PIX/ASA 7.x PIX-to-PIX Dynamic-to-Static IPsec with NAT and VPN Client Configuration Example

Contents

Introduction

In most cases, a remote PIX that connects to a central PIX does not use network address translation (NAT). Instead, the remote PIX uses a static outside IP address. In an instance when a central PIX that runs 7.x and later connects to a remote PIX using NAT, it is the same as a small home office such as a PIX 501 or 506 connected to a cable or DSL modem using Dynamic Host Control Protocol (DHCP). PIX 7.x and later and Cisco Adaptive Security Device Manager (ASDM) do not run on a PIX 501 or 506. Therefore, for this example the remote PIX with DHCP and NAT is presumed to be a PIX 501 or 506 that runs 6.x code. This configuration enables the central PIX to accept dynamic IPsec connections. The remote PIX uses NAT to join the privately addressed devices behind it to the privately addressed network behind the central PIX. The remote PIX can initiate connections to the central PIX (it knows the end-point), but the central PIX cannot initiate connections to the remote PIX (it does not know the endpoint).

In this sample configuration, Tiger is the remote PIX and Lion is the central PIX. Since the IP address of Tiger is unknown, you must configure Lion to dynamically accept connections from anywhere knowing the wild-card, pre-shared key. Tiger knows what traffic is to be encrypted (because it is specified by the access-list) and where the Lion endpoint is located. Tiger must initiate the connection. Both sides perform NAT and nat 0 in order to bypass NAT for IPsec traffic.

In addition, the remote user in this configuration connects to the central PIX (Lion) using the Cisco VPN Client 4.x. The remote user cannot connect to the remote PIX (Tiger) since both sides have dynamically assigned IP addresses and do not know where to send the request.

Refer to Configuring PIX to PIX Dynamic-to-Static IPsec with NAT and Cisco VPN Client in order to learn more about the same scenario in PIX 6.x with Cisco VPN Client 3.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:

- Cisco PIX Firewall Software Release 7.x and later (central PIX)
- Cisco PIX Firewall Software Release 6.3.4 (remote PIX)
- Cisco VPN Client Version 4.x

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

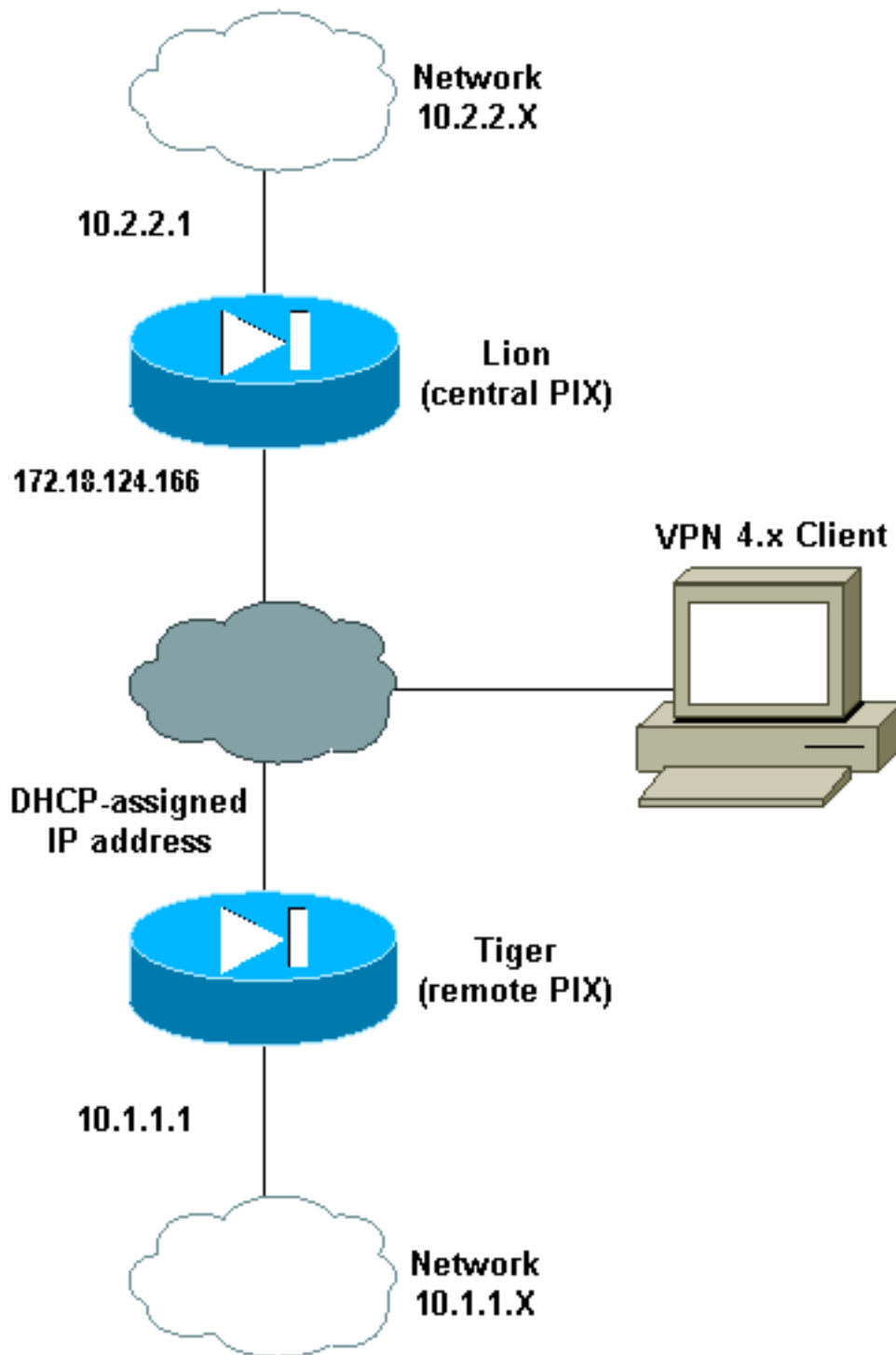Refer to Cisco Technical Tips Conventions for more information on document conventions.

