Troubleshoot IOS IKEv2 Debugs for Site-to-Site VPN with PSKs

Contents

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

Background Information

Core Issue

Router Configuration

Troubleshoot

- Router Debugs
- CHILD_SA Debugs

Tunnel Verification

- ISAKMP
- IPsec

Related Information

Introduction

This document describes Internet Key Exchange version 2 (IKEv2) debugs on Cisco IOS® when an unshared key (PSK) is used.

Prerequisites

Requirements

Cisco recommends that you have knowledge of the packet exchange for IKEv2. For more information, refer to IKEv2 Packet Exchange and Protocol Level Debugging.

Components Used

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

- Internet Key Exchange Version 2 (IKEv2)
- Cisco IOS 15.1(1)T or 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, ensure that you understand the potential impact of any command.

Conventions

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

Background Information

This document provides information on how to translate certain debug lines in a configuration.

Core Issue

The packet exchange in IKEv2 is radically different from packet exchange in IKEv1. In IKEv1 there was a clearly demarcated phase1 exchange that consisted of six (6) packets with a phase 2 exchange afterward that consisted of three (3) packets; the IKEv2 exchange is variable. For more information on the differences and an explanation of the packet exchange, again, refer to IKEv2 Packet Exchange and Protocol Level Debugging.

Router Configuration

This section lists the configurations used in this document.

Router 1

```
interface Loopback0
 ip address 192.168.1.1 255.255.255.0
!
interface Tunnel0
 ip address 172.16.0.101 255.255.255.0
 tunnel source Ethernet0/0
 tunnel mode ipsec ipv4
 tunnel destination 10.0.0.2
 tunnel protection ipsec profile phse2-prof
!
interface Ethernet0/0
 ip address 10.0.0.1 255.255.255.0

crypto ikev2 proposal PHASE1-prop
 encryption 3des aes-cbc-128
 integrity sha1
 group 2
!
crypto ikev2 policy site-pol
 proposal PHASE1-prop
!
crypto ikev2 keyring KEYRNG
 peer peer1
  address 10.0.0.2 255.255.255.0
  hostname host1
  pre-shared-key local cisco
  pre-shared-key remote cisco
 !
crypto ikev2 profile IKEV2-SETUP
 match identity remote address 0.0.0.0
 authentication remote pre-share
 authentication local pre-share
 keyring local KEYRNG
 lifetime 120
!
```

```
crypto ipsec transform-set TS esp-3des esp-sha-hmac
!
crypto ipsec profile phse2-prof
 set transform-set TS
 set ikev2-profile IKEV2-SETUP
!
ip route 0.0.0.0 0.0.0.0 10.0.0.2
ip route 192.168.2.1 255.255.255.255 Tunnel0
```

Router 2

```
crypto ikev2 proposal PHASE1-prop
 encryption 3des aes-cbc-128
 integrity sha1
 group 2
!
crypto ikev2 keyring KEYRNG
 peer peer2
  address 10.0.0.1 255.255.255.0
  hostname host2
  pre-shared-key local cisco
  pre-shared-key remote cisco
 !
crypto ikev2 profile IKEV2-SETUP
 match identity remote address 0.0.0.0
 authentication remote pre-share
 authentication local pre-share
 keyring local KEYRNG
 lifetime 120
!
crypto ipsec transform-set TS esp-3des esp-sha-hmac
!
!
crypto ipsec profile phse2-prof
 set transform-set TS
 set ikev2-profile IKEV2-SETUP
!
interface Loopback0
 ip address 192.168.2.1 255.255.255.0
!
interface Ethernet0/0
 ip address 10.0.0.2 255.255.255.0
!
interface Tunnel0
 ip address 172.16.0.102 255.255.255.0
 tunnel source Ethernet0/0
 tunnel mode ipsec ipv4
 tunnel destination 10.0.0.1
 tunnel protection ipsec profile phse2-prof
!
ip route 0.0.0.0 0.0.0.0 10.0.0.1
ip route 192.168.1.1 255.255.255.255 Tunnel0
```

Troubleshoot

Router Debugs

These debug commands are used in this document:

```
deb crypto ikev2 packet
deb crypto ikev2 internal
```

Router 1 (Initiator) Message Description	Debugs	Router 2 (Re Message De
Router 1 receives a packet that matches the crypto acl for peer ASA 10.0.0.2. Initiates SA creation	*Nov 11 20:28:34.003: IKEv2:Got a packet from dispatcher *Nov 11 20:28:34.003: IKEv2:Processing an item off the pak queue *Nov 11 19:30:34.811: IKEv2:% Getting preshared key by address 10.0.0.2 *Nov 11 19:30:34.811: IKEv2:Adding Proposal PHASE1-prop to toolkit policyle *Nov 11 19:30:34.811: IKEv2:(1): Choosing IKE profile IKEV2-SETUP *Nov 11 19:30:34.811: IKEv2:New ikev2 sa request admitted *Nov 11 19:30:34.811: IKEv2:Incrementing outgoing negotiating sa count by one	
First pair of messages is the IKE_SA_INIT exchange. These messages negotiate cryptographic algorithms, exchange nonces, and do a Diffie-Hellman exchange. **Relevant Configuration:** `crypto ikev2 proposal PHASE1-prop encryption 3des aes-cbc-128 integrity sha1 group 2crypto ikev2 keyring KEYRNG peer peer1 address 10.0.0.2 255.255.255.0 hostname host1 pre-shared-key local cisco pre-shared-key remote cisco`	*Nov 11 19:30:34.811: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000 (I) MsgID = 00000000 CurState: IDLE Event: EV_INIT_SA *Nov 11 19:30:34.811: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000 (I) MsgID = 00000000 CurState: I_BLD_INIT Event: EV_GET_IKE_POLICY *Nov 11 19:30:34.811: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000 (I) MsgID = 00000000 CurState: I_BLD_INIT Event:**EV_SET_POLICY** *Nov 11 19:30:34.811: IKEv2:(SA ID = 1):Setting configured policies *Nov 11 19:30:34.811: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000 (I) MsgID = 00000000 CurState: I_BLD_INIT Event: EV_CHK_AUTH4PKI *Nov 11 19:30:34.811: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000 (I) MsgID = 00000000 CurState: I_BLD_INIT Event:**EV_GEN_DH_KEY** *Nov 11 19:30:34.811: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000 (I) MsgID = 00000000 CurState: I_BLD_INIT Event: EV_NO_EVENT *Nov 11 19:30:34.811: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000 (I) MsgID = 00000000 CurState: I_BLD_INIT Event: EV_OK_RECD_DH_PUBKEY_RESP *Nov 11 19:30:34.811: IKEv2:(SA ID = 1):Action: Action_Null *Nov 11 19:30:34.811: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000 (I) MsgID = 00000000 CurState: I_BLD_INIT Event: EV_GET_CONFIG_MODE *Nov 11 19:30:34.811: IKEv2:IKEv2 initiator - no config data to send in IKE_SA_INIT exch *Nov 11 19:30:34.811: IKEv2:No config data to send to toolkit: *Nov 11 19:30:34.811: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000 (I) MsgID =	

	00000000 CurState: I_BLD_INIT Event: EV_BLD_MSG *Nov 11 19:30:34.811: IKEv2:Construct Vendor Specific Payload: DELETE-REASON *Nov 11 19:30:34.811: IKEv2:Construct Vendor Specific Payload: (CUSTOM) *Nov 11 19:30:34.811: IKEv2:Construct Notify Payload: NAT_DETECTION_SOURCE_IP *Nov 11 19:30:34.811: IKEv2:Construct Notify Payload: NAT_DETECTION_DESTINATION_IP	
Initiator building IKE_INIT_SA packet. It contains: ISAKMP Header (SPI/version/flags), SAi1 (cryptographic algorithm that IKE initiator supports), KEi (DH public Key value of the initiator), and N (Initiator Nonce).	*Nov 11 19:30:34.811: **IKEv2:(SA ID = 1)**:Next payload: SA, version: 2.0 Exchange type: **IKE_SA_INIT,** flags: **INITIATOR** Message id: 0, length: 344 Payload contents: **SA** Next payload: KE, reserved: 0x0, length: 56 last proposal: 0x0, reserved: 0x0, length: 52 Proposal: 1, Protocol id: IKE, SPI size: 0, #trans: 5 last transform: 0x3, reserved: 0x0: length: 8 type: 1, reserved: 0x0, id: 3DES last transform: 0x3, reserved: 0x0: length: 12 type: 1, reserved: 0x0, id: AES-CBC last transform: 0x3, reserved: 0x0: length: 8 type: 2, reserved: 0x0, id: SHA1 last transform: 0x3, reserved: 0x0: length: 8 type: 3, reserved: 0x0, id: SHA96 last transform: 0x0, reserved: 0x0: length: 8 type: 4, reserved: 0x0, id: DH_GROUP_1024_MODP/Group 2 **KE** Next payload: N, reserved: 0x0, length: 136 DH group: 2, Reserved: 0x0 N Next payload: VID, reserved: 0x0, length: 24 VID Next payload: VID, reserved: 0x0, length: 23 VID Next payload: NOTIFY, reserved: 0x0, length: 21 NOTIFY(NAT_DETECTION_SOURCE_IP) Next payload: NOTIFY, reserved: 0x0, length: 28 Security protocol id: IKE, spi size: 0, type: NAT_DETECTION_SOURCE_IP NOTIFY(NAT_DETECTION_DESTINATION_IP) Next payload: NONE, reserved: 0x0, length: 28 Security protocol id: IKE, spi size: 0, type: NAT_DETECTION_DESTINATION_IP	
----------Initiator sent IKE_INIT_SA ---------->		
	*Nov 11 19:30:34.814: IKEv2:Got a packet from dispatcher *Nov 11 19:30:34.814: IKEv2:Processing an item off the pak queue *Nov 11 19:30:34.814: IKEv2:New ikev2 sa request admitted *Nov 11 19:30:34.814: IKEv2:Incrementing incoming negotiating sa count by one	Responder re IKE_INIT_S
	*Nov 11 19:30:34.814: IKEv2:Next payload: SA, version: 2.0 Exchange type: IKE_SA_INIT, flags: INITIATOR Message id: 0, length: 344 Payload contents: SA Next payload: KE, reserved: 0x0, length: 56 last proposal: 0x0, reserved: 0x0, length: 52 Proposal: 1, Protocol id: IKE, SPI size: 0, #trans: 5 last transform: 0x3,	Responder in creation for t

