Debugs IOS IKEv2 para el VPN de sitio a sitio con la Nota Técnica del troubleshooting de PSKs

Contenido

Introducción

Este documento describe los debugs del intercambio de claves de Internet versión 2 (IKEv2) en el ® del Cisco IOS cuando se utiliza una clave previamente compartida (PSK). Además, este documento proporciona la información sobre cómo traducir ciertas líneas del debug en una configuración.

Prerrequisitos

Requisitos

Cisco recomienda que usted tiene conocimiento del intercambio de paquetes para IKEv2. Para más información, refiera al intercambio de paquetes IKEv2 y al debugging del nivel del protocolo.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Intercambio de claves de Internet versión 2 (IKEv2)
- Cisco IOS 15.1(1)T o más adelante

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Cuestión central

El intercambio de paquetes en IKEv2 es radicalmente diferente del intercambio de paquetes en IKEv1. En IKEv1 había un intercambio claramente demarcado phase1 que consistió en seis (6) paquetes seguidos por un intercambio de la fase 2 que consistió en tres (3) paquetes; el intercambio IKEv2 es variable. Para más información sobre las diferencias y una explicación del intercambio de paquetes, refiera al intercambio de paquetes IKEv2 y al debugging del nivel del protocolo.

Configuración del router

Esta sección enumera las configuraciones usadas en este documento.

