Resolución de Problemas de Depuraciones de IOS IKEv2 para VPN de Sitio a Sitio con PSKs

Contenido

Introducción

Este documento describe las depuraciones de Intercambio de claves de Internet versión 2 (IKEv2) en Cisco IOS® cuando se utiliza una clave no compartida (PSK).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento del intercambio de paquetes para IKEv2. Para obtener más información, consulte Intercambio de paquetes IKEv2 y Depuración a nivel de 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 posterior

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 tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Convenciones

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

Antecedentes

Este documento proporciona información sobre cómo traducir ciertas líneas de depuración en una configuración.

Problema principal

El intercambio de paquetes en IKEv2 es radicalmente diferente del intercambio de paquetes en IKEv1. En IKEv1 hubo un intercambio de fase 1 claramente delimitado que constaba de seis (6) paquetes con un intercambio de fase 2 posterior que constaba de tres (3) paquetes; el intercambio IKEv2 es variable. Para obtener más información sobre las diferencias y una explicación del intercambio de paquetes, refiérase nuevamente a Intercambio de Paquetes IKEv2 y Depuración a Nivel de Protocolo.

Configuración del router

Esta sección enumera las configuraciones utilizadas 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
```

Troubleshoot

Depuración del router

Estos comandos debug se utilizan en este documento:

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

Descripción del mensaje del router 1 (iniciador)	Depuraciones	Descripción mensaje del ro 2 (Responde
El router 1 recibe un paquete que coincide con la ACL de criptografía para el par ASA 10.0.0.2. Inicia la creación de SA	*11 de noviembre 20:28:34.003: IKEv2:Recibí un paquete del distribuidor *11 de noviembre 20:28:34.003: IKEv2:Procesamiento de un elemento de la cola de pak *11 de noviembre 19:30:34.811: IKEv2:% Obteniendo clave previamente compartida por dirección 10.0.0.2 *11 de noviembre 19:30:34.811: IKEv2:Adición de la propuesta PHASE1-prop al kit de herramientas policyle *11 de noviembre 19:30:34.811: IKEv2:(1): Elegir el perfil IKE IKEV2-SETUP *11 de noviembre 19:30:34.811: IKEv2:Nueva solicitud ikev2 sa admitida *11 de noviembre 19:30:34.811: IKEv2:Incremento del recuento de sa de negociación saliente por uno	
El primer par de mensajes es el intercambio IKE_SA_INIT. Estos mensajes negocian algoritmos criptográficos, intercambian nonces y realizan un intercambio Diffie-Hellman. **Configuración relevante:** `crypto ikev2 offer PHASE1-prop encryption 3des aes-cbc-128 integration sha1 group 2crypto ikev2 keyring KEYRNG peer peer1 address 10.0.0.2 255.255.255.0`	*11 de noviembre 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 *11 de noviembre 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 *11 de noviembre 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** *11 de noviembre 19:30:34.811: IKEv2:(ID de SA = 1):Definición de políticas configuradas *11 de noviembre 19:30:34.811: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000 (I) MsgID = 00000000 CurState: I_BLD_INIT Evento: EV_CHK_AUTH4PKI *11 de noviembre 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** *11 de noviembre 19:30:34.811: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000 (I) MsgID = 00000000 CurState: I_BLD_INIT Evento: EV_NO_EVENT *11 de noviembre 19:30:34.811: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000 (I) MsgID = 00000000 CurState: I_BLD_INIT Evento: EV_OK_RECD_DH_PUBKEY_RESP *11 de noviembre 19:30:34.811: IKEv2:(ID de SA = 1):Acción: Action_Null *11 de noviembre 19:30:34.811: IKEv2:(SA ID = 1):SM Trace-> SA:	

`hostname host1` `pre-shared-key local cisco pre-shared-key remote cisco`	I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000 (I) MsgID = 00000000 CurState: I_BLD_INIT Event: EV_GET_CONFIG_MODE *11 de noviembre 19:30:34.811: IKEv2:iniciador IKEv2 - no hay datos de configuración para enviar en el intercambio IKE_SA_INIT *11 de noviembre 19:30:34.811: IKEv2:No hay datos de configuración que enviar al kit de herramientas: *11 de noviembre 19:30:34.811: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000 (I) MsgID = 00000000 CurState: I_BLD_INIT Evento: EV_BLD_MSG *11 de noviembre 19:30:34.811: IKEv2:Carga útil específica del proveedor de construcción: DELETE-REASON *11 de noviembre 19:30:34.811: IKEv2:Carga útil específica del proveedor de construcción: (PERSONALIZADA) *11 de noviembre 19:30:34.811: IKEv2:Construct Notify Payload: NAT_DETECTION_SOURCE_IP *11 de noviembre 19:30:34.811: IKEv2:Construct Notify Payload: NAT_DETECTION_DESTINATION_IP	
Iniciador que genera el paquete IKE_INIT_SA. Contiene: Encabezado ISAKMP (SPI/version/flags), SAi1 (algoritmo criptográfico compatible con el iniciador IKE), KEi (valor de clave pública DH del iniciador) y N (nombre del iniciador).	*11 de noviembre 19:30:34.811: **IKEv2:(ID de SA = 1)**:Carga siguiente: SA, versión: 2.0 Tipo de intercambio: **IKE_SA_INIT,** indicadores: **INITIATOR** ID de mensaje: 0, longitud: 344 Contenido de la carga: **SA** Siguiente carga útil: KE, reservado: 0x0, longitud: 56 última propuesta: 0x0, reservado: 0x0, longitud: 52 Propuesta: 1, ID de protocolo: IKE, tamaño de SPI: 0, #trans: 5 última transformación: 0x3, reservado: 0x0: longitud: 8 tipo: 1, reservado: 0x0, id: 3DES última transformación: 0x3, reservado: 0x0: longitud: 12 tipo: 1, reservado: 0x0, id: AES-CBC última transformación: 0x3, reservado: 0x0: longitud: 8 tipo: 2, reservado: 0x0, id: SHA1 última transformación: 0x3, reservado: 0x0: longitud: 8 tipo: 3, reservado: 0x0, id: SHA96 última transformación: 0x0, reservado: 0x0: longitud: 8 tipo: 4, reservado: 0x0, id: DH_GROUP_1024_MODP/Grupo 2 **KE** Siguiente carga útil: N, reservado: 0x0, longitud: 136 Grupo DH: 2, reservado: 0x0 N Siguiente carga: VID, reservado: 0x0, longitud: 24 VID Carga siguiente: VID, reservado: 0x0, longitud: 23 Carga siguiente de VID: NOTIFICAR, reservada: 0x0, longitud: 21 NOTIFY(NAT_DETECTION_SOURCE_IP) Siguiente carga útil: NOTIFY, reservado: 0x0, longitud: 28 ID del protocolo de seguridad: IKE, tamaño de spi: 0, tipo: NAT_DETECTION_SOURCE_IP NOTIFY(NAT_DETECTION_DESTINATION_IP) Siguiente carga útil: NONE, reservado: 0x0, longitud: 28 ID de protocolo de seguridad: IKE, tamaño de spi: 0, tipo: NAT_DETECTION_DESTINATION_IP	
----------El iniciador envió IKE_INIT_SA ---------->		
	*11 de noviembre 19:30:34.814: IKEv2:Recibí un paquete del distribuidor *11 de noviembre 19:30:34.814: IKEv2:Procesamiento de un elemento de la cola de pak *11 de noviembre 19:30:34.814: IKEv2:Nueva solicitud ikev2 sa admitida	El respondedor recibe IKE_INIT_SA.

	*11 de noviembre 19:30:34.814: IKEv2:Aumento de un recuento de sa de negociación entrante	
	*11 de noviembre 19:30:34.814: IKEv2:Siguiente carga: SA, versión: 2.0 Tipo de intercambio: IKE_SA_INIT, indicadores: ID de mensaje del INICIADOR: 0, longitud: 344 Contenido de la carga: SA Próxima carga útil: KE, reservada: 0x0, longitud: 56 última propuesta: 0x0, reservado: 0x0, longitud: 52 Propuesta: 1, ID de protocolo: IKE, tamaño de SPI: 0, #trans: 5 última transformación: 0x3, reservado: 0x0: longitud: 8 tipo: 1, reservado: 0x0, id: 3DES última transformación: 0x3, reservado: 0x0: longitud: 12 tipo: 1, reservado: 0x0, id: AES-CBC última transformación: 0x3, reservado: 0x0: longitud: 8 tipo: 2, reservado: 0x0, id: SHA1 última transformación: 0x3, reservado: 0x0: longitud: 8 tipo: 3, reservado: 0x0, id: SHA96 última transformación: 0x0, reservado: 0x0: longitud: 8 tipo: 4, reservado: 0x0, id: DH_GROUP_1024_MODP/Grupo 2 Siguiente carga útil de KE: N, reservada: 0x0, longitud: 136 Grupo DH: 2, reservado: 0x0 N Siguiente carga: VID, reservado: 0x0, longitud: 24 *11 de noviembre 19:30:34.814: IKEv2:Analizar carga específica del proveedor: CISCO-DELETE-REASON VID Siguiente carga: VID, reservada: 0x0, longitud: 23 *11 de noviembre 19:30:34.814: IKEv2:Analizar carga específica del proveedor: (PERSONALIZADO) VID Carga siguiente: NOTIFICAR, reservada: 0x0, longitud: 21 *11 de noviembre 19:30:34.814: IKEv2:Analizar carga de notificación: NAT_DETECTION_SOURCE_IP NOTIFY(NAT_DETECTION_SOURCE_IP) Próxima carga: NOTIFY, reservada: 0x0, longitud: 28 ID del protocolo de seguridad: IKE, tamaño de spi: 0, tipo: NAT_DETECTION_SOURCE_IP *11 de noviembre 19:30:34.814: IKEv2:Analizar carga de notificación: NAT_DETECTION_DESTINATION_IP NOTIFY(NAT_DETECTION_DESTINATION_IP) Próxima carga: NONE, reservada: 0x0, longitud: 28 ID de protocolo de seguridad: IKE, tamaño de spi: 0, tipo: NAT_DETECTION_DESTINATION_IP	El respondedor la creación de S para ese par.
