 2
ISAKMP: encryption 3DES-CBC
ISAKMP: hash MD5
ISAKMP: extended auth pre-share
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x7f 0xff 0xff 0xff
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 3 against priority 1 policy
ISAKMP: default group 2
ISAKMP: encryption DES-CBC
ISAKMP: hash SHA
ISAKMP: extended auth pre-share
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x7f 0xff 0xff 0xff
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 4 against priority 1 policy
ISAKMP: default group 2
ISAKMP: encryption DES-CBC
ISAKMP: hash MD5
ISAKMP: extended auth pre-share
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x7f 0xff 0xff 0xff
ISAKMP (0): atts are acceptable. Next payload is 3
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): processing vendor id payload
ISAKMP (0): speaking to a Unity client
ISAKMP (0): ID payload
next-payload : 10
type : 2
protocol : 17
port : 500
length : 19
ISAKMP (0): Total payload length: 23
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 172.18.124.141, dest 172.18.124.128
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 172.18.124.141
ISAKMP (0): processing vendor id payload
ISAKMP (0): remote peer supports dead peer detection
ISAKMP (0): SA has been authenticated
return status is IKMP_NO_ERROR
ISAKMP/xauth: request attribute XAUTH_TYPE
ISAKMP/xauth: request attribute XAUTH_USER_NAME
ISAKMP/xauth: request attribute XAUTH_USER_PASSWORD
ISAKMP (0:0): initiating peer config to 172.18.124.141.
   ID = 2475083578 (0x9386c73a)
crypto_isakmp_process_block: src 172.18.124.141, dest 172.18.124.128
```

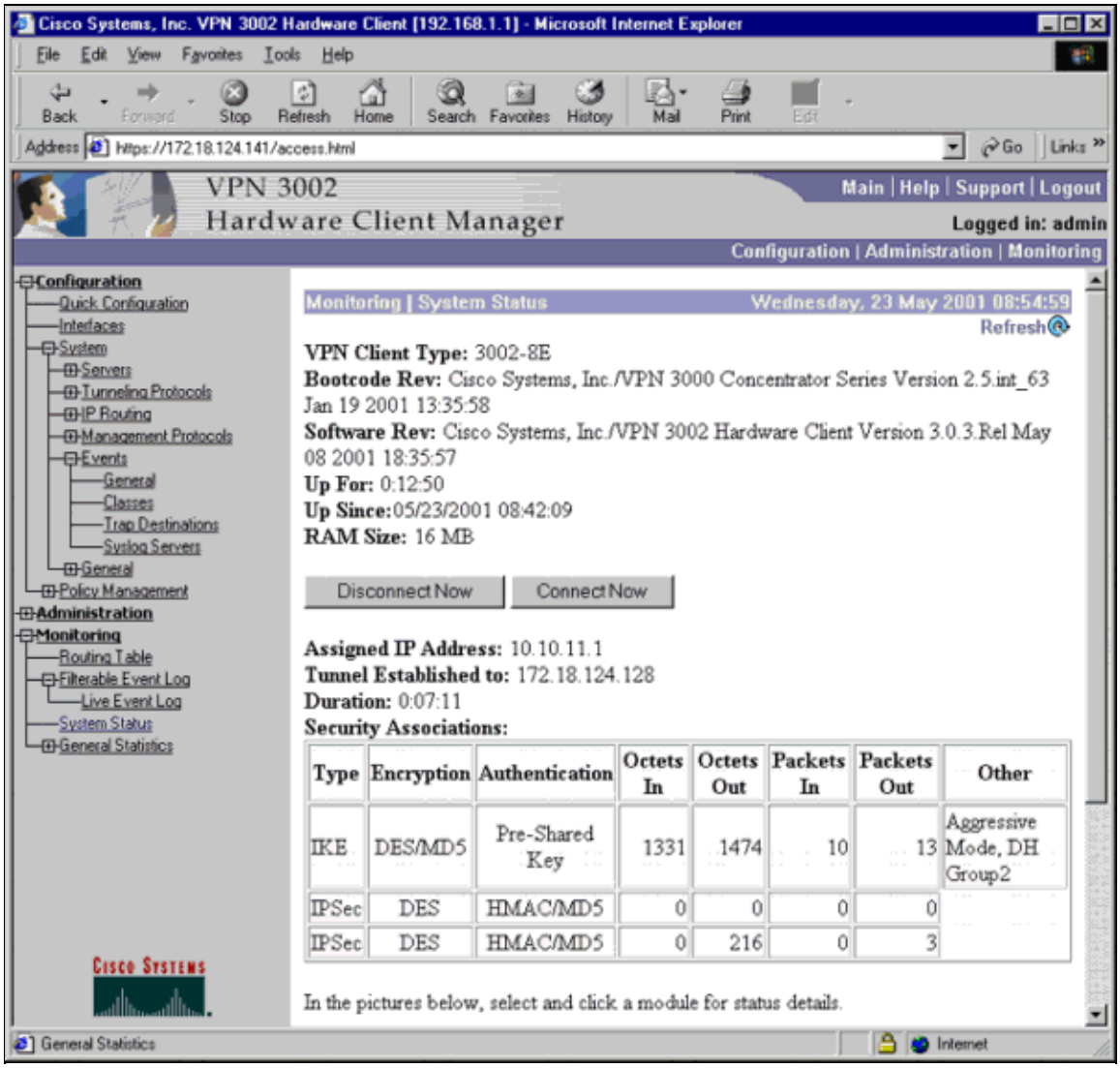
```
ISAKMP_TRANSACTION exchange
ISAKMP (0:0): processing transaction payload from 172.18.124.141.
   message ID = 76
ISAKMP: Config payload CFG_REPLY
return status is IKMP_ERR_NO_RETRANS
ISAKMP (0:0): initiating peer config to 172.18.124.141.
   ID = 1892625430 (0x70cf2c16)
crypto_isakmp_process_block: src 172.18.124.141, dest 172.18.124.128
ISAKMP_TRANSACTION exchange
ISAKMP (0:0): processing transaction payload from 172.18.124.141.
   message ID = 60
ISAKMP: Config payload CFG_ACK
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 172.18.124.141, dest 172.18.124.128
ISAKMP_TRANSACTION exchange
ISAKMP (0:0): processing transaction payload from 172.18.124.141.
   message ID = 0
ISAKMP: Config payload CFG_REQUEST
ISAKMP (0:0): checking request:
ISAKMP: attribute IP4_ADDRESS (1)
ISAKMP: attribute IP4_NETMASK (2)
ISAKMP: attribute IP4_DNS (3)
ISAKMP: attribute IP4_DNS (3)
ISAKMP: attribute IP4_NBNS (4)
ISAKMP: attribute IP4_NBNS (4)
ISAKMP: attribute UNKNOWN (28676)
ISAKMP: attribute UNKNOWN (28674)
ISAKMP: attribute UNKNOWN (28677)
Unsupported Attr: 28677
ISAKMP: attribute UNKNOWN (28679)
Unsupported Attr: 28679
ISAKMP (0:0): responding to peer config from 172.18.124.141. ID = 58811014
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 172.18.124.141, dest 172.18.124.128
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_IDLE
ISAKMP (0): processing SA payload. message ID = 1691366289
ISAKMP : Checking IPSec proposal 1
ISAKMP: transform 1, ESP_3DES
ISAKMP: attributes in transform:
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (VPI) of 0x7f 0xff 0xff 0xff
ISAKMP: encaps is 1
ISAKMP: authenticator is HMAC-SHAIPSEC(validate_proposal):
   transform proposal (prot 3, trans 3, hmac_alg 2) not supported
ISAKMP (0): atts not acceptable. Next payload is 3
ISAKMP: transform 2, ESP_3DES
ISAKMP: attributes in transform:
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (VPI) of 0x7f 0xff 0xff 0xff
ISAKMP: encaps is 1
ISAKMP: authenticator is HMAC-MD5IPSEC(validate_proposal):
   transform proposal (prot 3, trans 3, hmac_alg 1) not supported
ISAKMP (0): atts not acceptable. Next payload is 3
ISAKMP: transform 3, ESP_DES
ISAKMP: attributes in transform:
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (VPI) of 0x7f 0xff 0xff 0xff
ISAKMP: encaps is 1
ISAKMP: authenticator is HMAC-SHAIPSEC(validate_proposal):
   transform proposal (prot 3, trans 2, hmac_alg 2) not supported
ISAKMP (0): atts not acceptable. Next payload is 3
ISAKMP: transform 4, ESP_DES
ISAKMP: attributes in transform:
ISAKMP: SA life type in seconds
```