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
```

Troubleshooting

Depuración del router

Utilizan a estos comandos debug en este documento:

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

Descripción del mensaje del router1 (iniciador)	Depuraciones	Descripción del mensaje del router2 (respondedor)
	* 11 de noviembre 20:28:34.003: IKEv2:Got un paquete del repartidor * 11 de noviembre 20:28:34.003: IKEv2: Proceso de un elemento de la cola del pak	
El router1 recibe un paquete que haga juego el acl crypto para el par ASA 10.0.0.2. Creación iniciados SA	* 11 de noviembre 19:30:34.811: Clave del preshared del IKEv2:% que consigue por el direccionamiento 10.0.0.2 * 11 de noviembre 19:30:34.811: Oferta PHASE1-prop IKEv2:Adding al policyle del juego de herramientas * 11 de noviembre 19:30:34.811: IKEv2:(1): Elegir el perfil IKEV2-SETUP IKE * 11 de noviembre 19:30:34.811: Petición ikev2 sa IKEv2:New admitida * 11 de noviembre 19:30:34.811: Cuenta de negociación saliente sa IKEv2:Incrementing por una	
El primer par de mensajes es el intercambio IKE_SA_INIT. Estos mensajes negocian los algoritmos criptográficos, nonces del intercambio, y hacen a intercambio Diffie-Hellman. **Configuración pertinente:** `telecontrol local Cisco de la clave previamente compartida de Cisco ikev2 de la oferta PHASE1-prop del cifrado 3des aes-cbc-128 de la integridad sha1 del group2 ikev2 del llavero KEYRNG del`	* 11 de noviembre 19:30:34.811: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000 (i) MsgID = 00000000 CurState: Evento OCIOSO: EV_INIT_SA * 11 de noviembre 19:30:34.811: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000 (i) MsgID = 00000000 CurState: Evento I_BLD_INIT: EV_GET_IKE_POLICY * 11 de noviembre 19:30:34.811: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000 (i) MsgID = 00000000 CurState: Evento I_BLD_INIT: **EV_SET_POLICY** * 11 de noviembre 19:30:34.811: Directivas configuradas 1):Setting IKEv2:(SA ID= * 11 de noviembre 19:30:34.811: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000 (i) MsgID = 00000000 CurState: Evento I_BLD_INIT: EV_CHK_AUTH4PKI * 11 de noviembre 19:30:34.811: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000 (i) MsgID = 00000000 CurState: Evento I_BLD_INIT: **EV_GEN_DH_KEY** * 11 de noviembre 19:30:34.811: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B	

par peer1 del direccionamiento de 10.0.0.2 255.255.255.0 de la clave previamente compartida crypto crypto del nombre de host host1

Iniciador que construye el paquete IKE_INIT_SA. Contiene: Encabezado ISAKMP (SPI/version/flags), SAi1 (algoritmo criptográfico que soportes del iniciador IKE), KEi (valor de clave pública DH del iniciador), y N (nonce del iniciador).

R_SPI=0000000000000000 (i) MsgID = 00000000
CurState: Evento I_BLD_INIT: EV_NO_EVENT
* 11 de noviembre 19:30:34.811: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B
R_SPI=0000000000000000 (i) MsgID = 00000000
CurState: Evento I_BLD_INIT: EV_OK_RECD_DH_PUBKEY_RESP
* 11 de noviembre 19:30:34.811: IKEv2:(SA ID= 1):Action: Action_Null
* 11 de noviembre 19:30:34.811: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B
R_SPI=0000000000000000 (i) MsgID = 00000000
CurState: Evento I_BLD_INIT: EV_GET_CONFIG_MODE
* 11 de noviembre 19:30:34.811: Iniciador IKEv2:IKEv2 - ningunos datos de los config a enviar en el intercambio IKE_SA_INIT
* 11 de noviembre 19:30:34.811: Datos de los config IKEv2:No a enviar al juego de herramientas:
* 11 de noviembre 19:30:34.811: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B
R_SPI=0000000000000000 (i) MsgID = 00000000
CurState: Evento I_BLD_INIT: EV_BLD_MSG
* 11 de noviembre 19:30:34.811: Payload específico del vendedor IKEv2:Construct: DELETE-REASON
* 11 de noviembre 19:30:34.811: Payload específico del vendedor IKEv2:Construct: (ADUANA)
* 11 de noviembre 19:30:34.811: IKEv2:Construct notifican el payload: NAT_DETECTION_SOURCE_IP
* 11 de noviembre 19:30:34.811: IKEv2:Construct notifican el payload: NAT_DETECTION_DESTINATION_IP
* 11 de noviembre 19:30:34.811: Payload **IKEv2:(SA ID= 1):Next**: SA, versión: 2.0 Tipo del intercambio: **IKE_SA_INIT,** indicadores: ID del mensaje del **INICIADOR**: 0, longitud: 344
Contenido del payload:
 Payload siguiente **SA**: KE, reservado: 0x0, longitud: 56
 la oferta más reciente: 0x0, reservado: 0x0, longitud: 52
 Oferta: 1, ID del protocolo: IKE, tamaño de SPI: 0, #trans: el último 5 transforma: 0x3, reservado: 0x0: longitud: 8
   tipo: 1, reservado: 0x0, identificación: 3DES
   el último transforma: 0x3, reservado: 0x0: longitud: 12
   tipo: 1, reservado: 0x0, identificación: AES-CBC
   el último transforma: 0x3, reservado: 0x0: longitud: 8
   tipo: 2, reservado: 0x0, identificación: SHA1
   el último transforma: 0x3, reservado: 0x0: longitud: 8
   tipo: 3, reservado: 0x0, identificación: SHA96
   el último transforma: 0x0, reservado: 0x0: longitud: 8
   tipo: 4, reservado: 0x0, identificación: DH_GROUP_1024_MODP/Group 2
 Payload siguiente **KE**: N, reservada: 0x0, longitud: 136
   Grupo DH: 2, reservado: 0x0
 Payload siguiente N: VID, reservado: 0x0, longitud: 24
 Payload siguiente VID: VID, reservado: 0x0, longitud: 23

Payload siguiente VID: NOTIFIQUE, reservó: 0x0, longitud: 21
Payload siguiente NOTIFY(NAT_DETECTION_SOURCE_IP): NOTIFIQUE, reservó: 0x0, longitud: 28
Identificación del Security Protocol: IKE, tamaño del spi: 0, tipo: NAT_DETECTION_SOURCE_IP
Payload siguiente NOTIFY(NAT_DETECTION_DESTINATION_IP): NINGUNOS, reservado: 0x0, longitud: 28
Identificación del Security Protocol: IKE, tamaño del spi: 0, tipo: NAT_DETECTION_DESTINATION_IP
* 11 de noviembre 19:30:34.814: IKEv2:Got un paquete del repartidor
* 11 de noviembre 19:30:34.814: IKEv2:Processing un elemento de la cola del pak
* 11 de noviembre 19:30:34.814: Petición ikev2 sa IKEv2:New admitida
* 11 de noviembre 19:30:34.814: Cuenta de negociación entrante sa IKEv2:Incrementing por una
* 11 de noviembre 19:30:34.814: Payload IKEv2:Next: SA, versión: 2.0 Tipo del intercambio: IKE_SA_INIT, indicadores: ID del mensaje del INICIADOR: 0, longitud: 344
Contenido del payload:
Payload siguiente SA: KE, reservado: 0x0, longitud: 56
la oferta más reciente: 0x0, reservado: 0x0, longitud: 52
Oferta: 1, ID del protocolo: IKE, tamaño de SPI: 0, #trans: el último 5 transforma: 0x3, reservado: 0x0: longitud: 8
tipo: 1, reservado: 0x0, identificación: 3DES
el último transforma: 0x3, reservado: 0x0: longitud: 12
tipo: 1, reservado: 0x0, identificación: AES-CBC
el último transforma: 0x3, reservado: 0x0: longitud: 8
tipo: 2, reservado: 0x0, identificación: SHA1
el último transforma: 0x3, reservado: 0x0: longitud: 8
tipo: 3, reservado: 0x0, identificación: SHA96
el último transforma: 0x0, reservado: 0x0: longitud: 8
tipo: 4, reservado: 0x0, identificación: DH_GROUP_1024_MODP/Group 2
Payload siguiente KE: N, reservada: 0x0, longitud: 136
Grupo DH: 2, reservado: 0x0
Payload siguiente N: VID, reservado: 0x0, longitud: 24

* 11 de noviembre 19:30:34.814: Payload específico del vendedor IKEv2:Parse: Payload siguiente CISCO-DELETE-REASON VID: VID, reservado: 0x0, longitud: 23
* 11 de noviembre 19:30:34.814: Payload específico del vendedor IKEv2:Parse: (ADUANA) payload siguiente VID: NOTIFIQUE, reservó: 0x0, longitud: 21
* 11 de noviembre 19:30:34.814: IKEv2:Parse notifican el payload: Payload siguiente NAT_DETECTION_SOURCE_IP NOTIFY(NAT_DETECTION_SOURCE_IP): NOTIFIQUE,

El respondedor recibe IKE_INIT_SA.

El respondedor inicia la creación SA para ese par.

reservó: 0x0, longitud: 28
    Identificación del Security Protocol: IKE, tamaño del spi: 0, tipo: NAT_DETECTION_SOURCE_IP
* 11 de noviembre 19:30:34.814: IKEv2:Parse notifican el payload: Payload
siguiente NAT_DETECTION_DESTINATION_IP
NOTIFY(NAT_DETECTION_DESTINATION_IP): NINGUNOS, reservado: 0x0, longitud: 28
    Identificación del Security Protocol: IKE, tamaño del spi: 0, tipo: NAT_DETECTION_DESTINATION_IP
* 11 de noviembre 19:30:34.814: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000000 CurState: Evento OCIOSO: **EV_RECV_INIT**
* 11 de noviembre 19:30:34.814: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000000 CurState: Evento R_INIT: **EV_VERIFY_MSG**
* 11 de noviembre 19:30:34.814: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000000 CurState: Evento R_INIT: **EV_INSERT_SA**
* 11 de noviembre 19:30:34.814: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000000 CurState: Evento R_INIT: **EV_GET_IKE_POLICY**
* 11 de noviembre 19:30:34.814: Valor por defecto de la oferta IKEv2:Adding a la directiva del juego de herramientas
* 11 de noviembre 19:30:34.814: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000000 CurState: Evento R_INIT: **EV_PROC_MSG**
* 11 de noviembre 19:30:34.814: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000000 CurState: Evento R_INIT: EV_DETECT_NAT
* 11 de noviembre 19:30:34.814: La detección IKEv2:(SA ID= 1):Process NAT notifica
* 11 de noviembre 19:30:34.814: IKEv2:(SA ID= 1):Processing nacionales detectan el src para notificar
* 11 de noviembre 19:30:34.814: Direccionamiento IKEv2:(SA ID= 1):Remote correspondido con
* 11 de noviembre 19:30:34.814: IKEv2:(SA ID= 1):Processing nacionales detectan el dst para notificar
* 11 de noviembre 19:30:34.814: Direccionamiento IKEv2:(SA ID= 1):Local correspondido con
* 11 de noviembre 19:30:34.814: IKEv2:(SA ID= 1):No NAT encontrado
* 11 de noviembre 19:30:34.814: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000000 CurState: Evento R_INIT: EV_CHK_CONFIG_MODE

El respondedor verifica y procesa el mensaje IKE_INIT: (1) elige la habitación crypto de ésas ofrecidas por el iniciador, (2) computa su propia clave secreta DH, y (3) computa un valor del skeyid, del cual todas las claves se pueden derivar para este IKE_SA. Se cifran y se autentican todos pero las encabezados de todos los mensajes que siguen. Las claves usadas para la protección del cifrado y de la integridad se derivan de SKEYID y se conocen como: SK_e (cifrado), SK_a (autenticación), SK_d se deriva y se utiliza para la derivación del material de codificación adicional para CHILD_SAs, y un SK_e y un SK_a separados se computa para cada dirección.

Configuración pertinente: `telecontrol local Cisco de la clave`

* 11 de noviembre 19:30:34.814: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000000 CurState: Evento R_BLD_INIT: EV_SET_POLICY
* 11 de noviembre 19:30:34.814: IKEv2:(SA ID= 1): **Determinación de las directivas configuradas**
* 11 de noviembre 19:30:34.814: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000000 CurState: Evento R_BLD_INIT: EV_CHK_AUTH4PKI
* 11 de noviembre 19:30:34.814: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000000 CurState: Evento R_BLD_INIT: EV_PKI_SESH_OPEN
* 11 de noviembre 19:30:34.814: IKEv2:(SA ID= 1):Opening una sesión PKI
* 11 de noviembre 19:30:34.815: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000000 CurState: Evento R_BLD_INIT: **EV_GEN_DH_KEY**
* 11 de noviembre 19:30:34.815: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000000 CurState: Evento R_BLD_INIT: EV_NO_EVENT
* 11 de noviembre 19:30:34.815: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000000 CurState: Evento R_BLD_INIT: **EV_OK_RECD_DH_PUBKEY_RESP**
* 11 de noviembre 19:30:34.815: IKEv2:(SA ID= 1):Action: Action_Null