	reserved: 0x0: length: 8 type: 1, reserved: 0x0, id: 3DES last transform: 0x3, reserved: 0x0: length: 12 type: 1, reserved: 0x0, id: AES-CBC last transform: 0x3, reserved: 0x0: length: 8 type: 2, reserved: 0x0, id: SHA1 last transform: 0x3, reserved: 0x0: length: 8 type: 3, reserved: 0x0, id: SHA96 last transform: 0x0, reserved: 0x0: length: 8 type: 4, reserved: 0x0, id: DH_GROUP_1024_MODP/Group 2 KE Next payload: N, reserved: 0x0, length: 136 DH group: 2, Reserved: 0x0 N Next payload: VID, reserved: 0x0, length: 24 *Nov 11 19:30:34.814: IKEv2:Parse Vendor Specific Payload: CISCO-DELETE-REASON VID Next payload: VID, reserved: 0x0, length: 23 *Nov 11 19:30:34.814: IKEv2:Parse Vendor Specific Payload: (CUSTOM) VID Next payload: NOTIFY, reserved: 0x0, length: 21 *Nov 11 19:30:34.814: IKEv2:Parse Notify Payload: NAT_DETECTION_SOURCE_IP NOTIFY(NAT_DETECTION_SOURCE_IP) Next payload: NOTIFY, reserved: 0x0, length: 28 Security protocol id: IKE, spi size: 0, type: NAT_DETECTION_SOURCE_IP *Nov 11 19:30:34.814: IKEv2:Parse Notify Payload: NAT_DETECTION_DESTINATION_IP NOTIFY(NAT_DETECTION_DESTINATION_IP) Next payload: NONE, reserved: 0x0, length: 28 Security protocol id: IKE, spi size: 0, type: NAT_DETECTION_DESTINATION_IP	
	*Nov 11 19:30:34.814: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: IDLE Event:**EV_RECV_INIT** *Nov 11 19:30:34.814: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: R_INIT Event:**EV_VERIFY_MSG** *Nov 11 19:30:34.814: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: R_INIT Event:**EV_INSERT_SA** *Nov 11 19:30:34.814: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: R_INIT Event:**EV_GET_IKE_POLICY** *Nov 11 19:30:34.814: IKEv2:Adding Proposal default to toolkit policy *Nov 11 19:30:34.814: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: R_INIT Event:**EV_PROC_MSG** *Nov 11 19:30:34.814: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: R_INIT Event: EV_DETECT_NAT *Nov 11 19:30:34.814: IKEv2:(SA ID = 1):Process NAT discovery notify *Nov 11 19:30:34.814: IKEv2:(SA ID = 1):Processing nat detect src notify	Responder ve processes the IKE_INIT me (1) Chooses c suite from tho offered by the (2) computes DH secret key it computes a value, from w keys can be d this IKE_SA. the headers o messages that after are encr authenticated keys used for encryption an integrity prote derived from and are know

*Nov 11 19:30:34.814: IKEv2:(SA ID = 1):Remote address matched
*Nov 11 19:30:34.814: IKEv2:(SA ID = 1):Processing nat detect dst notify
*Nov 11 19:30:34.814: IKEv2:(SA ID = 1):Local address matched
*Nov 11 19:30:34.814: IKEv2:(SA ID = 1):No NAT found
*Nov 11 19:30:34.814: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: R_INIT Event: EV_CHK_CONFIG_MODE
*Nov 11 19:30:34.814: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: R_BLD_INIT Event: EV_SET_POLICY
*Nov 11 19:30:34.814: IKEv2:(SA ID = 1):**Setting configured policies**
*Nov 11 19:30:34.814: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: R_BLD_INIT Event: EV_CHK_AUTH4PKI
*Nov 11 19:30:34.814: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: R_BLD_INIT Event: EV_PKI_SESH_OPEN
*Nov 11 19:30:34.814: IKEv2:(SA ID = 1):Opening a PKI session
*Nov 11 19:30:34.815: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: R_BLD_INIT Event:**EV_GEN_DH_KEY**
*Nov 11 19:30:34.815: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: R_BLD_INIT Event: EV_NO_EVENT
*Nov 11 19:30:34.815: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: R_BLD_INIT Event:**EV_OK_RECD_DH_PUBKEY_RESP**
*Nov 11 19:30:34.815: IKEv2:(SA ID = 1):Action: Action_Null
*Nov 11 19:30:34.815: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: R_BLD_INIT Event:**EV_GEN_DH_SECRET**
*Nov 11 19:30:34.822: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: R_BLD_INIT Event: EV_NO_EVENT
*Nov 11 19:30:34.822: IKEv2:% **Getting preshared key by address 10.0.0.1**
*Nov 11 19:30:34.822: IKEv2:Adding Proposal default to toolkit policy
*Nov 11 19:30:34.822: IKEv2:(2): Choosing IKE profile IKEV2-SETUP
*Nov 11 19:30:34.822: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: R_BLD_INIT Event: EV_OK_RECD_DH_SECRET_RESP
*Nov 11 19:30:34.822: IKEv2:(SA ID = 1):Action: Action_Null
*Nov 11 19:30:34.822: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: R_BLD_INIT Event:**EV_GEN_SKEYID**
*Nov 11 19:30:34.822: IKEv2:(SA ID = 1):**Generate skeyid**
*Nov 11 19:30:34.822: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: R_BLD_INIT Event: EV_GET_CONFIG_MODE
*Nov 11 19:30:34.822: IKEv2:IKEv2 responder - no config data to send in IKE_SA_INIT exch

SK_e (encryp
SK_a (authen
SK_d is deriv
used for deriv
further keying
for CHILD_S
separate SK_
SK_a is comp
each direction

Relevant Configuratio

```
ikev2 propos
PHASE1-prop
encryption 3
cbc-128 inte
sha1 group 2
ikev2 keyrin
peer peer2 a
10.0.0.1
255.255.255.
hostname hos
shared-key l
cisco pre-sh
remote cisco
```

	*Nov 11 19:30:34.822: IKEv2:No config data to send to toolkit: *Nov 11 19:30:34.822: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: R_BLD_INIT Event: EV_BLD_MSG *Nov 11 19:30:34.822: IKEv2:Construct Vendor Specific Payload: DELETE-REASON *Nov 11 19:30:34.822: IKEv2:Construct Vendor Specific Payload: (CUSTOM) *Nov 11 19:30:34.822: IKEv2:Construct Notify Payload: NAT_DETECTION_SOURCE_IP *Nov 11 19:30:34.822: IKEv2:Construct Notify Payload: NAT_DETECTION_DESTINATION_IP *Nov 11 19:30:34.822: IKEv2:Construct Notify Payload: HTTP_CERT_LOOKUP_SUPPORTED	
	*Nov 11 19:30:34.822: IKEv2:(SA ID = 1):Next payload: SA, version: 2.0 Exchange type: **IKE_SA_INIT,** flags: **RESPONDER MSG-RESPONSE** Message id: 0, length: 449 Payload contents: **SA** Next payload: KE, reserved: 0x0, length: 48 last proposal: 0x0, reserved: 0x0, length: 44 Proposal: 1, Protocol id: IKE, SPI size: 0, #trans: 4 last transform: 0x3, reserved: 0x0: length: 12 type: 1, reserved: 0x0, id: AES-CBC last transform: 0x3, reserved: 0x0: length: 8 type: 2, reserved: 0x0, id: SHA1 last transform: 0x3, reserved: 0x0: length: 8 type: 3, reserved: 0x0, id: SHA96 last transform: 0x0, reserved: 0x0: length: 8 type: 4, reserved: 0x0, id: DH_GROUP_1024_MODP/Group 2 **KE** Next payload: N, reserved: 0x0, length: 136 DH group: 2, Reserved: 0x0 **N** Next payload: VID, reserved: 0x0, length: 24 VID Next payload: VID, reserved: 0x0, length: 23 VID Next payload: NOTIFY, reserved: 0x0, length: 21 NOTIFY(NAT_DETECTION_SOURCE_IP) Next payload: NOTIFY, reserved: 0x0, length: 28 Security protocol id: IKE, spi size: 0, type: NAT_DETECTION_SOURCE_IP NOTIFY(NAT_DETECTION_DESTINATION_IP) Next payload: CERTREQ, reserved: 0x0, length: 28 Security protocol id: IKE, spi size: 0, type: NAT_DETECTION_DESTINATION_IP CERTREQ Next payload: NOTIFY, reserved: 0x0, length: 105 Cert encoding Hash and URL of PKIX NOTIFY(HTTP_CERT_LOOKUP_SUPPORTED) Next payload: NONE, reserved: 0x0, length: 8 Security protocol id: IKE, spi size: 0, type: HTTP_CERT_LOOKUP_SUPPORTED	Router 2 buil responder me IKE_SA_INI exchange, wh received by A This packet c ISAKMP Hea version/flags) SAr1(cryptog algorithm tha responder cho KEr(DH publ value of the responder), ar Responder N
	*Nov 11 19:30:34.822: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID =	Router2 send responder me Router 1.