```
ISAKMP: SA life duration (VPI) of 0x7f 0xff 0xff 0xff
ISAKMP: encaps is 1
ISAKMP: authenticator is HMAC−MD5
ISAKMP (0): atts are acceptable.IPSEC(validate_proposal_request):
   proposal part #1,
(key eng. msg.) dest= 172.18.124.128, src= 172.18.124.141,
dest_proxy= 172.18.124.128/255.255.255.255/0/0 (type=1),
src_proxy= 172.18.124.141/255.255.255.255/0/0 (type=1),
protocol= ESP, transform= esp−des esp−md5−hmac ,
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
ISAKMP (0): processing NONCE payload. message ID = 1691366289
ISAKMP (0): processing ID payload. message ID = 1691366289
ISAKMP (0): ID_IPV4_ADDR src 172.18.124.141 prot 0 port 0
ISAKMP (0): processing ID payload. message ID = 1691366289
ISAKMP (0): ID_IPV4_ADDR dst 172.18.124.128 prot 0 port 0IPSEC(key_engine):
   got a queue event...
IPSEC(spi_response): getting spi 0x69ae1406(1773016070) for SA
from 172.18.124.141 to 172.18.124.128 for prot 3
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 172.18.124.141, dest 172.18.124.128
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_AUTH_AWAITmap_alloc_entry: allocating entry 3
map_alloc_entry: allocating entry 4
ISAKMP (0): Creating IPSec SAs
inbound SA from 172.18.124.141 to 172.18.124.128
   (proxy 172.18.124.141 to 172.18.124.128)
has spi 1773016070 and conn_id 3 and flags 4
lifetime of 2147483647 seconds
outbound SA from 172.18.124.128 to 172.18.124.141
   (proxy 172.18.124.128 to 172.18.124.141)
has spi 267074151 and conn_id 4 and flags 4
lifetime of 2147483647 secondsIPSEC(key_engine): got a queue event...
IPSEC(initialize_sas): ,
(key eng. msg.) dest= 172.18.124.128, src= 172.18.124.141,
dest_proxy= 172.18.124.128/0.0.0.0/0/0 (type=1),
src_proxy= 172.18.124.141/0.0.0.0/0/0 (type=1),
protocol= ESP, transform= esp−des esp−md5−hmac ,
lifedur= 2147483647s and 0kb,
spi= 0x69ae1406(1773016070), conn_id= 3, keysize= 0, flags= 0x4
IPSEC(initialize_sas): ,
(key eng. msg.) src= 172.18.124.128, dest= 172.18.124.141,
src_proxy= 172.18.124.128/0.0.0.0/0/0 (type=1),
dest_proxy= 172.18.124.141/0.0.0.0/0/0 (type=1),
protocol= ESP, transform= esp−des esp−md5−hmac ,
lifedur= 2147483647s and 0kb,
spi= 0xfeb3a67(267074151), conn_id= 4, keysize= 0, flags= 0x4
return status is IKMP_NO_ERROR
```

VPN 3002 Hardware Client Debug Control

In order to turn on debugging on the VPN 3002 Hardware Client, go to **Configuration > Systems > Events > Classes**.

This example shows classes IKE 1−13, IKEDBG 1−13, IPSEC 1−13, and IPSECDBG 1−13.



In order to see the debug output on the VPN 3002 Hardware Client, go to **Monitoring > Event Log**.

```
3 05/23/2001 08:47:47.800 SEV=4 IKE/41 RPT=1 172.18.124.128
IKE Initiator: New Phase 1, Intf 2, IKE Peer 172.18.124.128
local Proxy Address 172.18.124.141, remote Proxy Address 172.18.124.128,
SA (ESP-3DES-MD5)
6 05/23/2001 08:47:47.800 SEV=9 IKEDBG/0 RPT=2 172.18.124.128
constructing ISA_SA for isakmp
7 05/23/2001 08:47:47.930 SEV=9 IKEDBG/0 RPT=3 172.18.124.128
constructing ke payload
8 05/23/2001 08:47:47.930 SEV=9 IKEDBG/1 RPT=1 172.18.124.128
constructing nonce payload
9 05/23/2001 08:47:47.930 SEV=9 IKEDBG/1 RPT=2 172.18.124.128
constructing ID
10 05/23/2001 08:47:47.930 SEV=9 IKEDBG/46 RPT=1 172.18.124.128
constructing xauth V6 VID payload
11 05/23/2001 08:47:47.930 SEV=9 IKEDBG/46 RPT=2 172.18.124.128
constructing VID payload
12 05/23/2001 08:47:47.930 SEV=9 IKEDBG/48 RPT=1 172.18.124.128
Send Cisco Unity client VID
20 05/23/2001 08:47:47.990 SEV=9 IKEDBG/0 RPT=7 172.18.124.128
processing SA payload
21 05/23/2001 08:47:48.000 SEV=8 IKEDBG/0 RPT=8 172.18.124.128
Proposal # 1, Transform # 1, Type ISAKMP, Id IKE
Parsing received transform:
Phase 1 failure against global IKE proposal # 1:
Mismatched attr types for class Encryption Alg:
```