* 11 de noviembre 19:30:34.815: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000000 CurState: Evento R_BLD_INIT: **EV_GEN_DH_SECRET**
* 11 de noviembre 19:30:34.822: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000000 CurState: Evento R_BLD_INIT: EV_NO_EVENT
* 11 de noviembre 19:30:34.822: **Clave del preshared del** IKEv2:% **que consigue por el direccionamiento 10.0.0.1**
* 11 de noviembre 19:30:34.822: Valor por defecto de la oferta IKEv2:Adding a la directiva del juego de herramientas
* 11 de noviembre 19:30:34.822: IKEv2:(2): Elegir el perfil IKEV2-SETUP IKE
* 11 de noviembre 19:30:34.822: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000000 CurState: Evento R_BLD_INIT: EV_OK_RECD_DH_SECRET_RESP
* 11 de noviembre 19:30:34.822: IKEv2:(SA ID= 1):Action: Action_Null

previamente compartida de Cisco ikev2 de la oferta PHASE1-prop del cifrado 3des aes-cbc-128 de la integridad sha1 del group2 ikev2 del llavero KEYRNG del par peer2 del direccionamiento de 10.0.0.1 255.255.255.0 de la clave previamente compartida crypto crypto del nombre de host host2

* 11 de noviembre 19:30:34.822: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000000 CurState: Evento R_BLD_INIT: **EV_GEN_SKEYID**
* 11 de noviembre 19:30:34.822: IKEv2:(SA ID= 1): **Genere el skeyid**
* 11 de noviembre 19:30:34.822: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000000 CurState: Evento R_BLD_INIT: EV_GET_CONFIG_MODE
* 11 de noviembre 19:30:34.822: Respondedor IKEv2:IKEv2 - ningunos datos de los config a enviar en el intercambio IKE_SA_INIT
* 11 de noviembre 19:30:34.822: Datos de los config IKEv2:No a enviar al juego de herramientas:
* 11 de noviembre 19:30:34.822: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000000 CurState: Evento R_BLD_INIT: EV_BLD_MSG
* 11 de noviembre 19:30:34.822: Payload específico del vendedor IKEv2:Construct: DELETE-REASON
* 11 de noviembre 19:30:34.822: Payload específico del vendedor IKEv2:Construct: (ADUANA)
* 11 de noviembre 19:30:34.822: IKEv2:Construct notifican el payload: NAT_DETECTION_SOURCE_IP
* 11 de noviembre 19:30:34.822: IKEv2:Construct notifican el payload: NAT_DETECTION_DESTINATION_IP
* 11 de noviembre 19:30:34.822: IKEv2:Construct notifican el payload: HTTP_CERT_LOOKUP_SUPPORTED
* 11 de noviembre 19:30:34.822: Payload IKEv2:(SA ID= 1):Next: SA, versión: 2.0 Tipo del intercambio: **IKE_SA_INIT,** indicadores: ID del mensaje del **RESPONDEDOR MSG-RESPONSE**: 0, longitud: 449
Contenido del payload:
 Payload siguiente **SA**: KE, reservado: 0x0, longitud: 48
  la oferta más reciente: 0x0, reservado: 0x0, longitud: 44
  Oferta: 1, ID del protocolo: IKE, tamaño de SPI: 0, #trans: el último 4 transforma: 0x3, reservado: 0x0: longitud: 12
    tipo: 1, reservado: 0x0, identificación: AES-CBC
    el último transforma: 0x3, reservado: 0x0: longitud: 8
    tipo: 2, reservado: 0x0, identificación: SHA1
    el último transforma: 0x3, reservado: 0x0: longitud: 8
    tipo: 3, reservado: 0x0, identificación: SHA96
    el último transforma: 0x0, reservado: 0x0: longitud: 8
    tipo: 4, reservado: 0x0, identificación: DH_GROUP_1024_MODP/Group 2
 Payload siguiente **KE**: N, reservada: 0x0, longitud: 136
    Grupo DH: 2, reservado: 0x0
 Payload siguiente **N**: VID, reservado: 0x0, longitud: 24
 Payload siguiente VID: VID, reservado: 0x0, longitud: 23
 Payload siguiente VID: NOTIFIQUE, reservó: 0x0, longitud: 21
 Payload siguiente

El router2 construye el mensaje del respondedor para el intercambio IKE_SA_INIT, que es recibido por ASA1. Este paquete contiene: Encabezado ISAKMP (versión/indicadores SPI/), algoritmo SAr1(cryptographic que el respondedor IKE elige), KEr (valor de clave pública DH del respondedor), y nonce del respondedor.

	NOTIFY(NAT_DETECTION_SOURCE_IP): NOTIFIQUE, reservó: 0x0, longitud: 28 Identificación del Security Protocol: IKE, tamaño del spi: 0, tipo: NAT_DETECTION_SOURCE_IP Payload siguiente NOTIFY(NAT_DETECTION_DESTINATION_IP): CERTREQ, reservado: 0x0, longitud: 28 Identificación del Security Protocol: IKE, tamaño del spi: 0, tipo: NAT_DETECTION_DESTINATION_IP Payload siguiente CERTREQ: NOTIFIQUE, reservó: 0x0, longitud: 105 Hash de la codificación CERT y URL de PKIX Payload siguiente NOTIFY(HTTP_CERT_LOOKUP_SUPPORTED): NINGUNOS, reservado: 0x0, longitud: 8 Identificación del Security Protocol: IKE, tamaño del spi: 0, tipo: HTTP_CERT_LOOKUP_SUPPORTED * 11 de noviembre 19:30:34.822: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000000 CurState: Evento INIT_DONE: EV_DONE * 11 de noviembre 19:30:34.822: Se habilita IKEv2:(SA ID= 1):Cisco DeleteReason Notify * 11 de noviembre 19:30:34.822: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000000 CurState: Evento INIT_DONE: EV_CHK4_ROLE	El router2 envía el mensaje del respondedor al router1.
	* 11 de noviembre 19:30:34.822: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000000 CurState: Evento INIT_DONE: **EV_START_TMR** * 11 de noviembre 19:30:34.822: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000000 CurState: Evento R_WAIT_AUTH: EV_NO_EVENT * 11 de noviembre 19:30:34.822: IKEv2: **Nueva petición ikev2 sa admitida** * 11 de noviembre 19:30:34.822: IKEv2: **Incrementar la cuenta de negociación saliente sa por una** * 11 de noviembre 19:30:34.823: IKEv2:Got un paquete del repartidor		
El router1 recibe el paquete de respuesta IKE_SA_INIT del router2.	* 11 de noviembre 19:30:34.823: IKEv2:Got un paquete del repartidor * 11 de noviembre 19:30:34.823: IKEv2:Processing un elemento de la cola del pak	I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000000 CurState: Evento INIT_DONE: **EV_START_TMR**	El respondedor comienza el temporizador para el proceso del auth.
El router1 verifica y procesa la	* 11 de noviembre 19:30:34.823: Payload IKEv2:(SA ID= 1):Next: SA, versión: 2.0 Tipo del intercambio:		

IKE_SA_INIT, indicadores: ID del mensaje del
RESPONDEDOR MSG-RESPONSE: 0, longitud: 449
Contenido del payload:
Payload siguiente SA: KE, reservado: 0x0, longitud: 48
la oferta más reciente: 0x0, reservado: 0x0, longitud: 44
Oferta: 1, ID del protocolo: IKE, tamaño de SPI: 0, #trans:
el último 4 transforma: 0x3, reservado: 0x0: longitud: 12
tipo: 1, reservado: 0x0, identificación: AES-CBC
el último transforma: 0x3, reservado: 0x0: longitud: 8
tipo: 2, reservado: 0x0, identificación: SHA1
el último transforma: 0x3, reservado: 0x0: longitud: 8
tipo: 3, reservado: 0x0, identificación: SHA96
el último transforma: 0x0, reservado: 0x0: longitud: 8
tipo: 4, reservado: 0x0, identificación:
DH_GROUP_1024_MODP/Group 2
Payload siguiente KE: N, reservada: 0x0, longitud: 136
Grupo DH: 2, reservado: 0x0
Payload siguiente N: VID, reservado: 0x0, longitud: 24

* 11 de noviembre 19:30:34.823: Payload específico del
vendedor IKEv2:Parse: Payload siguiente CISCO-
DELETE-REASON VID: VID, reservado: 0x0, longitud: 23

respuesta: (1) se computa la clave secreta del iniciador DH, y (2) el skeyid del iniciador también se genera.

* 11 de noviembre 19:30:34.823: Payload específico del
vendedor IKEv2:Parse: (ADUANA) payload siguiente VID:
NOTIFIQUE, reservó: 0x0, longitud: 21

* 11 de noviembre 19:30:34.823: IKEv2:Parse notifican el
payload: Payload
siguiente NAT_DETECTION_SOURCE_IP
NOTIFY(NAT_DETECTION_SOURCE_IP): NOTIFIQUE,
reservó: 0x0, longitud: 28
Identificación del Security Protocol: IKE, tamaño del spi:
0, tipo: NAT_DETECTION_SOURCE_IP

* 11 de noviembre 19:30:34.824: IKEv2:Parse notifican el
payload: Payload
siguiente NAT_DETECTION_DESTINATION_IP
NOTIFY(NAT_DETECTION_DESTINATION_IP):
CERTREQ, reservado: 0x0, longitud: 28
Identificación del Security Protocol: IKE, tamaño del spi:
0, tipo: NAT_DETECTION_DESTINATION_IP
Payload siguiente CERTREQ: NOTIFIQUE, reservó: 0x0,
longitud: 105
Hash de la codificación CERT y URL de PKIX

* 11 de noviembre 19:30:34.824: IKEv2:Parse notifican el
payload: Payload
siguiente HTTP_CERT_LOOKUP_SUPPORTED
NOTIFY(HTTP_CERT_LOOKUP_SUPPORTED):
NINGUNOS, reservado: 0x0, longitud: 8
Identificación del Security Protocol: IKE, tamaño del spi:
0, tipo: HTTP_CERT_LOOKUP_SUPPORTED

* 11 de noviembre 19:30:34.824: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000000 CurState: Evento I_WAIT_INIT: EV_RECV_INIT
* 11 de noviembre 19:30:34.824: Mensaje IKEv2:(SA ID= 1):Processing IKE_SA_INIT
* 11 de noviembre 19:30:34.824: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000000 CurState: Evento I_PROC_INIT: EV_CHK4_NOTIFY
* 11 de noviembre 19:30:34.824: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000000 CurState: Evento I_PROC_INIT: EV_VERIFY_MSG
* 11 de noviembre 19:30:34.824: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000000 CurState: Evento I_PROC_INIT: EV_PROC_MSG
* 11 de noviembre 19:30:34.824: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000000 CurState: Evento I_PROC_INIT: EV_DETECT_NAT
* 11 de noviembre 19:30:34.824: La detección IKEv2:(SA ID= 1):Process NAT notifica
* 11 de noviembre 19:30:34.824: IKEv2:(SA ID= 1):Processing nacionales detectan el src para notificar
* 11 de noviembre 19:30:34.824: Direccionamiento IKEv2:(SA ID= 1):Remote correspondido con
* 11 de noviembre 19:30:34.824: IKEv2:(SA ID= 1):Processing nacionales detectan el dst para notificar
* 11 de noviembre 19:30:34.824: Direccionamiento IKEv2:(SA ID= 1):Local correspondido con
* 11 de noviembre 19:30:34.824: IKEv2:(SA ID= 1):No NAT encontrado
* 11 de noviembre 19:30:34.824: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000000 CurState: Evento I_PROC_INIT: EV_CHK_NAT_T
* 11 de noviembre 19:30:34.824: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000000 CurState: Evento I_PROC_INIT: EV_CHK_CONFIG_MODE
* 11 de noviembre 19:30:34.824: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000000 CurState: Evento INIT_DONE: EV_GEN_DH_SECRET
* 11 de noviembre 19:30:34.831: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000000 CurState: Evento INIT_DONE: EV_NO_EVENT
* 11 de noviembre 19:30:34.831: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000000

	CurState: Evento INIT_DONE: EV_OK_RECD_DH_SECRET_RESP * 11 de noviembre 19:30:34.831: IKEv2:(SA ID= 1):Action: Action_Null * 11 de noviembre 19:30:34.831: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000000 CurState: Evento INIT_DONE: **EV_GEN_SKEYID** * 11 de noviembre 19:30:34.831: IKEv2:(SA ID= 1): **Genere el skeyid** * 11 de noviembre 19:30:34.831: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000000 CurState: Evento INIT_DONE: EV_DONE * 11 de noviembre 19:30:34.831: Se habilita IKEv2:(SA ID= 1):Cisco DeleteReason Notify * 11 de noviembre 19:30:34.831: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000000 CurState: Evento INIT_DONE: EV_CHK4_ROLE * 11 de noviembre 19:30:34.831: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000000 CurState: Evento I_BLD_AUTH: EV_GET_CONFIG_MODE * 11 de noviembre 19:30:34.831: Datos de los config IKEv2:Sending al juego de herramientas * 11 de noviembre 19:30:34.831: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000000 CurState: Evento I_BLD_AUTH: EV_CHK_EAP