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:

Network
10.2.2.X

10.2.2.1

Lion
(central PIX)

172.18.124.166

VPN 4.x Client

DHCP-assigned
IP address

Tiger
(remote PIX)

10.1.1.1

Network
10.1.1.X

Configurations

This document uses these configurations:

- Lion
- Tiger

Lion
| ```
PIX Version 7.0(0)
names
!
interface Ethernet0
 nameif outside
 security-level 0
``` |

```
 ip address 172.18.124.166 255.255.255.0
!
interface Ethernet1
 nameif inside
 security-level 100
 ip address 10.2.2.1 255.255.255.0
!
interface Ethernet2
 shutdown
 nameif intf2
 security-level 4
 no ip address
!
interface Ethernet3
 shutdown
 nameif intf3
 security-level 6
 no ip address
!
interface Ethernet4
 shutdown
 nameif intf4
 security-level 8
 no ip address
!
interface Ethernet5
 shutdown
 nameif intf5
 security-level 10
 no ip address
!
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname lion
domain-name cisco.com
boot system flash:/image.bin
ftp mode passive
access-list 100 extended permit ip 10.2.2.0 255.255.255.0
10.1.1.0 255.255.255.0
access-list 100 extended permit ip 10.2.2.0 255.255.255.0
10.3.3.0 255.255.255.0
pager lines 24
mtu outside 1500
mtu inside 1500
mtu intf2 1500
mtu intf3 1500
mtu intf4 1500
mtu intf5 1500
ip local pool clientpool 10.3.3.1-10.3.3.10
no failover
monitor-interface outside
monitor-interface inside
monitor-interface intf2
monitor-interface intf3
monitor-interface intf4
monitor-interface intf5
asdm image flash:/asdm-501.bin
asdm history enable
arp timeout 14400
nat-control
global (outside) 1 interface
nat (inside) 0 access-list 100
nat (inside) 1 0.0.0.0 0.0.0.0
route outside 0.0.0.0 0.0.0.0 172.18.124.1 1
```

```
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp
0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00
timeout mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
group-policy unityclient internal
group-policy unityclient attributes
 wins-server value 10.1.1.3
 dns-server value 10.1.1.3
 vpn-idle-timeout 30
 default-domain value cisco.com
 user-authentication disable
username cisco password 3USUcOPFUiMCO4Jk encrypted
http server enable
http 0.0.0.0 0.0.0.0 outside
http 0.0.0.0 0.0.0.0 inside
no snmp-server location
no snmp-server contact
snmp-server community public
snmp-server enable traps snmp
crypto ipsec transform-set myset esp-des esp-md5-hmac
crypto dynamic-map cisco 1 set transform-set myset
crypto map dyn-map 20 ipsec-isakmp dynamic cisco
crypto map dyn-map interface outside
isakmp enable outside
isakmp policy 20 authentication pre-share
isakmp policy 20 encryption des
isakmp policy 20 hash md5
isakmp policy 20 group 2
isakmp policy 20 lifetime 3600
isakmp policy 65535 authentication pre-share
isakmp policy 65535 encryption 3des
isakmp policy 65535 hash sha
isakmp policy 65535 group 2
isakmp policy 65535 lifetime 86400
telnet timeout 5
ssh timeout 5
ssh version 1
console timeout 0
tunnel-group DefaultL2LGroup type ipsec-l2l
tunnel-group DefaultL2LGroup general-attributes
   authentication-server-group none
tunnel-group DefaultL2LGroup ipsec-attributes
   pre-shared-key *
tunnel-group unityclient type ipsec-ra
tunnel-group unityclient general-attributes
 address-pool clientpool
 authentication-server-group none
 default-group-policy unityclient
tunnel-group unityclient ipsec-attributes
 pre-shared-key *
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map global_policy
 class inspection_default
  inspect dns maximum-length 512
  inspect ftp
  inspect h323 h225
```

```
  inspect h323 ras
  inspect http
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
!
service-policy global_policy global
Cryptochecksum:4e20a2153437d60c7f01054808d41b42
: end
```

Tiger

```
PIX Version 6.3(4)
interface ethernet0 auto
interface ethernet1 auto
interface ethernet2 auto shutdown
interface ethernet3 auto shutdown
interface ethernet4 auto shutdown
interface ethernet5 auto shutdown
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 intf2 security4
nameif ethernet3 intf3 security6
nameif ethernet4 intf4 security8
nameif ethernet5 intf5 security10
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname tiger
domain-name cisco.com
fixup protocol dns maximum-length 512
fixup protocol ftp 21
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol http 80
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol sip 5060
fixup protocol sip udp 5060
fixup protocol skinny 2000
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol tftp 69
names
access-list 101 permit ip 10.1.1.0 255.255.255.0 10.2.2.0
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
```
!--- This command configures the outside interface !--- as a
DHCP client and it is assumed that the IP address !---
172.18.124.167 is assigned by the DHCP server. `ip address`
```
outside dhcp ip address inside 10.1.1.1 255.255.255.0 no ip
address intf2 no ip address intf3 no ip address intf4 no ip
address intf5 ip audit info action alarm ip audit attack
```

```
action alarm no failover failover timeout 0:00:00 failover
poll 15 no failover ip address outside no failover ip address
inside no failover ip address intf2 no failover ip address
intf3 no failover ip address intf4 no failover ip address
intf5 pdm history enable arp timeout 14400 nat (inside) 0
access-list 101 route outside 0.0.0.0 0.0.0.0 172.18.124.1 1
timeout xlate 3:00:00 timeout conn 1:00:00 half-closed
0:10:00 udp 0:02:00 rpc 0:10:00 h225 1:00:00 timeout h323
0:05:00 mgcp 0:05:00 sip 0:30:00 sip_media 0:02:00 timeout
uauth 0:05:00 absolute aaa-server TACACS+ protocol tacacs+
aaa-server TACACS+ max-failed-attempts 3 aaa-server TACACS+
deadtime 10 aaa-server RADIUS protocol radius aaa-server
RADIUS max-failed-attempts 3 aaa-server RADIUS deadtime 10
aaa-server LOCAL protocol local no snmp-server location no
snmp-server contact snmp-server community public no snmp-
server enable traps floodguard enable sysopt connection
permit-ipsec crypto ipsec transform-set myset esp-des esp-
md5-hmac crypto map newmap 10 ipsec-isakmp crypto map newmap
10 match address 101 crypto map newmap 10 set peer
172.18.124.166 crypto map newmap 10 set transform-set myset
crypto map newmap interface outside isakmp enable outside
isakmp key ******** address 172.18.124.166 netmask
255.255.255.255 isakmp policy 10 authentication pre-share
isakmp policy 10 encryption des isakmp policy 10 hash md5
isakmp policy 10 group 2 isakmp policy 10 lifetime 3600
telnet timeout 5 ssh timeout 5 console timeout 0 terminal
width 80 Cryptochecksum:906331b1b1ca162ea53e951588efb070 :
end
```

Verify

Use this section to confirm that your configuration works properly.

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

Note: You must perform the **clear** commands in config mode.

- **clear crypto ipsec sa**—Resets the IPsec associations after failed attempts to negotiate a VPN tunnel.
- **clear crypto isakmp sa**—Resets the Internet Security Association and Key Management Protocol (ISAKMP) security associations after failed attempts to negotiate a VPN tunnel.
- **show crypto engine ipsec**—Displays the encrypted sessions.

Troubleshoot

Identical Pre-Shared Keys

If the LAN-to-LAN (L2L) IPsec tunnel is not established, check whether the pre-shared key for the DefaultRAGroup and the pre-shared key for the DefaultL2LGroup are the same. If this is the case, then the PIX/ASA terminates the tunnel on the DefaultRAGroup first and the L2L tunnel is then likely to fail. Be certain that the pre-shared keys for the two default tunnel groups are different.

Troubleshooting Commands

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**—Used to see if a client negotiates the IPsec portion of the VPN connection.
- **debug crypto isakmp** *[level]* —Used to see if the peers negotiate the ISAKMP portion of the VPN.

Good Debug Output Examples

These are examples of some good **debug** command output:

- [Central PIX (7.0.0)](#)
- [Remote PIX Dynamic NAT (6.3.4)](#)
- [VPN Client 4.0.5 on Central PIX 7.0](#)

Central PIX (7.0.0)