```
Rcv'd: DES-CBC
Cfg'd: Triple-DES
26 05/23/2001 08:47:48.000 SEV=8 IKEDBG/0 RPT=9 172.18.124.128
Phase 1 failure against global IKE proposal # 2:
Mismatched attr types for class Encryption Alg:
Rcv'd: DES-CBC
Cfg'd: Triple-DES
29 05/23/2001 08:47:48.000 SEV=8 IKEDBG/0 RPT=10 172.18.124.128
Phase 1 failure against global IKE proposal # 3:
Mismatched attr types for class Hash Alg:
Rcv'd: MD5
Cfg'd: SHA
31 05/23/2001 08:47:48.000 SEV=7 IKEDBG/0 RPT=11 172.18.124.128
Oakley proposal is acceptable
32 05/23/2001 08:47:48.000 SEV=9 IKEDBG/47 RPT=1 172.18.124.128
processing VID payload
33 05/23/2001 08:47:48.000 SEV=9 IKEDBG/49 RPT=1 172.18.124.128
Received Cisco Unity client VID
34 05/23/2001 08:47:48.000 SEV=9 IKEDBG/47 RPT=2 172.18.124.128
processing VID payload
35 05/23/2001 08:47:48.000 SEV=9 IKEDBG/49 RPT=2 172.18.124.128
Received DPD VID
36 05/23/2001 08:47:48.000 SEV=9 IKEDBG/47 RPT=3 172.18.124.128
processing VID payload
37 05/23/2001 08:47:48.000 SEV=9 IKEDBG/38 RPT=1 172.18.124.128
Processing IOS/PIX Vendor ID payload (version: 1.0.0, capabilities: 00000025)
38 05/23/2001 08:47:48.000 SEV=9 IKEDBG/0 RPT=12 172.18.124.128
processing ke payload
39 05/23/2001 08:47:48.000 SEV=9 IKEDBG/0 RPT=13 172.18.124.128
processing ISA_KE
40 05/23/2001 08:47:48.000 SEV=9 IKEDBG/1 RPT=3 172.18.124.128
Processing ID
41 05/23/2001 08:47:48.000 SEV=9 IKEDBG/1 RPT=4 172.18.124.128
processing nonce payload
42 05/23/2001 08:47:48.130 SEV=9 IKE/0 RPT=1 172.18.124.128
Generating keys for Initiator...
43 05/23/2001 08:47:48.140 SEV=9 IKEDBG/0 RPT=14 172.18.124.128
Group [pix60.cisco.com]
processing hash
44 05/23/2001 08:47:48.140 SEV=9 IKEDBG/0 RPT=15 172.18.124.128
Group [pix60.cisco.com]
computing hash
45 05/23/2001 08:47:48.140 SEV=9 IKEDBG/0 RPT=16
Group [112.105.120.54]
construct hash payload
46 05/23/2001 08:47:48.140 SEV=9 IKEDBG/0 RPT=17 172.18.124.128
Group [112.105.120.54]
computing hash
47 05/23/2001 08:47:48.140 SEV=9 IKEDBG/46 RPT=3 172.18.124.128
Group [ 112.105.120.54 ]
constructing dpd vid payload
56 05/23/2001 08:47:50.060 SEV=9 IKEDBG/0 RPT=20 172.18.124.128
Group [112.105.120.54]
constructing blank hash
57 05/23/2001 08:47:50.060 SEV=9 IKEDBG/0 RPT=21 172.18.124.128
Group [112.105.120.54]
constructing qm hash
65 05/23/2001 08:47:51.210 SEV=9 IKEDBG/0 RPT=24 172.18.124.128
Group [112.105.120.54]
constructing blank hash
66 05/23/2001 08:47:51.210 SEV=9 IKEDBG/0 RPT=25 172.18.124.128
Group [112.105.120.54]
constructing qm hash
69 05/23/2001 08:47:51.210 SEV=9 IKEDBG/0 RPT=27 172.18.124.128
Group [112.105.120.54]
constructing blank hash
```

```
70 05/23/2001 08:47:51.210 SEV=9 IKEDBG/0 RPT=28 172.18.124.128
Group [112.105.120.54]
constructing qm hash
83 05/23/2001 08:47:51.290 SEV=5 IKE/115 RPT=1 172.18.124.128
Group [112.105.120.54]
Client rejected NAT enabled IPSec request,
falling back to standard IPSec
86 05/23/2001 08:47:51.290 SEV=9 IKEDBG/0 RPT=31 172.18.124.128
Group [112.105.120.54]
Oakley begin quick mode
87 05/23/2001 08:47:51.300 SEV=4 IKE/119 RPT=1 172.18.124.128
Group [112.105.120.54]
PHASE 1 COMPLETED
89 05/23/2001 08:47:51.300 SEV=7 IKEDBG/0 RPT=32 172.18.124.128
Group [112.105.120.54]
Starting phase 1 rekey timer: 82080000 (ms)
97 05/23/2001 08:47:51.300 SEV=9 IKEDBG/0 RPT=33 172.18.124.128
Group [112.105.120.54]
oakley constructing quick mode
98 05/23/2001 08:47:51.300 SEV=9 IKEDBG/0 RPT=34 172.18.124.128
Group [112.105.120.54]
constructing blank hash
99 05/23/2001 08:47:51.300 SEV=9 IKEDBG/0 RPT=35 172.18.124.128
Group [112.105.120.54]
constructing ISA_SA for ipsec
100 05/23/2001 08:47:51.300 SEV=9 IKEDBG/1 RPT=21 172.18.124.128
Group [112.105.120.54]
constructing ipsec nonce payload
101 05/23/2001 08:47:51.300 SEV=9 IKEDBG/1 RPT=22 172.18.124.128
Group [112.105.120.54]
constructing proxy ID
102 05/23/2001 08:47:51.300 SEV=7 IKEDBG/0 RPT=36 172.18.124.128
Group [112.105.120.54]
Transmitting Proxy Id:
Local host: 172.18.124.141 Protocol 0 Port 0
Remote host: 172.18.124.128 Protocol 0 Port 0
106 05/23/2001 08:47:51.300 SEV=9 IKEDBG/0 RPT=37 172.18.124.128
Group [112.105.120.54]
constructing qm hash
112 05/23/2001 08:47:52.370 SEV=9 IKEDBG/0 RPT=40 172.18.124.128
Group [112.105.120.54]
processing hash
113 05/23/2001 08:47:52.370 SEV=9 IKEDBG/0 RPT=41 172.18.124.128
Group [112.105.120.54]
processing SA payload
124 05/23/2001 08:47:52.370 SEV=9 IKEDBG/1 RPT=23 172.18.124.128
Group [112.105.120.54]
processing nonce payload
125 05/23/2001 08:47:52.370 SEV=9 IKEDBG/1 RPT=24 172.18.124.128
Group [112.105.120.54]
Processing ID
126 05/23/2001 08:47:52.370 SEV=9 IKEDBG/1 RPT=25 172.18.124.128
Group [112.105.120.54]
Processing ID
127 05/23/2001 08:47:52.370 SEV=9 IKEDBG/0 RPT=45 172.18.124.128
Group [112.105.120.54]
Processing Notify payload
128 05/23/2001 08:47:52.370 SEV=5 IKE/73 RPT=1 172.18.124.128
Group [112.105.120.54]
Responder forcing change of IPSec rekeying duration
   from 2147483647 to 28800 seconds
131 05/23/2001 08:47:52.370 SEV=9 IKEDBG/0 RPT=46 172.18.124.128
Group [112.105.120.54]
loading all IPSEC SAs
132 05/23/2001 08:47:52.370 SEV=9 IKEDBG/1 RPT=26 172.18.124.128
Group [112.105.120.54]
```