	*11 de noviembre 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** *11 de noviembre 19:30:34.814: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: R_INIT Evento:**EV_VERIFY_MSG** *11 de noviembre 19:30:34.814: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID =	El respondedor verifica y proce mensaje IKE_I (1) elige un con de criptografía entre los ofreci por el iniciador, calcula su propi

	00000000 CurState: R_INIT Evento:**EV_INSERT_SA**
	*11 de noviembre 19:30:34.814: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: R_INIT Evento:**EV_GET_IKE_POLICY**
	*11 de noviembre 19:30:34.814: IKEv2:Adición de la propuesta predeterminada a la política del kit de herramientas
	*11 de noviembre 19:30:34.814: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: R_INIT Evento:**EV_PROC_MSG**
	*11 de noviembre 19:30:34.814: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: R_INIT Evento: EV_DETECT_NAT
	*11 de noviembre 19:30:34.814: IKEv2:(ID de SA = 1):Notificación de detección de NAT de proceso
	*11 de noviembre 19:30:34.814: IKEv2:(ID de SA = 1):Procesamiento de nat detect src notify
	*11 de noviembre 19:30:34.814: IKEv2:(ID de SA = 1):Dirección remota coincidente
	*11 de noviembre 19:30:34.814: IKEv2:(ID de SA = 1):Procesamiento de notificación de detección de dst de NAT
	*11 de noviembre 19:30:34.814: IKEv2:(ID de SA = 1):Dirección local coincidente
	*11 de noviembre 19:30:34.814: IKEv2:(ID de SA = 1):No se ha encontrado NAT
	*11 de noviembre 19:30:34.814: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: R_INIT Evento: EV_CHK_CONFIG_MODE
	*11 de noviembre 19:30:34.814: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: R_BLD_INIT Evento: EV_SET_POLICY
	*11 de noviembre 19:30:34.814: IKEv2:(ID de SA = 1):**Definición de políticas configuradas**
	*11 de noviembre 19:30:34.814: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: R_BLD_INIT Evento: EV_CHK_AUTH4PKI
	*11 de noviembre 19:30:34.814: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: R_BLD_INIT Evento: EV_PKI_SESH_OPEN
	*11 de noviembre 19:30:34.814: IKEv2:(ID de SA = 1):Apertura de una sesión PKI
	*11 de noviembre 19:30:34.815: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: R_BLD_INIT Evento:**EV_GEN_DH_KEY**
	*11 de noviembre 19:30:34.815: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: R_BLD_INIT Evento: EV_NO_EVENT
	*11 de noviembre 19:30:34.815: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: R_BLD_INIT Evento:**EV_OK_RECD_DH_PUBKEY_RESP**
	*11 de noviembre 19:30:34.815: IKEv2:(ID de SA = 1):Acción: Action_Null
	*11 de noviembre 19:30:34.815: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID =
		clave secreta D
		(3) calcula un v
		skeyid, del cual
		pueden derivar
		las claves para
		IKE_SA. Todos
		encabezados de
		todos los mensa
		posteriores, exc
		los que vienen
		después, están
		cifrados y
		autenticados. La
		claves utilizada
		el cifrado y la
		protección de la
		integridad se de
		de SKEYID y s
		conocen como:
		(cifrado), SK_a
		(autenticación),
		SK_d se deriva
		utiliza para la
		derivación de
		material de clav
		adicional para
		CHILD_SAs, y
		computan un SI
		SK_a separados
		cada dirección.
		
		Configuración relevante: `prop`
		`crypto ikev2`
		`cifrado PHASE1`
		`3des aes-cbc-1`
		`integridad sha`
		`grupo 2 crypto`
		`ikev2 keyring`
		`KEYRNG peer pe`
		`dirección 10.0`
		`255.255.255.0`
		`nombre de host`
		`host2 clave`
		`previamente`
		`compartida loc`
		`cisco clave`
		`previamente`
		`compartida rem`
		`cisco`

	00000000 CurState: R_BLD_INIT Evento:**EV_GEN_DH_SECRET** *11 de noviembre 19:30:34.822: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: R_BLD_INIT Evento: EV_NO_EVENT *11 de noviembre 19:30:34.822: IKEv2:% **Obteniendo clave previamente compartida por la dirección 10.0.0.1** *11 de noviembre 19:30:34.822: IKEv2:Adición de la propuesta predeterminada a la política del kit de herramientas *11 de noviembre 19:30:34.822: IKEv2:(2): Elegir el perfil IKE IKEV2-SETUP *11 de noviembre 19:30:34.822: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: R_BLD_INIT Evento: EV_OK_RECD_DH_SECRET_RESP *11 de noviembre 19:30:34.822: IKEv2:(ID de SA = 1):Acción: Action_Null *11 de noviembre 19:30:34.822: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: R_BLD_INIT Evento:**EV_GEN_SKEYID** *11 de noviembre 19:30:34.822: IKEv2:(ID de SA = 1):**Generar skeyid** *11 de noviembre 19:30:34.822: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: R_BLD_INIT Evento: EV_GET_CONFIG_MODE *11 de noviembre 19:30:34.822: Respondedor IKEv2:IKEv2 - no hay datos de configuración para enviar en el intercambio IKE_SA_INIT *11 de noviembre 19:30:34.822: IKEv2:No hay datos de configuración que enviar al kit de herramientas: *11 de noviembre 19:30:34.822: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: R_BLD_INIT Evento: EV_BLD_MSG *11 de noviembre 19:30:34.822: IKEv2:Carga útil específica del proveedor de construcción: DELETE-REASON *11 de noviembre 19:30:34.822: IKEv2:Carga útil específica del proveedor de construcción: (PERSONALIZADA) *11 de noviembre 19:30:34.822: IKEv2:Construct Notify Payload: NAT_DETECTION_SOURCE_IP *11 de noviembre 19:30:34.822: IKEv2:Construct Notify Payload: NAT_DETECTION_DESTINATION_IP *11 de noviembre 19:30:34.822: IKEv2:Construct Notify Payload: HTTP_CERT_LOOKUP_SUPPORTED	
	*11 de noviembre 19:30:34.822: IKEv2:(SA ID = 1):Siguiente carga: SA, versión: 2.0 Tipo de intercambio: **IKE_SA_INIT,** indicadores: **RESPONDER MSG-RESPONSE** ID de mensaje: 0, longitud: 449 Contenido de la carga: **SA** Siguiente carga útil: KE, reservado: 0x0, longitud: 48 última propuesta: 0x0, reservado: 0x0, longitud: 44 Propuesta: 1, ID de protocolo: IKE, tamaño de SPI: 0, #trans: 4 última transformación: 0x3, reservado: 0x0: longitud: 12 tipo: 1, reservado: 0x0, id: AES-CBC última transformación: 0x3, reservado: 0x0: longitud: 8 tipo: 2, reservado: 0x0, id: SHA1 última transformación: 0x3, reservado: 0x0: longitud: 8	El router 2 gene mensaje de resp para el intercam IKE_SA_INIT, recibe ASA1. E paquete contien Encabezado ISAKMP (SPI/ version/flags), S (algoritmo criptográfico qu elige el respond IKE), KEr (valo clave pública D

	tipo: 3, reservado: 0x0, id: SHA96 última transformación: 0x0, reservado: 0x0: longitud: 8 tipo: 4, reservado: 0x0, id: DH_GROUP_1024_MODP/Grupo 2 **KE** Siguiente carga útil: N, reservado: 0x0, longitud: 136 Grupo DH: 2, reservado: 0x0 **N** Siguiente carga: VID, reservado: 0x0, longitud: 24 VID Carga siguiente: VID, reservado: 0x0, longitud: 23 Carga siguiente de VID: NOTIFICAR, reservada: 0x0, longitud: 21 NOTIFY(NAT_DETECTION_SOURCE_IP) Siguiente carga útil: NOTIFY, reservado: 0x0, longitud: 28 ID del protocolo de seguridad: IKE, tamaño de spi: 0, tipo: NAT_DETECTION_SOURCE_IP NOTIFY(NAT_DETECTION_DESTINATION_IP) Siguiente carga útil: CERTREQ, reservado: 0x0, longitud: 28 ID de protocolo de seguridad: IKE, tamaño de spi: 0, tipo: NAT_DETECTION_DESTINATION_IP Carga siguiente de CERTREQ: NOTIFY, reservada: 0x0, longitud: 105 Hash de codificación de certificados y URL de PKIX NOTIFY(HTTP_CERT_LOOKUP_SUPPORTED) Siguiente carga: NINGUNA, reservada: 0x0, longitud: 8 ID de protocolo de seguridad: IKE, tamaño de spi: 0, tipo: HTTP_CERT_LOOKUP_SUPPORTED		respondedor) y Responder Non
	*11 de noviembre 19:30:34.822: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: INIT_DONE Evento: EV_DONE *11 de noviembre 19:30:34.822: IKEv2:(ID de SA = 1):Cisco DeleteReason Notify está habilitado *11 de noviembre 19:30:34.822: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: INIT_DONE Evento: EV_CHK4_ROLE *11 de noviembre 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.** *11 de noviembre 19:30:34.822: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: R_WAIT_AUTH Evento: EV_NO_EVENT *11 de noviembre 19:30:34.822: IKEv2:**Nueva solicitud de ikev2 sa admitida** *11 de noviembre 19:30:34.822: IKEv2:**Incremento del recuento de sa de negociación saliente por uno**		El Router 2 env mensaje de resp al Router 1.
