

PIX/ASA 7.x and later : Dynamic IPsec Between a Statically addressed IOS Router and a Dynamically addressed PIX with NAT Configuration Example

Document ID: 82077

Introduction

Prerequisites

- Requirements
- Components Used
- Related Products
- Conventions

Background Information

Configure

- Network Diagram
- Configurations
- Clear Security Associations (SAs)

Verify

- PIX Security Appliance – show Commands
- Remote IOS Router – show Commands

Troubleshoot

- PIX Security Appliance – debug Output
- Remote IOS Router – debug Output

NetPro Discussion Forums – Featured Conversations

Related Information

Introduction

This document provides a sample configuration that shows you how to enable the router to accept dynamic IPsec connections from a PIX. The remote router performs Network Address Translation (NAT) if private network 10.2.1.x accesses the Internet. Traffic from 10.2.1.x to private network 10.1.1.x behind the PIX Security Appliance is excluded from the NAT process. The IPsec tunnel establishes only if the traffic (10.1.1.x) initiates the connection from the PIX Security Appliance with the router having remote network (10.2.1.x). The PIX can initiate connections to the router, but the router cannot initiate connections to the PIX.

This configuration uses a Cisco IOS® router in order to create dynamic IPsec LAN-to-LAN (L2L) tunnels with a security appliance that receives dynamic IP addresses on their public interface (outside interface). Dynamic Host Configuration Protocol (DHCP) provides a mechanism in order to allocate IP addresses dynamically from the service provider. This allows IP addresses to be reused when hosts no longer need them.

Refer to [Configuring PIX-to-Router Dynamic-to-Static IPsec With NAT](#) for more information on a scenario where the PIX 6.x accepts dynamic IPsec connections from the router.

Refer to [Router-to-PIX Dynamic-to-Static IPsec with NAT Configuration Example](#) for more information on a scenario where the router accepts dynamic IPsec connections from a PIX Firewall that runs 6.x.

Refer to [IPsec Between a Static IOS Router and a Dynamic PIX/ASA 7.x with NAT Configuration Example](#) in order to enable the PIX/ASA Security Appliance to accept dynamic IPsec connections from the Cisco IOS router.

Refer to PIX/ASA 7.x PIX-to-PIX Dynamic-to-Static IPsec with NAT and VPN Client Configuration Example for more information on the scenario where the PIX/ASA Security Appliance 7.x accepts dynamic IPsec connections from another PIX 6.x.

Prerequisites

Requirements

Ensure that both the PIX and the router have Internet connectivity for the establishment of the IPsec tunnel before you attempt this configuration.

This document assumes that you have already assigned the IP addresses on both the public and private interfaces and that you are able to ping the IP address of the remote VPN device.

Components Used

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

- Cisco 3600 that runs Cisco IOS Software Release 12.4
- PIX 515E Series Security Appliance Software Release 7.x and later

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.

Related Products

Cisco ASA 5500 Series version 7.x runs a similar software version of PIX version 7.x. The configurations in this document are applicable to both product lines.

Conventions

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

Background Information

On the PIX, the **access-list** and **nat 0** commands work together. When a user on the 10.1.1.0 network goes to the 10.2.1.0 network, the access list is used to permit the 10.1.1.0 network traffic to be encrypted without NAT. On the router, the **access-list** commands are used to permit the 10.2.1.0 network traffic to be encrypted without NAT. However, when the same users go anywhere else (like the Internet), they are translated to the outside interface IP address through Port Address Translation (PAT).

These are the configuration commands required on the PIX Security Appliance in order for traffic not to run through PAT over the tunnel, and traffic to the Internet to run through PAT.

```
access-list nonat permit ip 10.1.1.0 255.255.255.0 10.2.2.0 255.255.255.0
nat (inside) 0 access-list nonat
nat (inside) 1 10.1.1.0 255.255.255.0 0 0
```

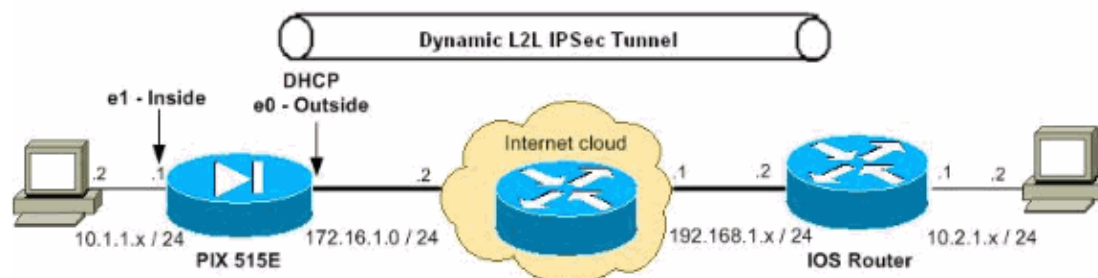
Configure

In this section, you are presented with the information to configure the features described in this document.

Note: Use the Command Lookup Tool (registered customers only) to obtain more information on the commands used in this section.

Network Diagram

This document uses this network setup:



Configurations

This document uses these configurations:

- PIX Security Appliance Configuration
- Router Configuration

PIX 7.x

```
pixfirewall#show running-config
PIX Version 7.2(2)
!
hostname pixfirewall
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
!-- The interface dynamically learns its IP address
!-- from the service provider.

interface Ethernet0
 nameif outside
 security-level 0
 ip address dhcp
!
interface Ethernet1
 nameif inside
 security-level 100
 ip address 10.1.1.2 255.255.255.0
!
!
!-- Output is suppressed.

!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
```

```
!--- This is the access list (IPsec-traffic) used for the VPN interesting traffic  
!--- to be encrypted.
```

```
access-list IPsec-traffic extended permit ip 10.1.1.0 255.255.255.0 10.2.1.0 255.255.255.0
```

```
!--- This access list (nonat) is used for a nat zero command that prevents  
!--- traffic which matches the access list from undergoing NAT.
```

```
access-list NO-NAT extended permit ip 10.1.1.0 255.255.255.0 10.2.1.0 255.255.255.0
```

```
pager lines 24  
mtu inside 1500  
mtu outside 1500  
no failover  
icmp unreachable rate-limit 1 burst-size 1  
no asdm history enable  
arp timeout 14400
```

```
!--- NAT 0 prevents NAT for networks specified in the ACL - nonat.  
!--- The nat 1 command specifies PAT using the  
!--- outside interface for all other traffic.
```

```
global (outside) 1 interface  
nat (inside) 0 access-list NO-NAT  
nat (inside) 1 0.0.0.0 0.0.0.0
```

```
route outside 0.0.0.0 0.0.0.0 172.16.1.2 1
```

```
timeout xlate 3:00:00  
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02  
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00  
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00  
timeout uauth 0:05:00 absolute  
no snmp-server location  
no snmp-server contact  
snmp-server enable traps snmp authentication linkup linkdown coldstart
```

```
!--- PHASE 2 CONFIGURATION ---!  
!--- The encryption types for Phase 2 are defined here.  
!--- A triple single DES encryption with  
!--- the md5 hash algorithm is used.
```

```
crypto ipsec transform-set DYN-TS esp-des esp-md5-hmac
```

```
!--- Define which traffic should be sent to the IPsec peer.
```

```
crypto map IPSEC 10 match address IPsec-traffic
```

```
!--- Sets the IPsec peer.
```

```
crypto map IPSEC 10 set peer 192.168.1.2

!--- Sets the IPsec transform set "DYN-TS"
!--- to be used with the crypto map entry "IPSEC".

crypto map IPSEC 10 set transform-set DYN-TS

!--- Specifies the interface to be used with
!--- the settings defined in this configuration.

crypto map IPSEC interface outside

!--- Enables IPsec on the outside interface.

crypto isakmp enable outside

!--- PHASE 1 CONFIGURATION ---!

!--- This configuration uses isakmp policy 10.
!--- Policy 65535 is included in the configuration by default.
!--- The configuration commands here define the Phase
!--- 1 policy parameters that are used.

crypto isakmp policy 10
 authentication pre-share
 encryption des
 hash md5
 group 1
 lifetime 86400

crypto isakmp policy 65535
 authentication pre-share
 encryption 3des
 hash sha
 group 2
 lifetime 86400

!--- In order to create and manage the database of connection-specific records
!--- for IPsec-L2L IPsec tunnels, use the tunnel-group
!--- command in global configuration mode.
!--- For L2L connections the name of the tunnel group MUST be the IP
!--- address of the IPsec peer.

tunnel-group 192.168.1.2 type ipsec-l2l

!--- Enter the pre-shared-key in IPsec-attribute parameters
!--- in order to configure the authentication method.

tunnel-group 192.168.1.2 ipsec-attributes
 pre-shared-key *

telnet timeout 5
ssh timeout 5
console timeout 0
```

```

!
class-map inspection_default
  match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
  parameters
    message-length maximum 512
policy-map global_policy
  class inspection_default
    inspect dns preset_dns_map
    inspect ftp
    inspect h323 h225
    inspect h323 ras
    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
prompt hostname context
Cryptochecksum:d609c9eaf51c154f147b3b4ba3c834e0
: end
pixfirewall#

```

Router

```

Router#show running-config
Current configuration : 1354 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
resource policy
!
!
!
ip cef
!

!--- Configuration for IKE policies.
!--- Enables the IKE policy configuration (config-isakmp)
!--- command mode, where you can specify the parameters that
!--- are used during an IKE negotiation.

crypto isakmp policy 10
  hash md5

```

authentication pre-share

*!--- Specifies the preshared key "cisco123" which should
!--- be identical at both peers. This is a global
!--- configuration mode command. It accepts any peer which matches
!--- the pre-shared key.*

crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0

!

*!--- Configuration for IPsec policies.
!--- Enables the crypto transform configuration mode,
!--- where you can specify the transform sets that are used
!--- during an IPsec negotiation.*

crypto ipsec transform-set DYN-TS esp-des esp-md5-hmac

!--- IPsec policy, Phase 2.

crypto dynamic-map DYN 10

*!--- Configures IPsec to use the transform-set
!--- "DYN-TS" defined earlier in this configuration.*

set transform-set DYN-TS

crypto map IPSEC 10 ipsec-isakmp dynamic DYN

!

interface Ethernet0/0
ip address 192.168.1.2 255.255.255.0
ip nat outside
ip virtual-reassembly
half-duplex

*!--- Configures the interface to use the
!--- crypto map "IPSEC" for IPsec.*

crypto map IPSEC

!

interface FastEthernet1/0
ip address 10.2.1.1 255.255.255.0
ip nat inside
ip virtual-reassembly
duplex auto
speed auto

!

interface Serial2/0
no ip address
shutdown
no fair-queue

!

interface Serial2/1
no ip address
shutdown

!

interface Serial2/2
no ip address

```

shutdown
!
interface Serial2/3
  no ip address
  shutdown
!
ip http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 192.168.1.1
!
ip nat inside source list 100 interface Ethernet0/0 overload
!

!--- This ACL 100 identifies the traffic flows and be PATed
!--- via the outside interface( Ethernet0/0).

access-list 100 deny ip 10.2.1.0 0.0.0.255 10.1.1.0 0.0.0.255
access-list 100 permit ip 10.2.1.0 0.0.0.255 any

control-plane
!
!
line con 0
line aux 0
line vty 0 4
!
!
end

```

Clear Security Associations (SAs)

Use these commands in the privilege mode of the PIX:

- **clear [crypto] ipsec sa** Deletes the active IPsec SAs. The keyword **crypto** is optional.
- **clear [crypto] isakmp sa** Deletes the active IKE SAs. The keyword **crypto** is optional.

Verify

Use this section to confirm that your configuration works properly.

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

- PIX Security Appliance – show Commands
- Remote IOS Router – show Commands

PIX Security Appliance – show Commands

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

```
pixfirewall#show crypto isakmp sa
```

```

Active SA: 1
Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

```

```

1  IKE Peer: 192.168.1.2
   Type      : L2L                Role      : initiator
   Rekey     : no                 State     : MM_ACTIVE

```

- **show crypto ipsec sa** Shows all current IPsec SAs at a peer.

```

pixfirewall#show crypto ipsec sa
                    interface: outside
Crypto map tag: IPSEC, seq num: 10, local addr: 172.16.1.1

access-list IPSEC-traffic permit ip 10.1.1.0 255.255.255.0 10.2.1.0 255.255.255.0
local ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (10.2.1.0/255.255.255.0/0/0)
current_peer: 192.168.1.2

#pkts encaps: 10, #pkts encrypt: 10, #pkts digest: 10
#pkts decaps: 10, #pkts decrypt: 10, #pkts verify: 10
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 10, #pkts comp failed: 0, #pkts decomp failed: 0
#pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
#send errors: 0, #recv errors: 0

local crypto endpt.: 172.16.1.1, remote crypto endpt.: 192.168.1.2

path mtu 1500, ipsec overhead 58, media mtu 1500
current outbound spi: 537BC76F

inbound esp sas:
spi: 0x64D800CB (1691877579)
transform: esp-des esp-md5-hmac none
in use settings = {L2L, Tunnel, }
slot: 0, conn_id: 1, crypto-map: IPSEC
sa timing: remaining key lifetime (kB/sec): (4274999/3506)
IV size: 8 bytes
replay detection support: Y
outbound esp sas:
spi: 0x537BC76F (1400620911)
transform: esp-des esp-md5-hmac none
in use settings = {L2L, Tunnel, }
slot: 0, conn_id: 1, crypto-map: IPSEC
sa timing: remaining key lifetime (kB/sec): (4274999/3506)
IV size: 8 bytes
replay detection support: Y