```
Generating Quick Mode Key!
133 05/23/2001 08:47:52.380 SEV=9 IKEDBG/1 RPT=27 172.18.124.128
Group [112.105.120.54]
Generating Quick Mode Key!
134 05/23/2001 08:47:52.380 SEV=7 IKEDBG/0 RPT=47 172.18.124.128
Group [112.105.120.54]
Loading host:
Dst: 172.18.124.128
Src: 172.18.124.141
136 05/23/2001 08:47:52.380 SEV=4 IKE/49 RPT=1 172.18.124.128
Group [112.105.120.54]
Security negotiation complete for peer (112.105.120.54)
Initiator, Inbound SPI = 0x0feb3a67, Outbound SPI = 0x69ae1406
139 05/23/2001 08:47:52.380 SEV=9 IKEDBG/0 RPT=48 172.18.124.128
Group [112.105.120.54]
oakley constructing final quick mode
165 05/23/2001 08:47:52.390 SEV=4 IKE/120 RPT=1 172.18.124.128
Group [112.105.120.54]
PHASE 2 COMPLETED (msgid=64d03391)
```

What Can Go Wrong?

VPN 3002 Hardware Client is not in Client Mode but in Network Extension Mode

On the VPN 3002 Hardware Client, PAT is not turned on. The tunnel comes up with no errors, and the IPSec session is established. No errors are generated with the standard debugs.

When you run the **show crypto ipsec sa** command on the PIX, (**recv**) errors increase.

```
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (192.168.1.1/255.255.255.0/0/0)
current_peer: 172.18.124.141
dynamic allocated peer ip: 10.10.11.1
PERMIT, flags={}
#pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0
#pkts decaps: 16, #pkts decrypt: 16, #pkts verify 16
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 16
```

The PIX debug log shows:

```
pix60(config)# logging on
pix60(config)# logging buffer debug
pix60(config)# sh logg
Syslog logging: enabled
Timestamp logging: disabled
Standby logging: disabled
Console logging: disabled
Monitor logging: disabled
Buffer logging: level debugging, 4 messages logged
Trap logging: disabled
History logging: disabled
402103: identity doesn't match negotiated identity (ip) dest_addr= 10.10.10.10,
   src_addr= 192.168.1.2, prot= icmp, (ident) local=172.18.124.128,
   remote=172.18.124.141, local proxy=0.0.0.0/0.0.0.0/0/0,
   remote_proxy=192.168.1.1/255.255.255.0/0/0
```

Cisco Bug CSCdu31246 was filed on this issue.

ISAKMP Proposal on Head End Does Not Have a DH Group 2

If the PIX has only DH group 1, the configuration will not work:

```
isakmp policy 1 group 1
```

For the VPN 3002 Hardware Client, the PIX configuration should use DH **group 2**:

```
isakmp policy 1 group 2
```

The PIX debug log shows:

```
ISAKMP (0): processing SA payload. message ID = 0
ISAKMP (0): Checking ISAKMP transform 1 against priority 1 policy
ISAKMP: default group 2
ISAKMP: encryption 3DES-CBC
ISAKMP: hash SHA
ISAKMP: extended auth pre-share
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x7f 0xff 0xff 0xff
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 2 against priority 1 policy
ISAKMP: default group 2
ISAKMP: encryption 3DES-CBC
ISAKMP: hash MD5
ISAKMP: extended auth pre-share
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x7f 0xff 0xff 0xff
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 3 against priority 1 policy
ISAKMP: default group 2
ISAKMP: encryption DES-CBC
ISAKMP: hash SHA
ISAKMP: extended auth pre-share
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x7f 0xff 0xff 0xff
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 4 against priority 1 policy
ISAKMP: default group 2
ISAKMP: encryption DES-CBC
ISAKMP: hash MD5
ISAKMP: extended auth pre-share
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x7f 0xff 0xff 0xff
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 5 against priority 1 policy
ISAKMP: default group 2
ISAKMP: encryption 3DES-CBC
ISAKMP: hash SHA
ISAKMP: auth pre-share
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x7f 0xff 0xff 0xff
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 6 against priority 1 policy
ISAKMP: default group 2
ISAKMP: encryption 3DES-CBC
ISAKMP: hash MD5
ISAKMP: auth pre-share
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x7f 0xff 0xff 0xff
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 7 against priority 1 policy
ISAKMP: default group 2
ISAKMP: encryption DES-CBC
```

```
ISAKMP: hash SHA
ISAKMP: auth pre-share
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x7f 0xff 0xff 0xff
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 8 against priority 1 policy
ISAKMP: default group 2
ISAKMP: encryption DES-CBC
ISAKMP: hash MD5
ISAKMP: auth pre-share
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x7f 0xff 0xff 0xff
ISAKMP (0): atts are not acceptable. Next payload is 0
ISAKMP (0): Checking ISAKMP transform 1 against priority 65535 policy
ISAKMP: default group 2
ISAKMP: encryption 3DES-CBC
ISAKMP: hash SHA
ISAKMP: extended auth pre-share
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x7f 0xff 0xff 0xff
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 2 against priority 65535 policy
ISAKMP: default group 2
ISAKMP: encryption 3DES-CBC
ISAKMP: hash MD5
ISAKMP: extended auth pre-share
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of
crypto_isakmp_process_block: src 172.18.124.141, dest 172.18.124.128
crypto_isakmp_process_block: src 172.18.124.141, dest 172.18.124.128
ISAKMP (0): deleting SA: src 172.18.124.141, dst 172.18.124.128
ISADB: reaper checking SA 0x80dff0b0, conn_id = 0 DELETE IT!
```

The VPN 3002 Hardware Client debug log shows:

```
5 05/23/2001 09:43:23.850 SEV=4 IKE/41 RPT=6 172.18.124.128 IKE Initiator:
   New Phase 1, Intf 2, IKE Peer 172.18.124.128
   local Proxy Address 172.18.124.141,
   remote Proxy Address 172.18.124.128, SA (ESP-3DES-MD5)
8 05/23/2001 09:43:23.850 SEV=9 IKEDBG/0 RPT=409 172.18.124.128
   constructing ISA_SA for isakmp
9 05/23/2001 09:43:23.980 SEV=9 IKEDBG/0 RPT=410 172.18.124.128
   constructing ke payload
10 05/23/2001 09:43:23.980 SEV=9 IKEDBG/1 RPT=70 172.18.124.128
   constructing nonce payload
11 05/23/2001 09:43:23.980 SEV=9 IKEDBG/1 RPT=71 172.18.124.128
   constructing ID
12 05/23/2001 09:43:23.980 SEV=9 IKEDBG/46 RPT=9 172.18.124.128
   constructing xauth V6 VID payload
13 05/23/2001 09:43:23.980 SEV=9 IKEDBG/46 RPT=10 172.18.124.128
   constructing VID payload
14 05/23/2001 09:43:23.980 SEV=9 IKEDBG/48 RPT=4 172.18.124.128
   Send Cisco Unity client VID
18 05/23/2001 09:43:47.980 SEV=9 IKEDBG/0 RPT=413 172.18.124.128
   IKE SA AM:a4d3b5d1 terminating: flags 0x00000021, refcnt 0, tuncnt 0
```

PIX VPNgroup is Missing the IP Pool

The PIX debug log shows:

```
ISAKMP (0): processing SA payload. message ID = 0
ISAKMP (0): Checking ISAKMP transform 1 against priority 1 policy
ISAKMP: default group 2
ISAKMP: encryption 3DES-CBC
ISAKMP: hash SHA
```

```
ISAKMP: extended auth pre-share
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x7f 0xff 0xff 0xff
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 2 against priority 1 policy
ISAKMP: default group 2
ISAKMP: encryption 3DES-CBC
ISAKMP: hash MD5
ISAKMP: extended auth pre-share
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x7f 0xff 0xff 0xff
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 3 against priority 1 policy
ISAKMP: default group 2
ISAKMP: encryption DES-CBC
ISAKMP: hash SHA
ISAKMP: extended auth pre-share
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x7f 0xff 0xff 0xff
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 4 against priority 1 policy
ISAKMP: default group 2
ISAKMP: encryption DES-CBC
ISAKMP: hash MD5
ISAKMP: extended auth pre-share
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x7f 0xff 0xff 0xff
ISAKMP (0): atts are acceptable. Next payload is 3
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): processing vendor id payload
ISAKMP (0): speaking to a Unity client
ISAKMP (0): ID payload
next-payload : 10
type : 2
protocol : 17
port : 500
length : 19
ISAKMP (0): Total payload length: 23
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 172.18.124.141, dest 172.18.124.128
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 172.18.124.141
ISAKMP (0): processing vendor id payload
ISAKMP (0): remote peer supports dead peer detection
ISAKMP (0): SA has been authenticated
return status is IKMP_NO_ERROR
ISAKMP/xauth: request attribute XAUTH_TYPE
ISAKMP/xauth: request attribute XAUTH_USER_NAME
ISAKMP/xauth: request attribute XAUTH_USER_PASSWORD
ISAKMP (0:0): initiating peer config to 172.18.124.141.
   ID = 1314666854 (0x4e5c3966)
crypto_isakmp_process_block: src 172.18.124.141, dest 172.18.124.128
ISAKMP_TRANSACTION exchange
ISAKMP (0:0): processing transaction payload from 172.18.124.141.
   message ID = 76
ISAKMP: Config payload CFG_REPLY
return status is IKMP_ERR_NO_RETRANS
```

```
ISAKMP (0:0): initiating peer config to 172.18.124.141.
   ID = 1355789026 (0x50cfb2e2)
crypto_isakmp_process_block: src 172.18.124.141, dest 172.18.124.128
ISAKMP_TRANSACTION exchange
ISAKMP (0:0): processing transaction payload from 172.18.124.141.
   message ID = 60
ISAKMP: Config payload CFG_ACK
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 172.18.124.141, dest 172.18.124.128
ISAKMP_TRANSACTION exchange
ISAKMP (0:0): processing transaction payload from 172.18.124.141.
   message ID = 0
ISAKMP: Config payload CFG_REQUEST
ISAKMP (0:0): checking request:
ISAKMP: attribute IP4_ADDRESS (1)
ISAKMP: attribute IP4_NETMASK (2)
ISAKMP: attribute IP4_DNS (3)
ISAKMP: attribute IP4_DNS (3)
ISAKMP: attribute IP4_NBNS (4)
ISAKMP: attribute IP4_NBNS (4)
ISAKMP: attribute UNKNOWN (28676)
ISAKMP: attribute UNKNOWN (28674)
ISAKMP: attribute UNKNOWN (28677)
Unsupported Attr: 28677
ISAKMP: attribute UNKNOWN (28679)
Unsupported Attr: 28679
ISAKMP (0:0): responding to peer config from 172.18.124.141. ID = 1924722190
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 172.18.124.141, dest 172.18.124.128
ISAKMP (0): processing DELETE payload. message ID = 1075158752
ISAKMP (0): deleting SA: src 172.18.124.141, dst 172.18.124.128
ISAKMP (0): deleting IPSEC SAs with peer at 172.18.124.141IPSEC(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 172.18.124.141
return status is IKMP_NO_ERR_NO_TRANS
ISADB: reaper checking SA 0x80dff0b0, conn_id = 0 DELETE IT!
IPSEC(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 172.18.124.141
```

The VPN 3002 Hardware Client debug log shows:

```
115 05/23/2001 09:55:25.730 SEV=8 IKEDBG/0 RPT=465 172.18.124.128
   Proposal # 1, Transform # 1, Type ISAKMP, Id IKE Parsing received transform:
   Phase 1 failure against global IKE proposal # 1:
   Mismatched attr types for class
   Encryption Alg: Rcv'd: DES-CBC Cfg'd: Triple-DES
120 05/23/2001 09:55:25.730 SEV=8 IKEDBG/0 RPT=466 172.18.124.128
   Phase 1 failure against global IKE proposal # 2:
   Mismatched attr types for class
   Encryption Alg: Rcv'd: DES-CBC Cfg'd: Triple-DES
123 05/23/2001 09:55:25.730 SEV=8 IKEDBG/0 RPT=467 172.18.124.128
   Phase 1 failure against global IKE proposal # 3:
   Mismatched attr types for class
   Hash Alg: Rcv'd: MD5 Cfg'd: SHA
125 05/23/2001 09:55:25.730 SEV=7 IKEDBG/0 RPT=468 172.18.124.128
   Oakley proposal is acceptable
126 05/23/2001 09:55:25.730 SEV=9 IKEDBG/47 RPT=10 172.18.124.128
   processing VID payload
127 05/23/2001 09:55:25.730 SEV=9 IKEDBG/49 RPT=7 172.18.124.128
   Received Cisco Unity client VID
128 05/23/2001 09:55:25.730 SEV=9 IKEDBG/47 RPT=11 172.18.124.128
   processing VID payload
129 05/23/2001 09:55:25.730 SEV=9 IKEDBG/49 RPT=8 172.18.124.128
   Received DPD VID
```