```
lion(config)# 2nd try, on central PIX from remote PIXApr 05 16:48:31 [IKEv1 DEBUG]:
 IP = 172.18.124.167, processing SA payload
Apr 05 16:48:31 [IKEv1 DEBUG]: IP = 172.18.124.167, Oakley proposal is acceptable
Apr 05 16:48:31 [IKEv1 DEBUG]: IP = 172.18.124.167, processing IKE SA
Apr 05 16:48:31 [IKEv1 DEBUG]: IP = 172.18.124.167, IKE SA Proposal # 1, Transform
 # 1 acceptable  Matches global IKE entry # 3
Apr 05 16:48:31 [IKEv1 DEBUG]: IP = 172.18.124.167, constructing ISA_SA for isakmp
Apr 05 16:48:31 [IKEv1 DEBUG]: IP = 172.18.124.167, constructing Fragmentation VID
 + extended capabilities payload
Apr 05 16:48:31 [IKEv1]: IP = 172.18.124.167, IKE DECODE SENDING Message (msgid=0)
 with payloads : HDR + SA (1) + VENDOR (13) + NONE (0) total length : 104
Apr 05 16:48:32 [IKEv1]: IP = 172.18.124.167, IKE DECODE RECEIVED Message (msgid=0)
 with payloads : HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) +VENDOR (13)
 + VENDOR (13) + NONE (0) total length : 256
Apr 05 16:48:32 [IKEv1 DEBUG]: IP = 172.18.124.167, processing ke payload
Apr 05 16:48:32 [IKEv1 DEBUG]: IP = 172.18.124.167, processing ISA_KE
Apr 05 16:48:32 [IKEv1 DEBUG]: IP = 172.18.124.167, processing nonce payload
Apr 05 16:48:32 [IKEv1 DEBUG]: IP = 172.18.124.167, processing VID payload
Apr 05 16:48:32 [IKEv1 DEBUG]: IP = 172.18.124.167, Received xauth V6 VID
Apr 05 16:48:32 [IKEv1 DEBUG]: IP = 172.18.124.167, processing VID payload
Apr 05 16:48:32 [IKEv1 DEBUG]: IP = 172.18.124.167, Received DPD VID
Apr 05 16:48:32 [IKEv1 DEBUG]: IP = 172.18.124.167, processing VID payload
Apr 05 16:48:32 [IKEv1 DEBUG]: IP = 172.18.124.167, Received Cisco Unity client VID
Apr 05 16:48:32 [IKEv1 DEBUG]: IP = 172.18.124.167, processing VID payload
Apr 05 16:48:32 [IKEv1 DEBUG]: IP = 172.18.124.167, Processing IOS/PIX Vendor ID
payload (version: 1.0.0, capabilities: 00000025)
Apr 05 16:48:32 [IKEv1 DEBUG]: IP = 172.18.124.167, constructing ke payload
Apr 05 16:48:32 [IKEv1 DEBUG]: IP = 172.18.124.167, constructing nonce payload
Apr 05 16:48:32 [IKEv1 DEBUG]: IP = 172.18.124.167, constructing Cisco Unity VID payload
Apr 05 16:48:32 [IKEv1 DEBUG]: IP = 172.18.124.167, constructing xauth V6 VID payload
Apr 05 16:48:32 [IKEv1 DEBUG]: IP = 172.18.124.167, Send IOS VID
Apr 05 16:48:32 [IKEv1 DEBUG]: IP = 172.18.124.167, Constructing ASA spoofing IOS
 Vendor ID payload (version: 1.0.0, capabilities: 20000001)
Apr 05 16:48:32 [IKEv1 DEBUG]: IP = 172.18.124.167, constructing VID payload
Apr 05 16:48:32 [IKEv1 DEBUG]: IP = 172.18.124.167, Send Altiga/Cisco VPN3000/Cisco
 ASA GW VID
Apr 05 16:48:32 [IKEv1]: IP = 172.18.124.167, Connection landed on tunnel_group
```