```

Remote IOS Router – show Commands

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

```

Router#show crypto isakmp sa
dst          src          state          conn-id slot status
192.168.1.2  172.16.1.1  QM_IDLE       2      0  ACTIVE

```

- **show crypto ipsec sa** Displays all current IPsec SAs at a peer.

```

Router#show crypto ipsec sa
                    interface: Ethernet0/0
Crypto map tag: IPSEC, local addr 192.168.1.2

protected vrf: (none)
local ident (addr/mask/prot/port): (10.2.1.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0)
current_peer 172.16.1.1 port 500
PERMIT, flags={}
#pkts encaps: 10, #pkts encrypt: 10, #pkts digest: 10

```

```

#pkts decaps: 10, #pkts decrypt: 10, #pkts verify: 10
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 192.168.1.2, remote crypto endpt.: 172.16.1.1
path mtu 1500, ip mtu 1500, ip mtu idb Ethernet0/0
current outbound spi: 0x64D800CB(1691877579)

inbound esp sas:
  spi: 0x537BC76F(1400620911)
  transform: esp-des esp-md5-hmac ,
  in use settings ={Tunnel, }
  conn id: 2001, flow_id: SW:1, crypto map: IPSEC
  sa timing: remaining key lifetime (k/sec): (4390267/3494)
  IV size: 8 bytes
  replay detection support: Y
  Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:
  spi: 0x64D800CB(1691877579)
  transform: esp-des esp-md5-hmac ,
  in use settings ={Tunnel, }
  conn id: 2002, flow_id: SW:2, crypto map: IPSEC
  sa timing: remaining key lifetime (k/sec): (4390267/3492)
  IV size: 8 bytes
  replay detection support: Y
  Status: ACTIVE

outbound ah sas:

outbound pcp sas:

```

Troubleshoot

This section provides information you can use to troubleshoot your configuration. Sample **debug** output is also shown.

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 and IP Security Troubleshooting – Understanding and Using debug Commands before you issue **debug** commands.

- PIX Security Appliance – debug Output

debug crypto ipsec 7 Displays the IPsec negotiations of Phase 2.

debug crypto isakmp 7 Displays the ISAKMP negotiations of Phase 1.

- Remote IOS Router – debug Output

debug crypto ipsec Displays the IPsec negotiations of Phase 2.

debug crypto isakmp Displays the ISAKMP negotiations of Phase 1.

PIX Security Appliance – debug Output

PIX#debug crypto isakmp 7

```
Feb 22 01:39:59 [IKEv1 DEBUG]: Pitcher: received a key acquire message, spi 0x0
Feb 22 01:39:59 [IKEv1]: IP = 192.168.1.2, IKE Initiator: New Phase 1, Intf inside, IKE Peer 192.168.1.2 local Proxy Address 10.1.1.0, remote Proxy Address 10.2.1.0, Crypto map (IPSEC)
Feb 22 01:39:59 [IKEv1 DEBUG]: IP = 192.168.1.2, constructing ISAKMP SA payload
Feb 22 01:39:59 [IKEv1 DEBUG]: IP = 192.168.1.2, constructing Fragmentation VID + extended capabilities payload
Feb 22 01:39:59 [IKEv1]: IP = 192.168.1.2, IKE_DECODE SENDING Message (msgid=0) with payloads : HDR + SA (1) + VENDOR (13) + NONE (0) total length : 144
Feb 22 01:39:59 [IKEv1]: IP = 192.168.1.2, IKE_DECODE RECEIVED Message (msgid=0) with payloads : HDR + SA (1) + NONE (0) total length : 84
Feb 22 01:39:59 [IKEv1 DEBUG]: IP = 192.168.1.2, processing SA payload
Feb 22 01:39:59 [IKEv1 DEBUG]: IP = 192.168.1.2, Oakley proposal is acceptable
Feb 22 01:39:59 [IKEv1 DEBUG]: IP = 192.168.1.2, constructing ke payload
Feb 22 01:39:59 [IKEv1 DEBUG]: IP = 192.168.1.2, constructing nonce payload
Feb 22 01:39:59 [IKEv1 DEBUG]: IP = 192.168.1.2, constructing Cisco Unity VID payload
Feb 22 01:39:59 [IKEv1 DEBUG]: IP = 192.168.1.2, constructing xauth V6 VID payload
Feb 22 01:39:59 [IKEv1 DEBUG]: IP = 192.168.1.2, Send IOS VID
Feb 22 01:39:59 [IKEv1 DEBUG]: IP = 192.168.1.2, Constructing ASA spoofing IOS Vendor ID payload (version: 1.0.0, capabilities: 20000001)
Feb 22 01:39:59 [IKEv1 DEBUG]: IP = 192.168.1.2, constructing VID payload
Feb 22 01:39:59 [IKEv1 DEBUG]: IP = 192.168.1.2, Send Altiga/Cisco VPN3000/Cisco ASA GW VID
Feb 22 01:39:59 [IKEv1]: IP = 192.168.1.2, 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 : 224
Feb 22 01:39:59 [IKEv1]: IP = 192.168.1.2, 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 : 224
Feb 22 01:39:59 [IKEv1 DEBUG]: IP = 192.168.1.2, processing ke payload
Feb 22 01:39:59 [IKEv1 DEBUG]: IP = 192.168.1.2, processing ISA_KE payload
Feb 22 01:39:59 [IKEv1 DEBUG]: IP = 192.168.1.2, processing nonce payload
Feb 22 01:39:59 [IKEv1 DEBUG]: IP = 192.168.1.2, processing VID payload
Feb 22 01:39:59 [IKEv1 DEBUG]: IP = 192.168.1.2, Received Cisco Unity client VID
Feb 22 01:39:59 [IKEv1 DEBUG]: IP = 192.168.1.2, processing VID payload
Feb 22 01:39:59 [IKEv1 DEBUG]: IP = 192.168.1.2, Received DPD VID
Feb 22 01:39:59 [IKEv1 DEBUG]: IP = 192.168.1.2, processing VID payload
Feb 22 01:39:59 [IKEv1 DEBUG]: IP = 192.168.1.2, Processing IOS/PIX Vendor ID payload (version: 1.0.0, capabilities: 0000077f)
Feb 22 01:39:59 [IKEv1 DEBUG]: IP = 192.168.1.2, processing VID payload
Feb 22 01:39:59 [IKEv1 DEBUG]: IP = 192.168.1.2, Received xauth V6 VID
Feb 22 01:39:59 [IKEv1]: IP = 192.168.1.2, Connection landed on tunnel_group 192.168.1.2
Feb 22 01:39:59 [IKEv1 DEBUG]: Group = 192.168.1.2, IP = 192.168.1.2, Generating keys for Initiator...
Feb 22 01:39:59 [IKEv1 DEBUG]: Group = 192.168.1.2, IP = 192.168.1.2, constructing ID payload
Feb 22 01:39:59 [IKEv1 DEBUG]: Group = 192.168.1.2, IP = 192.168.1.2, constructing hash payload
Feb 22 01:39:59 [IKEv1 DEBUG]: Group = 192.168.1.2, IP = 192.168.1.2, Computing hash for ISAKMP
Feb 22 01:39:59 [IKEv1 DEBUG]: IP = 192.168.1.2, Constructing IOS keep alive payload: proposal=32767/32767 sec.
Feb 22 01:39:59 [IKEv1 DEBUG]: Group = 192.168.1.2, IP = 192.168.1.2, constructing dpd vid payload
Feb 22 01:39:59 [IKEv1]: IP = 192.168.1.2, IKE_DECODE SENDING Message (msgid=0) with payloads : HDR + ID (5) + HASH (8) + IOS KEEPALIVE (128) + VENDOR (13) + NONE (0) total length : 92
Feb 22 01:39:59 [IKEv1]: IP = 192.168.1.2, IKE_DECODE RECEIVED Message (msgid=0) with payloads : HDR + ID (5) + HASH (8) + NONE (0) total length : 60
```