<----------El respondedor envió IKE_INIT_SA ----------			
El Router 1 recibe el paquete de respuesta IKE_SA_INIT del Router 2.	*11 de noviembre 19:30:34.823: IKEv2:Recibí un paquete del distribuidor *11 de noviembre 19:30:34.823: IKEv2:Recibí un paquete del distribuidor	I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: INIT_DONE Evento:**EV_START_TMR**	Responder inici temporizador pa proceso de autenticación.

	*11 de noviembre 19:30:34.823: IKEv2:Procesamiento de un elemento de la cola de pak		
El Router1 verifica y procesa la respuesta: (1) Se calcula la clave secreta DH del iniciador y (2) también se genera el Id. de clave del iniciador.	*11 de noviembre 19:30:34.823: IKEv2:(ID de SA = 1):Siguiente carga: SA, versión: 2.0 Tipo de intercambio: IKE_SA_INIT, indicadores: **RESPONDER MSG-RESPONSE** ID de mensaje: 0, longitud: 449 Contenido de la carga: **SA** Siguiente carga útil: KE, reservado: 0x0, longitud: 48 última propuesta: 0x0, reservado: 0x0, longitud: 44 Propuesta: 1, ID de protocolo: IKE, tamaño de SPI: 0, #trans: 4 última transformación: 0x3, reservado: 0x0: longitud: 12 tipo: 1, reservado: 0x0, id: AES-CBC última transformación: 0x3, reservado: 0x0: longitud: 8 tipo: 2, reservado: 0x0, id: SHA1 última transformación: 0x3, reservado: 0x0: longitud: 8 tipo: 3, reservado: 0x0, id: SHA96 última transformación: 0x0, reservado: 0x0: longitud: 8 tipo: 4, reservado: 0x0, id: DH_GROUP_1024_MODP/Grupo 2 **KE** Siguiente carga útil: N, reservado: 0x0, longitud: 136 Grupo DH: 2, reservado: 0x0 **N** Siguiente carga: VID, reservado: 0x0, longitud: 24 *11 de noviembre 19:30:34.823: IKEv2:Analizar carga específica del proveedor: CISCO-DELETE-REASON VID Siguiente carga: VID, reservada: 0x0, longitud: 23 *11 de noviembre 19:30:34.823: IKEv2:Analizar carga específica del proveedor: (PERSONALIZADO) VID Carga siguiente: NOTIFICAR, reservada: 0x0, longitud: 21 *11 de noviembre 19:30:34.823: IKEv2:Analizar carga de notificación: NAT_DETECTION_SOURCE_IP NOTIFY(NAT_DETECTION_SOURCE_IP) Próxima carga: NOTIFY, reservada: 0x0, longitud: 28 ID del protocolo de seguridad: IKE, tamaño de spi: 0, tipo: NAT_DETECTION_SOURCE_IP *11 de noviembre 19:30:34.824: IKEv2:Analizar carga de notificación: NAT_DETECTION_DESTINATION_IP NOTIFY(NAT_DETECTION_DESTINATION_IP) Próxima carga: CERTREQ, reservada: 0x0, longitud: 28 ID de protocolo de seguridad: IKE, tamaño de spi: 0, tipo: NAT_DETECTION_DESTINATION_IP Carga siguiente de CERTREQ: NOTIFY, reservada: 0x0, longitud: 105 Hash de codificación de certificados y URL de PKIX *11 de noviembre 19:30:34.824: IKEv2:Analizar carga de notificación: HTTP_CERT_LOOKUP_SUPPORTED NOTIFY(HTTP_CERT_LOOKUP_SUPPORTED) Siguiente carga: NINGUNA, reservada: 0x0, longitud: 8 ID de protocolo de seguridad: IKE, tamaño de spi: 0, tipo:	

HTTP_CERT_LOOKUP_SUPPORTED

*11 de noviembre 19:30:34.824: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState: I_WAIT_INIT Evento: EV_RECV_INIT
*11 de noviembre 19:30:34.824: IKEv2:(ID de SA = 1):Procesando mensaje IKE_SA_INIT
*11 de noviembre 19:30:34.824: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState: I_PROC_INIT Evento: EV_CHK4_NOTIFY
*11 de noviembre 19:30:34.824: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState: I_PROC_INIT Evento: EV_VERIFY_MSG
*11 de noviembre 19:30:34.824: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState: I_PROC_INIT Evento: EV_PROC_MSG
*11 de noviembre 19:30:34.824: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState: I_PROC_INIT Evento: EV_DETECT_NAT
*11 de noviembre 19:30:34.824: IKEv2:(ID de SA = 1):Notificación de detección de NAT de proceso
*11 de noviembre 19:30:34.824: IKEv2:(ID de SA = 1):Procesamiento de nat detect src notify
*11 de noviembre 19:30:34.824: IKEv2:(ID de SA = 1):Dirección remota coincidente
*11 de noviembre 19:30:34.824: IKEv2:(ID de SA = 1):Procesamiento de notificación de detección de dst de NAT
*11 de noviembre 19:30:34.824: IKEv2:(ID de SA = 1):Dirección local coincidente
*11 de noviembre 19:30:34.824: IKEv2:(ID de SA = 1):No se ha encontrado NAT
*11 de noviembre 19:30:34.824: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState: I_PROC_INIT Evento: EV_CHK_NAT_T
*11 de noviembre 19:30:34.824: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState: I_PROC_INIT Evento: EV_CHK_CONFIG_MODE
*11 de noviembre 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**
*11 de noviembre 19:30:34.831: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState: INIT_DONE Evento: EV_NO_EVENT
*11 de noviembre 19:30:34.831: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState: INIT_DONE Evento: EV_OK_RECD_DH_SECRET_RESP
*11 de noviembre 19:30:34.831: IKEv2:(ID de SA = 1):Acción: Action_Null
*11 de noviembre 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**
*11 de noviembre 19:30:34.831: IKEv2:(ID de SA = 1):**Generar skeyid**
*11 de noviembre 19:30:34.831: IKEv2:(SA ID = 1):SM Trace-> SA:

	I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState: INIT_DONE Evento: EV_DONE *11 de noviembre 19:30:34.831: IKEv2:(ID de SA = 1):Cisco DeleteReason Notify está habilitado *11 de noviembre 19:30:34.831: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState: INIT_DONE Evento: EV_CHK4_ROLE *11 de noviembre 19:30:34.831: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState: I_BLD_AUTH Evento: EV_GET_CONFIG_MODE *11 de noviembre 19:30:34.831: IKEv2:Envío de datos de configuración al kit de herramientas *11 de noviembre 19:30:34.831: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState: I_BLD_AUTH Evento: EV_CHK_EAP	
El iniciador inicia el intercambio IKE_AUTH y genera la carga útil de autenticación. El paquete IKE_AUTH contiene: Encabezado ISAKMP (SPI/ versión/flags), IDi (identidad del iniciador), carga útil AUTH, SAi2 (inicia SA-similar al intercambio de conjunto de transformación de fase 2 en IKEv1) y TSi y TSr (selectores de tráfico del iniciador y del respondedor). Contienen las direcciones de origen y destino del iniciador y el respondedor respectivamente para reenviar/recibir tráfico cifrado. El rango de direcciones especifica que todo	*11 de noviembre 19:30:34.831: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState: I_BLD_AUTH Evento:**EV_GEN_AUTH** *11 de noviembre 19:30:34.831: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState: I_BLD_AUTH Evento: EV_CHK_AUTH_TYPE *11 de noviembre 19:30:34.831: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState: I_BLD_AUTH Evento: EV_OK_AUTH_GEN *11 de noviembre 19:30:34.831: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState: I_BLD_AUTH Evento: EV_SEND_AUTH *11 de