El intercambio del comienzo IKE_AUTH del iniciador y genera el payload de la autenticación. El paquete IKE_AUTH contiene: La encabezado ISAKMP (versión/indicadores SPI/), IDI (la identidad del iniciador), payload AUTH, SAi2(initiates el SA-similar a la fase 2 transforma el intercambio del conjunto en IKEv1), y TSi y TSr (el iniciador y el respondedor	* 11 de noviembre 19:30:34.831: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000000 CurState: Evento I_BLD_AUTH: **EV_GEN_AUTH** * 11 de noviembre 19:30:34.831: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000000 CurState: Evento I_BLD_AUTH: EV_CHK_AUTH_TYPE * 11 de noviembre 19:30:34.831: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000000 CurState: Evento I_BLD_AUTH: EV_OK_AUTH_GEN * 11 de noviembre 19:30:34.831: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000000 CurState: Evento I_BLD_AUTH: EV_SEND_AUTH * 11 de noviembre 19:30:34.831: Payload específico del vendedor IKEv2:Construct: CISCO-GRANITE * 11 de noviembre 19:30:34.831: IKEv2:Construct notifican el payload: INITIAL_CONTACT * 11 de noviembre 19:30:34.831: IKEv2:Construct notifican el payload: SET_WINDOW_SIZE * 11 de noviembre 19:30:34.831: IKEv2:Construct notifican

el payload: ESP_TFC_NO_SUPPORT
* 11 de noviembre 19:30:34.831: IKEv2:Construct notifican el payload: NON_FIRST_FRAGS
Contenido del payload:
Payload siguiente VID: IDI, reservada: 0x0, longitud: 20
Payload siguiente **IDI**: AUTH, reservado: 0x0, longitud: 12
Tipo identificación: Direccionamiento del IPv4, reservado: 0x0 0x0
Payload siguiente **AUTH**: CFG, reservado: 0x0, longitud: 28
PSK del método del auth, reservado: 0x0, 0x0 reservado
Payload siguiente **CFG**: SA, reservado: 0x0, longitud: 309
tipo del cfg: CFG_REQUEST, reservado: 0x0, reservado: 0x0
* 11 de noviembre 19:30:34.831: Payload siguiente SA: **TSi**, reservado: 0x0, longitud: 40
la oferta más reciente: 0x0, reservado: 0x0, longitud: 36
Oferta: 1, ID del protocolo: ESP, tamaño de SPI: 4, #trans: el último 3 transforma: 0x3, reservado: 0x0: longitud: 8
tipo: 1, reservado: 0x0, identificación: 3DES
el último transforma: 0x3, reservado: 0x0: longitud: 8
tipo: 3, reservado: 0x0, identificación: SHA96
el último transforma: 0x0, reservado: 0x0: longitud: 8
tipo: 5, reservado: 0x0, identificación: No utilice ESN
Payload siguiente de **TSi**: TSr, reservado: 0x0, longitud: 24
Numérico de los TS: 1, 0x0 reservado, 0x0 reservado
Tipo TS: TS_IPV4_ADDR_RANGE, identificación proto: 0, longitud: 16
puerto del comienzo: 0, puerto del extremo: 65535
addr del comienzo: 0.0.0.0, addr del final: 255.255.255.255
Payload siguiente de **TSr**: NOTIFIQUE, reservó: 0x0, longitud: 24
Numérico de los TS: 1, 0x0 reservado, 0x0 reservado
Tipo TS: TS_IPV4_ADDR_RANGE, identificación proto: 0, longitud: 16
puerto del comienzo: 0, puerto del extremo: 65535
addr del comienzo: 0.0.0.0, addr del final: 255.255.255.255
Payload siguiente NOTIFY(INITIAL_CONTACT): NOTIFIQUE, reservó: 0x0, longitud: 8
Identificación del Security Protocol: IKE, tamaño del spi: 0, tipo: INITIAL_CONTACT
Payload siguiente NOTIFY(SET_WINDOW_SIZE): NOTIFIQUE, reservó: 0x0, longitud: 12
Identificación del Security Protocol: IKE, tamaño del spi: 0, tipo: SET_WINDOW_SIZE
Payload siguiente NOTIFY(ESP_TFC_NO_SUPPORT): NOTIFIQUE, reservó: 0x0, longitud: 8
Identificación del Security Protocol: IKE, tamaño del spi: 0, tipo: ESP_TFC_NO_SUPPORT
Payload siguiente NOTIFY(NON_FIRST_FRAGS): NINGUNOS, reservado: 0x0, longitud: 8
Identificación del Security Protocol: IKE, tamaño del spi: 0, tipo: NON_FIRST_FRAGS

trafican los selectores): Contienen a las direcciones de origen y de destino del iniciador y del respondedor respectivamente para remitir/que recibe el tráfico encriptado. El intervalo de direcciones especifica que todo el tráfico a y desde ese rango es tunneled. Si la oferta es aceptable por el respondedor, devuelve las cargas útiles idénticas TS. El primer CHILD_SA se crea para el par del proxy_ID que hace juego el paquete del activador.

Configuración pertinente:
```
transforme el conjunto determinado crypto TS ikev2-profile determinado IKEV2-SETUP del perfil de ipsec phse2-prof del IPSec del transforme el conjunto TS del esp-sha-hmac crypto del esp-3des
```

* 11 de noviembre 19:30:34.832: Payload IKEv2:(SA ID= 1):Next: ENCR, versión: 2.0 Tipo del intercambio: **IKE_AUTH**, indicadores: ID del mensaje del **INICIADOR**: 1, longitud: 556
Contenido del payload:
Payload siguiente ENCR: VID, reservado: 0x0, longitud: 528

* 11 de noviembre 19:30:34.833: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000001 **CurState:** Evento **I_WAIT_AUTH**: EV_NO_EVENT
* 11 de noviembre 19:30:34.832: IKEv2:Got un paquete del repartidor
* 11 de noviembre 19:30:34.832: IKEv2:Processing un elemento de la cola del pak
* 11 de noviembre 19:30:34.832: IKEv2:(SA ID= 1):Request tiene mess_id 1; 1 previsto a 1
* 11 de noviembre 19:30:34.832: Payload **IKEv2:(SA ID= 1):Next**: ENCR, versión: 2.0 Tipo del intercambio: **IKE_AUTH**, indicadores: ID del mensaje del **INICIADOR**: 1, longitud: 556
Contenido del payload:
* 11 de noviembre 19:30:34.832: Payload específico del vendedor IKEv2:Parse: (ADUANA) payload siguiente VID: IDI, reservada: 0x0, longitud: 20
Payload siguiente **IDI**: AUTH, reservado: 0x0, longitud: 12
Tipo identificación: Direccionamiento del IPv4, reservado: 0x0 0x0
Payload siguiente **AUTH**: CFG, reservado: 0x0, longitud: 28
PSK del método del auth, reservado: 0x0, 0x0 reservado
Payload siguiente **CFG**: SA, reservado: 0x0, longitud: 309
tipo del cfg: CFG_REQUEST, reservado: 0x0, reservado: 0x0
* 11 de noviembre 19:30:34.832: tipo del attrib: IP4 interno DNS, longitud: 0
* 11 de noviembre 19:30:34.832: tipo del attrib: IP4 interno DNS, longitud: 0
* 11 de noviembre 19:30:34.832: tipo del attrib: IP4 interno NBNS, longitud: 0
* 11 de noviembre 19:30:34.832: tipo del attrib: IP4 interno NBNS, longitud: 0
* 11 de noviembre 19:30:34.832: tipo del attrib: subred interna IP4, longitud: 0
* 11 de noviembre 19:30:34.832: tipo del attrib: versión de aplicación, longitud: 257
tipo del attrib: Desconocido - 28675, longitud: 0
* 11 de noviembre 19:30:34.832: tipo del attrib: Desconocido - 28672, longitud: 0
* 11 de noviembre 19:30:34.832: tipo del attrib:

El router2 recibe y verifica los datos de autenticación recibidos del router1.
Configuración pertinente: `md5 crypto de la integridad sha-1 del protocolo del aes-256 del cifrado del protocolo de la IPSec-oferta AES256 del IPSec ikev2 especialmente especialmente`

Desconocido - 28692, longitud: 0
* 11 de noviembre 19:30:34.832: tipo del attrib:
Desconocido - 28681, longitud: 0
* 11 de noviembre 19:30:34.832: tipo del attrib:
Desconocido - 28674, longitud: 0
* 11 de noviembre 19:30:34.832: Payload siguiente **SA**:
TSi, reservado: 0x0, longitud: 40
la oferta más reciente: 0x0, reservado: 0x0, longitud: 36
Oferta: 1, ID del protocolo: ESP, tamaño de SPI: 4,
#trans: el último 3 transforma: 0x3, reservado: 0x0:
longitud: 8
tipo: 1, reservado: 0x0, identificación: 3DES
el último transforma: 0x3, reservado: 0x0: longitud: 8
tipo: 3, reservado: 0x0, identificación: SHA96
el último transforma: 0x0, reservado: 0x0: longitud: 8
tipo: 5, reservado: 0x0, identificación: No utilice ESN
Payload siguiente de **TSi**: TSr, reservado: 0x0, longitud:
24
Numérico de los TS: 1, 0x0 reservado, 0x0 reservado
Tipo TS: TS_IPV4_ADDR_RANGE, identificación proto:
0, longitud: 16
puerto del comienzo: 0, puerto del extremo: 65535
addr del comienzo: 0.0.0.0, addr del final:
255.255.255.255
Payload siguiente de **TSr**: NOTIFIQUE, reservó: 0x0,
longitud: 24
Numérico de los TS: 1, 0x0 reservado, 0x0 reservado
Tipo TS: TS_IPV4_ADDR_RANGE, identificación proto:
0, longitud: 16
puerto del comienzo: 0, puerto del extremo: 65535
addr del comienzo: 0.0.0.0, addr del final:
255.255.255.255
* 11 de noviembre 19:30:34.832: Trace-> SA IKEv2:(SA
ID= 1):SM: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000001
CurState: Evento R_WAIT_AUTH: EV_RECV_AUTH
* 11 de noviembre 19:30:34.832: Trace-> SA IKEv2:(SA
ID= 1):SM: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000001
CurState: Evento R_WAIT_AUTH: EV_CHK_NAT_T
* 11 de noviembre 19:30:34.832: Trace-> SA IKEv2:(SA
ID= 1):SM: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000001
CurState: Evento R_WAIT_AUTH: EV_PROC_ID
* 11 de noviembre 19:30:34.832: Parameteres válidos
IKEv2:(SA ID= 1):Received en el identificador de proceso
* 11 de noviembre 19:30:34.832: Trace-> SA IKEv2:(SA
ID= 1):SM: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000001
CurState: Evento R_WAIT_AUTH:
EV_CHK_IF_PEER_CERT_NEEDS_TO_BE_FETCHED_F
OR_PROF_SEL
* 11 de noviembre 19:30:34.832: Trace-> SA IKEv2:(SA

El router2 construye la respuesta al paquete IKE_AUTH que recibió del router1. Este paquete de respuesta contiene: La encabezado ISAKMP (versión/indicadores SPI/), IDR (la identidad del respondedor), payload AUTH, SAr2(initiates el SA-similar a la fase 2 transforma el intercambio del conjunto en IKEv1), y TSi y TSr (el

ID= 1):SM: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000001
CurState: Evento R_WAIT_AUTH:
EV_GET_POLICY_BY_PEERID
* 11 de noviembre 19:30:34.833: IKEv2:(1): Elegir el perfil
IKEV2-SETUP IKE
* 11 de noviembre 19:30:34.833: Clave del preshared del
IKEv2:% que consigue por el direccionamiento 10.0.0.1
* 11 de noviembre 19:30:34.833: Clave del preshared del
IKEv2:% que consigue por el direccionamiento 10.0.0.1
* 11 de noviembre 19:30:34.833: Valor por defecto de la
oferta IKEv2:Adding a la directiva del juego de
herramientas
* 11 de noviembre 19:30:34.833: Perfil 'IKEV2-SETUP
IKEv2:(SA ID= 1):Using IKEv2
* 11 de noviembre 19:30:34.833: Trace-> SA IKEv2:(SA
ID= 1):SM: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000001
CurState: Evento R_WAIT_AUTH: EV_SET_POLICY
* 11 de noviembre 19:30:34.833: Directivas configuradas
1):Setting IKEv2:(SA ID=
* 11 de noviembre 19:30:34.833: Trace-> SA IKEv2:(SA
ID= 1):SM: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000001
CurState: Evento R_WAIT_AUTH:
EV_VERIFY_POLICY_BY_PEERID
* 11 de noviembre 19:30:34.833: Trace-> SA IKEv2:(SA
ID= 1):SM: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000001
CurState: Evento R_WAIT_AUTH: EV_CHK_AUTH4EAP
* 11 de noviembre 19:30:34.833: Trace-> SA IKEv2:(SA
ID= 1):SM: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000001
CurState: Evento R_WAIT_AUTH: EV_CHK_POLREQEAP
* 11 de noviembre 19:30:34.833: Trace-> SA IKEv2:(SA
ID= 1):SM: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000001
CurState: Evento R_VERIFY_AUTH:
EV_CHK_AUTH_TYPE
* 11 de noviembre 19:30:34.833: Trace-> SA IKEv2:(SA
ID= 1):SM: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000001
CurState: Evento R_VERIFY_AUTH:
EV_GET_PRESHR_KEY
* 11 de noviembre 19:30:34.833: Trace-> SA IKEv2:(SA
ID= 1):SM: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000001
CurState: Evento R_VERIFY_AUTH: EV_VERIFY_AUTH
* 11 de noviembre 19:30:34.833: Trace-> SA IKEv2:(SA
ID= 1):SM: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000001
CurState: Evento R_VERIFY_AUTH: EV_CHK4_IC
* 11 de noviembre 19:30:34.833: Trace-> SA IKEv2:(SA

iniciador y el respondedor trafican los selectores). Contienen a las direcciones de origen y de destino del iniciador y del respondedor respectivamente para remitir/que recibe el tráfico encriptado. El intervalo de direcciones especifica que todo el tráfico a y desde ese rango está hecho un túnel. Estos parámetros son idénticos al que fue recibido de ASA1.

ID= 1):SM: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000001
CurState: Evento R_VERIFY_AUTH: EV_CHK_REDIRECT