Feb 22 01:39:59 [IKEv1 DEBUG]: Group = 192.168.1.2, IP = 192.168.1.2, processing ID payload
Feb 22 01:39:59 [IKEv1 DEBUG]: Group = 192.168.1.2, IP = 192.168.1.2, processing hash payload
Feb 22 01:39:59 [IKEv1 DEBUG]: Group = 192.168.1.2, IP = 192.168.1.2, Computing hash for ISAKMP
Feb 22 01:39:59 [IKEv1]: IP = 192.168.1.2, Connection landed on tunnel_group 192.168.1.2
Feb 22 01:39:59 [IKEv1]: Group = 192.168.1.2, IP = 192.168.1.2, Freeing previously allocated memory for authorization-dn-attributes
Feb 22 01:39:59 [IKEv1 DEBUG]: Group = 192.168.1.2, IP = 192.168.1.2, Oakley begins quick mode
Feb 22 01:39:59 [IKEv1]: Group = 192.168.1.2, IP = 192.168.1.2, PHASE 1 COMPLETE
Feb 22 01:39:59 [IKEv1]: IP = 192.168.1.2, Keep-alive type for this connection: DPD
Feb 22 01:39:59 [IKEv1 DEBUG]: Group = 192.168.1.2, IP = 192.168.1.2, Starting P1 rekey timer: 82080 seconds.
Feb 22 01:39:59 [IKEv1 DEBUG]: Group = 192.168.1.2, IP = 192.168.1.2, IKE got SPI from key engine: SPI = 0x81004014
Feb 22 01:39:59 [IKEv1 DEBUG]: Group = 192.168.1.2, IP = 192.168.1.2, oakley constructing quick mode
Feb 22 01:39:59 [IKEv1 DEBUG]: Group = 192.168.1.2, IP = 192.168.1.2, constructing blank hash payload
Feb 22 01:39:59 [IKEv1 DEBUG]: Group = 192.168.1.2, IP = 192.168.1.2, constructing IPsec SA payload
Feb 22 01:39:59 [IKEv1 DEBUG]: Group = 192.168.1.2, IP = 192.168.1.2, constructing IPsec nonce payload
Feb 22 01:39:59 [IKEv1 DEBUG]: Group = 192.168.1.2, IP = 192.168.1.2, constructing proxy ID
Feb 22 01:39:59 [IKEv1 DEBUG]: Group = 192.168.1.2, IP = 192.168.1.2, Transmitting Proxy Id:
Local subnet: 10.1.1.0 mask 255.255.255.0 Protocol 0 Port 0
Remote subnet: 10.2.1.0 Mask 255.255.255.0 Protocol 0 Port 0
Feb 22 01:39:59 [IKEv1 DEBUG]: Group = 192.168.1.2, IP = 192.168.1.2, constructing qm hash payload
Feb 22 01:39:59 [IKEv1]: IP = 192.168.1.2, IKE_DECODE SENDING Message (msgid=27072fbd) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NOTIFY (11) + NONE (0) total length : 192
Feb 22 01:39:59 [IKEv1]: IP = 192.168.1.2, IKE_DECODE RECEIVED Message (msgid=27072fbd) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NOTIFY (11) + NONE (0) total length : 192
Feb 22 01:39:59 [IKEv1 DEBUG]: Group = 192.168.1.2, IP = 192.168.1.2, processing hash payload
Feb 22 01:39:59 [IKEv1 DEBUG]: Group = 192.168.1.2, IP = 192.168.1.2, processing SA payload
Feb 22 01:39:59 [IKEv1 DEBUG]: Group = 192.168.1.2, IP = 192.168.1.2, processing nonce payload
Feb 22 01:39:59 [IKEv1 DEBUG]: Group = 192.168.1.2, IP = 192.168.1.2, processing ID payload
Feb 22 01:39:59 [IKEv1 DEBUG]: Group = 192.168.1.2, IP = 192.168.1.2, processing ID payload
Feb 22 01:39:59 [IKEv1 DEBUG]: Group = 192.168.1.2, IP = 192.168.1.2, processing notify payload
Feb 22 01:39:59 [IKEv1]: Group = 192.168.1.2, IP = 192.168.1.2, Responder forcing change of IPsec rekeying duration from 28800 to 3600 seconds
Feb 22 01:39:59 [IKEv1 DEBUG]: Group = 192.168.1.2, IP = 192.168.1.2, loading all IPSEC SAs
Feb 22 01:39:59 [IKEv1 DEBUG]: Group = 192.168.1.2, IP = 192.168.1.2, Generating Quick Mode Key!
Feb 22 01:39:59 [IKEv1 DEBUG]: Group = 192.168.1.2, IP = 192.168.1.2, Generating Quick Mode Key!
Feb 22 01:39:59 [IKEv1]: Group = 192.168.1.2, IP = 192.168.1.2, Security negotiation complete for LAN-to-LAN Group (192.168.1.2) Initiator, Inbound SPI = 0x81004014, Outbound SPI = 0x07502a09
Feb 22 01:39:59 [IKEv1 DEBUG]: Group = 192.168.1.2, IP = 192.168.1.2, oakley con

```
structuring final quick mode
Feb 22 01:39:59 [IKEv1]: IP = 192.168.1.2, IKE_DECODE SENDING Message (msgid=270
72fbd) with payloads : HDR + HASH (8) + NONE (0) total length : 72
Feb 22 01:39:59 [IKEv1 DEBUG]: Group = 192.168.1.2, IP = 192.168.1.2, IKE got a
KEY_ADD msg for SA: SPI = 0x07502a09
Feb 22 01:39:59 [IKEv1 DEBUG]: Group = 192.168.1.2, IP = 192.168.1.2, Pitcher: r
eceived KEY_UPDATE, spi 0x81004014
Feb 22 01:39:59 [IKEv1 DEBUG]: Group = 192.168.1.2, IP = 192.168.1.2, Starting P
2 rekey timer: 3060 seconds.
Feb 22 01:39:59 [IKEv1]: Group = 192.168.1.2, IP = 192.168.1.2, PHASE 2 COMPLETE
D (msgid=27072fbd)
Feb 22 01:40:14 [IKEv1 DEBUG]: Group = 192.168.1.2, IP = 192.168.1.2, Sending ke
ep-alive of type DPD R-U-THERE (seq number 0x280e6479)
Feb 22 01:40:14 [IKEv1 DEBUG]: Group = 192.168.1.2, IP = 192.168.1.2, constructi
ng blank hash payload
Feb 22 01:40:14 [IKEv1 DEBUG]: Group = 192.168.1.2, IP = 192.168.1.2, constructi
ng qm hash payload
Feb 22 01:40:14 [IKEv1]: IP = 192.168.1.2, IKE_DECODE SENDING Message (msgid=8fb
a0b26) with payloads : HDR + HASH (8) + NOTIFY (11) + NONE (0) total length : 80
Feb 22 01:40:14 [IKEv1]: IP = 192.168.1.2, IKE_DECODE RECEIVED Message (msgid=7a
18c21c) with payloads : HDR + HASH (8) + NOTIFY (11) + NONE (0) total length : 8
0
Feb 22 01:40:14 [IKEv1 DEBUG]: Group = 192.168.1.2, IP = 192.168.1.2, processing
hash payload
Feb 22 01:40:14 [IKEv1 DEBUG]: Group = 192.168.1.2, IP = 192.168.1.2, processing
notify payload
Feb 22 01:40:14 [IKEv1 DEBUG]: Group = 192.168.1.2, IP = 192.168.1.2, Received k
eep-alive of type DPD R-U-THERE-ACK (seq number 0x280e6479)
```