noviembre 19:30:34.831: IKEv2:Carga útil específica del proveedor de construcción: CISCO-GRANITE *11 de noviembre 19:30:34.831: IKEv2:Construir carga de notificación: INITIAL_CONTACT *11 de noviembre 19:30:34.831: IKEv2:Construct Notify Payload: SET_WINDOW_SIZE *11 de noviembre 19:30:34.831: IKEv2:Construct Notify Payload: ESP_TFC_NO_SUPPORT *11 de noviembre 19:30:34.831: IKEv2:Construct Notify Payload: NON_FIRST_FRAGS **Contenido de la carga:** VID Carga siguiente: IDi, reservado: 0x0, longitud: 20 **IDi** Siguiente carga: AUTH, reservado: 0x0, longitud: 12 Tipo de ID: dirección IPv4, reservada: 0x0 0x0 **AUTH** Siguiente carga: CFG, reservado: 0x0, longitud: 28 Método de autenticación PSK, reservado: 0x0, reservado 0x0 **CFG** Siguiente carga útil: SA, reservado: 0x0, longitud: 309 tipo cfg: CFG_REQUEST, reservado: 0x0, reservado: 0x0 *11 de noviembre 19:30:34.831: SA Carga siguiente: **TSi**, reservada: 0x0, longitud: 40 última propuesta: 0x0, reservado: 0x0, longitud: 36 Propuesta: 1, ID de protocolo: ESP, tamaño de SPI: 4, #trans: 3 última transformación: 0x3, reservado: 0x0: longitud: 8	

el tráfico hacia y desde ese rango se tuneliza. Si la propuesta es aceptable para el respondedor, devuelve cargas útiles de TS idénticas. El primer CHILD_SA se crea para el par proxy_ID que coincide con el paquete de desencadenador. **Configuración relevante:** `crypto ipsec transform-set TS esp-3des esp-sha-hmac crypto ipsec profile phse2-prof set transform-set TS set ikev2-profile IKEV2-SETUP`	tipo: 1, reservado: 0x0, id: 3DES última transformación: 0x3, reservado: 0x0: longitud: 8 tipo: 3, reservado: 0x0, id: SHA96 última transformación: 0x0, reservado: 0x0: longitud: 8 tipo: 5, reservado: 0x0, id: No usar ESN **TSi** Siguiente carga útil: TSr, reservado: 0x0, longitud: 24 Número de TS: 1, reservado 0x0, reservado 0x0 Tipo de TS: TS_IPV4_ADDR_RANGE, id de proto: 0, longitud: 16 puerto inicial: 0, puerto final: 65535 dirección inicial: 0.0.0.0, dirección final: 255.255.255.255 **TSr** Siguiente carga útil: NOTIFICAR, reservado: 0x0, longitud: 24 Número de TS: 1, reservado 0x0, reservado 0x0 Tipo de TS: TS_IPV4_ADDR_RANGE, id de proto: 0, longitud: 16 puerto inicial: 0, puerto final: 65535 dirección inicial: 0.0.0.0, dirección final: 255.255.255.255 NOTIFY(INITIAL_CONTACT) Siguiente carga útil: NOTIFY, reservado: 0x0, longitud: 8 ID de protocolo de seguridad: IKE, tamaño de spi: 0, tipo: INITIAL_CONTACT NOTIFY(SET_WINDOW_SIZE) Siguiente carga útil: NOTIFY, reservado: 0x0, longitud: 12 ID de protocolo de seguridad: IKE, tamaño de spi: 0, tipo: SET_WINDOW_SIZE NOTIFY(ESP_TFC_NO_SUPPORT) Siguiente carga útil: NOTIFY, reservada: 0x0, longitud: 8 ID de protocolo de seguridad: IKE, tamaño de spi: 0, tipo: ESP_TFC_NO_SUPPORT NOTIFY(NON_FIRST_FRAGS) Siguiente carga útil: NONE, reservado: 0x0, longitud: 8 ID de protocolo de seguridad: IKE, tamaño de spi: 0, tipo: NON_FIRST_FRAGS *11 de noviembre 19:30:34.832: IKEv2:(SA ID = 1):Siguiente carga: ENCR, versión: 2.0 Tipo de intercambio: **IKE_AUTH**, indicadores: **INITIATOR** ID de mensaje: 1, longitud: 556 Contenido de la carga: ENCR Siguiente carga útil: VID, reservado: 0x0, longitud: 528 *11 de noviembre 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 0000001 **CurState: I_WAIT_AUTH** Evento: EV_NO_EVENT	

----------El iniciador envió IKE_AUTH ---------->

	*11 de noviembre 19:30:34.832: IKEv2:Recibí un paquete del distribuidor *11 de noviembre 19:30:34.832: IKEv2:Procesamiento de un elemento de la cola de pak *11 de noviembre 19:30:34.832: IKEv2:(ID de SA = 1):La solicitud tiene el id_desorden 1; se espera del 1 al 1 *11 de noviembre 19:30:34.832: **IKEv2:(SA ID = 1)**:Siguiente carga: ENCR, versión: 2.0 Tipo de intercambio: **IKE_AUTH**, indicadores: **INITIATOR** ID de mensaje: 1, longitud: 556	El Router 2 reci verifica los dato autenticación recibidos del Ro 1. **Configuración relevante**: cryp

	Contenido de la carga:
	*11 de noviembre 19:30:34.832: IKEv2:Analizar carga específica del proveedor: (PERSONALIZADO) VID Carga siguiente: IDi, reservada: 0x0, longitud: 20
	IDi Siguiente carga: AUTH, reservado: 0x0, longitud: 12
	Tipo de ID: dirección IPv4, reservada: 0x0 0x0
	AUTH Siguiente carga útil: CFG, reservado: 0x0, longitud: 28
	Método de autenticación PSK, reservado: 0x0, reservado 0x0
	CFG Siguiente carga útil: SA, reservado: 0x0, longitud: 309
	tipo cfg: CFG_REQUEST, reservado: 0x0, reservado: 0x0
	*11 de noviembre 19:30:34.832: tipo de atributo: DNS IP4 interno, longitud: 0
	*11 de noviembre 19:30:34.832: tipo de atributo: DNS IP4 interno, longitud: 0
	*11 de noviembre 19:30:34.832: tipo de atributo: NBNS IP4 interno, longitud: 0
	*11 de noviembre 19:30:34.832: tipo de atributo: NBNS IP4 interno, longitud: 0
	*11 de noviembre 19:30:34.832: tipo de atributo: subred IP4 interna, longitud: 0
	*11 de noviembre 19:30:34.832: tipo de atributo: versión de la aplicación, longitud: 257
	Tipo de atributo: Desconocido - 28675, longitud: 0
	*11 de noviembre 19:30:34.832: tipo de atributo: Desconocido - 28672, longitud: 0
	*11 de noviembre 19:30:34.832: tipo de atributo: Desconocido - 28692, longitud: 0
	*11 de noviembre 19:30:34.832: tipo de atributo: Desconocido - 28681, longitud: 0
	*11 de noviembre 19:30:34.832: tipo de atributo: Desconocido - 28674, longitud: 0
	*11 de noviembre 19:30:34.832: **SA** Carga siguiente: TSi, reservada: 0x0, longitud: 40
	última propuesta: 0x0, reservado: 0x0, longitud: 36
	Propuesta: 1, ID de protocolo: ESP, tamaño de SPI: 4, #trans: 3 última transformación: 0x3, reservado: 0x0: longitud: 8
	tipo: 1, reservado: 0x0, id: 3DES
	última transformación: 0x3, reservado: 0x0: longitud: 8
	tipo: 3, reservado: 0x0, id: SHA96
	última transformación: 0x0, reservado: 0x0: longitud: 8
	tipo: 5, reservado: 0x0, id: No usar ESN
	TSi Siguiente carga útil: TSr, reservado: 0x0, longitud: 24
	Número de TS: 1, reservado 0x0, reservado 0x0
	Tipo de TS: TS_IPV4_ADDR_RANGE, id de proto: 0, longitud: 16
	puerto inicial: 0, puerto final: 65535
	dirección inicial: 0.0.0.0, dirección final: 255.255.255.255
	TSr Siguiente carga útil: NOTIFICAR, reservado: 0x0, longitud: 24
	Número de TS: 1, reservado 0x0, reservado 0x0
	Tipo de TS: TS_IPV4_ADDR_RANGE, id de proto: 0, longitud: 16
	puerto inicial: 0, puerto final: 65535
	dirección inicial: 0.0.0.0, dirección final: 255.255.255.255
		`ipsec ikev2 ip`
		`offer AES256`
		`protocol esp`
		`encryption aes`
		`protocol esp`
		`integration sh`
		`md5`