	00000000 CurState: INIT_DONE Event: EV_DONE *Nov 11 19:30:34.822: IKEv2:(SA ID = 1):Cisco DeleteReason Notify is enabled *Nov 11 19:30:34.822: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: INIT_DONE Event: EV_CHK4_ROLE *Nov 11 19:30:34.822: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: INIT_DONE Event:**EV_START_TMR** *Nov 11 19:30:34.822: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: R_WAIT_AUTH Event: EV_NO_EVENT *Nov 11 19:30:34.822: IKEv2:**New ikev2 sa request admitted** *Nov 11 19:30:34.822: IKEv2:**Incrementing outgoing negotiating sa count by one**		
<----------Responder sent IKE_INIT_SA ----------			
Router 1 receives the IKE_SA_INIT response packet from Router 2.	*Nov 11 19:30:34.823: IKEv2:Got a packet from dispatcher *Nov 11 19:30:34.823: IKEv2:Got a packet from dispatcher *Nov 11 19:30:34.823: IKEv2:Processing an item off the pak queue	I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: INIT_DONE Event:**EV_START_TMR**	Responder sta for Auth proc
Router1 verifies and processes the response: (1) The initiator DH secret key is computed, and (2) the initiator skeyid is also generated.	*Nov 11 19:30:34.823: IKEv2:(SA ID = 1):Next payload: SA, version: 2.0 Exchange type: IKE_SA_INIT, flags: **RESPONDER MSG-RESPONSE** Message id: 0, length: 449 Payload contents: **SA** Next payload: KE, reserved: 0x0, length: 48 last proposal: 0x0, reserved: 0x0, length: 44 Proposal: 1, Protocol id: IKE, SPI size: 0, #trans: 4 last transform: 0x3, reserved: 0x0: length: 12 type: 1, reserved: 0x0, id: AES-CBC last transform: 0x3, reserved: 0x0: length: 8 type: 2, reserved: 0x0, id: SHA1 last transform: 0x3, reserved: 0x0: length: 8 type: 3, reserved: 0x0, id: SHA96 last transform: 0x0, reserved: 0x0: length: 8 type: 4, reserved: 0x0, id: DH_GROUP_1024_MODP/Group 2 **KE** Next payload: N, reserved: 0x0, length: 136 DH group: 2, Reserved: 0x0 **N** Next payload: VID, reserved: 0x0, length: 24 *Nov 11 19:30:34.823: IKEv2:Parse Vendor Specific Payload: CISCO-DELETE-REASON VID Next payload: VID, reserved: 0x0, length: 23 *Nov 11 19:30:34.823: IKEv2:Parse Vendor Specific Payload: (CUSTOM) VID Next payload: NOTIFY, reserved: 0x0, length: 21		

*Nov 11 19:30:34.823: IKEv2:Parse Notify Payload:
NAT_DETECTION_SOURCE_IP
NOTIFY(NAT_DETECTION_SOURCE_IP) Next payload: NOTIFY,
reserved: 0x0, length: 28
   Security protocol id: IKE, spi size: 0, type:
NAT_DETECTION_SOURCE_IP

*Nov 11 19:30:34.824: IKEv2:Parse Notify Payload:
NAT_DETECTION_DESTINATION_IP
NOTIFY(NAT_DETECTION_DESTINATION_IP) Next payload:
CERTREQ, reserved: 0x0, length: 28
   Security protocol id: IKE, spi size: 0, type:
NAT_DETECTION_DESTINATION_IP
 CERTREQ Next payload: NOTIFY, reserved: 0x0, length: 105
   Cert encoding Hash and URL of PKIX

*Nov 11 19:30:34.824: IKEv2:Parse Notify Payload:
HTTP_CERT_LOOKUP_SUPPORTED
NOTIFY(HTTP_CERT_LOOKUP_SUPPORTED) Next payload: NONE,
reserved: 0x0, length: 8
   Security protocol id: IKE, spi size: 0, type:
HTTP_CERT_LOOKUP_SUPPORTED

*Nov 11 19:30:34.824: IKEv2:(SA ID = 1):SM Trace-> SA:
I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID =
00000000 CurState: I_WAIT_INIT Event: EV_RECV_INIT
*Nov 11 19:30:34.824: IKEv2:(SA ID = 1):Processing IKE_SA_INIT
message
*Nov 11 19:30:34.824: IKEv2:(SA ID = 1):SM Trace-> SA:
I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID =
00000000 CurState: I_PROC_INIT Event: EV_CHK4_NOTIFY
*Nov 11 19:30:34.824: IKEv2:(SA ID = 1):SM Trace-> SA:
I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID =
00000000 CurState: I_PROC_INIT Event: EV_VERIFY_MSG
*Nov 11 19:30:34.824: IKEv2:(SA ID = 1):SM Trace-> SA:
I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID =
00000000 CurState: I_PROC_INIT Event: EV_PROC_MSG
*Nov 11 19:30:34.824: IKEv2:(SA ID = 1):SM Trace-> SA:
I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID =
00000000 CurState: I_PROC_INIT Event: EV_DETECT_NAT
*Nov 11 19:30:34.824: IKEv2:(SA ID = 1):Process NAT discovery notify
*Nov 11 19:30:34.824: IKEv2:(SA ID = 1):Processing nat detect src notify
*Nov 11 19:30:34.824: IKEv2:(SA ID = 1):Remote address matched
*Nov 11 19:30:34.824: IKEv2:(SA ID = 1):Processing nat detect dst notify
*Nov 11 19:30:34.824: IKEv2:(SA ID = 1):Local address matched
*Nov 11 19:30:34.824: IKEv2:(SA ID = 1):No NAT found
*Nov 11 19:30:34.824: IKEv2:(SA ID = 1):SM Trace-> SA:
I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID =
00000000 CurState: I_PROC_INIT Event: EV_CHK_NAT_T
*Nov 11 19:30:34.824: IKEv2:(SA ID = 1):SM Trace-> SA:
I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID =
00000000 CurState: I_PROC_INIT Event: EV_CHK_CONFIG_MODE
*Nov 11 19:30:34.824: IKEv2:(SA ID = 1):SM Trace-> SA:

	I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState: INIT_DONE Event:**EV_GEN_DH_SECRET** *Nov 11 19:30:34.831: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState: INIT_DONE Event: EV_NO_EVENT *Nov 11 19:30:34.831: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState: INIT_DONE Event: EV_OK_RECD_DH_SECRET_RESP *Nov 11 19:30:34.831: IKEv2:(SA ID = 1):Action: Action_Null *Nov 11 19:30:34.831: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState: INIT_DONE Event:**EV_GEN_SKEYID** *Nov 11 19:30:34.831: IKEv2:(SA ID = 1):**Generate skeyid** *Nov 11 19:30:34.831: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState: INIT_DONE Event: EV_DONE *Nov 11 19:30:34.831: IKEv2:(SA ID = 1):Cisco DeleteReason Notify is enabled *Nov 11 19:30:34.831: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState: INIT_DONE Event: EV_CHK4_ROLE *Nov 11 19:30:34.831: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState: I_BLD_AUTH Event: EV_GET_CONFIG_MODE *Nov 11 19:30:34.831: IKEv2:Sending config data to toolkit *Nov 11 19:30:34.831: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState: I_BLD_AUTH Event: EV_CHK_EAP	
Initiator starts IKE_AUTH exchange and generates the authentication payload. The IKE_AUTH packet contains: ISAKMP Header (SPI/ version/flags), IDi (initiator identity), AUTH payload, SAi2 (initiates the SA-similar to the phase 2 transform set exchange in IKEv1), and TSi and TSr (Initiator and Responder Traffic selectors). They contain the source and destination address of the initiator and responder respectively for	*Nov 11 19:30:34.831: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState: I_BLD_AUTH Event:**EV_GEN_AUTH** *Nov 11 19:30:34.831: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState: I_BLD_AUTH Event: EV_CHK_AUTH_TYPE *Nov 11 19:30:34.831: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState: I_BLD_AUTH Event: EV_OK_AUTH_GEN *Nov 11 19:30:34.831: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState: I_BLD_AUTH Event: EV_SEND_AUTH *Nov 11 19:30:34.831: IKEv2:Construct Vendor Specific Payload: CISCO-GRANITE *Nov 11 19:30:34.831: IKEv2:Construct Notify Payload: INITIAL_CONTACT *Nov 11 19:30:34.831: IKEv2:Construct Notify Payload: SET_WINDOW_SIZE *Nov 11 19:30:34.831: IKEv2:Construct Notify Payload: ESP_TFC_NO_SUPPORT *Nov 11 19:30:34.831: IKEv2:Construct Notify Payload: NON_FIRST_FRAGS	