pixfirewall#debug crypto ipsec 7

```
IPSEC: New embryonic SA created @ 0x01B84200,
  SCB: 0x028BB1D8,
  Direction: inbound
  SPI      : 0xAD0608C2
  Session ID: 0x00000004
  VPIF num : 0x00000002
  Tunnel type: l2l
  Protocol  : esp
  Lifetime  : 240 seconds
IPSEC: New embryonic SA created @ 0x029956A0,
  SCB: 0x0291BAD0,
  Direction: outbound
  SPI      : 0x9BEF30FB
  Session ID: 0x00000004
  VPIF num : 0x00000002
  Tunnel type: l2l
  Protocol  : esp
  Lifetime  : 240 seconds
IPSEC: Completed host OBSA update, SPI 0x9BEF30FB
IPSEC: Creating outbound VPN context, SPI 0x9BEF30FB
  Flags: 0x00000005
  SA    : 0x029956A0
  SPI   : 0x9BEF30FB
  MTU   : 1500 bytes
  VCID  : 0x00000000
  Peer  : 0x00000000
  SCB   : 0x0291BAD0
  Channel: 0x01727178
IPSEC: Completed outbound VPN context, SPI 0x9BEF30FB
  VPN handle: 0x0001C9AC
IPSEC: New outbound encrypt rule, SPI 0x9BEF30FB
  Src addr: 10.1.1.0
  Src mask: 255.255.255.0
  Dst addr: 10.2.1.0
  Dst mask: 255.255.255.0
```

```
Src ports
  Upper: 0
  Lower: 0
  Op   : ignore
Dst ports
  Upper: 0
  Lower: 0
  Op   : ignore
Protocol: 0
Use protocol: false
SPI: 0x00000000
Use SPI: false
IPSEC: Completed outbound encrypt rule, SPI 0x9BEF30FB
  Rule ID: 0x029197A8
IPSEC: New outbound permit rule, SPI 0x9BEF30FB
  Src addr: 172.16.1.1
  Src mask: 255.255.255.255
  Dst addr: 192.168.1.2
  Dst mask: 255.255.255.255
  Src ports
    Upper: 0
    Lower: 0
    Op   : ignore
  Dst ports
    Upper: 0
    Lower: 0
    Op   : ignore
  Protocol: 50
  Use protocol: true
  SPI: 0x9BEF30FB
  Use SPI: true
IPSEC: Completed outbound permit rule, SPI 0x9BEF30FB
  Rule ID: 0x02996888
IPSEC: Completed host IBSA update, SPI 0xAD0608C2
IPSEC: Creating inbound VPN context, SPI 0xAD0608C2
  Flags: 0x00000006
  SA   : 0x01B84200
  SPI  : 0xAD0608C2
  MTU  : 0 bytes
  VCID : 0x00000000
  Peer : 0x0001C9AC
  SCB  : 0x028BB1D8
  Channel: 0x01727178
IPSEC: Completed inbound VPN context, SPI 0xAD0608C2
  VPN handle: 0x00020724
IPSEC: Updating outbound VPN context 0x0001C9AC, SPI 0x9BEF30FB
  Flags: 0x00000005
  SA   : 0x029956A0
  SPI  : 0x9BEF30FB
  MTU  : 1500 bytes
  VCID : 0x00000000
  Peer : 0x00020724
  SCB  : 0x0291BAD0
  Channel: 0x01727178
IPSEC: Completed outbound VPN context, SPI 0x9BEF30FB
  VPN handle: 0x0001C9AC
IPSEC: Completed outbound inner rule, SPI 0x9BEF30FB
  Rule ID: 0x029197A8
IPSEC: Completed outbound outer SPD rule, SPI 0x9BEF30FB
  Rule ID: 0x02996888
IPSEC: New inbound tunnel flow rule, SPI 0xAD0608C2
  Src addr: 10.2.1.0
  Src mask: 255.255.255.0
  Dst addr: 10.1.1.0
  Dst mask: 255.255.255.0
  Src ports
```

```
Upper: 0
Lower: 0
Op   : ignore
Dst ports
  Upper: 0
  Lower: 0
  Op   : ignore
Protocol: 0
Use protocol: false
SPI: 0x00000000
Use SPI: false
IPSEC: Completed inbound tunnel flow rule, SPI 0xAD0608C2
  Rule ID: 0x02918E30
IPSEC: New inbound decrypt rule, SPI 0xAD0608C2
  Src addr: 192.168.1.2
  Src mask: 255.255.255.255
  Dst addr: 172.16.1.1
  Dst mask: 255.255.255.255
  Src ports
    Upper: 0
    Lower: 0
    Op   : ignore
  Dst ports
    Upper: 0
    Lower: 0
    Op   : ignore
  Protocol: 50
  Use protocol: true
  SPI: 0xAD0608C2
  Use SPI: true
IPSEC: Completed inbound decrypt rule, SPI 0xAD0608C2
  Rule ID: 0x02997CD0
IPSEC: New inbound permit rule, SPI 0xAD0608C2
  Src addr: 192.168.1.2
  Src mask: 255.255.255.255
  Dst addr: 172.16.1.1
  Dst mask: 255.255.255.255
  Src ports
    Upper: 0
    Lower: 0
    Op   : ignore
  Dst ports
    Upper: 0
    Lower: 0
    Op   : ignore
  Protocol: 50
  Use protocol: true
  SPI: 0xAD0608C2
  Use SPI: true
IPSEC: Completed inbound permit rule, SPI 0xAD0608C2
  Rule ID: 0x029964F0
```