```
DefaultL2LGroup
Apr 05 16:48:32 [IKEv1 DEBUG]: Group = DefaultL2LGroup, IP = 172.18.124.167,
 Generating keys for Responder...
Apr 05 16:48:32 [IKEv1]: IP = 172.18.124.167, IKE DECODE SENDING Message
 (msgid=0) with payloads : HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13)
 + VENDOR (13) + VENDOR (13) + NONE (0) total length : 256
Apr 05 16:48:32 [IKEv1]: IP = 172.18.124.167, IKE DECODE RECEIVED Message (msg
id=0) with payloads : HDR + ID (5) + HASH (8) + NONE (0) total length : 71
Apr 05 16:48:32 [IKEv1 DEBUG]: Group = DefaultL2LGroup, IP = 172.18.124.167,
 Processing ID
Apr 05 16:48:32 [IKEv1 DEBUG]: Group = DefaultL2LGroup, IP = 172.18.124.167,
 processing hash
Apr 05 16:48:32 [IKEv1 DEBUG]: Group = DefaultL2LGroup, IP = 172.18.124.167,
 computing hash
Apr 05 16:48:32 [IKEv1]: IP = 172.18.124.167, Connection landed on tunnel_group
 DefaultL2LGroup
Apr 05 16:48:32 [IKEv1 DEBUG]: Group = DefaultL2LGroup, IP = 172.18.124.167,
 constructing ID
Apr 05 16:48:32 [IKEv1 DEBUG]: Group = DefaultL2LGroup, IP = 172.18.124.167,
 construct hash payload
Apr 05 16:48:32 [IKEv1 DEBUG]: Group = DefaultL2LGroup, IP = 172.18.124.167,
 computing hash
Apr 05 16:48:32 [IKEv1 DEBUG]: IP = 172.18.124.167, Constructing IOS keep
 alive payload: proposal=32767/32767 sec.
Apr 05 16:48:32 [IKEv1 DEBUG]: Group = DefaultL2LGroup, IP = 172.18.124.167,
 constructing dpd vid payload
Apr 05 16:48:32 [IKEv1]: IP = 172.18.124.167, IKE DECODE SENDING Message
 (msgid=0) with payloads : HDR + ID (5) + HASH (8) + IOS KEEPALIVE (14)
+ VENDOR (13) + NONE (0) total length : 102
Apr 05 16:48:33 [IKEv1]: IP = 172.18.124.167, IKE DECODE RECEIVED Message
 (msgid=ba80c56e) with payloads : HDR + HASH (8) + NOTIFY (11) + NONE (0)
 total length : 76
Apr 05 16:48:33 [IKEv1 DEBUG]: Group = DefaultL2LGroup, IP = 172.18.124.167,
 processing hash
Apr 05 16:48:33 [IKEv1 DEBUG]: Group = DefaultL2LGroup, IP = 172.18.124.167,
 Processing Notify payload
Apr 05 16:48:33 [IKEv1]: Received unexpected event EV_ACTIVATE_NEW_SA in
 state MM_TM_INIT_MODECFG_H
Apr 05 16:48:33 [IKEv1 DEBUG]: Group = DefaultL2LGroup, IP = 172.18.124.167,
 Delay Quick Mode processing, Cert/Trans Exch/RM DSID in progress
Apr 05 16:48:33 [IKEv1 DEBUG]: Group = DefaultL2LGroup, IP = 172.18.124.167,
 Resume Quick Mode processing, Cert/Trans Exch/RM DSID completed
Apr 05 16:48:33 [IKEv1]: Group = DefaultL2LGroup, IP = 172.18.124.167, PHASE 1COMPLETED
Apr 05 16:48:33 [IKEv1]: IP = 172.18.124.167, Keep-alive type for this connection: DPD
Apr 05 16:48:33 [IKEv1 DEBUG]: Group = DefaultL2LGroup, IP = 172.18.124.167,
 Starting phase 1 rekey timer: 3420000 (ms)
Apr 05 16:48:33 [IKEv1]: IP = 172.18.124.167, IKE DECODE RECEIVED Message
 (msgid=20c2120e) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID
 (5) + ID (5) + NONE (0) total length : 164
Apr 05 16:48:33 [IKEv1 DEBUG]: Group = DefaultL2LGroup, IP = 172.18.124.167,
 processing hash
Apr 05 16:48:33 [IKEv1 DEBUG]: Group = DefaultL2LGroup, IP = 172.18.124.167,
 processing SA payload
Apr 05 16:48:33 [IKEv1 DEBUG]: Group = DefaultL2LGroup, IP = 172.18.124.167,
 processing nonce payload
Apr 05 16:48:33 [IKEv1 DEBUG]: Group = DefaultL2LGroup, IP = 172.18.124.167,
 Processing ID
Apr 05 16:48:33 [IKEv1]: Group = DefaultL2LGroup, IP = 172.18.124.167,
 Received remote IP Proxy Subnet data in ID Payload:   Address 10.1.1.0,
 Mask 255.255.255.0, Protocol 0, Port 0
Apr 05 16:48:33 [IKEv1 DEBUG]: Group = DefaultL2LGroup, IP = 172.18.124.167,
 Processing ID
Apr 05 16:48:33 [IKEv1]: Group = DefaultL2LGroup, IP = 172.18.124.167,
 Received local IP Proxy Subnet data in ID Payload:   Address 10.2.2.0,
```

```
     Mask 255.255.255.0, Protocol 0, Port 0
Apr 05 16:48:33 [IKEv1]: QM IsRekeyed old sa not found by addr
Apr 05 16:48:33 [IKEv1]: Group = DefaultL2LGroup, IP = 172.18.124.167,
 IKE Remote Peer configured for SA: cisco
Apr 05 16:48:33 [IKEv1]: Group = DefaultL2LGroup, IP = 172.18.124.167,
 processing IPSEC SA
Apr 05 16:48:33 [IKEv1 DEBUG]: Group = DefaultL2LGroup, IP = 172.18.124.167,
 IPSec SA Proposal # 1, Transform # 1 acceptable  Matches global IPSec SA entry # 1
Apr 05 16:48:33 [IKEv1]: Group = DefaultL2LGroup, IP = 172.18.124.167,
 IKE: requesting SPI!
Apr 05 16:48:33 [IKEv1 DEBUG]: IKE got SPI from key engine: SPI = 0xd5243861
Apr 05 16:48:33 [IKEv1 DEBUG]: Group = DefaultL2LGroup, IP = 172.18.124.167,
 oakley constucting quick mode
Apr 05 16:48:33 [IKEv1 DEBUG]: Group = DefaultL2LGroup, IP = 172.18.124.167,
 constructing blank hash
Apr 05 16:48:33 [IKEv1 DEBUG]: Group = DefaultL2LGroup, IP = 172.18.124.167,
 constructing ISA_SA for ipsec
Apr 05 16:48:33 [IKEv1 DEBUG]: Group = DefaultL2LGroup, IP = 172.18.124.167,
 constructing ipsec nonce payload
Apr 05 16:48:33 [IKEv1 DEBUG]: Group = DefaultL2LGroup, IP = 172.18.124.167,
 constructing proxy ID
Apr 05 16:48:33 [IKEv1 DEBUG]: Group = DefaultL2LGroup, IP = 172.18.124.167,
 Transmitting Proxy Id:
  Remote subnet: 10.1.1.0  Mask 255.255.255.0 Protocol 0  Port 0
  Local subnet:  10.2.2.0  mask 255.255.255.0 Protocol 0  Port 0
Apr 05 16:48:33 [IKEv1 DEBUG]: Group = DefaultL2LGroup, IP = 172.18.124.167,
 constructing qm hash
Apr 05 16:48:33 [IKEv1]: IP = 172.18.124.167, IKE DECODE SENDING Message
 (msgid=20c2120e) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) +
 ID (5) + ID (5) + NONE (0) total length : 164
Apr 05 16:48:33 [IKEv1]: IP = 172.18.124.167, IKE DECODE RECEIVED Message
 (msgid=20c2120e) with payloads : HDR + HASH (8) + NONE (0) total length : 48
Apr 05 16:48:33 [IKEv1 DEBUG]: Group = DefaultL2LGroup, IP = 172.18.124.167,
 processing hash
Apr 05 16:48:33 [IKEv1 DEBUG]: Group = DefaultL2LGroup, IP = 172.18.124.167,
 loading all IPSEC SAs
Apr 05 16:48:33 [IKEv1 DEBUG]: Group = DefaultL2LGroup, IP = 172.18.124.167,
 Generating Quick Mode Key!
Apr 05 16:48:33 [IKEv1 DEBUG]: Group = DefaultL2LGroup, IP = 172.18.124.167,
 Generating Quick Mode Key!
Apr 05 16:48:33 [IKEv1]: Group = DefaultL2LGroup, IP = 172.18.124.167,
 Security negotiation complete for User (DefaultL2LGroup)  Responder,
 Inbound SPI = 0xd5243861, Outbound SPI = 0x7bb11ead
Apr 05 16:48:33 [IKEv1 DEBUG]: IKE got a KEY_ADD msg for SA: SPI = 0x7bb11ead
Apr 05 16:48:33 [IKEv1 DEBUG]: pitcher: rcv KEY_UPDATE, spi 0xd5243861
Apr 05 16:48:33 [IKEv1]: Group = DefaultL2LGroup, IP = 172.18.124.167,
 PHASE 2 COMPLETED (msgid=20c2120e)
```

Remote PIX Dynamic NAT (6.3.4)