forwarding/receiving encrypted traffic. The address range specifies that all traffic to and from that range is tunneled. If the proposal is acceptable to the responder, it sends identical TS payloads back. The first CHILD_SA is created for the proxy_ID pair that matches the trigger packet. **Relevant Configuration:** `crypto ipsec transform-set TS esp-3des esp-sha-hmac crypto ipsec profile phse2-prof set transform-set TS set ikev2-profile IKEV2-SETUP`	**Payload contents:** VID Next payload: IDi, reserved: 0x0, length: 20 **IDi** Next payload: AUTH, reserved: 0x0, length: 12 Id type: IPv4 address, Reserved: 0x0 0x0 **AUTH** Next payload: CFG, reserved: 0x0, length: 28 Auth method PSK, reserved: 0x0, reserved 0x0 **CFG** Next payload: SA, reserved: 0x0, length: 309 cfg type: CFG_REQUEST, reserved: 0x0, reserved: 0x0 *Nov 11 19:30:34.831: SA Next payload: **TSi**, reserved: 0x0, length: 40 last proposal: 0x0, reserved: 0x0, length: 36 Proposal: 1, Protocol id: ESP, SPI size: 4, #trans: 3 last transform: 0x3, reserved: 0x0: length: 8 type: 1, reserved: 0x0, id: 3DES last transform: 0x3, reserved: 0x0: length: 8 type: 3, reserved: 0x0, id: SHA96 last transform: 0x0, reserved: 0x0: length: 8 type: 5, reserved: 0x0, id: Do not use ESN **TSi** Next payload: TSr, reserved: 0x0, length: 24 Num of TSs: 1, reserved 0x0, reserved 0x0 TS type: TS_IPV4_ADDR_RANGE, proto id: 0, length: 16 start port: 0, end port: 65535 start addr: 0.0.0.0, end addr: 255.255.255.255 **TSr** Next payload: NOTIFY, reserved: 0x0, length: 24 Num of TSs: 1, reserved 0x0, reserved 0x0 TS type: TS_IPV4_ADDR_RANGE, proto id: 0, length: 16 start port: 0, end port: 65535 start addr: 0.0.0.0, end addr: 255.255.255.255 NOTIFY(INITIAL_CONTACT) Next payload: NOTIFY, reserved: 0x0, length: 8 Security protocol id: IKE, spi size: 0, type: INITIAL_CONTACT NOTIFY(SET_WINDOW_SIZE) Next payload: NOTIFY, reserved: 0x0, length: 12 Security protocol id: IKE, spi size: 0, type: SET_WINDOW_SIZE NOTIFY(ESP_TFC_NO_SUPPORT) Next payload: NOTIFY, reserved: 0x0, length: 8 Security protocol id: IKE, spi size: 0, type: ESP_TFC_NO_SUPPORT NOTIFY(NON_FIRST_FRAGS) Next payload: NONE, reserved: 0x0, length: 8 Security protocol id: IKE, spi size: 0, type: NON_FIRST_FRAGS *Nov 11 19:30:34.832: IKEv2:(SA ID = 1):Next payload: ENCR, version: 2.0 Exchange type: **IKE_AUTH**, flags: **INITIATOR** Message id: 1, length: 556 Payload contents: ENCR Next payload: VID, reserved: 0x0, length: 528 *Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 **CurState: I_WAIT_AUTH** Event: EV_NO_EVENT	
----------Initiator sent IKE_AUTH ---------->		
	*Nov 11 19:30:34.832: IKEv2:Got a packet from dispatcher	Router 2 rece

	*Nov 11 19:30:34.832: IKEv2:Processing an item off the pak queue
	*Nov 11 19:30:34.832: IKEv2:(SA ID = 1):Request has mess_id 1; expected 1 through 1
	*Nov 11 19:30:34.832: **IKEv2:(SA ID = 1)**:Next payload: ENCR, version: 2.0 Exchange type: **IKE_AUTH**, flags: **INITIATOR** Message id: 1, length: 556
	Payload contents:
	*Nov 11 19:30:34.832: IKEv2:Parse Vendor Specific Payload: (CUSTOM) VID Next payload: IDi, reserved: 0x0, length: 20
	IDi Next payload: AUTH, reserved: 0x0, length: 12
	Id type: IPv4 address, Reserved: 0x0 0x0
	AUTH Next payload: CFG, reserved: 0x0, length: 28
	Auth method PSK, reserved: 0x0, reserved 0x0
	CFG Next payload: SA, reserved: 0x0, length: 309
	cfg type: CFG_REQUEST, reserved: 0x0, reserved: 0x0
	*Nov 11 19:30:34.832: attrib type: internal IP4 DNS, length: 0
	*Nov 11 19:30:34.832: attrib type: internal IP4 DNS, length: 0
	*Nov 11 19:30:34.832: attrib type: internal IP4 NBNS, length: 0
	*Nov 11 19:30:34.832: attrib type: internal IP4 NBNS, length: 0
	*Nov 11 19:30:34.832: attrib type: internal IP4 subnet, length: 0
	*Nov 11 19:30:34.832: attrib type: application version, length: 257
	attrib type: Unknown - 28675, length: 0
	*Nov 11 19:30:34.832: attrib type: Unknown - 28672, length: 0
	*Nov 11 19:30:34.832: attrib type: Unknown - 28692, length: 0
	*Nov 11 19:30:34.832: attrib type: Unknown - 28681, length: 0
	*Nov 11 19:30:34.832: attrib type: Unknown - 28674, length: 0
	*Nov 11 19:30:34.832: **SA** Next payload: TSi, reserved: 0x0, length: 40
	last proposal: 0x0, reserved: 0x0, length: 36
	Proposal: 1, Protocol id: ESP, SPI size: 4, #trans: 3 last transform: 0x3, reserved: 0x0: length: 8
	type: 1, reserved: 0x0, id: 3DES
	last transform: 0x3, reserved: 0x0: length: 8
	type: 3, reserved: 0x0, id: SHA96
	last transform: 0x0, reserved: 0x0: length: 8
	type: 5, reserved: 0x0, id: Do not use ESN
	TSi Next payload: TSr, reserved: 0x0, length: 24
	Num of TSs: 1, reserved 0x0, reserved 0x0
	TS type: TS_IPV4_ADDR_RANGE, proto id: 0, length: 16
	start port: 0, end port: 65535
	start addr: 0.0.0.0, end addr: 255.255.255.255
	TSr Next payload: NOTIFY, reserved: 0x0, length: 24
	Num of TSs: 1, reserved 0x0, reserved 0x0
	TS type: TS_IPV4_ADDR_RANGE, proto id: 0, length: 16
	start port: 0, end port: 65535
	start addr: 0.0.0.0, end addr: 255.255.255.255
		verifies the authentication received from 1.
		
		Relevant Configuratio
		`ipsec ikev2`
		`proposal AES`
		`protocol esp`
		`encryption a`
		`protocol esp`
		`integrity sh`

	*Nov 11 19:30:34.832: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_WAIT_AUTH Event: EV_RECV_AUTH *Nov 11 19:30:34.832: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_WAIT_AUTH Event: EV_CHK_NAT_T	Router 2 buil response to IKE_AUTH that it receive Router 1. Thi response pacl contains: ISA Header(SPI/

	*Nov 11 19:30:34.832: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_WAIT_AUTH Event: EV_PROC_ID *Nov 11 19:30:34.832: IKEv2:(SA ID = 1):Received valid parameteres in process id *Nov 11 19:30:34.832: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_WAIT_AUTH Event: EV_CHK_IF_PEER_CERT_NEEDS_TO_BE_FETCHED_FOR_PROF_SEL *Nov 11 19:30:34.832: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_WAIT_AUTH Event: EV_GET_POLICY_BY_PEERID *Nov 11 19:30:34.833: IKEv2:(1): Choosing IKE profile IKEV2-SETUP *Nov 11 19:30:34.833: IKEv2:% Getting preshared key by address 10.0.0.1 *Nov 11 19:30:34.833: IKEv2:% Getting preshared key by address 10.0.0.1 *Nov 11 19:30:34.833: IKEv2:Adding Proposal default to toolkit policy *Nov 11 19:30:34.833: IKEv2:(SA ID = 1):Using IKEv2 profile 'IKEV2-SETUP' *Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_WAIT_AUTH Event: EV_SET_POLICY *Nov 11 19:30:34.833: IKEv2:(SA ID = 1):Setting configured policies *Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_WAIT_AUTH Event: EV_VERIFY_POLICY_BY_PEERID *Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_WAIT_AUTH Event: EV_CHK_AUTH4EAP *Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_WAIT_AUTH Event: EV_CHK_POLREQEAP *Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_VERIFY_AUTH Event: EV_CHK_AUTH_TYPE *Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_VERIFY_AUTH Event: EV_GET_PRESHR_KEY *Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_VERIFY_AUTH Event: EV_VERIFY_AUTH *Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_VERIFY_AUTH Event: EV_CHK4_IC *Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_VERIFY_AUTH Event: EV_CHK_REDIRECT *Nov 11 19:30:34.833: IKEv2:(SA ID = 1):Redirect check is not needed, skipping it *Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_VERIFY_AUTH Event:	version/flags) IDr(responde identity), AU payload, SAr the SA-simila phase 2 transf exchange in I and TSi and TSr(Initiator Responder Tr selectors). Th contain the so destination ad the initiator a responder res for forwarding/re encrypted tra address range that all traffic from that rang tunnelled. Th parameters ar identical to th that was recei ASA1.