```
130 05/23/2001 09:55:25.730 SEV=9 IKEDBG/47 RPT=12 172.18.124.128
   processing VID payload
131 05/23/2001 09:55:25.730 SEV=9 IKEDBG/38 RPT=4 172.18.124.128
   Processing IOS/PIX Vendor ID payload
   (version: 1.0.0, capabilities: 00000025)
132 05/23/2001 09:55:25.730 SEV=9 IKEDBG/0 RPT=469 172.18.124.128
   processing ke payload
133 05/23/2001 09:55:25.730 SEV=9 IKEDBG/0 RPT=470 172.18.124.128
   processing ISA_KE 134 05/23/2001 09:55:25.730
   SEV=9 IKEDBG/1 RPT=96 172.18.124.128 Processing ID
135 05/23/2001 09:55:25.730 SEV=9 IKEDBG/1 RPT=97 172.18.124.128
   processing nonce payload
136 05/23/2001 09:55:25.860 SEV=9 IKE/0 RPT=4 172.18.124.128
   Generating keys for Initiator...
137 05/23/2001 09:55:25.870 SEV=9 IKEDBG/0 RPT=471 172.18.124.128
   Group [pix60.cisco.com] processing hash
138 05/23/2001 09:55:25.870 SEV=9 IKEDBG/0 RPT=472 172.18.124.128
   Group [pix60.cisco.com] computing hash
139 05/23/2001 09:55:25.870 SEV=9 IKEDBG/0 RPT=473
   Group [112.105.120.54] construct hash payload
140 05/23/2001 09:55:25.870 SEV=9 IKEDBG/0 RPT=474 172.18.124.128
   Group [112.105.120.54] computing hash
141 05/23/2001 09:55:25.870 SEV=9 IKEDBG/46 RPT=18 172.18.124.128
   Group [ 112.105.120.54 ] constructing dpd vid payload
150 05/23/2001 09:55:27.790 SEV=9 IKEDBG/0 RPT=477 172.18.124.128
   Group [112.105.120.54] constructing blank hash
151 05/23/2001 09:55:27.790 SEV=9 IKEDBG/0 RPT=478 172.18.124.128
   Group [112.105.120.54] constructing qm hash
159 05/23/2001 09:55:28.940 SEV=9 IKEDBG/0 RPT=481 172.18.124.128
   Group [112.105.120.54] constructing blank hash
160 05/23/2001 09:55:28.940 SEV=9 IKEDBG/0 RPT=482 172.18.124.128
   Group [112.105.120.54] constructing qm hash
163 05/23/2001 09:55:28.940 SEV=9 IKEDBG/0 RPT=484 172.18.124.128
   Group [112.105.120.54] constructing blank hash
164 05/23/2001 09:55:28.940 SEV=9 IKEDBG/0 RPT=485 172.18.124.128
   Group [112.105.120.54] constructing qm hash
176 05/23/2001 09:55:29.030 SEV=7 IKEDBG/1 RPT=113 172.18.124.128
   Group [112.105.120.54] Client did not get necessary information!
177 05/23/2001 09:55:29.030 SEV=9 IKEDBG/0 RPT=488 172.18.124.128
   Group [112.105.120.54] IKE SA AM:ec0b67bf terminating:
   flags 0x00004021, refcnt 0, tuncnt 0
```

PIX and VPN 3002 Hardware Client Group Passwords Do Not Match

The PIX debug log shows:

```
ISAKMP (0): processing SA payload. message ID = 0
ISAKMP (0): Checking ISAKMP transform 1 against priority 1 policy
ISAKMP: default group 2
ISAKMP: encryption 3DES-CBC
ISAKMP: hash SHA
ISAKMP: extended auth pre-share
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x7f 0xff 0xff 0xff
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 2 against priority 1 policy
ISAKMP: default group 2
ISAKMP: encryption 3DES-CBC
ISAKMP: hash MD5
ISAKMP: extended auth pre-share
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x7f 0xff 0xff 0xff
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 3 against priority 1 policy
ISAKMP: default group 2
```

```
ISAKMP: encryption DES-CBC
ISAKMP: hash SHA
ISAKMP: extended auth pre-share
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x7f 0xff 0xff 0xff
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 4 against priority 1 policy
ISAKMP: default group 2
ISAKMP: encryption DES-CBC
ISAKMP: hash MD5
ISAKMP: extended auth pre-share
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x7f 0xff 0xff 0xff
ISAKMP (0): atts are acceptable. Next payload is 3
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): processing vendor id payload
ISAKMP (0): speaking to a Unity client
ISAKMP: Created a peer node for 172.18.124.141
ISAKMP (0): ID payload
next-payload : 10
type : 2
protocol : 17
port : 500
length : 19
ISAKMP (0): Total payload length: 23
return status is IKMP_NO_ERROR
ISAKMP (0): retransmitting phase 1...
ISAKMP (0): retransmitting phase 1...
ISAKMP (0): deleting SA: src 172.18.124.141, dst 172.18.124.128
ISAKMP (0): deleting IPSEC SAs with peer at 172.18.124.141IPSEC(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 172.18.124.141
ISADB: reaper checking SA 0x80dff0b0, conn_id = 0 DELETE IT!
ISAKMP: Deleting peer node for 172.18.124.141
```

The VPN 3002 Hardware Client debug log shows:

```
5 05/23/2001 10:01:04.480 SEV=4 IKE/41 RPT=12 172.18.124.128 IKE Initiator:
   New Phase 1, Intf 2, IKE Peer 172.18.124.128
   local Proxy Address 172.18.124.141,
   remote Proxy Address 172.18.124.128, SA (ESP-3DES-MD5)
8 05/23/2001 10:01:04.480 SEV=9 IKEDBG/0 RPT=567 172.18.124.128
   constructing ISA_SA for isakmp
9 05/23/2001 10:01:04.610 SEV=9 IKEDBG/0 RPT=568 172.18.124.128
   constructing ke payload
10 05/23/2001 10:01:04.610 SEV=9 IKEDBG/1 RPT=154 172.18.124.128
   constructing nonce payload
11 05/23/2001 10:01:04.620 SEV=9 IKEDBG/1 RPT=155 172.18.124.128
   constructing ID
12 05/23/2001 10:01:04.620 SEV=9 IKEDBG/46 RPT=25 172.18.124.128
   constructing xauth V6 VID payload
13 05/23/2001 10:01:04.620 SEV=9 IKEDBG/46 RPT=26 172.18.124.128
   constructing VID payload
14 05/23/2001 10:01:04.620 SEV=9 IKEDBG/48 RPT=10 172.18.124.128
   Send Cisco Unity client VID
22 05/23/2001 10:01:04.680 SEV=9 IKEDBG/0 RPT=572 172.18.124.128
   processing SA payload
23 05/23/2001 10:01:04.680 SEV=8 IKEDBG/0 RPT=573 172.18.124.128
   Proposal # 1, Transform # 1, Type ISAKMP, Id IKE Parsing received transform:
   Phase 1 failure against global IKE proposal # 1:
   Mismatched attr types for class
   Encryption Alg: Rcv'd: DES-CBC Cfg'd: Triple-DES
```