```
tiger(config)#
ISAKMP (0): beginning Main Mode exchange

crypto_isakmp_process_block:src:172.18.124.166, dest:172.18.124.167 spt:500
 dpt:500 OAK_MM exchange
ISAKMP (0): processing SA payload. message ID = 0

ISAKMP (0): Checking ISAKMP transform 1 against priority 10 policy
ISAKMP:      encryption DES-CBC
ISAKMP:      hash MD5
ISAKMP:      default group 2
ISAKMP:      auth pre-share
```

```
ISAKMP:        life type in seconds
ISAKMP:        life duration (basic) of 3600
ISAKMP (0): atts are acceptable. Next payload is 0
ISAKMP (0): processing vendor id payload


ISAKMP (0): SA is doing pre-shared key authentication using id type
 ID_FQDN return status is IKMP_NO_ERROR
crypto_isakmp_process_block:src:172.18.124.166, dest:172.18.124.167
 spt:500 dpt:500 OAK_MM exchange
ISAKMP (0): processing KE payload. message ID = 0
ISAKMP (0): processing NONCE payload. message ID = 0
ISAKMP (0): processing vendor id payload
ISAKMP (0): processing vendor id payload
ISAKMP (0): received xauth v6 vendor id
ISAKMP (0): processing vendor id payload
ISAKMP (0): speaking to another IOS box!
ISAKMP (0): processing vendor id payload
ISAKMP (0): speaking to a VPN3000 concentrator
ISAKMP (0): ID payload
        next-payload : 8
        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:172.18.124.166, dest:172.18.124.167 spt:500 dpt:500
OAK_MM exchange
ISAKMP (0): processing ID payload. message ID = 0
ISAKMP (0): processing HASH payload. message ID = 0
ISAKMP (0): processing vendor id payload


ISAKMP (0): remote peer supports dead peer detection


ISAKMP (0): SA has been authenticated


ISAKMP (0): beginning Quick Mode exchange, M-ID of 549589518:20c2120eIPSEC(key_engine):
 got a queue event...
IPSEC(spi_response): getting spi 0x7bb11ead(2075205293) for SA
        from  172.18.124.166 to  172.18.124.167 for prot 3


return status is IKMP_NO_ERROR
ISAKMP (0): sending INITIAL_CONTACT notify
ISAKMP (0): sending NOTIFY message 24578 protocol 1
VPN Peer: ISAKMP: Added new peer: ip:172.18.124.166/500 Total VPN Peers:1
VPN Peer: ISAKMP: Peer ip:172.18.124.166/500 Ref cnt incremented to:1 Total VPN Peers:1
crypto_isakmp_process_block:src:172.18.124.166, dest:172.18.124.167 spt:500 dpt:500
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_IDLE
ISAKMP (0): processing SA payload. message ID = 549589518


ISAKMP : Checking IPSec proposal 1


ISAKMP: transform 1, ESP_DES
ISAKMP:    attributes in transform:
ISAKMP:        SA life type in seconds
ISAKMP:        SA life duration (basic) of 28800
ISAKMP:        SA life type in kilobytes
ISAKMP:        SA life duration (VPI) of  0x0 0x46 0x50 0x0
ISAKMP:        encaps is 1
ISAKMP:        authenticator is HMAC-MD5
ISAKMP (0): atts are acceptable.IPSEC(validate_proposal_request): proposal part #1,
  (key eng. msg.) dest= 172.18.124.166, src= 172.18.124.167,
```

```
     dest_proxy= 10.2.2.0/255.255.255.0/0/0 (type=4),
     src_proxy= 10.1.1.0/255.255.255.0/0/0 (type=4),
     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 = 549589518


ISAKMP (0): processing ID payload. message ID = 549589518
ISAKMP (0): processing ID payload. message ID = 549589518
ISAKMP (0): Creating IPSec SAs
        inbound SA from  172.18.124.166 to  172.18.124.167 (proxy 10.2.2.0 to 10.1.1.0)
        has spi 2075205293 and conn_id 1 and flags 4
        lifetime of 28800 seconds
        lifetime of 4608000 kilobytes
        outbound SA from  172.18.124.167 to  172.18.124.166 (proxy 10.1.1.0 to 10.2.2.0)
        has spi 3575920737 and conn_id 2 and flags 4
        lifetime of 28800 seconds
        lifetime of 4608000 kilobytesIPSEC(key_engine): got a queue event...
IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 172.18.124.167, src= 172.18.124.166,
    dest_proxy= 10.1.1.0/255.255.255.0/0/0 (type=4),
    src_proxy= 10.2.2.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-des esp-md5-hmac ,
    lifedur= 28800s and 4608000kb,
    spi= 0x7bb11ead(2075205293), conn_id= 1, keysize= 0, flags= 0x4IPSEC(initialize_sas): ,
  (key eng. msg.) src= 172.18.124.167, dest= 172.18.124.166,
    src_proxy= 10.1.1.0/255.255.255.0/0/0 (type=4),
    dest_proxy= 10.2.2.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-des esp-md5-hmac ,
    lifedur= 28800s and 4608000kb,
    spi= 0xd5243861(3575920737), conn_id= 2, keysize= 0, flags= 0x4