	EV_NOTIFY_AUTH_DONE *Nov 11 19:30:34.833: IKEv2:AAA group authorization is not configured *Nov 11 19:30:34.833: IKEv2:AAA user authorization is not configured *Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_VERIFY_AUTH Event: EV_CHK_CONFIG_MODE *Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_VERIFY_AUTH Event: EV_SET_RECD_CONFIG_MODE *Nov 11 19:30:34.833: IKEv2:Received config data from toolkit: *Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_VERIFY_AUTH Event: EV_PROC_SA_TS *Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_VERIFY_AUTH Event: EV_GET_CONFIG_MODE *Nov 11 19:30:34.833: IKEv2:Error constructing config reply *Nov 11 19:30:34.833: IKEv2:No config data to send to toolkit: *Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_BLD_AUTH Event: EV_MY_AUTH_METHOD *Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_BLD_AUTH Event: EV_GET_PRESHR_KEY *Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_BLD_AUTH Event: EV_GEN_AUTH *Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_BLD_AUTH Event: EV_CHK4_SIGN *Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_BLD_AUTH Event: EV_OK_AUTH_GEN *Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_BLD_AUTH Event: EV_SEND_AUTH *Nov 11 19:30:34.833: IKEv2:Construct Vendor Specific Payload: CISCO-GRANITE *Nov 11 19:30:34.833: IKEv2:Construct Notify Payload: SET_WINDOW_SIZE *Nov 11 19:30:34.833: IKEv2:Construct Notify Payload: ESP_TFC_NO_SUPPORT *Nov 11 19:30:34.833: IKEv2:Construct Notify Payload: NON_FIRST_FRAGS	
	*Nov 11 19:30:34.833: IKEv2:(SA ID = 1):Next payload: ENCR, version: 2.0 Exchange type: **IKE_AUTH**, flags: **RESPONDER MSG-RESPONSE** Message id: 1, length: 252 Payload contents: **ENCR** Next payload: VID, reserved: 0x0, length: 224 *Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA:	Responder se response for IKE_AUTH.

	I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: AUTH_DONE Event: EV_OK *Nov 11 19:30:34.833: IKEv2:(SA ID = 1):Action: Action_Null *Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: AUTH_DONE Event: EV_PKI_SESH_CLOSE *Nov 11 19:30:34.833: IKEv2:(SA ID = 1):Closing the PKI session *Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: AUTH_DONE Event: EV_UPDATE_CAC_STATS *Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: AUTH_DONE Event:**EV_INSERT_IKE** *Nov 11 19:30:34.834: IKEv2:Store mib index ikev2 1, platform 60 *Nov 11 19:30:34.834: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: AUTH_DONE Event: EV_GEN_LOAD_IPSEC *Nov 11 19:30:34.834: IKEv2:(SA ID = 1):Asynchronous request queued *Nov 11 19:30:34.834: IKEv2:(SA ID = 1): *Nov 11 19:30:34.834: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: **AUTH_DONE** Event: EV_NO_EVENT	
<----------Responder sent IKE_AUTH----------			
Initiator receives response from Responder.	*Nov 11 19:30:34.834: IKEv2:Got a packet from dispatcher *Nov 11 19:30:34.834: IKEv2:Processing an item off the pak queue	*Nov 11 19:30:34.840: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: AUTH_DONE Event: EV_OK_RECD_LOAD_IPSEC *Nov 11 19:30:34.840: IKEv2:(SA ID = 1):Action: Action_Null *Nov 11 19:30:34.840: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: AUTH_DONE Event: EV_START_ACCT *Nov 11 19:30:34.840: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: AUTH_DONE Event: EV_CHECK_DUPE *Nov 11 19:30:34.840: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState:	Responder in entry into the

		AUTH_DONE Event: EV_CHK4_ROLE	
Router 1 verifies and processes the authentication data in this packet. Router 1 then inserts this SA into its SAD.	*Nov 11 19:30:34.834: IKEv2:(SA ID = 1):Next payload: ENCR, version: 2.0 Exchange type: **IKE_AUTH**, flags: **RESPONDER MSG-RESPONSE** Message id: 1, length: 252 **Payload contents:** *Nov 11 19:30:34.834: IKEv2:Parse Vendor Specific Payload: (CUSTOM) VID Next payload: IDr, reserved: 0x0, length: 20 **IDr** Next payload: AUTH, reserved: 0x0, length: 12 Id type: IPv4 address, Reserved: 0x0 0x0 **AUTH** Next payload: SA, reserved: 0x0, length: 28 Auth method PSK, reserved: 0x0, reserved 0x0 **SA** Next payload: TSi, reserved: 0x0, length: 40 last proposal: 0x0, reserved: 0x0, length: 36 Proposal: 1, Protocol id: ESP, SPI size: 4, #trans: 3 last transform: 0x3, reserved: 0x0: length: 8 type: 1, reserved: 0x0, id: 3DES last transform: 0x3, reserved: 0x0: length: 8 type: 3, reserved: 0x0, id: SHA96 last transform: 0x0, reserved: 0x0: length: 8 type: 5, reserved: 0x0, id: Do not use ESN **TSi** Next payload: TSr, reserved: 0x0, length: 24 Num of TSs: 1, reserved 0x0, reserved 0x0 TS type: TS_IPV4_ADDR_RANGE, proto id: 0, length: 16 start port: 0, end port: 65535 start addr: 0.0.0.0, end addr: 255.255.255.255 **TSr** Next payload: NOTIFY, reserved: 0x0, length: 24 Num of TSs: 1, reserved 0x0, reserved 0x0 TS type: TS_IPV4_ADDR_RANGE, proto id: 0, length: 16 start port: 0, end port: 65535 start addr: 0.0.0.0, end addr: 255.255.255.255 *Nov 11 19:30:34.834: IKEv2:Parse Notify Payload: SET_WINDOW_SIZE NOTIFY(SET_WINDOW_SIZE) Next payload: NOTIFY, reserved: 0x0, length: 12 Security protocol id: IKE, spi size: 0, type: SET_WINDOW_SIZE *Nov 11 19:30:34.834: IKEv2:Parse Notify Payload: ESP_TFC_NO_SUPPORT NOTIFY(ESP_TFC_NO_SUPPORT) Next payload: NOTIFY, reserved: 0x0, length: 8 Security protocol id: IKE, spi size: 0, type: ESP_TFC_NO_SUPPORT *Nov 11 19:30:34.834: IKEv2:Parse Notify Payload: NON_FIRST_FRAGS NOTIFY(NON_FIRST_FRAGS) Next payload: NONE, reserved: 0x0, length: 8 Security protocol id: IKE, spi size: 0, type: NON_FIRST_FRAGS *Nov 11 19:30:34.834: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: I_WAIT_AUTH Event:**EV_RECV_AUTH**	

*Nov 11 19:30:34.834: IKEv2:(SA ID = 1):Action: Action_Null
*Nov 11 19:30:34.834: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: I_PROC_AUTH Event: EV_CHK4_NOTIFY
*Nov 11 19:30:34.834: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: I_PROC_AUTH Event:**EV_PROC_MSG**
*Nov 11 19:30:34.834: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: I_PROC_AUTH Event: EV_CHK_IF_PEER_CERT_NEEDS_TO_BE_FETCHED_FOR_PROF_SEL
*Nov 11 19:30:34.834: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: I_PROC_AUTH Event: EV_GET_POLICY_BY_PEERID
*Nov 11 19:30:34.834: IKEv2:Adding Proposal PHASE1-prop to toolkit policy
*Nov 11 19:30:34.834: IKEv2:(SA ID = 1):Using IKEv2 profile 'IKEV2-SETUP'
*Nov 11 19:30:34.834: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: I_PROC_AUTH Event: EV_VERIFY_POLICY_BY_PEERID
*Nov 11 19:30:34.834: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: I_PROC_AUTH Event: EV_CHK_AUTH_TYPE
*Nov 11 19:30:34.834: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: I_PROC_AUTH Event: EV_GET_PRESHR_KEY
*Nov 11 19:30:34.835: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: I_PROC_AUTH Event:**EV_VERIFY_AUTH**
*Nov 11 19:30:34.835: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: I_PROC_AUTH Event: EV_CHK_EAP
*Nov 11 19:30:34.835: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: I_PROC_AUTH Event:**EV_NOTIFY_AUTH_DONE**
*Nov 11 19:30:34.835: IKEv2:AAA group authorization is not configured
*Nov 11 19:30:34.835: IKEv2:AAA user authorization is not configured
*Nov 11 19:30:34.835: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: I_PROC_AUTH Event: EV_CHK_CONFIG_MODE
*Nov 11 19:30:34.835: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: I_PROC_AUTH Event: EV_CHK4_IC
*Nov 11 19:30:34.835: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: I_PROC_AUTH Event: EV_CHK_IKE_ONLY
*Nov 11 19:30:34.835: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: I_PROC_AUTH Event: EV_PROC_SA_TS
*Nov 11 19:30:34.835: IKEv2:(SA ID = 1):SM Trace-> SA:

	I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: AUTH_DONE Event: EV_OK *Nov 11 19:30:34.835: IKEv2:(SA ID = 1):Action: Action_Null *Nov 11 19:30:34.835: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: AUTH_DONE Event: EV_PKI_SESH_CLOSE *Nov 11 19:30:34.835: IKEv2:(SA ID = 1):Closing the PKI session *Nov 11 19:30:34.835: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: AUTH_DONE Event: EV_UPDATE_CAC_STATS *Nov 11 19:30:34.835: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: AUTH_DONE Event: EV_INSERT_IKE *Nov 11 19:30:34.835: IKEv2:Store mib index ikev2 1, platform 60 *Nov 11 19:30:34.835: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: AUTH_DONE Event: EV_GEN_LOAD_IPSEC *Nov 11 19:30:34.835: IKEv2:(SA ID = 1):Asynchronous request queued *Nov 11 19:30:34.835: IKEv2:(SA ID = 1): *Nov 11 19:30:34.835: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: AUTH_DONE Event: EV_NO_EVENT *Nov 11 19:30:34.835: IKEv2:KMI message 8 consumed. No action taken. *Nov 11 19:30:34.835: IKEv2:KMI message 12 consumed. No action taken. *Nov 11 19:30:34.835: IKEv2:No data to send in mode config set. *Nov 11 19:30:34.841: IKEv2:Adding ident handle 0x80000002 associated with SPI 0x9506D414 for session 8 *Nov 11 19:30:34.841: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: AUTH_DONE Event: EV_OK_RECD_LOAD_IPSEC *Nov 11 19:30:34.841: IKEv2:(SA ID = 1):Action: Action_Null *Nov 11 19:30:34.841: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: AUTH_DONE Event: EV_START_ACCT *Nov 11 19:30:34.841: IKEv2:(SA ID = 1):Accounting not required *Nov 11 19:30:34.841: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: AUTH_DONE Event: EV_CHECK_DUPE *Nov 11 19:30:34.841: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: **AUTH_DONE** Event: EV_CHK4_ROLE		
Tunnel is up on the Initiator and the status shows*READY*.	*Nov 11 19:30:34.841: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: **READY**Event: EV_CHK_IKE_ONLY *Nov 11 19:30:34.841: IKEv2:(SA	*****Nov 11 19:30:34.840: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: **READY** Event: EV_R_OK *Nov 11 19:30:34.840: IKEv2:(SA ID = 1):SM Trace-> SA:	Tunnel is up Responder. T Responder tu usually come before the Ini

	ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: READY Event: EV_I_OK	I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: READY Event: EV_NO_EVENT	

CHILD_SA Debugs

This exchange consists of a single request/response pair and was referred to as a phase 2 exchange in IKEv1. It can be initiated by either end of the IKE_SA after the initial exchanges are completed.

Router 1 CHILD_SA Message Description	Debugs	Router 2 CI Message De
Router 1 initiates the CHILD_SA exchange. This is the CREATE_CHILD_SA request. The CHILD_SA packet typically contains: • SA HDR (version.flags/exchange type) • Nonce Ni (optional): If the CHILD_SA is created as part of the initial exchange, a second KE payload and nonce must not be sent) • SA Payload • KEi (Key-optional): The CREATE_CHILD_SA request can optionally contain a KE payload for an additional DH exchange to enable stronger guarantees of forward secrecy for the CHILD_SA. If the SA offers include different DH groups, KEi must be an element of the group the initiator expects the responder to accept. If it guesses wrong, the CREATE_CHILD_SA exchange fails, and it can retry with a different KEi • N(Notify payload-optional). The Notify	*Nov 11 19:31:35.873: IKEv2:Got a packet from dispatcher *Nov 11 19:31:35.873: IKEv2:Processing an item off the pak queue *Nov 11 19:31:35.873: IKEv2:(SA ID = 2):Request has mess_id 3; expected 3 through 7 *Nov 11 19:31:35.873: IKEv2:(SA ID = 2):Next payload: ENCR, version: 2.0 **Exchange type: CREATE_CHILD_SA**, flags: **INITIATOR** Message id: 3, length: 396 Payload contents: **SA** Next payload: N, reserved: 0x0, length: 152 last proposal: 0x0, reserved: 0x0, length: 148 Proposal: 1, Protocol id: IKE, SPI size: 8, #trans: 15 last transform: 0x3, reserved: 0x0: length: 12 type: 1, reserved: 0x0, id: AES-CBC last transform: 0x3, reserved: 0x0: length: 12 type: 1, reserved: 0x0, id: AES-CBC last transform: 0x3, reserved: 0x0: length: 12 type: 1, reserved: 0x0, id: AES-CBC last transform: 0x3, reserved: 0x0: length: 8 type: 2, reserved: 0x0, id: SHA512 last transform: 0x3, reserved: 0x0: length: 8 type: 2, reserved: 0x0, id: SHA384 last transform: 0x3, reserved: 0x0: length: 8 type: 2, reserved: 0x0, id: SHA256 last transform: 0x3, reserved: 0x0: length: 8 type: 2, reserved: 0x0, id: SHA1 last transform: 0x3, reserved: 0x0: length: 8 type: 2, reserved: 0x0, id: MD5 last transform: 0x3, reserved: 0x0: length: 8 type: 3, reserved: 0x0, id: SHA512 last transform: 0x3, reserved: 0x0: length: 8 type: 3, reserved: 0x0, id: SHA384 last transform: 0x3, reserved: 0x0: length: 8 type: 3, reserved: 0x0, id: SHA256 last transform: 0x3, reserved: 0x0: length: 8 type: 3, reserved: 0x0, id: SHA96	

Payload, is used to transmit informational data, such as error conditions and state transitions, to an IKE peer. A Notify Payload can appear in a response message (usually it specifies why a request was rejected), in an INFORMATIONAL Exchange (to report an error not in an IKE request), or in any other message to indicate sender capabilities or to modify the meaning of the request.If this CREATE_CHILD_SA exchange is rekeying an existing SA other than the IKE_SA, the leading N payload of type REKEY_SA MUST identify the SA being rekeyed. If this CREATE_CHILD_SA exchange is not rekeying an existing SA, the N payload MUST be omitted.	last transform: 0x3, reserved: 0x0: length: 8 type: 3, reserved: 0x0, id: MD596 last transform: 0x3, reserved: 0x0: length: 8 type: 4, reserved: 0x0, id: DH_GROUP_1536_MODP/Group 5 last transform: 0x0, reserved: 0x0: length: 8 type: 4, reserved: 0x0, id: DH_GROUP_1024_MODP/Group 2 **N** Next payload: KE, reserved: 0x0, length: 24 **KE** Next payload: NOTIFY, reserved: 0x0, length: 136 DH group: 2, Reserved: 0x0 *Nov 11 19:31:35.874: IKEv2:Parse Notify Payload: SET_WINDOW_SIZE **NOTIFY**(SET_WINDOW_SIZE) Next payload: NONE, reserved: 0x0, length: 12 Security protocol id: IKE, spi size: 0, type: SET_WINDOW_SIZE *Nov 11 19:31:35.874: IKEv2:(**SA ID = 2**):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: READY Event: **EV_RECV_CREATE_CHILD** *Nov 11 19:31:35.874: IKEv2:(SA ID = 2):Action: Action_Null *Nov 11 19:31:35.874: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: CHILD_R_INIT Event: EV_RECV_CREATE_CHILD *Nov 11 19:31:35.874: IKEv2:(SA ID = 2):Action: Action_Null *Nov 11 19:31:35.874: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: CHILD_R_INIT Event: EV_VERIFY_MSG *Nov 11 19:31:35.874: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: CHILD_R_INIT Event: EV_CHK_CC_TYPE *Nov 11 19:31:35.874: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: CHILD_R_IKE Event: **EV_REKEY_IKESA** *Nov 11 19:31:35.874: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: CHILD_R_IKE Event: EV_GET_IKE_POLICY *Nov 11 19:31:35.874: IKEv2:% **Getting preshared key by address 10.0.0.2** *Nov 11 19:31:35.874: IKEv2:% Getting preshared key by address 10.0.0.2 *Nov 11 19:31:35.874: IKEv2:Adding Proposal PHASE1-prop to toolkit policy *Nov 11 19:31:35.874: IKEv2:(SA ID = 2):Using IKEv2 profile 'IKEV2-SETUP' *Nov 11 19:31:35.874: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: CHILD_R_IKE Event: EV_PROC_MSG	