```
28 05/23/2001 10:01:04.680 SEV=8 IKEDBG/0 RPT=574 172.18.124.128
   Phase 1 failure against global IKE proposal # 2:
   Mismatched attr types for class
   Encryption Alg: Rcv'd: DES-CBC Cfg'd: Triple-DES
31 05/23/2001 10:01:04.680 SEV=8 IKEDBG/0 RPT=575 172.18.124.128
   Phase 1 failure against global IKE proposal # 3:
   Mismatched attr types for class
   Hash Alg: Rcv'd: MD5 Cfg'd: SHA
33 05/23/2001 10:01:04.680 SEV=7 IKEDBG/0 RPT=576 172.18.124.128
   Oakley proposal is acceptable
34 05/23/2001 10:01:04.680 SEV=9 IKEDBG/47 RPT=19 172.18.124.128
   processing VID payload
35 05/23/2001 10:01:04.680 SEV=9 IKEDBG/49 RPT=13 172.18.124.128
   Received Cisco Unity client VID
36 05/23/2001 10:01:04.680 SEV=9 IKEDBG/47 RPT=20 172.18.124.128
   processing VID payload
37 05/23/2001 10:01:04.680 SEV=9 IKEDBG/49 RPT=14 172.18.124.128
   Received DPD VID
38 05/23/2001 10:01:04.680 SEV=9 IKEDBG/47 RPT=21 172.18.124.128
   processing VID payload
39 05/23/2001 10:01:04.680 SEV=9 IKEDBG/38 RPT=7 172.18.124.128
   Processing IOS/PIX Vendor ID payload
   (version: 1.0.0, capabilities: 00000025)
40 05/23/2001 10:01:04.680 SEV=9 IKEDBG/0 RPT=577 172.18.124.128
   processing ke payload
41 05/23/2001 10:01:04.680 SEV=9 IKEDBG/0 RPT=578 172.18.124.128
   processing ISA_KE
42 05/23/2001 10:01:04.680 SEV=9 IKEDBG/1 RPT=156 172.18.124.128
   Processing ID
43 05/23/2001 10:01:04.680 SEV=9 IKEDBG/1 RPT=157 172.18.124.128
   processing nonce payload
44 05/23/2001 10:01:04.810 SEV=9 IKE/0 RPT=7 172.18.124.128
   Generating keys for Initiator...
45 05/23/2001 10:01:04.820 SEV=9 IKEDBG/0 RPT=579 172.18.124.128
   Group [pix60.cisco.com] processing hash
46 05/23/2001 10:01:04.820 SEV=9 IKEDBG/0 RPT=580 172.18.124.128
   Group [pix60.cisco.com] computing hash
47 05/23/2001 10:01:04.820 SEV=4 IKE/1 RPT=1 172.18.124.128
   Group [pix60.cisco.com] Rxed Hash is incorrect:
   Pre-shared key or Digital Signature mismatch
49 05/23/2001 10:01:04.820 SEV=9 IKEDBG/0 RPT=581 172.18.124.128
   Group [pix60.cisco.com] IKE SA AM:6917506b terminating:
   flags 0x00004021, refcnt 0, tuncnt 0
```

User Password is Incorrect with the Radius Server

The PIX debug log shows:

```
ISAKMP (0): processing SA payload. message ID = 0
ISAKMP (0): Checking ISAKMP transform 1 against priority 1 policy
ISAKMP: default group 2
ISAKMP: encryption 3DES-CBC
ISAKMP: hash SHA
ISAKMP: extended auth pre-share
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x7f 0xff 0xff 0xff
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 2 against priority 1 policy
ISAKMP: default group 2
ISAKMP: encryption 3DES-CBC
ISAKMP: hash MD5
ISAKMP: extended auth pre-share
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x7f 0xff 0xff 0xff
ISAKMP (0): atts are not acceptable. Next payload is 3
```

```
ISAKMP (0): Checking ISAKMP transform 3 against priority 1 policy
ISAKMP: default group 2
ISAKMP: encryption DES−CBC
ISAKMP: hash SHA
ISAKMP: extended auth pre−share
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x7f 0xff 0xff 0xff
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 4 against priority 1 policy
ISAKMP: default group 2
ISAKMP: encryption DES−CBC
ISAKMP: hash MD5
ISAKMP: extended auth pre−share
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x7f 0xff 0xff 0xff
ISAKMP (0): atts are acceptable. Next payload is 3
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): processing vendor id payload
ISAKMP (0): speaking to a Unity client
ISAKMP: Created a peer node for 172.18.124.141
ISAKMP (0): ID payload
next−payload : 10
type : 2
protocol : 17
port : 500
length : 19
ISAKMP (0): Total payload length: 23
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 172.18.124.141, dest 172.18.124.128
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 172.18.124.141
ISAKMP (0): processing vendor id payload
ISAKMP (0): remote peer supports dead peer detection
ISAKMP (0): SA has been authenticated
return status is IKMP_NO_ERROR
ISAKMP/xauth: request attribute XAUTH_TYPE
ISAKMP/xauth: request attribute XAUTH_USER_NAME
ISAKMP/xauth: request attribute XAUTH_USER_PASSWORD
ISAKMP (0:0): initiating peer config to 172.18.124.141.
   ID = 2022436548 (0x788beec4)
crypto_isakmp_process_block: src 172.18.124.141, dest 172.18.124.128
ISAKMP_TRANSACTION exchange
ISAKMP (0:0): processing transaction payload from 172.18.124.141.
   message ID = 76
ISAKMP: Config payload CFG_REPLY
return status is IKMP_ERR_NO_RETRANS
ISAKMP (0:0): initiating peer config to 172.18.124.141.
   ID = 3427988631 (0xcc52f497)
crypto_isakmp_process_block: src 172.18.124.141, dest 172.18.124.128
ISAKMP (0): processing DELETE payload. message ID = 2878747768
ISAKMP (0): deleting SA: src 172.18.124.141, dst 172.18.124.128
ISAKMP (0): deleting IPSEC SAs with peer at 172.18.124.141IPSEC(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 172.18.124.141
return status is IKMP_NO_ERR_NO_TRANS
ISADB: reaper checking SA 0x80dff0b0, conn_id = 0 DELETE IT!
```

```
IPSEC(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 172.18.124.141
```

The VPN 3002 Hardware Client debug log shows:

```
5 05/23/2001 10:10:02.370 SEV=4 IKE/41 RPT=16 172.18.124.128 IKE Initiator:
   New Phase 1, Intf 2, IKE Peer 172.18.124.128
   local Proxy Address 172.18.124.141,
   remote Proxy Address 172.18.124.128, SA (ESP-3DES-MD5)
8 05/23/2001 10:10:02.370 SEV=9 IKEDBG/0 RPT=859 172.18.124.128
   constructing ISA_SA for isakmp
9 05/23/2001 10:10:02.500 SEV=9 IKEDBG/0 RPT=860 172.18.124.128
   constructing ke payload
10 05/23/2001 10:10:02.500 SEV=9 IKEDBG/1 RPT=186 172.18.124.128
   constructing nonce payload
11 05/23/2001 10:10:02.500 SEV=9 IKEDBG/1 RPT=187 172.18.124.128
   constructing ID
12 05/23/2001 10:10:02.500 SEV=9 IKEDBG/46 RPT=33 172.18.124.128
   constructing xauth V6 VID payload
13 05/23/2001 10:10:02.500 SEV=9 IKEDBG/46 RPT=34 172.18.124.128
   constructing VID payload
14 05/23/2001 10:10:02.500 SEV=9 IKEDBG/48 RPT=14 172.18.124.128
   Send Cisco Unity client VID
22 05/23/2001 10:10:02.560 SEV=9 IKEDBG/0 RPT=864 172.18.124.128
   processing SA payload
23 05/23/2001 10:10:02.560 SEV=8 IKEDBG/0 RPT=865 172.18.124.128
   Proposal # 1, Transform # 1, Type ISAKMP, Id IKE Parsing received transform:
   Phase 1 failure against global IKE proposal # 1:
   Mismatched attr types for class
   Encryption Alg: Rcv'd: DES-CBC Cfg'd: Triple-DES
28 05/23/2001 10:10:02.560 SEV=8 IKEDBG/0 RPT=866 172.18.124.128
   Phase 1 failure against global IKE proposal # 2:
   Mismatched attr types for class
   Encryption Alg: Rcv'd: DES-CBC Cfg'd: Triple-DES
31 05/23/2001 10:10:02.560 SEV=8 IKEDBG/0 RPT=867 172.18.124.128
   Phase 1 failure against global IKE proposal # 3:
   Mismatched attr types for class
   Hash Alg: Rcv'd: MD5 Cfg'd: SHA
33 05/23/2001 10:10:02.560 SEV=7 IKEDBG/0 RPT=868 172.18.124.128
   Oakley proposal is acceptable
34 05/23/2001 10:10:02.560 SEV=9 IKEDBG/47 RPT=55 172.18.124.128
   processing VID payload
35 05/23/2001 10:10:02.560 SEV=9 IKEDBG/49 RPT=37 172.18.124.128
   Received Cisco Unity client VID
36 05/23/2001 10:10:02.560 SEV=9 IKEDBG/47 RPT=56 172.18.124.128
   processing VID payload 37 05/23/2001 10:10:02.560
   SEV=9 IKEDBG/49 RPT=38 172.18.124.128 Received DPD VID
38 05/23/2001 10:10:02.560 SEV=9 IKEDBG/47 RPT=57 172.18.124.128
   processing VID payload
39 05/23/2001 10:10:02.560 SEV=9 IKEDBG/38 RPT=11 172.18.124.128
   Processing IOS/PIX Vendor ID payload
   (version: 1.0.0, capabilities: 00000025)
   40 05/23/2001 10:10:02.560 SEV=9 IKEDBG/0 RPT=869
   172.18.124.128 processing ke payload
41 05/23/2001 10:10:02.560 SEV=9 IKEDBG/0 RPT=870
   172.18.124.128 processing ISA_KE
42 05/23/2001 10:10:02.560 SEV=9 IKEDBG/1 RPT=188
   172.18.124.128 Processing ID
43 05/23/2001 10:10:02.560 SEV=9 IKEDBG/1 RPT=189
   172.18.124.128 processing nonce payload
44 05/23/2001 10:10:02.690 SEV=9 IKE/0 RPT=11
   172.18.124.128 Generating keys for Initiator...
45 05/23/2001 10:10:02.700 SEV=9 IKEDBG/0 RPT=871 172.18.124.128
   Group [pix60.cisco.com] processing hash
46 05/23/2001 10:10:02.700 SEV=9 IKEDBG/0 RPT=872 172.18.124.128
```

```
   Group [pix60.cisco.com] computing hash
47 05/23/2001 10:10:02.700 SEV=9 IKEDBG/0 RPT=873
   Group [112.105.120.54] construct hash payload
48 05/23/2001 10:10:02.700 SEV=9 IKEDBG/0 RPT=874 172.18.124.128
   Group [112.105.120.54] computing hash
49 05/23/2001 10:10:02.700 SEV=9 IKEDBG/46 RPT=35 172.18.124.128
   Group [ 112.105.120.54 ] constructing dpd vid payload
58 05/23/2001 10:10:04.670 SEV=9 IKEDBG/0 RPT=877 172.18.124.128
   Group [112.105.120.54] constructing blank hash
59 05/23/2001 10:10:04.670 SEV=9 IKEDBG/0 RPT=878 172.18.124.128
   Group [112.105.120.54] constructing qm hash
67 05/23/2001 10:10:05.820 SEV=4 IKE/48 RPT=9 172.18.124.128
   Group [112.105.120.54] Error processing payload: Payload ID: 14
68 05/23/2001 10:10:05.820 SEV=9 IKEDBG/0 RPT=881 172.18.124.128
   Group [112.105.120.54] IKE SA AM:fd9d0953 terminating: flags 0x00004021,
   refcnt 0, tuncnt 0
```

The Cisco Secure RADIUS debug shows:

```
May 29 13:06:52 rtp−cherry CiscoSecure: DEBUG − RADIUS ;
   Incoming Packet id=1 (172.18.124.128)
May 29 13:06:52 rtp−cherry     NAS−IP−Address = 172.18.124.128
May 29 13:06:52 rtp−cherry     NAS−Port = 2
May 29 13:06:52 rtp−cherry     NAS−Port−Type = Virtual
May 29 13:06:52 rtp−cherry     User−Name = "3002"
May 29 13:06:52 rtp−cherry     Calling−Station−Id = "172.18.124.128"
May 29 13:06:52 rtp−cherry     User−Password = "\220\257t"
May 29 13:06:52 rtp−cherry CiscoSecure: DEBUG − RADIUS ;
   Authenticate (172.18.124.128)
May 29 13:06:52 rtp−cherry CiscoSecure: DEBUG − RADIUS ;
   User PASSWORD type is Normal
May 29 13:06:52 rtp−cherry CiscoSecure: DEBUG − RADIUS ;
   authPapPwd (172.18.124.128)
May 29 13:06:52 rtp−cherry CiscoSecure: INFO − Profile: user = 3002 {
May 29 13:06:52 rtp−cherry      set server current−failed−logins = 1
May 29 13:06:52 rtp−cherry profile_cycle = 8
May 29 13:06:52 rtp−cherry }
May 29 13:06:52 rtp−cherry CiscoSecure: DEBUG − RADIUS ;
   Sending Reject of id 1 to a150131 (172.18.124.128)
```

Related Information

- **Cisco PIX 500 Series Security Appliances Product Support**
- **Cisco PIX Firewall Documentation**
- **Cisco Secure PIX Firewall Command References**
- **Cisco Secure ACS for UNIX Documentation**
- **Cisco VPN Client Product Support**
- **IPSec Negotiation/IKE Protocols Technology Support**
- **IETF Requests for Comments (RFCs)**
- **Technical Support & Documentation − Cisco Systems**

Updated: Sep 26, 2008 Document ID: 6421