* 11 de noviembre 19:30:34.833: El control IKEv2:(SA ID=
1):Redirect no es necesario, saltándolo
* 11 de noviembre 19:30:34.833: Trace-> SA IKEv2:(SA
ID= 1):SM: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000001
CurState: Evento R_VERIFY_AUTH:
EV_NOTIFY_AUTH_DONE
* 11 de noviembre 19:30:34.833: La autorización del grupo
IKEv2:AAA no se configura
* 11 de noviembre 19:30:34.833: La autorización de
usuario IKEv2:AAA no se configura
* 11 de noviembre 19:30:34.833: Trace-> SA IKEv2:(SA
ID= 1):SM: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000001
CurState: Evento R_VERIFY_AUTH:
EV_CHK_CONFIG_MODE
* 11 de noviembre 19:30:34.833: Trace-> SA IKEv2:(SA
ID= 1):SM: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000001
CurState: Evento R_VERIFY_AUTH:
EV_SET_RECD_CONFIG_MODE
* 11 de noviembre 19:30:34.833: Datos de los config
IKEv2:Received del juego de herramientas:
* 11 de noviembre 19:30:34.833: Trace-> SA IKEv2:(SA
ID= 1):SM: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000001
CurState: Evento R_VERIFY_AUTH: EV_PROC_SA_TS
* 11 de noviembre 19:30:34.833: Trace-> SA IKEv2:(SA
ID= 1):SM: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000001
CurState: Evento R_VERIFY_AUTH:
EV_GET_CONFIG_MODE
* 11 de noviembre 19:30:34.833: IKEv2:Error que
construye la contestación de los config
* 11 de noviembre 19:30:34.833: Datos de los config
IKEv2:No a enviar al juego de herramientas:
* 11 de noviembre 19:30:34.833: Trace-> SA IKEv2:(SA
ID= 1):SM: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000001
CurState: Evento R_BLD_AUTH: EV_MY_AUTH_METHOD
* 11 de noviembre 19:30:34.833: Trace-> SA IKEv2:(SA
ID= 1):SM: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000001
CurState: Evento R_BLD_AUTH: EV_GET_PRESHR_KEY
* 11 de noviembre 19:30:34.833: Trace-> SA IKEv2:(SA
ID= 1):SM: I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000001
CurState: Evento R_BLD_AUTH: EV_GEN_AUTH
* 11 de noviembre 19:30:34.833: Trace-> SA IKEv2:(SA
ID= 1):SM: I_SPI=F074D8BBD5A59F0B

R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000001
CurState: Evento R_BLD_AUTH: EV_CHK4_SIGN
* 11 de noviembre 19:30:34.833: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000001 CurState: Evento R_BLD_AUTH: EV_OK_AUTH_GEN
* 11 de noviembre 19:30:34.833: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000001 CurState: Evento R_BLD_AUTH: EV_SEND_AUTH
* 11 de noviembre 19:30:34.833: Payload específico del vendedor IKEv2:Construct: CISCO-GRANITE
* 11 de noviembre 19:30:34.833: IKEv2:Construct notifican el payload: SET_WINDOW_SIZE
* 11 de noviembre 19:30:34.833: IKEv2:Construct notifican el payload: ESP_TFC_NO_SUPPORT
* 11 de noviembre 19:30:34.833: IKEv2:Construct notifican el payload: NON_FIRST_FRAGS
* 11 de noviembre 19:30:34.833: Payload IKEv2:(SA ID= 1):Next: ENCR, versión: 2.0 Tipo del intercambio: **IKE_AUTHENTIC**, indicadores: ID del mensaje del **RESPONDEDOR MSG-RESPONSE**: 1, longitud: 252
Contenido del payload:
Payload siguiente **ENCR**: VID, reservado: 0x0, longitud: 224
* 11 de noviembre 19:30:34.833: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000001 CurState: Evento AUTH_DONE: EV_OK
* 11 de noviembre 19:30:34.833: IKEv2:(SA ID= 1):Action: Action_Null
* 11 de noviembre 19:30:34.833: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000001 CurState: Evento AUTH_DONE: EV_PKI_SESH_CLOSE

El respondedor envía la respuesta para IKE_AUTH.

* 11 de noviembre 19:30:34.833: IKEv2:(SA ID= 1):Closing la sesión PKI
* 11 de noviembre 19:30:34.833: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000001 CurState: Evento AUTH_DONE: EV_UPDATE_CAC_STATS
* 11 de noviembre 19:30:34.833: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000001 CurState: Evento AUTH_DONE: **EV_INSERT_IKE**
* 11 de noviembre 19:30:34.834: Índice ikev2 1 MIB IKEv2:Store, plataforma 60
* 11 de noviembre 19:30:34.834: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000001 CurState: Evento AUTH_DONE: EV_GEN_LOAD_IPSEC

	* 11 de noviembre 19:30:34.834: Petición IKEv2:(SA ID= 1):Asynchronous hecha cola * 11 de noviembre 19:30:34.834: IKEv2:(SA ID= 1): * 11 de noviembre 19:30:34.834: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000001 CurState: Evento **AUTH_DONE**: EV_NO_EVENT		
		* 11 de noviembre 19:30:34.840: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000001 CurState: Evento AUTH_DONE: EV_OK_RECD_LOAD_IPSEC * 11 de noviembre 19:30:34.840: IKEv2:(SA ID= 1):Action: Action_Null * 11 de noviembre 19:30:34.840: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000001 CurState: Evento AUTH_DONE: EV_START_ACCT * 11 de noviembre 19:30:34.840: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000001 CurState: Evento AUTH_DONE: EV_CHECK_DUPE * 11 de noviembre 19:30:34.840: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000001 CurState: Evento AUTH_DONE: EV_CHK4_ROLE	
El iniciador recibe la respuesta del respondedor.	* 11 de noviembre 19:30:34.834: IKEv2:Got un paquete del repartidor * 11 de noviembre 19:30:34.834: IKEv2:Processing un elemento de la cola del pak		El respondedor inserta una entrada en el TRISTE.
El router1 verifica y procesa los datos de autenticación en este paquete. El router1 entonces inserta este SA en	* 11 de noviembre 19:30:34.834: Payload IKEv2:(SA ID= 1):Next: ENCR, versión: 2.0 Tipo del intercambio: **IKE_AUTH**, indicadores: ID del mensaje del **RESPONDEDOR MSG-RESPONSE**: 1, longitud: 252 **Contenido del payload:**		

* 11 de noviembre 19:30:34.834: Payload específico del vendedor IKEv2:Parse: (ADUANA) payload siguiente VID: IDR, reservado: 0x0, longitud: 20
Payload siguiente **IDR**: AUTH, reservado: 0x0, longitud: 12
Tipo identificación: Direccionamiento del IPv4, reservado: 0x0 0x0
Payload siguiente **AUTH**: SA, reservado: 0x0, longitud: 28
PSK del método del auth, reservado: 0x0, 0x0 reservado
Payload siguiente **SA**: TSi, reservado: 0x0, longitud: 40
la oferta más reciente: 0x0, reservado: 0x0, longitud: 36
Oferta: 1, ID del protocolo: ESP, tamaño de SPI: 4, #trans: el último 3 transforma: 0x3, reservado: 0x0: longitud: 8
tipo: 1, reservado: 0x0, identificación: 3DES
el último transforma: 0x3, reservado: 0x0: longitud: 8
tipo: 3, reservado: 0x0, identificación: SHA96
el último transforma: 0x0, reservado: 0x0: longitud: 8
tipo: 5, reservado: 0x0, identificación: No utilice ESN
Payload siguiente de **TSi**: TSr, reservado: 0x0, longitud: 24
Numérico de los TS: 1, 0x0 reservado, 0x0 reservado
Tipo TS: TS_IPV4_ADDR_RANGE, identificación proto: 0, longitud: 16
puerto del comienzo: 0, puerto del extremo: 65535
addr del comienzo: 0.0.0.0, addr del final: 255.255.255.255

su TRISTE.

Payload siguiente de **TSr**: NOTIFIQUE, reservó: 0x0, longitud: 24
Numérico de los TS: 1, 0x0 reservado, 0x0 reservado
Tipo TS: TS_IPV4_ADDR_RANGE, identificación proto: 0, longitud: 16
puerto del comienzo: 0, puerto del extremo: 65535
addr del comienzo: 0.0.0.0, addr del final: 255.255.255.255

* 11 de noviembre 19:30:34.834: IKEv2:Parse notifican el payload: Payload siguiente SET_WINDOW_SIZE NOTIFY(SET_WINDOW_SIZE): NOTIFIQUE, reservó: 0x0, longitud: 12
Identificación del Security Protocol: IKE, tamaño del spi: 0, tipo: SET_WINDOW_SIZE

* 11 de noviembre 19:30:34.834: IKEv2:Parse notifican el payload: Payload siguiente ESP_TFC_NO_SUPPORT NOTIFY(ESP_TFC_NO_SUPPORT): NOTIFIQUE, reservó: 0x0, longitud: 8
Identificación del Security Protocol: IKE, tamaño del spi: 0, tipo: ESP_TFC_NO_SUPPORT

* 11 de noviembre 19:30:34.834: IKEv2:Parse notifican el payload: Payload siguiente NON_FIRST_FRAGS NOTIFY(NON_FIRST_FRAGS): NINGUNOS, reservado: 0x0, longitud: 8

Identificación del Security Protocol: IKE, tamaño del spi: 0, tipo: NON_FIRST_FRAGS

* 11 de noviembre 19:30:34.834: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000001 CurState: Evento I_WAIT_AUTH: **EV_RECV_AUTH**
* 11 de noviembre 19:30:34.834: IKEv2:(SA ID= 1):Action: Action_Null
* 11 de noviembre 19:30:34.834: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000001 CurState: Evento I_PROC_AUTH: EV_CHK4_NOTIFY
* 11 de noviembre 19:30:34.834: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000001 CurState: Evento I_PROC_AUTH: **EV_PROC_MSG**
* 11 de noviembre 19:30:34.834: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000001 CurState: Evento I_PROC_AUTH: EV_CHK_IF_PEER_CERT_NEEDS_TO_BE_FETCHED_FOR_PROF_SEL
* 11 de noviembre 19:30:34.834: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000001 CurState: Evento I_PROC_AUTH: EV_GET_POLICY_BY_PEERID
* 11 de noviembre 19:30:34.834: Oferta PHASE1-prop IKEv2:Adding a la directiva del juego de herramientas
* 11 de noviembre 19:30:34.834: Perfil 'IKEV2-SETUP IKEv2:(SA ID= 1):Using IKEv2
* 11 de noviembre 19:30:34.834: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000001 CurState: Evento I_PROC_AUTH: EV_VERIFY_POLICY_BY_PEERID
* 11 de noviembre 19:30:34.834: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000001 CurState: Evento I_PROC_AUTH: EV_CHK_AUTH_TYPE
* 11 de noviembre 19:30:34.834: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000001 CurState: Evento I_PROC_AUTH: EV_GET_PRESHR_KEY
* 11 de noviembre 19:30:34.835: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000001 CurState: Evento I_PROC_AUTH: **EV_VERIFY_AUTH**
* 11 de noviembre 19:30:34.835: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000001 CurState: Evento I_PROC_AUTH: EV_CHK_EAP

* 11 de noviembre 19:30:34.835: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000001 CurState: Evento I_PROC_AUTH: EV_NOTIFY_AUTH_DONE
* 11 de noviembre 19:30:34.835: La autorización del grupo IKEv2:AAA no se configura
* 11 de noviembre 19:30:34.835: La autorización de usuario IKEv2:AAA no se configura
* 11 de noviembre 19:30:34.835: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000001 CurState: Evento I_PROC_AUTH: EV_CHK_CONFIG_MODE
* 11 de noviembre 19:30:34.835: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000001 CurState: Evento I_PROC_AUTH: EV_CHK4_IC
* 11 de noviembre 19:30:34.835: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000001 CurState: Evento I_PROC_AUTH: EV_CHK_IKE_ONLY
* 11 de noviembre 19:30:34.835: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000001 CurState: Evento I_PROC_AUTH: EV_PROC_SA_TS
* 11 de noviembre 19:30:34.835: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000001 CurState: Evento AUTH_DONE: EV_OK
* 11 de noviembre 19:30:34.835: IKEv2:(SA ID= 1):Action: Action_Null
* 11 de noviembre 19:30:34.835: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000001 CurState: Evento AUTH_DONE: EV_PKI_SESH_CLOSE
* 11 de noviembre 19:30:34.835: IKEv2:(SA ID= 1):Closing la sesión PKI
* 11 de noviembre 19:30:34.835: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000001 CurState: Evento AUTH_DONE: EV_UPDATE_CAC_STATS
* 11 de noviembre 19:30:34.835: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000001 CurState: Evento AUTH_DONE: EV_INSERT_IKE
* 11 de noviembre 19:30:34.835: Índice ikev2 1 MIB IKEv2:Store, plataforma 60
* 11 de noviembre 19:30:34.835: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000001 CurState: Evento AUTH_DONE: EV_GEN_LOAD_IPSEC