*Nov 11 19:31:35.874: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: CHILD_R_IKE Event: EV_SET_POLICY
*Nov 11 19:31:35.874: IKEv2:(SA ID = 2):**Setting configured policies**
*Nov 11 19:31:35.874: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: CHILD_R_BLD_MSG Event: EV_GEN_DH_KEY
*Nov 11 19:31:35.874: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: CHILD_R_BLD_MSG Event: EV_NO_EVENT
*Nov 11 19:31:35.874: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: CHILD_R_BLD_MSG Event: EV_OK_RECD_DH_PUBKEY_RESP
*Nov 11 19:31:35.874: IKEv2:(SA ID = 2):Action: Action_Null
*Nov 11 19:31:35.874: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: CHILD_R_BLD_MSG Event:**EV_GEN_DH_SECRET**
*Nov 11 19:31:35.881: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: CHILD_R_BLD_MSG Event: EV_NO_EVENT
*Nov 11 19:31:35.882: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: CHILD_R_BLD_MSG Event: EV_OK_RECD_DH_SECRET_RESP
*Nov 11 19:31:35.882: IKEv2:(SA ID = 2):Action: Action_Null
*Nov 11 19:31:35.882: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: CHILD_R_BLD_MSG Event: EV_BLD_MSG
*Nov 11 19:31:35.882: **IKEv2:ConstructNotify Payload**: SET_WINDOW_SIZE
Payload contents:
SA Next payload: N, reserved: 0x0, length: 56
last proposal: 0x0, reserved: 0x0, length: 52
Proposal: 1, Protocol id: IKE, SPI size: 8, #trans: 4 last transform: 0x3, reserved: 0x0: length: 12
type: 1, reserved: 0x0, id: AES-CBC
last transform: 0x3, reserved: 0x0: length: 8
type: 2, reserved: 0x0, id: SHA1
last transform: 0x3, reserved: 0x0: length: 8
type: 3, reserved: 0x0, id: SHA96
last transform: 0x0, reserved: 0x0: length: 8
type: 4, reserved: 0x0, id: DH_GROUP_1024_MODP/Group 2
N Next payload: KE, reserved: 0x0, length: 24
KE Next payload: NOTIFY, reserved: 0x0, length: 136
DH group: 2, Reserved: 0x0

	NOTIFY(SET_WINDOW_SIZE) Next payload: NONE, reserved: 0x0, length: 12 Security protocol id: IKE, spi size: 0, type: SET_WINDOW_SIZE	
	*Nov 11 19:31:35.869: IKEv2:(**SA ID = 2**):Next payload: ENCR, version: 2.0 Exchange type: **CREATE_CHILD_SA**, flags: **INITIATOR** Message id: 2, length: 460 Payload contents: ENCR Next payload: SA, reserved: 0x0, length: 432 *Nov 11 19:31:35.873: IKEv2:Construct Notify Payload: SET_WINDOW_SIZE Payload contents: **SA** Next payload: N, reserved: 0x0, length: 152 last proposal: 0x0, reserved: 0x0, length: 148 Proposal: 1, Protocol id: IKE, SPI size: 8, #trans: 15 last transform: 0x3, reserved: 0x0: length: 12 type: 1, reserved: 0x0, id: AES-CBC last transform: 0x3, reserved: 0x0: length: 12 type: 1, reserved: 0x0, id: AES-CBC last transform: 0x3, reserved: 0x0: length: 12 type: 1, reserved: 0x0, id: AES-CBC last transform: 0x3, reserved: 0x0: length: 8 type: 2, reserved: 0x0, id: SHA512 last transform: 0x3, reserved: 0x0: length: 8 type: 2, reserved: 0x0, id: SHA384 last transform: 0x3, reserved: 0x0: length: 8 type: 2, reserved: 0x0, id: SHA256 last transform: 0x3, reserved: 0x0: length: 8 type: 2, reserved: 0x0, id: SHA1 last transform: 0x3, reserved: 0x0: length: 8 type: 2, reserved: 0x0, id: MD5 last transform: 0x3, reserved: 0x0: length: 8 type: 3, reserved: 0x0, id: SHA512 last transform: 0x3, reserved: 0x0: length: 8 type: 3, reserved: 0x0, id: SHA384 last transform: 0x3, reserved: 0x0: length: 8 type: 3, reserved: 0x0, id: SHA256 last transform: 0x3, reserved: 0x0: length: 8 type: 3, reserved: 0x0, id: SHA96 last transform: 0x3, reserved: 0x0: length: 8 type: 3, reserved: 0x0, id: MD596 last transform: 0x3, reserved: 0x0: length: 8 type: 4, reserved: 0x0, id: DH_GROUP_1536_MODP/Group 5 last transform: 0x0, reserved: 0x0: length: 8 type: 4, reserved: 0x0, id: DH_GROUP_1024_MODP/Group 2 **N** Next payload: KE, reserved: 0x0, length: 24 **KE** Next payload: NOTIFY, reserved: 0x0, length: 136 DH group: 2, Reserved: 0x0 **NOTIFY**(SET_WINDOW_SIZE) Next payload: NONE, reserved: 0x0, length: 12 Security protocol id: IKE, spi size: 0, type: SET_WINDOW_SIZE	This packet is re Router 2.

	*Nov 11 19:31:35.882: IKEv2:(**SA ID = 2**):Next payload: ENCR, version: 2.0 Exchange type: **CREATE_CHILD_SA,** flags: **RESPONDER MSG-RESPONSE** Message id: 3, length: 300 Payload contents: **SA** Next payload: N, reserved: 0x0, length: 56 last proposal: 0x0, reserved: 0x0, length: 52 Proposal: 1, Protocol id: IKE, SPI size: 8, #trans: 4 last transform: 0x3, reserved: 0x0: length: 12 type: 1, reserved: 0x0, id: AES-CBC last transform: 0x3, reserved: 0x0: length: 8 type: 2, reserved: 0x0, id: SHA1 last transform: 0x3, reserved: 0x0: length: 8 type: 3, reserved: 0x0, id: SHA96 last transform: 0x0, reserved: 0x0: length: 8 type: 4, reserved: 0x0, id: DH_GROUP_1024_MODP/Group 2 **N** Next payload: KE, reserved: 0x0, length: 24 **KE** Next payload: NOTIFY, reserved: 0x0, length: 136 DH group: 2, Reserved: 0x0 *Nov 11 19:31:35.882: IKEv2:Parse Notify Payload: SET_WINDOW_SIZE **NOTIFY**(SET_WINDOW_SIZE) Next payload: NONE, reserved: 0x0, length: 12 Security protocol id: IKE, spi size: 0, type: SET_WINDOW_SIZE *Nov 11 19:31:35.882: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState: **CHILD_I_WAIT** Event: **EV_RECV_CREATE_CHILD** *Nov 11 19:31:35.882: IKEv2:(SA ID = 2):Action: Action_Null *Nov 11 19:31:35.882: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState: **CHILD_I_PROC** Event: EV_CHK4_NOTIFY *Nov 11 19:31:35.882: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState: CHILD_I_PROC Event: **EV_VERIFY_MSG** *Nov 11 19:31:35.882: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState: CHILD_I_PROC Event: EV_PROC_MSG *Nov 11 19:31:35.882: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState: CHILD_I_PROC Event: EV_CHK4_PFS *Nov 11 19:31:35.882: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState: CHILD_I_PROC Event: EV_GEN_DH_SECRET *Nov 11 19:31:35.890: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState: CHILD_I_PROC Event:	Router 2 now bu for the CHILD_ This is the CREATE_CHI response. The C packet typically • SA HDR (version.f type) • Nonce Ni the CHIL created as initial exc second K nonce mu • SA Paylo • KEi (Key The CREATE request ca contain a for an add exchange stronger g forward s CHILD_S offers inc DH group be an elem group the expects th to accept. wrong, th CREATE exchange must retry different • N (Notify optional): Payload is transmit i data, such condition transition peer. A N can appea response (usually i why a req rejected), informati (to report in an IKE