Remote IOS Router – debug Output

```
Router#debug crypto isakmp
*Feb 22 13:51:57.319: ISAKMP (0:0): received packet from 172.16.1.1 dport 500 sport 500 Global (N) NEW SA
*Feb 22 13:51:57.319: ISAKMP: Created a peer struct for 172.16.1.1, peer port 500
*Feb 22 13:51:57.319: ISAKMP: New peer created peer = 0x64C2864C peer_handle = 0x80000005
*Feb 22 13:51:57.319: ISAKMP: Locking peer struct 0x64C2864C, IKE refcount 1 for crypto_isakmp_process_block
*Feb 22 13:51:57.319: ISAKMP: local port 500, remote port 500
```

*Feb 22 13:51:57.323: insert sa successfully sa = 65166F40
*Feb 22 13:51:57.323: ISAKMP:(0:0:N/A:0):Input = IKE_MSG_FROM_PEER, IKE_MM_EXCH
*Feb 22 13:51:57.323: ISAKMP:(0:0:N/A:0):Old State = IKE_READY New State = IKE_R_MM1

*Feb 22 13:51:57.323: ISAKMP:(0:0:N/A:0): processing SA payload. message ID = 0
*Feb 22 13:51:57.327: ISAKMP:(0:0:N/A:0): processing vendor id payload
*Feb 22 13:51:57.327: ISAKMP:(0:0:N/A:0): vendor ID seems Unity/DPD but major 194 mismatch
*Feb 22 13:51:57.327: ISAKMP:(0:0:N/A:0):found peer pre-shared key matching 172.16.1.1
*Feb 22 13:51:57.327: ISAKMP:(0:0:N/A:0): local preshared key found
*Feb 22 13:51:57.327: ISAKMP : Scanning profiles for xauth ...
*Feb 22 13:51:57.327: ISAKMP:(0:0:N/A:0):Checking ISAKMP transform 1 against priority 10 policy
*Feb 22 13:51:57.327: ISAKMP: default group 1
*Feb 22 13:51:57.327: ISAKMP: encryption DES-CBC
*Feb 22 13:51:57.327: ISAKMP: hash MD5
*Feb 22 13:51:57.327: ISAKMP: auth pre-share
*Feb 22 13:51:57.327: ISAKMP: life type in seconds
*Feb 22 13:51:57.327: ISAKMP: life duration (VPI) of 0x0 0x1 0x51 0x80
*Feb 22 13:51:57.331: ISAKMP:(0:0:N/A:0):atts are acceptable. Next payload is 3
*Feb 22 13:51:57.415: ISAKMP:(0:1:SW:1): processing vendor id payload
*Feb 22 13:51:57.415: ISAKMP:(0:1:SW:1): vendor ID seems Unity/DPD but major 194 mismatch
*Feb 22 13:51:57.419: ISAKMP:(0:1:SW:1):Input = IKE_MSG_INTERNAL, IKE_PROCESS_MAIN_MODE
*Feb 22 13:51:57.419: ISAKMP:(0:1:SW:1):Old State = IKE_R_MM1 New State = IKE_R_MM1

*Feb 22 13:51:57.423: ISAKMP:(0:1:SW:1): sending packet to 172.16.1.1 my_port 500 peer_port 500 (R) MM_SA_SETUP
*Feb 22 13:51:57.423: ISAKMP:(0:1:SW:1):Input = IKE_MSG_INTERNAL, IKE_PROCESS_COMPLETE
*Feb 22 13:51:57.423: ISAKMP:(0:1:SW:1):Old State = IKE_R_MM1 New State = IKE_R_MM2

*Feb 22 13:51:57.427: ISAKMP (0:134217729): received packet from 172.16.1.1 dport 500 sport 500 Global (R) MM_SA_SETUP
*Feb 22 13:51:57.427: ISAKMP:(0:1:SW:1):Input = IKE_MSG_FROM_PEER, IKE_MM_EXCH
*Feb 22 13:51:57.431: ISAKMP:(0:1:SW:1):Old State = IKE_R_MM2 New State = IKE_R_MM3

*Feb 22 13:51:57.431: ISAKMP:(0:1:SW:1): processing KE payload. message ID = 0
*Feb 22 13:51:57.539: ISAKMP:(0:1:SW:1): processing NONCE payload. message ID = 0
*Feb 22 13:51:57.539: ISAKMP:(0:1:SW:1):found peer pre-shared key matching 172.16.1.1
*Feb 22 13:51:57.543: ISAKMP:(0:1:SW:1):SKEYID state generated
*Feb 22 13:51:57.543: ISAKMP:(0:1:SW:1): processing vendor id payload
*Feb 22 13:51:57.543: ISAKMP:(0:1:SW:1): vendor ID is Unity
*Feb 22 13:51:57.543: ISAKMP:(0:1:SW:1): processing vendor id payload
*Feb 22 13:51:57.543: ISAKMP:(0:1:SW:1): vendor ID seems Unity/DPD but major 46 mismatch
*Feb 22 13:51:57.543: ISAKMP:(0:1:SW:1): vendor ID is XAUTH
*Feb 22 13:51:57.543: ISAKMP:(0:1:SW:1): processing vendor id payload
*Feb 22 13:51:57.547: ISAKMP:(0:1:SW:1): speaking to another IOS box!
*Feb 22 13:51:57.547: ISAKMP:(0:1:SW:1): processing vendor id payload
*Feb 22 13:51:57.547: ISAKMP:(0:1:SW:1):vendor ID seems Unity/DPD but hash mismatch
*Feb 22 13:51:57.547: ISAKMP:(0:1:SW:1):Input = IKE_MSG_INTERNAL, IKE_PROCESS_MAIN_MODE
*Feb 22 13:51:57.547: ISAKMP:(0:1:SW:1):Old State = IKE_R_MM3 New State = IKE_R_MM3

*Feb 22 13:51:57.551: ISAKMP:(0:1:SW:1): sending packet to 172.16.1.1 my_port 500