	*11 de noviembre 19:30:34.832: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_WAIT_AUTH Evento: EV_RECV_AUTH *11 de noviembre 19:30:34.832: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_WAIT_AUTH Evento: EV_CHK_NAT_T *11 de noviembre 19:30:34.832: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_WAIT_AUTH Evento: EV_PROC_ID *11 de noviembre 19:30:34.832: IKEv2:(ID de SA = 1):Parámetros válidos recibidos en ID de proceso *11 de noviembre 19:30:34.832: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_WAIT_AUTH Evento: EV_CHK_IF_PEER_CERT_NEEDS_TO_BE_FETCHED_FOR_PROF_SEL *11 de noviembre 19:30:34.832: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_WAIT_AUTH Evento: EV_GET_POLICY_BY_PEERID *11 de noviembre 19:30:34.833: IKEv2:(1): Elegir el perfil IKE IKEV2-SETUP *11 de noviembre 19:30:34.833: IKEv2:% Obteniendo clave previamente compartida por dirección 10.0.0.1 *11 de noviembre 19:30:34.833: IKEv2:% Obteniendo clave previamente compartida por dirección 10.0.0.1 *11 de noviembre 19:30:34.833: IKEv2:Adición de la propuesta predeterminada a la política del kit de herramientas *11 de noviembre 19:30:34.833: IKEv2:(ID de SA = 1):Uso del perfil IKEv2 'IKEV2-SETUP' *11 de noviembre 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_WAIT_AUTH Evento: EV_SET_POLICY *11 de noviembre 19:30:34.833: IKEv2:(ID de SA = 1):Definición de políticas configuradas *11 de noviembre 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_WAIT_AUTH Evento: EV_VERIFY_POLICY_BY_PEERID *11 de noviembre 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_WAIT_AUTH Evento: EV_CHK_AUTH4EAP *11 de noviembre 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_WAIT_AUTH Evento: EV_CHK_POLREQEAP *11 de noviembre 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_VERIFY_AUTH Evento: EV_CHK_AUTH_TYPE *11 de noviembre 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_VERIFY_AUTH Evento: EV_GET_PRESHR_KEY *11 de noviembre 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_VERIFY_AUTH Evento: EV_VERIFY_AUTH	El Router 2 gen respuesta al pac IKE_AUTH qu recibió del Rou Este paquete de respuesta contie encabezado ISAKMP (SPI/ versión/flags), I (identidad del respondedor), c útil AUTH, SA (inicia el interca de conjuntos de transformación SA similar al intercambio de conjuntos de transformación fase 2 en IKEv1 selectores de trá TSi y TSr (inici y respondedor). Contienen las direcciones de o y destino del iniciador y el respondedor respectivamente reenviar/recibir tráfico cifrado. rango de direcc especifica que t el tráfico hacia desde ese rango tuneliza. Estos parámetros son idénticos al que recibió de ASA

*11 de noviembre 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_VERIFY_AUTH Evento: EV_CHK4_IC
*11 de noviembre 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_VERIFY_AUTH Evento: EV_CHK_REDIRECT
*11 de noviembre 19:30:34.833: IKEv2:(ID de SA = 1):La comprobación de redirección no es necesaria, se salta
*11 de noviembre 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_VERIFY_AUTH Evento: EV_NOTIFY_AUTH_DONE
*11 de noviembre 19:30:34.833: IKEv2:La autorización de grupo AAA no está configurada
*11 de noviembre 19:30:34.833: IKEv2:La autorización de usuario AAA no está configurada
*11 de noviembre 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_VERIFY_AUTH Evento: EV_CHK_CONFIG_MODE
*11 de noviembre 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_VERIFY_AUTH Evento: EV_SET_RECD_CONFIG_MODE
*11 de noviembre 19:30:34.833: IKEv2:Datos de configuración recibidos del kit de herramientas:
*11 de noviembre 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_VERIFY_AUTH Evento: EV_PROC_SA_TS
*11 de noviembre 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_VERIFY_AUTH Evento: EV_GET_CONFIG_MODE
*11 de noviembre 19:30:34.833: IKEv2:Error al crear la respuesta de configuración
*11 de noviembre 19:30:34.833: IKEv2:No hay datos de configuración que enviar al kit de herramientas:
*11 de noviembre 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_BLD_AUTH Evento: EV_MY_AUTH_METHOD
*11 de noviembre 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_BLD_AUTH Evento: EV_GET_PRESHR_KEY
*11 de noviembre 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_BLD_AUTH Evento: EV_GEN_AUTH
*11 de noviembre 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_BLD_AUTH Evento: EV_CHK4_SIGN
*11 de noviembre 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_BLD_AUTH Evento: EV_OK_AUTH_GEN
*11 de noviembre 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID =

	00000001 CurState: R_BLD_AUTH Evento: EV_SEND_AUTH *11 de noviembre 19:30:34.833: IKEv2:Carga útil específica del proveedor de construcción: CISCO-GRANITE *11 de noviembre 19:30:34.833: IKEv2:Construct Notify Payload: SET_WINDOW_SIZE *11 de noviembre 19:30:34.833: IKEv2:Construct Notify Payload: ESP_TFC_NO_SUPPORT *11 de noviembre 19:30:34.833: IKEv2:Construct Notify Payload: NON_FIRST_FRAGS		
	*11 de noviembre 19:30:34.833: IKEv2:(SA ID = 1):Siguiente carga: ENCR, versión: 2.0 Tipo de intercambio: **IKE_AUTH**, indicadores: **RESPONDER MSG-RESPONSE** ID de mensaje: 1, longitud: 252 Contenido de la carga: **ENCR** Siguiente carga útil: VID, reservado: 0x0, longitud: 224 *11 de noviembre 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: AUTH_DONE Evento: EV_OK *11 de noviembre 19:30:34.833: IKEv2:(ID de SA = 1):Acción: Action_Null *11 de noviembre 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: AUTH_DONE Evento: EV_PKI_SESH_CLOSE *11 de noviembre 19:30:34.833: IKEv2:(ID de SA = 1):Cierre de la sesión PKI *11 de noviembre 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: AUTH_DONE Evento: EV_UPDATE_CAC_STATS *11 de noviembre 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** *11 de noviembre 19:30:34.834: IKEv2:Índice mib de tienda ikev2 1, plataforma 60 *11 de noviembre 19:30:34.834: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: AUTH_DONE Evento: EV_GEN_LOAD_IPSEC *11 de noviembre 19:30:34.834: IKEv2:(ID de SA = 1):Solicitud asíncrona en cola *11 de noviembre 19:30:34.834: IKEv2:(ID de SA = 1): *11 de noviembre 19:30:34.834: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: **AUTH_DONE** Evento: EV_NO_EVENT		El respondedor la respuesta par IKE_AUTH.
<----------El respondedor envió IKE_AUTH----------			
El iniciador recibe la respuesta del respondedor.	*11 de noviembre 19:30:34.834: IKEv2:Recibí un paquete del distribuidor *11 de noviembre 19:30:34.834: IKEv2:Procesamiento de un elemento de la cola de pak	*11 de noviembre 19:30:34.840: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: AUTH_DONE Evento: EV_OK_RECD_LOAD_IPSEC *11 de noviembre 19:30:34.840:	Responder inse una entrada en SAD.