	EV_NO_EVENT *Nov 11 19:31:35.890: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState: CHILD_I_PROC Event: EV_OK_RECD_DH_SECRET_RESP *Nov 11 19:31:35.890: IKEv2:(SA ID = 2):Action: Action_Null *Nov 11 19:31:35.890: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState: CHILD_I_PROC Event: EV_CHK_IKE_REKEY *Nov 11 19:31:35.890: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState: CHILD_I_PROC Event: EV_GEN_SKEYID *Nov 11 19:31:35.890: IKEv2:(SA ID = 2):Generate skeyid *Nov 11 19:31:35.890: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState: **CHILD_I_DONE** Event: **EV_ACTIVATE_NEW_SA** *Nov 11 19:31:35.890: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState: CHILD_I_DONE Event: EV_UPDATE_CAC_STATS *Nov 11 19:31:35.890: IKEv2:New ikev2 sa request activated *Nov 11 19:31:35.890: IKEv2:Failed to decrement count for outgoing negotiating *Nov 11 19:31:35.890: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState: CHILD_I_DONE Event: EV_CHECK_DUPE *Nov 11 19:31:35.890: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState: CHILD_I_DONE Event: EV_OK *Nov 11 19:31:35.890: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState: EXIT Event: EV_CHK_PENDING *Nov 11 19:31:35.890: IKEv2:(SA ID = 2):Processed response with message id 3, Requests can be sent from range 4 to 8 *Nov 11 19:31:35.890: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 **CurState: EXIT** Event: EV_NO_EVENT	in any oth indicate s capabiliti modify th the reques CREATE exchange an existin than the I leading N type REK identify th rekeyed. I CREATE exchange rekeying SA, the N must be o Router 2 sends t out and complet the new CHILD
Router 1 receives the response packet from Router 2 and completes activating the CHILD_SA.	*Nov 11 19:31:35.882: IKEv2:(SA ID = 2):Next payload: ENCR, version: 2.0 Exchange type: **CREATE_CHILD_SA**, flags: **RESPONDER MSG-RESPONSE** Message id: 3, length: 300 Payload contents: ENCR Next payload: SA, reserved: 0x0, length: 272 *Nov 11 19:31:35.882: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: CHILD_R_BLD_MSG	

	Event:**EV_CHK_IKE_REKEY** *Nov 11 19:31:35.882: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: CHILD_R_BLD_MSG Event: EV_GEN_SKEYID *Nov 11 19:31:35.882: IKEv2:(SA ID = 2):**Generate skeyid** *Nov 11 19:31:35.882: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: CHILD_R_DONE Event:**EV_ACTIVATE_NEW_SA** *Nov 11 19:31:35.882: IKEv2:Store mib index ikev2 3, platform 62 *Nov 11 19:31:35.882: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: CHILD_R_DONE Event: EV_UPDATE_CAC_STATS *Nov 11 19:31:35.882: IKEv2:New ikev2 sa request activated *Nov 11 19:31:35.882: IKEv2:Failed to decrement count for incoming negotiating *Nov 11 19:31:35.882: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: **CHILD_R_DONE** Event: EV_CHECK_DUPE *Nov 11 19:31:35.882: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: CHILD_R_DONE Event: EV_OK *Nov 11 19:31:35.882: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: CHILD_R_DONE Event: EV_START_DEL_NEG_TMR *Nov 11 19:31:35.882: IKEv2:(SA ID = 2):Action: Action_Null *Nov 11 19:31:35.882: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: EXIT Event: EV_CHK_PENDING *Nov 11 19:31:35.882: IKEv2:(SA ID = 2):Sent response with message id 3, Requests can be accepted from range 4 to 8 *Nov 11 19:31:35.882: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 **CurState: EXIT** Event: EV_NO_EVENT	

Tunnel Verification

ISAKMP

Command

<#root>

```
show crypto ikev2 sa detailed
```

Router 1 Output

<#root>

```
Router1#
```

show crypto ikev2 sa detailed

```
 IPv4 Crypto IKEv2  SA

Tunnel-id Local                 Remote             fvrf/ivrf         Status
1         10.0.0.1/500          10.0.0.2/500       none/none         READY
      Encr: AES-CBC, keysize: 128,
         Hash: SHA96, DH Grp:2,
         Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 120/10 sec
      CE id: 1006, Session-id: 4
      Status Description: Negotiation done
      Local spi: E58F925107F8B73F     Remote spi: AFD098F4147869DA
      Local id: 10.0.0.1
      Remote id: 10.0.0.2
      Local req msg id:  2       Remote req msg id:  0
      Local next msg id: 2       Remote next msg id: 0
      Local req queued:  2       Remote req queued:  0
      Local window:      5       Remote window:      5
      DPD configured for 0 seconds, retry 0
      NAT-T is not detected
      Cisco Trust Security SGT is disabled
      Initiator of SA : Yes
```

Router 2 Output

<#root>

```
Router2#
```

show crypto ikev2 sa detailed

```
 IPv4 Crypto IKEv2  SA

Tunnel-id Local           Remote              fvrf/ivrf          Status
2         10.0.0.2/500    10.0.0.1/500        none/none          READY
      Encr: AES-CBC, keysize: 128, Hash: SHA96,
         DH Grp:2, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 120/37 sec
      CE id: 1006, Session-id: 4
      Status Description: Negotiation done
      Local spi: AFD098F4147869DA       Remote spi: E58F925107F8B73F
      Local id: 10.0.0.2
      Remote id: 10.0.0.1
      Local req msg id:  0              Remote req msg id:  2
      Local next msg id: 0              Remote next msg id: 2
      Local req queued:  0              Remote req queued:  2
      Local window:      5              Remote window:      5
      DPD configured for 0 seconds, retry 0
      NAT-T is not detected
      Cisco Trust Security SGT is disabled
```

```
      Initiator of SA : No
```

IPsec

Command

<#root>

show crypto ipsec sa

Note: In this output, unlike in IKEv1, the PFS DH group value appears as "PFS (Y/N): N, DH group: none" during the first tunnel negotiation, but, after a rekey occurs, the right values appear. This is not a bug, even though the behavior is described in Cisco bug ID CSCug67056. (Only registered Cisco users can access internal Cisco tools or information.)
The difference between IKEv1 and IKEv2 is that, in the latter, the Child SAs are created as part of AUTH exchange itself. The DH Group configured under the crypto map would be used only during rekey. Hence, you would see 'PFS (Y/N): N, DH group: none' until the first rekey.
With IKEv1, you see a different behavior, because Child SA creation happens during Quick Mode, and the CREATE_CHILD_SA message has a provision to carry the Key Exchange payload that specifies the DH parameters to derive a new shared secret.

Router 1 Output

<#root>

Router1#

show crypto ipsec sa

```
interface: Tunnel0
    Crypto map tag: Tunnel0-head-0,
         local addr 10.0.0.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port):
         (0.0.0.0/0.0.0.0/256/0)
   remote ident (addr/mask/prot/port):
         (0.0.0.0/0.0.0.0/256/0)
   current_peer 10.0.0.2 port 500
     PERMIT, flags={origin_is_acl,}
    #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.: 10.0.0.1,
         remote crypto endpt.: 10.0.0.2
```

```
     path mtu 1500, ip mtu 1500, ip mtu idb Ethernet0/0
     current outbound spi: 0xF6083ADD(4127734493)
     PFS (Y/N): N, DH group: none

     inbound esp sas:
      spi: 0x6B74CB79(1802816377)
        transform: esp-3des esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 18, flow_id: SW:18,
         sibling_flags 80000040,
         crypto map: Tunnel0-head-0
        sa timing: remaining key lifetime (k/sec):
         (4276853/3592)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0xF6083ADD(4127734493)
        transform: esp-3des esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 17, flow_id: SW:17,
         sibling_flags 80000040,
         crypto map: Tunnel0-head-0
        sa timing: remaining key
         lifetime (k/sec): (4276853/3592)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     outbound ah sas:

     outbound pcp sas:
```

Router 2 Output

<#root>

```
Router2#
```

show crypto ipsec sa

```
interface: Tunnel0
    Crypto map tag: Tunnel0-head-0, local addr 10.0.0.2

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/256/0)
   remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/256/0)
   current_peer 10.0.0.1 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5
    #pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
```

```
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 10.0.0.2,
         remote crypto endpt.: 10.0.0.1
     path mtu 1500, ip mtu 1500, ip mtu idb Ethernet0/0
     current outbound spi: 0x6B74CB79(1802816377)
     PFS (Y/N): N, DH group: none

     inbound esp sas:
      spi: 0xF6083ADD(4127734493)
        transform: esp-3des esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 17, flow_id: SW:17,
         sibling_flags 80000040,
         crypto map: Tunnel0-head-0
        sa timing: remaining key lifetime
         (k/sec): (4347479/3584)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x6B74CB79(1802816377)
        transform: esp-3des esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 18, flow_id: SW:18,
         sibling_flags 80000040,
         crypto map: Tunnel0-head-0
        sa timing: remaining key
         lifetime (k/sec): (4347479/3584)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     outbound ah sas:

     outbound pcp sas:
```

You can also check the output of the **show crypto session** command on both routers; this output shows the tunnel session status as UP-ACTIVE.

<#root>

```
Router1#
```

show crypto session

```
Crypto session current status

Interface: Tunnel0
Session status: UP-ACTIVE
Peer: 10.0.0.2 port 500
  IKEv2 SA: local 10.0.0.1/500 remote 10.0.0.2/500 Active
  IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
```

```
        Active SAs: 2, origin: crypto map

Router2#
```

show cry session

```
Crypto session current status

Interface: Tunnel0
Session status: UP-ACTIVE
Peer: 10.0.0.1 port 500
  IKEv2 SA: local 10.0.0.2/500 remote 10.0.0.1/500 Active
  IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
        Active SAs: 2, origin: crypto map
```

Related Information

- **IKEv2 Packet Exchange and Protocol Level Debugging**
- **Cisco Technical Support & Downloads**