	* 11 de noviembre 19:30:34.835: Petición IKEv2:(SA ID= 1):Asynchronous hecha cola * 11 de noviembre 19:30:34.835: IKEv2:(SA ID= 1): * 11 de noviembre 19:30:34.835: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000001 CurState: Evento AUTH_DONE: EV_NO_EVENT * 11 de noviembre 19:30:34.835: Mensaje 8 IKEv2:KMI consumido. No acción realizada. * 11 de noviembre 19:30:34.835: Mensaje 12 IKEv2:KMI consumido. No acción realizada. * 11 de noviembre 19:30:34.835: Datos IKEv2:No a enviar en el conjunto de la configuración de modo. * 11 de noviembre 19:30:34.841: Manija 0x80000002 identificación IKEv2:Adding asociada a SPI 0x9506D414 para la sesión 8 * 11 de noviembre 19:30:34.841: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000001 CurState: Evento AUTH_DONE: EV_OK_RECD_LOAD_IPSEC * 11 de noviembre 19:30:34.841: IKEv2:(SA ID= 1):Action: Action_Null * 11 de noviembre 19:30:34.841: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000001 CurState: Evento AUTH_DONE: EV_START_ACCT * 11 de noviembre 19:30:34.841: IKEv2:(SA ID= 1):Accounting no requerido * 11 de noviembre 19:30:34.841: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000001 CurState: Evento AUTH_DONE: EV_CHECK_DUPE * 11 de noviembre 19:30:34.841: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000001 CurState: Evento **AUTH_DONE**: EV_CHK4_ROLE		
El túnel está para arriba en el iniciador y el showsREADY del estatus.	* 11 de noviembre 19:30:34.841: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000001 CurState: **READYEvent**: EV_CHK_IKE_ONLY * 11 de noviembre 19:30:34.841: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000001	***** 11 de noviembre 19:30:34.840: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000001 CurState: Evento **LISTO**: EV_R_OK * 11 de noviembre 19:30:34.840: Trace-> SA IKEv2:(SA ID= 1):SM: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000001	El túnel está para arriba en el respondedor. El túnel del respondedor sube generalmente antes del iniciador.

CurState: Evento LISTO: EV_I_OK	CurState: Evento LISTO: EV_NO_EVENT

Debugs CHILD_SA

Este intercambio consiste en un solo par de la petición/de la respuesta y fue referido como un intercambio de la fase 2 en IKEv1. Puede ser que sea iniciado por cualquier final del IKE_SA después de que se completen los intercambios iniciales.

Descripción del mensaje del router1 CHILD_SA	Depuraciones	Descripción del mensaje del router2 CHILD_SA
El router1 inicia el intercambio CHILD_SA. Ésta es la petición CREATE_CHILD_SA. El paquete CHILD_SA contiene típicamente: • SA HDR (version.flags/tipo del intercambio) • Ni del nonce (opcional): Si el CHILD_SA se crea como parte del intercambio inicial, un segundo payload y el nonce KE no deben ser enviados) • Payload SA • KEi (Clave-opcional): La petición CREATE_CHILD_SA pudo contener opcionalmente un payload KE para que un intercambio adicional DH	* 11 de noviembre 19:31:35.873: IKEv2:Got un paquete del repartidor * 11 de noviembre 19:31:35.873: IKEv2:Processing un elemento de la cola del pak * 11 de noviembre 19:31:35.873: IKEv2:(SA ID= 2):Request tiene mess_id 3; 3 a 7 previstos * 11 de noviembre 19:31:35.873: Payload IKEv2:(SA ID= 2):Next: ENCR, versión: 2.0 **Tipo del intercambio: CREATE_CHILD_SA**, indicadores: ID del mensaje del **INICIADOR**: 3, longitud: 396 Contenido del payload: Payload siguiente **SA**: N, reservada: 0x0, longitud: 152 la oferta más reciente: 0x0, reservado: 0x0, longitud: 148 Oferta: 1, ID del protocolo: IKE, tamaño de SPI: 8, #trans: el último 15 transforma: 0x3, reservado: 0x0: longitud: 12 tipo: 1, reservado: 0x0, identificación: AES-CBC el último transforma: 0x3, reservado: 0x0: longitud: 12 tipo: 1, reservado: 0x0, identificación: AES-CBC el último transforma: 0x3, reservado: 0x0: longitud: 12 tipo: 1, reservado: 0x0, identificación: AES-CBC el último transforma: 0x3, reservado: 0x0: longitud: 8 tipo: 2, reservado: 0x0, identificación: SHA512 el último transforma: 0x3, reservado: 0x0: longitud: 8 tipo: 2, reservado: 0x0, identificación: SHA384 el último transforma: 0x3, reservado: 0x0: longitud: 8 tipo: 2, reservado: 0x0, identificación: SHA256 el último transforma: 0x3, reservado: 0x0: longitud: 8 tipo: 2, reservado: 0x0, identificación: SHA1 el último transforma: 0x3, reservado: 0x0: longitud: 8 tipo: 2, reservado: 0x0, identificación: MD5 el último transforma: 0x3, reservado: 0x0: longitud: 8 tipo: 3, reservado: 0x0, identificación: SHA512 el último transforma: 0x3, reservado: 0x0: longitud: 8 tipo: 3, reservado: 0x0, identificación: SHA384 el último transforma: 0x3, reservado: 0x0: longitud: 8 tipo: 3, reservado: 0x0, identificación: SHA256 el último transforma: 0x3, reservado: 0x0: longitud: 8	

habilite garantías más fuertes del secreto delantero para el CHILD_SA. Si las ofertas SA incluyen a diversos grupos DH, KEi debe ser un elemento del grupo que el iniciador espera que el respondedor valide. Si conjetura mal, el intercambio CREATE_CHILD_SA falla, y tendrá que revisar con un diverso KEi

- N (notifique payload-opcional). El payload de la notificación, se utiliza para transmitir los datos informativos, tales como condiciones de error y transiciones de estado, a un par IKE. Un payload de la notificación puede aparecer en un mensaje de respuesta (que especifica generalmente

tipo: 3, reservado: 0x0, identificación: SHA96
el último transforma: 0x3, reservado: 0x0: longitud: 8
tipo: 3, reservado: 0x0, identificación: MD596
el último transforma: 0x3, reservado: 0x0: longitud: 8
tipo: 4, reservado: 0x0, identificación: DH_GROUP_1536_MODP/Group 5
el último transforma: 0x0, reservado: 0x0: longitud: 8
tipo: 4, reservado: 0x0, identificación: DH_GROUP_1024_MODP/Group 2
Payload siguiente **N**: KE, reservado: 0x0, longitud: 24
Payload siguiente **KE**: NOTIFIQUE, reservó: 0x0, longitud: 136
Grupo DH: 2, reservado: 0x0

* 11 de noviembre 19:31:35.874: IKEv2:Parse notifican el payload: Payload siguiente SET_WINDOW_SIZE **NOTIFY(SET_WINDOW_SIZE)**: NINGUNOS, reservado: 0x0, longitud: 12
Identificación del Security Protocol: IKE, tamaño del spi: 0, tipo: SET_WINDOW_SIZE

* 11 de noviembre 19:31:35.874: IKEv2: (Trace-> SA **SA ID= 2):SM**: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (r) MsgID = 00000003 CurState: Evento LISTO: **EV_RECV_CREATE_CHILD**
* 11 de noviembre 19:31:35.874: IKEv2:(SA ID= 2):Action: Action_Null
* 11 de noviembre 19:31:35.874: Trace-> SA IKEv2:(SA ID= 2):SM: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (r) MsgID = 00000003 CurState: Evento CHILD_R_INIT: EV_RECV_CREATE_CHILD
* 11 de noviembre 19:31:35.874: IKEv2:(SA ID= 2):Action: Action_Null
* 11 de noviembre 19:31:35.874: Trace-> SA IKEv2:(SA ID= 2):SM: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (r) MsgID = 00000003 CurState: Evento CHILD_R_INIT: EV_VERIFY_MSG
* 11 de noviembre 19:31:35.874: Trace-> SA IKEv2:(SA ID= 2):SM: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (r) MsgID = 00000003 CurState: Evento CHILD_R_INIT: EV_CHK_CC_TYPE
* 11 de noviembre 19:31:35.874: Trace-> SA IKEv2:(SA ID= 2):SM: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (r) MsgID = 00000003 CurState: Evento CHILD_R_IKE: **EV_REKEY_IKESA**
* 11 de noviembre 19:31:35.874: Trace-> SA IKEv2:(SA ID= 2):SM: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (r) MsgID = 00000003 CurState: Evento CHILD_R_IKE: EV_GET_IKE_POLICY
* 11 de noviembre 19:31:35.874: **Clave del preshared del** IKEv2:% **que consigue por el direccionamiento 10.0.0.2**
* 11 de noviembre 19:31:35.874: Clave del preshared del

porqué una petición fue rechazada), en un intercambio INFORMATIVO (señalar un error no en una petición IKE), o en cualquier otro mensaje para indicar las capacidades del remitente o para modificar el significado de la petición. Si este intercambio CREATE_CHILD_SA está reintroduciendo un SA existente con excepción del IKE_SA, el payload principal N del tipo REKEY_SA DEBE identificar el SA que es reintroducido. Si este intercambio CREATE_CHILD_SA no está reintroduciendo un SA existente, el payload N DEBE ser omitido.

IKEv2:% que consigue por el direccionamiento 10.0.0.2
* 11 de noviembre 19:31:35.874: Oferta PHASE1-prop
IKEv2:Adding a la directiva del juego de herramientas
* 11 de noviembre 19:31:35.874: Perfil 'IKEV2-SETUP
IKEv2:(SA ID= 2):Using IKEv2
* 11 de noviembre 19:31:35.874: Trace-> SA IKEv2:(SA ID= 2):SM: I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (r) MsgID = 00000003
CurState: Evento CHILD_R_IKE: EV_PROC_MSG
* 11 de noviembre 19:31:35.874: Trace-> SA IKEv2:(SA ID= 2):SM: I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (r) MsgID = 00000003
CurState: Evento CHILD_R_IKE: EV_SET_POLICY
* 11 de noviembre 19:31:35.874: IKEv2:(SA ID= 2):
Determinación de las directivas configuradas
* 11 de noviembre 19:31:35.874: Trace-> SA IKEv2:(SA ID= 2):SM: I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (r) MsgID = 00000003
CurState: Evento CHILD_R_BLD_MSG:
EV_GEN_DH_KEY
* 11 de noviembre 19:31:35.874: Trace-> SA IKEv2:(SA ID= 2):SM: I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (r) MsgID = 00000003
CurState: Evento CHILD_R_BLD_MSG: EV_NO_EVENT
* 11 de noviembre 19:31:35.874: Trace-> SA IKEv2:(SA ID= 2):SM: I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (r) MsgID = 00000003
CurState: Evento CHILD_R_BLD_MSG:
EV_OK_RECD_DH_PUBKEY_RESP
* 11 de noviembre 19:31:35.874: IKEv2:(SA ID= 2):Action:
Action_Null
* 11 de noviembre 19:31:35.874: Trace-> SA IKEv2:(SA ID= 2):SM: I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (r) MsgID = 00000003
CurState: Evento CHILD_R_BLD_MSG:
EV_GEN_DH_SECRET
* 11 de noviembre 19:31:35.881: Trace-> SA IKEv2:(SA ID= 2):SM: I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (r) MsgID = 00000003
CurState: Evento CHILD_R_BLD_MSG: EV_NO_EVENT
* 11 de noviembre 19:31:35.882: Trace-> SA IKEv2:(SA ID= 2):SM: I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (r) MsgID = 00000003
CurState: Evento CHILD_R_BLD_MSG:
EV_OK_RECD_DH_SECRET_RESP
* 11 de noviembre 19:31:35.882: IKEv2:(SA ID= 2):Action:
Action_Null
* 11 de noviembre 19:31:35.882: Trace-> SA IKEv2:(SA ID= 2):SM: I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (r) MsgID = 00000003
CurState: Evento CHILD_R_BLD_MSG: EV_BLD_MSG
* 11 de noviembre 19:31:35.882: **IKEv2:Construct notifican el payload**: SET_WINDOW_SIZE

Contenido del payload:
Payload siguiente SA: N, reservada: 0x0, longitud: 56
la oferta más reciente: 0x0, reservado: 0x0, longitud: 52
Oferta: 1, ID del protocolo: IKE, tamaño de SPI: 8, #trans:
el último 4 transforma: 0x3, reservado: 0x0: longitud: 12
tipo: 1, reservado: 0x0, identificación: AES-CBC
el último transforma: 0x3, reservado: 0x0: longitud: 8
tipo: 2, reservado: 0x0, identificación: SHA1
el último transforma: 0x3, reservado: 0x0: longitud: 8
tipo: 3, reservado: 0x0, identificación: SHA96
el último transforma: 0x0, reservado: 0x0: longitud: 8
tipo: 4, reservado: 0x0, identificación:
DH_GROUP_1024_MODP/Group 2
Payload siguiente N: KE, reservado: 0x0, longitud: 24
Payload siguiente KE: NOTIFIQUE, reservó: 0x0, longitud:
136
Grupo DH: 2, reservado: 0x0
Payload siguiente NOTIFY(SET_WINDOW_SIZE):
NINGUNOS, reservado: 0x0, longitud: 12
Identificación del Security Protocol: IKE, tamaño del spi:
0, tipo: SET_WINDOW_SIZE
* 11 de noviembre 19:31:35.869: IKEv2: (Payload SA ID=
2):Next: ENCR, versión: 2.0 Tipo del
intercambio: CREATE_CHILD_SA, indicadores: ID del
mensaje del INICIADOR: 2, longitud: 460
Contenido del payload:
Payload siguiente ENCR: SA, reservado: 0x0, longitud:
432
* 11 de noviembre 19:31:35.873: IKEv2:Construct notifican
el payload: SET_WINDOW_SIZE
Contenido del payload:
Payload siguiente SA: N, reservada: 0x0, longitud: 152
la oferta más reciente: 0x0, reservado: 0x0, longitud: 148
Oferta: 1, ID del protocolo: IKE, tamaño de SPI: 8, #trans:
el último 15 transforma: 0x3, reservado: 0x0: longitud: 12
tipo: 1, reservado: 0x0, identificación: AES-CBC
el último transforma: 0x3, reservado: 0x0: longitud: 12
tipo: 1, reservado: 0x0, identificación: AES-CBC
el último transforma: 0x3, reservado: 0x0: longitud: 12
tipo: 1, reservado: 0x0, identificación: AES-CBC
el último transforma: 0x3, reservado: 0x0: longitud: 8
tipo: 2, reservado: 0x0, identificación: SHA512
el último transforma: 0x3, reservado: 0x0: longitud: 8
tipo: 2, reservado: 0x0, identificación: SHA384
el último transforma: 0x3, reservado: 0x0: longitud: 8
tipo: 2, reservado: 0x0, identificación: SHA256
el último transforma: 0x3, reservado: 0x0: longitud: 8
tipo: 2, reservado: 0x0, identificación: SHA1
el último transforma: 0x3, reservado: 0x0: longitud: 8
tipo: 2, reservado: 0x0, identificación: MD5
el último transforma: 0x3, reservado: 0x0: longitud: 8
tipo: 3, reservado: 0x0, identificación: SHA512
el último transforma: 0x3, reservado: 0x0: longitud: 8

Este paquete es recibido por el router2.

tipo: 3, reservado: 0x0, identificación: SHA384
el último transforma: 0x3, reservado: 0x0: longitud: 8
tipo: 3, reservado: 0x0, identificación: SHA256
el último transforma: 0x3, reservado: 0x0: longitud: 8
tipo: 3, reservado: 0x0, identificación: SHA96
el último transforma: 0x3, reservado: 0x0: longitud: 8
tipo: 3, reservado: 0x0, identificación: MD596
el último transforma: 0x3, reservado: 0x0: longitud: 8
tipo: 4, reservado: 0x0, identificación:
DH_GROUP_1536_MODP/Group 5
el último transforma: 0x0, reservado: 0x0: longitud: 8
tipo: 4, reservado: 0x0, identificación:
DH_GROUP_1024_MODP/Group 2
Payload siguiente **N**: KE, reservado: 0x0, longitud: 24
Payload siguiente **KE**: NOTIFIQUE, reservó: 0x0, longitud:
136
Grupo DH: 2, reservado: 0x0
Payload siguiente **NOTIFY(SET_WINDOW_SIZE)**:
NINGUNOS, reservado: 0x0, longitud: 12
Identificación del Security Protocol: IKE, tamaño del spi: 0,
tipo: SET_WINDOW_SIZE

* 11 de noviembre 19:31:35.882: IKEv2: (Payload **SA ID=
2):Next**: ENCR, versión: 2.0 Tipo del
intercambio: **CREATE_CHILD_SA,** indicadores: ID del
mensaje del **RESPONDEDOR MSG-RESPONSE**: 3,
longitud: 300
Contenido del payload:
Payload siguiente **SA**: N, reservada: 0x0, longitud: 56
la oferta más reciente: 0x0, reservado: 0x0, longitud: 52
Oferta: 1, ID del protocolo: IKE, tamaño de SPI: 8, #trans:
el último 4 transforma: 0x3, reservado: 0x0: longitud: 12
tipo: 1, reservado: 0x0, identificación: AES-CBC
el último transforma: 0x3, reservado: 0x0: longitud: 8
tipo: 2, reservado: 0x0, identificación: SHA1
el último transforma: 0x3, reservado: 0x0: longitud: 8
tipo: 3, reservado: 0x0, identificación: SHA96
el último transforma: 0x0, reservado: 0x0: longitud: 8
tipo: 4, reservado: 0x0, identificación:
DH_GROUP_1024_MODP/Group 2
Payload siguiente **N**: KE, reservado: 0x0, longitud: 24
Payload siguiente **KE**: NOTIFIQUE, reservó: 0x0, longitud:
136
Grupo DH: 2, reservado: 0x0

* 11 de noviembre 19:31:35.882: IKEv2:Parse notifican el
payload: Payload siguiente SET_WINDOW_SIZE
NOTIFY(SET_WINDOW_SIZE): NINGUNOS, reservado:
0x0, longitud: 12
Identificación del Security Protocol: IKE, tamaño del spi:
0, tipo: SET_WINDOW_SIZE

* 11 de noviembre 19:31:35.882: Trace-> SA IKEv2:(SA
ID= 2):SM: I_SPI=0C33DB40DBAAADE6

El router2 ahora construye la contestación para el intercambio CHILD_SA. Ésta es la respuesta CREATE_CHILD_SA. El paquete CHILD_SA contiene típicamente:

- SA HDR (version.flags/tipo del intercambio)
- Nonce Ni(optional): Si el CHILD_SA se crea como parte del intercambio inicial, un segundo payload y el nonce KE no deben ser enviados.
- Payload SA
- KEi (Clave-opcional): La

R_SPI=F14E2BBA78024DE3 (i) MsgID = 00000003 CurState: Evento **CHILD_I_WAIT**: **EV_RECV_CREATE_CHILD**
* 11 de noviembre 19:31:35.882: IKEv2:(SA ID= 2):Action: Action_Null
* 11 de noviembre 19:31:35.882: Trace-> SA IKEv2:(SA ID= 2):SM: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (i) MsgID = 00000003 CurState: Evento **CHILD_I_PROC**: EV_CHK4_NOTIFY
* 11 de noviembre 19:31:35.882: Trace-> SA IKEv2:(SA ID= 2):SM: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (i) MsgID = 00000003 CurState: Evento CHILD_I_PROC: **EV_VERIFY_MSG**
* 11 de noviembre 19:31:35.882: Trace-> SA IKEv2:(SA ID= 2):SM: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (i) MsgID = 00000003 CurState: Evento CHILD_I_PROC: EV_PROC_MSG
* 11 de noviembre 19:31:35.882: Trace-> SA IKEv2:(SA ID= 2):SM: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (i) MsgID = 00000003 CurState: Evento CHILD_I_PROC: EV_CHK4_PFS
* 11 de noviembre 19:31:35.882: Trace-> SA IKEv2:(SA ID= 2):SM: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (i) MsgID = 00000003 CurState: Evento CHILD_I_PROC: EV_GEN_DH_SECRET
* 11 de noviembre 19:31:35.890: Trace-> SA IKEv2:(SA ID= 2):SM: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (i) MsgID = 00000003 CurState: Evento CHILD_I_PROC: EV_NO_EVENT
* 11 de noviembre 19:31:35.890: Trace-> SA IKEv2:(SA ID= 2):SM: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (i) MsgID = 00000003 CurState: Evento CHILD_I_PROC: EV_OK_RECD_DH_SECRET_RESP
* 11 de noviembre 19:31:35.890: IKEv2:(SA ID= 2):Action: Action_Null
* 11 de noviembre 19:31:35.890: Trace-> SA IKEv2:(SA ID= 2):SM: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (i) MsgID = 00000003 CurState: Evento CHILD_I_PROC: EV_CHK_IKE_REKEY
* 11 de noviembre 19:31:35.890: Trace-> SA IKEv2:(SA ID= 2):SM: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (i) MsgID = 00000003 CurState: Evento CHILD_I_PROC: EV_GEN_SKEYID
* 11 de noviembre 19:31:35.890: Skeyid IKEv2:(SA ID= 2):Generate
* 11 de noviembre 19:31:35.890: Trace-> SA IKEv2:(SA ID= 2):SM: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (i) MsgID = 00000003 CurState: Evento **CHILD_I_DONE**: **EV_ACTIVATE_NEW_SA**
* 11 de noviembre 19:31:35.890: Trace-> SA IKEv2:(SA ID= 2):SM: I_SPI=0C33DB40DBAAADE6

petición CREATE_CHILD_SA pudo contener opcionalmente un payload KE para que un intercambio adicional DH habilite garantías más fuertes del secreto delantero para el CHILD_SA. Si las ofertas SA incluyen a diversos grupos DH, KEi debe ser un elemento del grupo que el iniciador espera que el respondedor valide. Si conjetura mal, el intercambio CREATE_CHILD_SA falla, y debe revisar con un diverso KEi.

- N (notifique payload-opcional): El payload de la notificación se utiliza para transmitir los datos informativos, tales como condiciones de error y transiciones de estado, a un

R_SPI=F14E2BBA78024DE3 (i) MsgID = 00000003 CurState: Evento CHILD_I_DONE: EV_UPDATE_CAC_STATS
* 11 de noviembre 19:31:35.890: Petición ikev2 sa IKEv2:New activada
* 11 de noviembre 19:31:35.890: IKEv2:Failed para decrement la cuenta para la negociación saliente
* 11 de noviembre 19:31:35.890: Trace-> SA IKEv2:(SA ID= 2):SM: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (i) MsgID = 00000003 CurState: Evento CHILD_I_DONE: EV_CHECK_DUPE
* 11 de noviembre 19:31:35.890: Trace-> SA IKEv2:(SA ID= 2):SM: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (i) MsgID = 00000003 CurState: Evento CHILD_I_DONE: EV_OK
* 11 de noviembre 19:31:35.890: Trace-> SA IKEv2:(SA ID= 2):SM: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (i) MsgID = 00000003 CurState: Evento de la SALIDA: EV_CHK_PENDING
* 11 de noviembre 19:31:35.890: La respuesta IKEv2:(SA ID= 2):Processed con el ID del mensaje 3, las peticiones se puede enviar del rango 4 a 8
* 11 de noviembre 19:31:35.890: Trace-> SA IKEv2:(SA ID= 2):SM: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (i) MsgID = 00000003 **CurState:** Evento de la **SALIDA**: EV_NO_EVENT

par IKE. Un payload de la notificación pudo aparecer en un mensaje de respuesta (que especifica generalmente porqué una petición fue rechazada), en un intercambio informativo (señalar un error no en una petición IKE), o en cualquier otro mensaje para indicar las capacidades del remitente o para modificar el significado de la petición. Si este intercambio CREATE_CHILD_SA está reintroduciendo un SA existente con excepción del IKE_SA, el payload principal N del tipo REKEY_SA debe identificar el SA que es reintroducido. Si este intercambio CREATE_CHILD_SA no está reintroduciendo un SA existente, el

payload N debe ser omitido.

El router2 manda la respuesta y completa activando nuevo NIÑO SA.

* 11 de noviembre 19:31:35.882: Payload IKEv2:(SA ID= 2):Next: ENCR, versión: 2.0 Tipo del intercambio: **CREATE_CHILD_SA**, indicadores: ID del mensaje del **RESPONDEDOR MSG-RESPONSE**: 3, longitud: 300
Contenido del payload:
Payload siguiente ENCR: SA, reservado: 0x0, longitud: 272

* 11 de noviembre 19:31:35.882: Trace-> SA IKEv2:(SA ID= 2):SM: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (r) MsgID = 00000003 CurState: Evento CHILD_R_BLD_MSG: **EV_CHK_IKE_REKEY**
* 11 de noviembre 19:31:35.882: Trace-> SA IKEv2:(SA ID= 2):SM: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (r) MsgID = 00000003 CurState: Evento CHILD_R_BLD_MSG: EV_GEN_SKEYID
* 11 de noviembre 19:31:35.882: IKEv2:(SA ID= 2): **Genere el skeyid**

El router1 recibe el paquete de respuesta del router2 y completa activando el CHILD_SA.

* 11 de noviembre 19:31:35.882: Trace-> SA IKEv2:(SA ID= 2):SM: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (r) MsgID = 00000003 CurState: Evento CHILD_R_DONE: **EV_ACTIVATE_NEW_SA**
* 11 de noviembre 19:31:35.882: Índice ikev2 3 MIB IKEv2:Store, plataforma 62
* 11 de noviembre 19:31:35.882: Trace-> SA IKEv2:(SA ID= 2):SM: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (r) MsgID = 00000003 CurState: Evento CHILD_R_DONE: EV_UPDATE_CAC_STATS
* 11 de noviembre 19:31:35.882: Petición ikev2 sa IKEv2:New activada
* 11 de noviembre 19:31:35.882: IKEv2:Failed para decrement la cuenta para la negociación entrante
* 11 de noviembre 19:31:35.882: Trace-> SA IKEv2:(SA ID= 2):SM: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (r) MsgID = 00000003 CurState: Evento **CHILD_R_DONE**: EV_CHECK_DUPE
* 11 de noviembre 19:31:35.882: Trace-> SA IKEv2:(SA ID= 2):SM: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (r) MsgID = 00000003 CurState: Evento CHILD_R_DONE: EV_OK
* 11 de noviembre 19:31:35.882: Trace-> SA IKEv2:(SA

ID= 2):SM: I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (r) MsgID = 00000003
CurState: Evento CHILD_R_DONE:
EV_START_DEL_NEG_TMR
* 11 de noviembre 19:31:35.882: IKEv2:(SA ID= 2):Action:
Action_Null
* 11 de noviembre 19:31:35.882: Trace-> SA IKEv2:(SA
ID= 2):SM: I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (r) MsgID = 00000003
CurState: Evento de la SALIDA: EV_CHK_PENDING
* 11 de noviembre 19:31:35.882: La respuesta IKEv2:(SA
ID= 2):Sent con el ID del mensaje 3, las peticiones puede
ser el rango validado 4 a 8
* 11 de noviembre 19:31:35.882: Trace-> SA IKEv2:(SA
ID= 2):SM: I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (r) MsgID =
00000003 **CurState:** Evento de la **SALIDA**:
EV_NO_EVENT

Verificación del túnel

ISAKMP

Comando

show crypto ikev2 sa detailed

Salida del router1