		IKEv2:(ID de SA = 1):Acción: Action_Null *11 de noviembre 19:30:34.840: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: AUTH_DONE Evento: EV_START_ACCT *11 de noviembre 19:30:34.840: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: AUTH_DONE Evento: EV_CHECK_DUPE *11 de noviembre 19:30:34.840: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: AUTH_DONE Evento: EV_CHK4_ROLE	
El Router 1 verifica y procesa los datos de autenticación en este paquete. El Router 1 luego inserta esta SA en su SAD.	*11 de noviembre 19:30:34.834: IKEv2:(SA ID = 1):Siguiente carga: ENCR, versión: 2.0 Tipo de intercambio: **IKE_AUTH**, indicadores: **RESPONDER MSG-RESPONSE** ID de mensaje: 1, longitud: 252 **Contenido de la carga:** *11 de noviembre 19:30:34.834: IKEv2:Analizar carga específica del proveedor: (PERSONALIZADO) VID Carga siguiente: IDr, reservada: 0x0, longitud: 20 **IDr.** Siguiente carga útil: AUTH, reservado: 0x0, longitud: 12 Tipo de ID: dirección IPv4, reservada: 0x0 0x0 **AUTH** Siguiente carga útil: SA, reservado: 0x0, longitud: 28 Método de autenticación PSK, reservado: 0x0, reservado 0x0 **SA** Siguiente carga útil: TSi, reservado: 0x0, longitud: 40 última propuesta: 0x0, reservado: 0x0, longitud: 36 Propuesta: 1, ID de protocolo: ESP, tamaño de SPI: 4, #trans: 3 última transformación: 0x3, reservado: 0x0: longitud: 8 tipo: 1, reservado: 0x0, id: 3DES última transformación: 0x3, reservado: 0x0: longitud: 8 tipo: 3, reservado: 0x0, id: SHA96 última transformación: 0x0, reservado: 0x0: longitud: 8 tipo: 5, reservado: 0x0, id: No usar ESN **TSi** Siguiente carga útil: TSr, reservado: 0x0, longitud: 24 Número de TS: 1, reservado 0x0, reservado 0x0 Tipo de TS: TS_IPV4_ADDR_RANGE, id de proto: 0, longitud: 16 puerto inicial: 0, puerto final: 65535 dirección inicial: 0.0.0.0, dirección final: 255.255.255.255 **TSr** Siguiente carga útil: NOTIFICAR, reservado: 0x0, longitud: 24 Número de TS: 1, reservado 0x0, reservado 0x0	

Tipo de TS: TS_IPV4_ADDR_RANGE, id de proto: 0, longitud: 16
puerto inicial: 0, puerto final: 65535
dirección inicial: 0.0.0.0, dirección final: 255.255.255.255

*11 de noviembre 19:30:34.834: IKEv2:Analizar carga de notificación: SET_WINDOW_SIZE_NOTIFY(SET_WINDOW_SIZE) Siguiente carga: NOTIFICAR, reservado: 0x0, longitud: 12
ID de protocolo de seguridad: IKE, tamaño de spi: 0, tipo: SET_WINDOW_SIZE

*11 de noviembre 19:30:34.834: IKEv2:Analizar carga de notificación: ESP_TFC_NO_SUPPORT NOTIFY(ESP_TFC_NO_SUPPORT) Próxima carga: NOTIFY, reservada: 0x0, longitud: 8
ID de protocolo de seguridad: IKE, tamaño de spi: 0, tipo: ESP_TFC_NO_SUPPORT

*11 de noviembre 19:30:34.834: IKEv2:Analizar carga de notificación: NON_FIRST_FRAGS NOTIFY(NON_FIRST_FRAGS) Siguiente carga: NONE, reservada: 0x0, longitud: 8
ID de protocolo de seguridad: IKE, tamaño de spi: 0, tipo: NON_FIRST_FRAGS

*11 de noviembre 19:30:34.834: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: I_WAIT_AUTH Evento:**EV_RECV_AUTH**
*11 de noviembre 19:30:34.834: IKEv2:(ID de SA = 1):Acción: Action_Null
*11 de noviembre 19:30:34.834: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: I_PROC_AUTH Evento: EV_CHK4_NOTIFY
*11 de noviembre 19:30:34.834: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: I_PROC_AUTH Evento:**EV_PROC_MSG**
*11 de noviembre 19:30:34.834: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: I_PROC_AUTH Evento: EV_CHK_IF_PEER_CERT_NEEDS_TO_BE_FETCHED_FOR_PROF_SEL
*11 de noviembre 19:30:34.834: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: I_PROC_AUTH Evento: EV_GET_POLICY_BY_PEERID
*11 de noviembre 19:30:34.834: IKEv2:Adición de la propuesta PHASE1-prop a la política del kit de herramientas
*11 de noviembre 19:30:34.834: IKEv2:(ID de SA = 1):Uso del perfil IKEv2 'IKEV2-SETUP'
*11 de noviembre 19:30:34.834: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: I_PROC_AUTH Evento: EV_VERIFY_POLICY_BY_PEERID
*11 de noviembre 19:30:34.834: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: I_PROC_AUTH Evento: EV_CHK_AUTH_TYPE
*11 de noviembre 19:30:34.834: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID =

00000001 CurState: I_PROC_AUTH Evento: EV_GET_PRESHR_KEY
*11 de noviembre 19:30:34.835: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: I_PROC_AUTH Evento:**EV_VERIFY_AUTH**
*11 de noviembre 19:30:34.835: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: I_PROC_AUTH Evento: EV_CHK_EAP
*11 de noviembre 19:30:34.835: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: I_PROC_AUTH Evento:**EV_NOTIFY_AUTH_DONE**
*11 de noviembre 19:30:34.835: IKEv2:La autorización de grupo AAA no está configurada
*11 de noviembre 19:30:34.835: IKEv2:La autorización de usuario AAA no está configurada
*11 de noviembre 19:30:34.835: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: I_PROC_AUTH Evento: EV_CHK_CONFIG_MODE
*11 de noviembre 19:30:34.835: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: I_PROC_AUTH Evento: EV_CHK4_IC
*11 de noviembre 19:30:34.835: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: I_PROC_AUTH Evento: EV_CHK_IKE_ONLY
*11 de noviembre 19:30:34.835: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: I_PROC_AUTH Evento: EV_PROC_SA_TS
*11 de noviembre 19:30:34.835: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: AUTH_DONE Evento: EV_OK
*11 de noviembre 19:30:34.835: IKEv2:(ID de SA = 1):Acción: Action_Null
*11 de noviembre 19:30:34.835: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: AUTH_DONE Evento: EV_PKI_SESH_CLOSE
*11 de noviembre 19:30:34.835: IKEv2:(ID de SA = 1):Cierre de la sesión PKI
*11 de noviembre 19:30:34.835: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: AUTH_DONE Evento: EV_UPDATE_CAC_STATS
*11 de noviembre 19:30:34.835: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: AUTH_DONE Evento: EV_INSERT_IKE
*11 de noviembre 19:30:34.835: IKEv2:Índice mib de tienda ikev2 1, plataforma 60
*11 de noviembre 19:30:34.835: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: AUTH_DONE Evento: EV_GEN_LOAD_IPSEC
*11 de noviembre 19:30:34.835: IKEv2:(ID de SA = 1):Solicitud asíncrona en cola

*11 de noviembre 19:30:34.835: IKEv2:(ID de SA = 1):
*11 de noviembre 19:30:34.835: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: AUTH_DONE Evento: EV_NO_EVENT

	*11 de noviembre 19:30:34.835: se consume el mensaje IKEv2:KMI 8. No se ha realizado ninguna acción. *11 de noviembre 19:30:34.835: se consume el mensaje IKEv2:KMI 12. No se ha realizado ninguna acción. *11 de noviembre 19:30:34.835: IKEv2:No hay datos que enviar en el conjunto de configuraciones de modo. *11 de noviembre 19:30:34.841: IKEv2:Adición de un identificador ident 0x80000002 asociado con SPI 0x9506D414 para la sesión 8 *11 de noviembre 19:30:34.841: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: AUTH_DONE Evento: EV_OK_RECD_LOAD_IPSEC *11 de noviembre 19:30:34.841: IKEv2:(ID de SA = 1):Acción: Action_Null *11 de noviembre 19:30:34.841: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: AUTH_DONE Evento: EV_START_ACCT *11 de noviembre 19:30:34.841: IKEv2:(ID de SA = 1):No se requiere contabilidad *11 de noviembre 19:30:34.841: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: AUTH_DONE Evento: EV_CHECK_DUPE *11 de noviembre 19:30:34.841: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: **AUTH_DONE** Evento: EV_CHK4_ROLE		
El túnel está activo en el iniciador y el estado *muestraREADY*.	*11 de noviembre 19:30:34.841: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: READYEvent: EV_CHK_IKE_ONLY *11 de noviembre 19:30:34.841: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: READY Evento: EV_I_OK	*****11 de noviembre 19:30:34.840: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: **READY** Evento: EV_R_OK *11 de noviembre 19:30:34.840: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: READY Evento: EV_NO_EVENT	El túnel está act en el Responde El túnel Respon suele aparecer a que el iniciador

Depuraciones de CHILD_SA

Este intercambio consta de un único par de solicitud/respuesta y se denominó intercambio de fase 2 en IKEv1. Puede ser iniciado por cualquiera de los extremos de IKE_SA después de que se completen los intercambios iniciales.