VPN Peer: IPSEC: Peer ip:172.18.124.166/500 Ref cnt incremented to:2 Total VPN Peers:1
VPN Peer: IPSEC: Peer ip:172.18.124.166/500 Ref cnt incremented to:3 Total VPN Peers:1
 return status is IKMP_NO_ERROR
```

VPN Client 4.0.5 on Central PIX 7.0

```
lion(config)# Apr 05 16:49:56 [IKEv1 DEBUG]: IP = 64.102.51.191, processing SA payload
Apr 05 16:49:56 [IKEv1 DEBUG]: IP = 64.102.51.191, processing ke payload
Apr 05 16:49:56 [IKEv1 DEBUG]: IP = 64.102.51.191, processing ISA_KE
Apr 05 16:49:56 [IKEv1 DEBUG]: IP = 64.102.51.191, processing nonce payload
Apr 05 16:49:56 [IKEv1 DEBUG]: IP = 64.102.51.191, Processing ID
Apr 05 16:49:56 [IKEv1 DEBUG]: IP = 64.102.51.191, processing VID payload
Apr 05 16:49:56 [IKEv1 DEBUG]: IP = 64.102.51.191, Received xauth V6 VID
Apr 05 16:49:56 [IKEv1 DEBUG]: IP = 64.102.51.191, processing VID payload
Apr 05 16:49:56 [IKEv1 DEBUG]: IP = 64.102.51.191, Received DPD VID
Apr 05 16:49:56 [IKEv1 DEBUG]: IP = 64.102.51.191, processing VID payload
Apr 05 16:49:56 [IKEv1 DEBUG]: IP = 64.102.51.191, Received NAT-Traversal ver02 VID
Apr 05 16:49:56 [IKEv1 DEBUG]: IP = 64.102.51.191, processing VID payload
Apr 05 16:49:56 [IKEv1 DEBUG]: IP = 64.102.51.191, Received Fragmentation VID
Apr 05 16:49:56 [IKEv1 DEBUG]: IP = 64.102.51.191, IKE Peer included IKE fragmentation
 capability flags:  Main Mode:        True  Aggressive Mode:  False
Apr 05 16:49:56 [IKEv1 DEBUG]: IP = 64.102.51.191, processing VID payload
Apr 05 16:49:56 [IKEv1 DEBUG]: IP = 64.102.51.191, Received Cisco Unity client VID
Apr 05 16:49:56 [IKEv1]: IP = 64.102.51.191, Connection landed on tunnel_group unityclient
Apr 05 16:49:56 [IKEv1 DEBUG]: Group = unityclient, IP = 64.102.51.191, processing IKE SA
Apr 05 16:49:56 [IKEv1 DEBUG]: Group = unityclient, IP = 64.102.51.191, IKE SA Proposal # 1,
 Transform # 14 acceptable  Matches global IKE entry # 3
Apr 05 16:49:56 [IKEv1 DEBUG]: Group = unityclient, IP = 64.102.51.191, constructing ISA_SA
 for isakmp
```

```
Apr 05 16:49:56 [IKEv1 DEBUG]: Group = unityclient, IP = 64.102.51.191,
 constructing ke payload
Apr 05 16:49:56 [IKEv1 DEBUG]: Group = unityclient, IP = 64.102.51.191,
 constructing nonce payload
Apr 05 16:49:56 [IKEv1 DEBUG]: Group = unityclient, IP = 64.102.51.191,
 Generating keys for Responder...
Apr 05 16:49:56 [IKEv1 DEBUG]: Group = unityclient, IP = 64.102.51.191,
 constructing ID
Apr 05 16:49:56 [IKEv1 DEBUG]: Group = unityclient, IP = 64.102.51.191,
 construct hash payload
Apr 05 16:49:56 [IKEv1 DEBUG]: Group = unityclient, IP = 64.102.51.191,
 computing hash
Apr 05 16:49:56 [IKEv1 DEBUG]: Group = unityclient, IP = 64.102.51.191,
 constructing Cisco Unity VID payload
Apr 05 16:49:56 [IKEv1 DEBUG]: Group = unityclient, IP = 64.102.51.191,
 constructing xauth V6 VID payload
Apr 05 16:49:56 [IKEv1 DEBUG]: Group = unityclient, IP = 64.102.51.191,
 constructing dpd vid payload
Apr 05 16:49:56 [IKEv1 DEBUG]: Group = unityclient, IP = 64.102.51.191,
 constructing Fragmentation VID + extended capabilities payload
Apr 05 16:49:56 [IKEv1 DEBUG]: Group = unityclient, IP = 64.102.51.191,
 constructing VID payload
Apr 05 16:49:56 [IKEv1 DEBUG]: Group = unityclient, IP = 64.102.51.191,
 Send Altiga/Cisco VPN3000/Cisco ASA GW VID
Apr 05 16:49:56 [IKEv1]: IP = 64.102.51.191, IKE DECODE SENDING Message
 (msgid=0) with payloads : HDR + SA (1) + KE (4) + NONCE (10) + ID (5) +
 HASH (8) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR
 (13) + NONE (0) total length : 378
Apr 05 16:49:56 [IKEv1]: IP = 64.102.51.191, IKE DECODE RECEIVED Message
 (msgid=0) with payloads : HDR + HASH (8) + NOTIFY (11) + VENDOR (13) +
 VENDOR (13) + NONE (0) total length : 116
Apr 05 16:49:56 [IKEv1 DEBUG]: Group = unityclient, IP = 64.102.51.191, processing hash
Apr 05 16:49:56 [IKEv1 DEBUG]: Group = unityclient, IP = 64.102.51.191, computing hash
Apr 05 16:49:56 [IKEv1 DEBUG]: Group = unityclient, IP = 64.102.51.191,
 Processing Notify payload
Apr 05 16:49:56 [IKEv1 DEBUG]: Group = unityclient, IP = 64.102.51.191,
 processing VID payload
Apr 05 16:49:56 [IKEv1 DEBUG]: Group = unityclient, IP = 64.102.51.191,
 Processing IOS/PIX Vendor ID payload (version: 1.0.0, capabilities: 00000408)
Apr 05 16:49:56 [IKEv1 DEBUG]: Group = unityclient, IP = 64.102.51.191,
 processing VID payload
Apr 05 16:49:56 [IKEv1 DEBUG]: Group = unityclient, IP = 64.102.51.191,
 Received Cisco Unity client VID
Apr 05 16:49:56 [IKEv1]: IP = 64.102.51.191, IKE DECODE RECEIVED Message
 (msgid=a0bb428) with payloads : HDR + HASH (8) + ATTR (14) + NONE (0)
 total length: 196
Apr 05 16:49:56 [IKEv1 DEBUG]: process_attr(): Enter!
Apr 05 16:49:56 [IKEv1 DEBUG]: Processing cfg Request attributes
Apr 05 16:49:56 [IKEv1 DEBUG]: MODE_CFG: Received request for IPV4 address!
Apr 05 16:49:56 [IKEv1 DEBUG]: MODE_CFG: Received request for IPV4 net mask!
Apr 05 16:49:56 [IKEv1 DEBUG]: MODE_CFG: Received request for DNS server address!
Apr 05 16:49:56 [IKEv1 DEBUG]: MODE_CFG: Received request for WINS server address!
Apr 05 16:49:56 [IKEv1]: Group = unityclient, IP = 64.102.51.191, Received
 unsupported transaction mode attribute: 5
Apr 05 16:49:56 [IKEv1 DEBUG]: MODE_CFG: Received request for Banner!
Apr 05 16:49:56 [IKEv1 DEBUG]: MODE_CFG: Received request for Save PW setting!
Apr 05 16:49:56 [IKEv1 DEBUG]: MODE_CFG: Received request for Default Domain Name!
Apr 05 16:49:56 [IKEv1 DEBUG]: MODE_CFG: Received request for Split Tunnel List!
Apr 05 16:49:56 [IKEv1 DEBUG]: MODE_CFG: Received request for Split DNS!
Apr 05 16:49:56 [IKEv1 DEBUG]: MODE_CFG: Received request for PFS setting!
Apr 05 16:49:56 [IKEv1 DEBUG]: MODE_CFG: Received request for backup ip-sec peer list!
Apr 05 16:49:56 [IKEv1 DEBUG]: MODE_CFG: Received request for Application Version!
Apr 05 16:49:56 [IKEv1]: Group = unityclient, IP = 64.102.51.191, Client Type: WinNT
  Client Application Version: 4.0.5 (Rel)
```