0 peer_port 500 (R) MM_KEY_EXCH
*Feb 22 13:51:57.551: ISAKMP:(0:1:SW:1):Input = IKE_MSG_INTERNAL, IKE_PROCESS_C
COMPLETE
*Feb 22 13:51:57.551: ISAKMP:(0:1:SW:1):Old State = IKE_R_MM3 New State = IKE_R
_MM4

*Feb 22 13:51:57.559: ISAKMP (0:134217729): received packet from 172.16.1.1 dpor
t 500 sport 500 Global (R) MM_KEY_EXCH
*Feb 22 13:51:57.559: ISAKMP:(0:1:SW:1):Input = IKE_MSG_FROM_PEER, IKE_MM_EXCH
*Feb 22 13:51:57.559: ISAKMP:(0:1:SW:1):Old State = IKE_R_MM4 New State = IKE_R
_MM5

*Feb 22 13:51:57.563: ISAKMP:(0:1:SW:1): processing ID payload. message ID = 0
*Feb 22 13:51:57.563: ISAKMP (0:134217729): ID payload
next-payload : 8
type : 1
address : 172.16.1.1
protocol : 17
port : 500
length : 12
*Feb 22 13:51:57.563: ISAKMP:(0:1:SW:1):: peer matches *none* of the profiles
*Feb 22 13:51:57.563: ISAKMP:(0:1:SW:1): processing HASH payload. message ID = 0
*Feb 22 13:51:57.567: ISAKMP:received payload type 17
*Feb 22 13:51:57.567: ISAKMP:(0:1:SW:1): processing vendor id payload
*Feb 22 13:51:57.567: ISAKMP:(0:1:SW:1): vendor ID is DPD
*Feb 22 13:51:57.567: ISAKMP:(0:1:SW:1):SA authentication status:
authenticated
*Feb 22 13:51:57.567: ISAKMP:(0:1:SW:1):SA has been authenticated with 172.16.1.
1
*Feb 22 13:51:57.567: ISAKMP: Trying to insert a peer 192.168.1.2/172.16.1.1/500
/, and inserted successfully 64C2864C.
*Feb 22 13:51:57.567: ISAKMP:(0:1:SW:1):Input = IKE_MSG_INTERNAL, IKE_PROCESS_M
AIN_MODE
*Feb 22 13:51:57.567: ISAKMP:(0:1:SW:1):Old State = IKE_R_MM5 New State = IKE_R
_MM5

*Feb 22 13:51:57.571: ISAKMP:(0:1:SW:1):SA is doing pre-shared key authenticatio
n using id type ID_IPV4_ADDR
*Feb 22 13:51:57.571: ISAKMP (0:134217729): ID payload
next-payload : 8
type : 1
address : 192.168.1.2
protocol : 17
port : 500
length : 12
*Feb 22 13:51:57.571: ISAKMP:(0:1:SW:1):Total payload length: 12
*Feb 22 13:51:57.575: ISAKMP:(0:1:SW:1): sending packet to 172.16.1.1 my_port 50
0 peer_port 500 (R) MM_KEY_EXCH
*Feb 22 13:51:57.575: ISAKMP:(0:1:SW:1):Input = IKE_MSG_INTERNAL, IKE_PROCESS_C
COMPLETE
*Feb 22 13:51:57.575: ISAKMP:(0:1:SW:1):Old State = IKE_R_MM5 New State = IKE_P
1_COMPLETE

*Feb 22 13:51:57.579: ISAKMP:(0:1:SW:1):Input = IKE_MSG_INTERNAL, IKE_PHASE1_CO
MPLETE
*Feb 22 13:51:57.579: ISAKMP:(0:1:SW:1):Old State = IKE_P1_COMPLETE New State =
IKE_P1_COMPLETE

*Feb 22 13:51:57.583: ISAKMP (0:134217729): received packet from 172.16.1.1 dpor
t 500 sport 500 Global (R) QM_IDLE
*Feb 22 13:51:57.583: ISAKMP: set new node 328663488 to QM_IDLE
*Feb 22 13:51:57.587: ISAKMP:(0:1:SW:1): processing HASH payload. message ID = 3
28663488
*Feb 22 13:51:57.587: ISAKMP:(0:1:SW:1): processing SA payload. message ID = 328
663488
*Feb 22 13:51:57.587: ISAKMP:(0:1:SW:1):Checking IPsec proposal 1

```

*Feb 22 13:51:57.587: ISAKMP: transform 1, ESP_DES
*Feb 22 13:51:57.591: ISAKMP:   attributes in transform:
*Feb 22 13:51:57.591: ISAKMP:     SA life type in seconds
*Feb 22 13:51:57.591: ISAKMP:     SA life duration (basic) of 28800
*Feb 22 13:51:57.591: ISAKMP:     SA life type in kilobytes
*Feb 22 13:51:57.591: ISAKMP:     SA life duration (VPI) of 0x0 0x46 0x50 0x0
*Feb 22 13:51:57.595: ISAKMP:     encaps is 1 (Tunnel)
*Feb 22 13:51:57.595: ISAKMP:     authenticator is HMAC-MD5
*Feb 22 13:51:57.595: ISAKMP:(0:1:SW:1):atts are acceptable.
*Feb 22 13:51:57.595: ISAKMP:(0:1:SW:1): processing NONCE payload. message ID =
328663488
*Feb 22 13:51:57.595: ISAKMP:(0:1:SW:1): processing ID payload. message ID = 328
663488
*Feb 22 13:51:57.599: ISAKMP:(0:1:SW:1): processing ID payload. message ID = 328
663488
*Feb 22 13:51:57.599: ISAKMP:(0:1:SW:1): processing NOTIFY_INITIAL_CONTACT proto
col 1
    spi 0, message ID = 328663488, sa = 65166F40
*Feb 22 13:51:57.599: ISAKMP:(0:1:SW:1):SA authentication status:
    authenticated
*Feb 22 13:51:57.599: ISAKMP:(0:1:SW:1): Process initial contact,
bring down existing phase 1 and 2 SA's with local 192.168.1.2 remote 172.16.1.1
remote port 500
*Feb 22 13:51:57.599: ISAKMP:(0:1:SW:1): asking for 1 spis from ipsec
*Feb 22 13:51:57.603: ISAKMP:(0:1:SW:1):Node 328663488, Input = IKE_MESG_FROM_PE
ER, IKE_QM_EXCH
*Feb 22 13:51:57.603: ISAKMP:(0:1:SW:1):Old State = IKE_QM_READY  New State = IK
E_QM_SPI_STARVE
*Feb 22 13:51:57.603: ISAKMP: received ke message (2/1)
*Feb 22 13:51:57.611: ISAKMP: Locking peer struct 0x64C2864C, IPSEC refcount 1 f
or for stuff_ke
*Feb 22 13:51:57.611: ISAKMP:(0:1:SW:1): Creating IPsec SAs
*Feb 22 13:51:57.611:     inbound SA from 172.16.1.1 to 192.168.1.2 (f/i) 0
/ 0
    (proxy 10.1.1.0 to 10.2.1.0)
*Feb 22 13:51:57.611:     has spi 0x1BB01835 and conn_id 0 and flags 2
*Feb 22 13:51:57.611:     lifetime of 28800 seconds
*Feb 22 13:51:57.611:     lifetime of 4608000 kilobytes
*Feb 22 13:51:57.611:     has client flags 0x0
*Feb 22 13:51:57.611:     outbound SA from 192.168.1.2 to 172.16.1.1 (f/i) 0
/0
    (proxy 10.2.1.0 to 10.1.1.0)
*Feb 22 13:51:57.611:     has spi 1995623635 and conn_id 0 and flags A
*Feb 22 13:51:57.611:     lifetime of 28800 seconds
*Feb 22 13:51:57.611:     lifetime of 4608000 kilobytes
*Feb 22 13:51:57.611:     has client flags 0x0
*Feb 22 13:51:57.615: ISAKMP:(0:1:SW:1): sending packet to 172.16.1.1 my_port 50
0 peer_port 500 (R) QM_IDLE
*Feb 22 13:51:57.615: ISAKMP:(0:1:SW:1):Node 328663488, Input = IKE_MESG_FROM_IP
SEC, IKE_SPI_REPLY
*Feb 22 13:51:57.615: ISAKMP:(0:1:SW:1):Old State = IKE_QM_SPI_STARVE  New State
= IKE_QM_R_QM2
*Feb 22 13:51:57.619: ISAKMP: Locking peer struct 0x64C2864C, IPSEC refcount 2 f
or from create_transforms
*Feb 22 13:51:57.619: ISAKMP: Unlocking IPSEC struct 0x64C2864C from create_tran
sforms, count 1
*Feb 22 13:51:57.631: ISAKMP (0:134217729): received packet from 172.16.1.1 dpor
t 500 sport 500 Global (R) QM_IDLE
*Feb 22 13:51:57.635: ISAKMP:(0:1:SW:1):deleting node 328663488 error FALSE reas
on "QM done (await)"
*Feb 22 13:51:57.635: ISAKMP:(0:1:SW:1):Node 328663488, Input = IKE_MESG_FROM_PE
ER, IKE_QM_EXCH
*Feb 22 13:51:57.635: ISAKMP:(0:1:SW:1):Old State = IKE_QM_R_QM2  New State = IK
E_QM_PHASE2_COMPLETE