Descripción del Mensaje CHILD_SA del Router 1	Depuraciones	Descripción del Mensaje CHILD_SA del Router 2
El router 1 inicia el intercambio CHILD_SA. Esta es la solicitud CREATE_CHILD_SA. El	*11 de noviembre 19:31:35.873: IKEv2:Recibí un paquete del distribuidor	

paquete CHILD_SA normalmente contiene: • SA HDR (version.flags/exchange type) • Nonce Ni (opcional): Si se crea CHILD_SA como parte del intercambio inicial, no se debe enviar una segunda carga KE ni nonce) • Carga útil de SA • KEi (clave opcional): la solicitud CREATE_CHILD_SA puede contener opcionalmente una carga útil KE para un intercambio DH adicional a fin de habilitar garantías más sólidas de confidencialidad de reenvío para CHILD_SA. Si las ofertas SA incluyen diferentes grupos DH, KEi debe ser un elemento del grupo que el iniciador espera que acepte el respondedor. Si se calcula que no es correcto, el intercambio CREATE_CHILD_SA falla y puede volver a intentarlo con una KEi diferente • N(Notificar carga útil: opcional). La carga útil de notificación se utiliza para transmitir datos informativos, como condiciones de error y transiciones de estado, a un par IKE. Una carga útil de notificación puede aparecer en un mensaje de respuesta (normalmente especifica por qué se rechazó una solicitud),	*11 de noviembre 19:31:35.873: IKEv2:Procesamiento de un elemento de la cola de pak *11 de noviembre 19:31:35.873: IKEv2:(ID de SA = 2):La solicitud tiene el id_desorden 3; se espera del 3 al 7 *11 de noviembre 19:31:35.873: IKEv2:(SA ID = 2):Siguiente carga: ENCR, versión: 2.0 **Tipo de intercambio: CREATE_CHILD_SA**, indicadores: **INITIATOR** ID de mensaje: 3, longitud: 396 Contenido de la carga: **SA** Siguiente carga útil: N, reservado: 0x0, longitud: 152 última propuesta: 0x0, reservado: 0x0, longitud: 148 Propuesta: 1, ID de protocolo: IKE, tamaño de SPI: 8, #trans: 15 última transformación: 0x3, reservado: 0x0: longitud: 12 tipo: 1, reservado: 0x0, id: AES-CBC última transformación: 0x3, reservado: 0x0: longitud: 12 tipo: 1, reservado: 0x0, id: AES-CBC última transformación: 0x3, reservado: 0x0: longitud: 12 tipo: 1, reservado: 0x0, id: AES-CBC última transformación: 0x3, reservado: 0x0: longitud: 8 tipo: 2, reservado: 0x0, id: SHA512 última transformación: 0x3, reservado: 0x0: longitud: 8 tipo: 2, reservado: 0x0, id: SHA384 última transformación: 0x3, reservado: 0x0: longitud: 8 tipo: 2, reservado: 0x0, id: SHA256 última transformación: 0x3, reservado: 0x0: longitud: 8 tipo: 2, reservado: 0x0, id: SHA1 última transformación: 0x3, reservado: 0x0: longitud: 8 tipo: 2, reservado: 0x0, id: MD5 última transformación: 0x3, reservado: 0x0: longitud: 8 tipo: 3, reservado: 0x0, id: SHA512 última transformación: 0x3, reservado: 0x0: longitud: 8 tipo: 3, reservado: 0x0, id: SHA384 última transformación: 0x3, reservado: 0x0: longitud: 8	

en un intercambio INFORMATIONAL (para informar de un error que no está en una solicitud IKE) o en cualquier otro mensaje para indicar las capacidades del remitente o modificar el significado de la solicitud.Si este intercambio CREATE_CHILD_SA está volviendo a introducir una SA existente que no sea IKE_SA, la carga útil N inicial de tipo REKEY_SA DEBE identificar la SA que se va a volver a introducir. Si este intercambio CREATE_CHILD_SA no vuelve a generar una SA existente, la carga N DEBE omitirse.	tipo: 3, reservado: 0x0, id: SHA256 última transformación: 0x3, reservado: 0x0: longitud: 8 tipo: 3, reservado: 0x0, id: SHA96 última transformación: 0x3, reservado: 0x0: longitud: 8 tipo: 3, reservado: 0x0, id: MD596 última transformación: 0x3, reservado: 0x0: longitud: 8 tipo: 4, reservado: 0x0, id: DH_GROUP_1536_MODP/Grupo 5 última transformación: 0x0, reservado: 0x0: longitud: 8 tipo: 4, reservado: 0x0, id: DH_GROUP_1024_MODP/Grupo 2 **N** Siguiente carga útil: KE, reservado: 0x0, longitud: 24 **Carga** útil **KE** siguiente: NOTIFICAR, reservada: 0x0, longitud: 136 Grupo DH: 2, reservado: 0x0 *11 de noviembre 19:31:35.874: IKEv2:Analizar carga de notificación: SET_WINDOW_SIZE **NOTIFY**(SET_WINDOW_SIZE) Carga siguiente: NINGUNA, reservada: 0x0, longitud: 12 ID de protocolo de seguridad: IKE, tamaño de spi: 0, tipo: SET_WINDOW_SIZE *11 de noviembre 19:31:35.874: IKEv2:(**SA ID = 2**):SM Trace-> SA: I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: READY Evento: **EV_RECV_CREATE_CHILD** *11 de noviembre 19:31:35.874: IKEv2:(ID de SA = 2):Acción: Action_Null *11 de noviembre 19:31:35.874: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: CHILD_R_INIT Evento: EV_RECV_CREATE_CHILD *11 de noviembre 19:31:35.874: IKEv2:(ID de SA = 2):Acción: Action_Null *11 de noviembre 19:31:35.874: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: CHILD_R_INIT Evento: EV_VERIFY_MSG	

	*11 de noviembre 19:31:35.874: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: CHILD_R_INIT Evento: EV_CHK_CC_TYPE *11 de noviembre 19:31:35.874: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: CHILD_R_IKE Evento: **EV_REKEY_IKESA** *11 de noviembre 19:31:35.874: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: CHILD_R_IKE Evento: EV_GET_IKE_POLICY *11 de noviembre 19:31:35.874: IKEv2:% **Obteniendo clave previamente compartida por la dirección 10.0.0.2** *11 de noviembre 19:31:35.874: IKEv2:% Obteniendo clave previamente compartida por dirección 10.0.0.2 *11 de noviembre 19:31:35.874: IKEv2:Adición de la propuesta PHASE1-prop a la política del kit de herramientas *11 de noviembre 19:31:35.874: IKEv2:(ID de SA = 2):Uso del perfil IKEv2 'IKEV2-SETUP' *11 de noviembre 19:31:35.874: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: CHILD_R_IKE Evento: EV_PROC_MSG *11 de noviembre 19:31:35.874: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: CHILD_R_IKE Evento: EV_SET_POLICY *11 de noviembre 19:31:35.874: IKEv2:(ID de SA = 2):**Definición de políticas configuradas** *11 de noviembre 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 Evento: EV_GEN_DH_KEY *11 de noviembre 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 Evento: EV_NO_EVENT
*11 de noviembre 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 Evento: EV_OK_RECD_DH_PUBKEY_RESP
*11 de noviembre 19:31:35.874: IKEv2:(ID de SA = 2):Acción: Action_Null
*11 de noviembre 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**
*11 de noviembre 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 Evento: EV_NO_EVENT
*11 de noviembre 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 Evento: EV_OK_RECD_DH_SECRET_RESP
*11 de noviembre 19:31:35.882: IKEv2:(ID de SA = 2):Acción: Action_Null
*11 de noviembre 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 Evento: EV_BLD_MSG
*11 de noviembre 19:31:35.882: **IKEv2:ConstructNotify Payload**: SET_WINDOW_SIZE
Contenido de la carga:
SA Siguiente carga útil: N, reservado: 0x0, longitud: 56
  última propuesta: 0x0, reservado: 0x0, longitud: 52
  Propuesta: 1, ID de protocolo: IKE, tamaño de SPI: 8, #trans: 4 última transformación: 0x3, reservado: 0x0: longitud: 12
    tipo: 1, reservado: 0x0, id: AES-CBC
    última transformación: 0x3, reservado:

	0x0: longitud: 8 tipo: 2, reservado: 0x0, id: SHA1 última transformación: 0x3, reservado: 0x0: longitud: 8 tipo: 3, reservado: 0x0, id: SHA96 última transformación: 0x0, reservado: 0x0: longitud: 8 tipo: 4, reservado: 0x0, id: DH_GROUP_1024_MODP/Grupo 2 **N** Siguiente carga útil: KE, reservado: 0x0, longitud: 24 **Carga** útil **KE** siguiente: NOTIFICAR, reservada: 0x0, longitud: 136 Grupo DH: 2, reservado: 0x0 **NOTIFY**(SET_WINDOW_SIZE) Siguiente carga: NONE, reservado: 0x0, longitud: 12 ID de protocolo de seguridad: IKE, tamaño de spi: 0, tipo: SET_WINDOW_SIZE	
	*11 de noviembre 19:31:35.869: IKEv2:(**SA ID = 2**):Carga siguiente: ENCR, versión: 2.0 Tipo de intercambio: **CREATE_CHILD_SA**, indicadores: **INITIATOR** ID de mensaje: 2, longitud: 460 Contenido de la carga: ENCR Carga útil siguiente: SA, reservada: 0x0, longitud: 432 *11 de noviembre 19:31:35.873: IKEv2:Construct Notify Payload: SET_WINDOW_SIZE Contenido de la carga: **SA** Siguiente carga útil: N, reservado: 0x0, longitud: 152 última propuesta: 0x0, reservado: 0x0, longitud: 148 Propuesta: 1, ID de protocolo: IKE, tamaño de SPI: 8, #trans: 15 última transformación: 0x3, reservado: 0x0: longitud: 12 tipo: 1, reservado: 0x0, id: AES-CBC última transformación: 0x3, reservado: 0x0: longitud: 12 tipo: 1, reservado: 0x0, id: AES-CBC última transformación: 0x3, reservado: 0x0: longitud: 12 tipo: 1, reservado: 0x0, id: AES-CBC última transformación: 0x3, reservado: 0x0: longitud: 8 tipo: 2, reservado: 0x0, id: SHA512 última transformación: 0x3, reservado: 0x0:	El router 2 recibe este paquete.