```
Apr 05 16:49:56 [IKEv1 DEBUG]: MODE_CFG: Received request for FWTYPE!
Apr 05 16:49:56 [IKEv1 DEBUG]: MODE_CFG: Received request for DHCP hostname
 for DDNS is: tthotus-xp!
Apr 05 16:49:56 [IKEv1 DEBUG]: MODE_CFG: Received request for UDP Port!
Apr 05 16:49:56 [IKEv1 DEBUG]: Group = unityclient, IP = 64.102.51.191,
 constructing blank hash
Apr 05 16:49:56 [IKEv1 DEBUG]: Group = unityclient, IP = 64.102.51.191,
 constructing qm hash
Apr 05 16:49:56 [IKEv1]: IP = 64.102.51.191, IKE DECODE SENDING Message
 (msgid=a0bb428) with payloads : HDR + HASH (8) + ATTR (14) + NONE (0)
 total length : 157
Apr 05 16:49:56 [IKEv1 DEBUG]: Group = unityclient, IP = 64.102.51.191,
 Delay Quick Mode processing, Cert/Trans Exch/RM DSID in progress
Apr 05 16:49:56 [IKEv1 DEBUG]: Group = unityclient, IP = 64.102.51.191,
 Resume Quick Mode processing, Cert/Trans Exch/RM DSID completed
Apr 05 16:49:56 [IKEv1]: Group = unityclient, IP = 64.102.51.191, PHASE 1 COMPLETED
Apr 05 16:49:56 [IKEv1]: IP = 64.102.51.191, Keep-alive type for this connection: DPD
Apr 05 16:49:56 [IKEv1 DEBUG]: Group = unityclient, IP = 64.102.51.191,
 Starting phase 1 rekey timer: 3420000 (ms)
Apr 05 16:49:56 [IKEv1 DEBUG]: Group = unityclient, IP = 64.102.51.191,
 sending notify message
Apr 05 16:49:56 [IKEv1 DEBUG]: Group = unityclient, IP = 64.102.51.191,
 constructing blank hash
Apr 05 16:49:56 [IKEv1 DEBUG]: Group = unityclient, IP = 64.102.51.191,
 constructing qm hash
Apr 05 16:49:56 [IKEv1]: IP = 64.102.51.191, IKE DECODE SENDING Message
 (msgid=9be7674c) with payloads : HDR + HASH (8) + NOTIFY (11) + NONE
 (0) total length : 84
Apr 05 16:49:57 [IKEv1]: IP = 64.102.51.191, IKE DECODE RECEIVED Message
 (msgid=833e7945) with payloads : HDR + HASH (8) + SA (1) + NONCE (10)
 + ID (5) + ID (5) + NONE (0) total length : 1022
Apr 05 16:49:57 [IKEv1 DEBUG]: Group = unityclient, IP = 64.102.51.191, processing hash
Apr 05 16:49:57 [IKEv1 DEBUG]: Group = unityclient, IP = 64.102.51.191,
 processing SA payload
Apr 05 16:49:57 [IKEv1 DEBUG]: Group = unityclient, IP = 64.102.51.191,
 processing nonce payload
Apr 05 16:49:57 [IKEv1 DEBUG]: Group = unityclient, IP = 64.102.51.191, Processing ID
Apr 05 16:49:57 [IKEv1]: Group = unityclient, IP = 64.102.51.191,
 Received remote Proxy Host data in ID Payload:  Address 10.3.3.1, Protocol 0, Port 0
Apr 05 16:49:57 [IKEv1 DEBUG]: Group = unityclient, IP = 64.102.51.191, Processing ID
Apr 05 16:49:57 [IKEv1]: Group = unityclient, IP = 64.102.51.191,
 Received local IP Proxy Subnet data in ID Payload:   Address 0.0.0.0,
 Mask 0.0.0.0, Protocol 0, Port 0
Apr 05 16:49:57 [IKEv1]: QM IsRekeyed old sa not found by addr
Apr 05 16:49:57 [IKEv1]: Group = unityclient, IP = 64.102.51.191,
 IKE Remote Peer configured for SA: cisco
Apr 05 16:49:57 [IKEv1 DEBUG]: Group = unityclient, IP = 64.102.51.191,
 processing IPSEC SA
Apr 05 16:49:57 [IKEv1 DEBUG]: Group = unityclient, IP = 64.102.51.191,
 IPSecSA Proposal # 14, Transform # 1 acceptable  Matches global IPSec SA entry # 1
Apr 05 16:49:57 [IKEv1]: Group = unityclient, IP = 64.102.51.191, IKE: requesting SPI!
Apr 05 16:49:57 [IKEv1 DEBUG]: IKE got SPI from key engine: SPI = 0x05953824
Apr 05 16:49:57 [IKEv1 DEBUG]: Group = unityclient, IP = 64.102.51.191,
 oakley constucting quick mode
Apr 05 16:49:57 [IKEv1 DEBUG]: Group = unityclient, IP = 64.102.51.191,
 constructing blank hash
Apr 05 16:49:57 [IKEv1 DEBUG]: Group = unityclient, IP = 64.102.51.191,
 constructing ISA_SA for ipsec
Apr 05 16:49:57 [IKEv1]: Group = unityclient, IP = 64.102.51.191,
 Overriding Initiator's IPSec rekeying duration from 2147483 to 28800 seconds
Apr 05 16:49:57 [IKEv1 DEBUG]: Group = unityclient, IP = 64.102.51.191,
 constructing ipsec nonce payload
Apr 05 16:49:57 [IKEv1 DEBUG]: Group = unityclient, IP = 64.102.51.191,
 constructing proxy ID
```