```

Router#**debug crypto ipsec**

```

*Feb 22 13:57:41.187: IPSEC(validate_proposal_request): proposal part #1,
  (key eng. msg.) INBOUND local= 192.168.1.2, remote= 172.16.1.1,
    local_proxy= 10.2.1.0/255.255.255.0/0/0 (type=4),
    remote_proxy= 10.1.1.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-des esp-md5-hmac (Tunnel),
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2
*Feb 22 13:57:41.187: Crypto mapdb : proxy_match
  src addr      : 10.2.1.0
  dst addr      : 10.1.1.0
  protocol      : 0
  src port      : 0
  dst port      : 0
*Feb 22 13:57:41.191: IPSEC(key_engine): got a queue event with 1 kei messages
*Feb 22 13:57:41.191: IPSEC(key_engine): got a queue event with 1 kei messages
*Feb 22 13:57:41.191: IPSEC(spi_response): getting spi 2616144123 for SA
  from 192.168.1.2 to 172.16.1.1 for prot 3
*Feb 22 13:57:41.199: IPSEC(key_engine): got a queue event with 2 kei messages
*Feb 22 13:57:41.199: IPSEC(initialize_sas): ,
  (key eng. msg.) INBOUND local= 192.168.1.2, remote= 172.16.1.1,
    local_proxy= 10.2.1.0/255.255.255.0/0/0 (type=4),
    remote_proxy= 10.1.1.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-des esp-md5-hmac (Tunnel),
    lifedur= 28800s and 4608000kb,
    spi= 0x9BEF30FB(2616144123), conn_id= 0, keysize= 0, flags= 0x2
*Feb 22 13:57:41.203: IPSEC(initialize_sas): ,
  (key eng. msg.) OUTBOUND local= 192.168.1.2, remote= 172.16.1.1,
    local_proxy= 10.2.1.0/255.255.255.0/0/0 (type=4),
    remote_proxy= 10.1.1.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-des esp-md5-hmac (Tunnel),
    lifedur= 28800s and 4608000kb,
    spi= 0xAD0608C2(2902853826), conn_id= 0, keysize= 0, flags= 0xA
*Feb 22 13:57:41.203: Crypto mapdb : proxy_match
  src addr      : 10.2.1.0
  dst addr      : 10.1.1.0
  protocol      : 0
  src port      : 0
  dst port      : 0
*Feb 22 13:57:41.203: IPsec: Flow_switching Allocated flow for sibling 80000005
*Feb 22 13:57:41.207: IPSEC(policy_db_add_ident): src 10.2.1.0, dest 10.1.1.0, d
est_port 0

*Feb 22 13:57:41.207: IPSEC(create_sa): sa created,
  (sa) sa_dest= 192.168.1.2, sa_proto= 50,
    sa_spi= 0x9BEF30FB(2616144123),
    sa_trans= esp-des esp-md5-hmac , sa_conn_id= 2002
*Feb 22 13:57:41.207: IPSEC(create_sa): sa created,
  (sa) sa_dest= 172.16.1.1, sa_proto= 50,
    sa_spi= 0xAD0608C2(2902853826),
    sa_trans= esp-des esp-md5-hmac , sa_conn_id= 2001
*Feb 22 13:57:41.475: IPSEC(key_engine): got a queue event with 1 kei messages
*Feb 22 13:57:41.475: IPSEC(key_engine_enable_outbound): rec'd enable notify fro
m ISAKMP
*Feb 22 13:57:41.475: IPSEC(key_engine_enable_outbound): enable SA with spi 2902
853826/50

```

NetPro Discussion Forums – Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

Security: Intrusion Detection [Systems]
Security: AAA
Security: General
Security: Firewalling

Related Information

- [Cisco PIX 500 Series Security Appliances](#)
- [Cisco ASA 5500 Series Adaptive Security Appliances](#)
- [Cisco Router Product Support](#)
- [Documentation for Cisco PIX Security Appliance OS Software](#)
- [Cisco Secure PIX Firewall Command References](#)
- [IPSec Negotiation/IKE Protocols Support Page](#)
- [Requests for Comments \(RFCs\)](#)
- [Technical Support & Documentation – Cisco Systems](#)

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

© 2008 – 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Oct 10, 2008

Document ID: 82077