```
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
```

Salida del router2

```
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

Comando

show crypto ipsec sa

> Nota: En esta salida, a diferencia en de IKEv1, el valor de grupo PFS DH aparece como “PFS (Y/N): N, grupo DH: ningunos” durante la primera negociación de túnel, pero, después de que ocurra una reintroducción, los valores correctos aparecen. Esto no es un bug, aunque el comportamiento se describe en el Id. de bug Cisco CSCug67056.
>
> La diferencia entre IKEv1 e IKEv2 es que, en estos últimos, crean al niño SA como parte del intercambio sí mismo AUTH. Utilizarían al grupo DH configurado bajo correspondencia de criptografía solamente durante reintroduce. Por lo tanto, usted vería el “PFS (Y/N): N, grupo DH: ningunos” hasta los primeros reintroducen.
>
> Con IKEv1, usted ve un diverso comportamiento, porque la creación niño SA sucede durante el Quick Mode, y el mensaje CREATE_CHILD_SA tiene una disposición de llevar el payload del intercambio de claves que especifique los parámetros DH para derivar un nuevo secreto compartido.

Salida del router1

```
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:
```

Salida del router2

```
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:
```

Usted puede también marcar la salida del comando de **sesión de criptografía de la demostración** en ambo Routers; esta salida muestra el estatus de la sesión de túnel como UP-ACTIVE.

```
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
```

Información Relacionada

- Intercambio de paquetes IKEv2 y debugging del nivel del protocolo
- Soporte Técnico y Documentación - Cisco Systems