```
Apr 05 16:49:57 [IKEv1 DEBUG]: Group = unityclient, IP = 64.102.51.191,
 Transmitting Proxy Id:
  Remote host: 10.3.3.1  Protocol 0  Port 0
  Local subnet:  0.0.0.0  mask 0.0.0.0 Protocol 0  Port 0
Apr 05 16:49:57 [IKEv1 DEBUG]: Group = unityclient, IP = 64.102.51.191,
 Sending RESPONDER LIFETIME notification to Initiator
Apr 05 16:49:57 [IKEv1 DEBUG]: Group = unityclient, IP = 64.102.51.191,
 constructing qm hash
Apr 05 16:49:57 [IKEv1]: IP = 64.102.51.191, IKE DECODE SENDING Message
 (msgid=833e7945) with payloads : HDR + HASH (8) + SA (1) + NONCE (10)
 + ID (5) + ID (5) + NOTIFY (11) + NONE (0) total length : 176
Apr 05 16:49:57 [IKEv1]: IP = 64.102.51.191, IKE DECODE RECEIVED Message
 (msgid=833e7945) with payloads : HDR + HASH (8) + NONE (0) total length : 48
Apr 05 16:49:57 [IKEv1 DEBUG]: Group = unityclient, IP = 64.102.51.191,
 processing hash
Apr 05 16:49:57 [IKEv1 DEBUG]: Group = unityclient, IP = 64.102.51.191,
 loading all IPSEC SAs
Apr 05 16:49:57 [IKEv1 DEBUG]: Group = unityclient, IP = 64.102.51.191,
 Generating Quick Mode Key!
Apr 05 16:49:57 [IKEv1 DEBUG]: Group = unityclient, IP = 64.102.51.191,
 Generating Quick Mode Key!
Apr 05 16:49:57 [IKEv1]: Group = unityclient, IP = 64.102.51.191,
 Security negotiation complete for User (unityclient)  Responder,
 Inbound SPI = 0x05953824, Outbound SPI = 0xd08c6486
Apr 05 16:49:57 [IKEv1 DEBUG]: IKE got a KEY_ADD msg for SA: SPI = 0xd08c6486
Apr 05 16:49:57 [IKEv1 DEBUG]: pitcher: rcv KEY_UPDATE, spi 0x5953824
Apr 05 16:49:57 [IKEv1]: Group = unityclient, IP = 64.102.51.191,
 Adding static route for client address: 10.3.3.1
Apr 05 16:49:57 [IKEv1]: Group = unityclient, IP = 64.102.51.191, PHASE 2 COMP
LETED (msgid=833e7945)
Apr 05 16:50:07 [IKEv1]: IP = 64.102.51.191, IKE DECODE RECEIVED Message
 (msgid=403ee701) with payloads : HDR + HASH (8) + NOTIFY (11) + NONE
 (0) total length : 80
Apr 05 16:50:07 [IKEv1 DEBUG]: Group = unityclient, IP = 64.102.51.191,
 processing hash
Apr 05 16:50:07 [IKEv1 DEBUG]: Group = unityclient, IP = 64.102.51.191,
 Processing Notify payload
Apr 05 16:50:07 [IKEv1 DEBUG]: Group = unityclient, IP = 64.102.51.191,
 Received keep-alive of type DPD R-U-THERE (seq number 0x4b55b6e4)
Apr 05 16:50:07 [IKEv1 DEBUG]: Group = unityclient, IP = 64.102.51.191,
 Sending keep-alive of type DPD R-U-THERE-ACK (seq number 0x4b55b6e4)
Apr 05 16:50:07 [IKEv1 DEBUG]: Group = unityclient, IP = 64.102.51.191,
 constructing blank hash
Apr 05 16:50:07 [IKEv1 DEBUG]: Group = unityclient, IP = 64.102.51.191,
 constructing qm hash
Apr 05 16:50:07 [IKEv1]: IP = 64.102.51.191, IKE DECODE SENDING Message
 (msgid=78998a29) with payloads : HDR + HASH (8) + NOTIFY (11) + NONE
 (0) total length : 80
Apr 05 16:50:17 [IKEv1]: IP = 64.102.51.191, IKE DECODE RECEIVED Message
 (msgid=dba719e9) with payloads : HDR + HASH (8) + NOTIFY (11) + NONE (0)
 total length : 80
Apr 05 16:50:17 [IKEv1 DEBUG]: Group = unityclient, IP = 64.102.51.191, processing hash
Apr 05 16:50:17 [IKEv1 DEBUG]: Group = unityclient, IP = 64.102.51.191,
 Processing Notify payload
Apr 05 16:50:17 [IKEv1 DEBUG]: Group = unityclient, IP = 64.102.51.191,
 Received keep-alive of type DPD R-U-THERE (seq number 0x4b55b6e5)
Apr 05 16:50:17 [IKEv1 DEBUG]: Group = unityclient, IP = 64.102.51.191,
 Sending keep-alive of type DPD R-U-THERE-ACK (seq number 0x4b55b6e5)
Apr 05 16:50:17 [IKEv1 DEBUG]: Group = unityclient, IP = 64.102.51.191,
 constructing blank hash
Apr 05 16:50:17 [IKEv1 DEBUG]: Group = unityclient, IP = 64.102.51.191,
 constructing qm hash
Apr 05 16:50:17 [IKEv1]: IP = 64.102.51.191, IKE DECODE SENDING Message
 (msgid=40456779) with payloads : HDR + HASH (8) + NOTIFY (11) + NONE
```

```
     (0) total length : 80
```

Related Information

- **Cisco ASA 5500 Series Adaptive Security Appliances Product Support**
- **Cisco PIX Firewall Software**
- **Cisco Secure PIX Firewall Command References**
- **Security Product Field Notices (including PIX)**
- **Requests for Comments (RFCs)** ↗
- **Technical Support & Documentation - Cisco Systems**