	longitud: 8 tipo: 2, reservado: 0x0, id: SHA384 última transformación: 0x3, reservado: 0x0: longitud: 8 tipo: 2, reservado: 0x0, id: SHA256 última transformación: 0x3, reservado: 0x0: longitud: 8 tipo: 2, reservado: 0x0, id: SHA1 última transformación: 0x3, reservado: 0x0: longitud: 8 tipo: 2, reservado: 0x0, id: MD5 última transformación: 0x3, reservado: 0x0: longitud: 8 tipo: 3, reservado: 0x0, id: SHA512 última transformación: 0x3, reservado: 0x0: longitud: 8 tipo: 3, reservado: 0x0, id: SHA384 última transformación: 0x3, reservado: 0x0: longitud: 8 tipo: 3, reservado: 0x0, id: SHA256 última transformación: 0x3, reservado: 0x0: longitud: 8 tipo: 3, reservado: 0x0, id: SHA96 última transformación: 0x3, reservado: 0x0: longitud: 8 tipo: 3, reservado: 0x0, id: MD596 última transformación: 0x3, reservado: 0x0: longitud: 8 tipo: 4, reservado: 0x0, id: DH_GROUP_1536_MODP/Grupo 5 última transformación: 0x0, reservado: 0x0: longitud: 8 tipo: 4, reservado: 0x0, id: DH_GROUP_1024_MODP/Grupo 2 **N** Siguiente carga útil: KE, reservado: 0x0, longitud: 24 **Carga** útil siguiente de KE: NOTIFICAR, reservada: 0x0, longitud: 136 Grupo DH: 2, reservado: 0x0 **NOTIFY**(SET_WINDOW_SIZE) Siguiente carga: NONE, reservado: 0x0, longitud: 12 ID de protocolo de seguridad: IKE, tamaño de spi: 0, tipo: SET_WINDOW_SIZE	
	*11 de noviembre 19:31:35.882: IKEv2:(**SA ID = 2**):Carga siguiente: ENCR, versión: 2.0 Tipo de intercambio: **CREATE_CHILD_SA,** indicadores: **RESPONDER MSG-RESPONSE** ID de mensaje: 3, longitud: 300 Contenido de la carga: **SA** Siguiente carga útil: N, reservado: 0x0,	El Router 2 ahora genera la respuesta para el intercambio CHILD_SA. Esta es la respuesta CREATE_CHILD_SA. El paquete CHILD_SA normalmente contiene: • SA HDR

	longitud: 56 última propuesta: 0x0, reservado: 0x0, longitud: 52 Propuesta: 1, ID de protocolo: IKE, tamaño de SPI: 8, #trans: 4 última transformación: 0x3, reservado: 0x0: longitud: 12 tipo: 1, reservado: 0x0, id: AES-CBC última transformación: 0x3, reservado: 0x0: longitud: 8 tipo: 2, reservado: 0x0, id: SHA1 última transformación: 0x3, reservado: 0x0: longitud: 8 tipo: 3, reservado: 0x0, id: SHA96 última transformación: 0x0, reservado: 0x0: longitud: 8 tipo: 4, reservado: 0x0, id: DH_GROUP_1024_MODP/Grupo 2 **N** Siguiente carga útil: KE, reservado: 0x0, longitud: 24 **Carga** útil siguiente de KE: NOTIFICAR, reservada: 0x0, longitud: 136 Grupo DH: 2, reservado: 0x0 *11 de noviembre 19:31:35.882: IKEv2:Analizar carga de notificación: SET_WINDOW_SIZE **NOTIFY**(SET_WINDOW_SIZE) Carga siguiente: NINGUNA, reservada: 0x0, longitud: 12 ID de protocolo de seguridad: IKE, tamaño de spi: 0, tipo: SET_WINDOW_SIZE *11 de noviembre 19:31:35.882: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState: **CHILD_I_WAIT** Evento: **EV_RECV_CREATE_CHILD** *11 de noviembre 19:31:35.882: IKEv2:(ID de SA = 2):Acción: Action_Null *11 de noviembre 19:31:35.882: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState: **CHILD_I_PROC** Evento: EV_CHK4_NOTIFY *11 de noviembre 19:31:35.882: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState: CHILD_I_PROC Evento: **EV_VERIFY_MSG**	(version.flags/exchange type) • Nonce Ni (opcional): Si se crea CHILD_SA como parte del intercambio inicial, no se debe enviar una segunda carga KE ni nonce. • Carga útil de SA • KEi (clave opcional): la solicitud CREATE_CHILD_SA puede contener opcionalmente una carga útil KE para un intercambio DH adicional a fin de habilitar garantías más sólidas de confidencialidad de reenvío para CHILD_SA. Si las ofertas SA incluyen diferentes grupos DH, KEi debe ser un elemento del grupo que el iniciador espera que acepte el respondedor. Si se calcula que no es correcto, el intercambio CREATE_CHILD_SA falla y debe volver a intentarlo con una KEi diferente. • N (carga útil de notificación opcional): la carga útil de notificación se utiliza para transmitir datos informativos, como condiciones de error y transiciones de estado, a un par IKE. Una carga útil de notificación puede aparecer en un mensaje de respuesta (normalmente especifica por qué se rechazó una solicitud), en un intercambio de información (para

	*11 de noviembre 19:31:35.882: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState: CHILD_I_PROC Evento: EV_PROC_MSG *11 de noviembre 19:31:35.882: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState: CHILD_I_PROC Evento: EV_CHK4_PFS *11 de noviembre 19:31:35.882: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState: CHILD_I_PROC Evento: EV_GEN_DH_SECRET *11 de noviembre 19:31:35.890: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState: CHILD_I_PROC Evento: EV_NO_EVENT *11 de noviembre 19:31:35.890: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState: CHILD_I_PROC Evento: EV_OK_RECD_DH_SECRET_RESP *11 de noviembre 19:31:35.890: IKEv2:(ID de SA = 2):Acción: Action_Null *11 de noviembre 19:31:35.890: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState: CHILD_I_PROC Evento: EV_CHK_IKE_REKEY *11 de noviembre 19:31:35.890: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState: CHILD_I_PROC Evento: EV_GEN_SKEYID *11 de noviembre 19:31:35.890: IKEv2:(ID de SA = 2):Generar skeyid *11 de noviembre 19:31:35.890: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState: **CHILD_I_DONE** Evento: **EV_ACTIVATE_NEW_SA**	informar de un error que no está en una solicitud IKE) o en cualquier otro mensaje para indicar las capacidades del remitente o modificar el significado de la solicitud. Si este intercambio CREATE_CHILD_SA está volviendo a introducir una SA existente distinta de IKE_SA, la carga N inicial de tipo REKEY_SA debe identificar la SA que se va a volver a introducir. Si este intercambio CREATE_CHILD_SA no vuelve a generar una SA existente, debe omitirse la carga N. El Router 2 envía la respuesta y completa la activación de la nueva SA SECUNDARIA.

	*11 de noviembre 19:31:35.890: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState: CHILD_I_DONE Evento: EV_UPDATE_CAC_STATS *11 de noviembre 19:31:35.890: IKEv2:Nueva solicitud ikev2 sa activada *11 de noviembre 19:31:35.890: IKEv2: error al reducir el recuento para la negociación saliente *11 de noviembre 19:31:35.890: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState: CHILD_I_DONE Evento: EV_CHECK_DUPE *11 de noviembre 19:31:35.890: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState: CHILD_I_DONE Evento: EV_OK *11 de noviembre 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 *11 de noviembre 19:31:35.890: IKEv2:(ID de SA = 2):Respuesta procesada con ID de mensaje 3, las solicitudes se pueden enviar del intervalo 4 al 8 *11 de noviembre 19:31:35.890: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 0000003 **CurState: EXIT** Evento: EV_NO_EVENT	
El Router 1 recibe el paquete de respuesta del Router 2 y completa la activación de CHILD_SA.	*11 de noviembre 19:31:35.882: IKEv2:(SA ID = 2):Siguiente carga: ENCR, versión: 2.0 Tipo de intercambio: **CREATE_CHILD_SA**, indicadores: **RESPONDER MSG-RESPONSE** ID de mensaje: 3, longitud: 300 Contenido de la carga: ENCR Carga útil siguiente: SA, reservada: 0x0, longitud: 272 *11 de noviembre 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** *11 de noviembre 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 Evento: EV_GEN_SKEYID *11 de noviembre 19:31:35.882: IKEv2:(ID de SA = 2):**Generar skeyid** *11 de noviembre 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** *11 de noviembre 19:31:35.882: IKEv2:Store mib index ikev2 3, platform 62 *11 de noviembre 19:31:35.882: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: CHILD_R_DONE Evento: EV_UPDATE_CAC_STATS *11 de noviembre 19:31:35.882: IKEv2:Nueva solicitud ikev2 sa activada *11 de noviembre 19:31:35.882: IKEv2: error al reducir el recuento de las negociaciones entrantes *11 de noviembre 19:31:35.882: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: **CHILD_R_DONE** Evento: EV_CHECK_DUPE *11 de noviembre 19:31:35.882: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: CHILD_R_DONE Evento: EV_OK *11 de noviembre 19:31:35.882: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: CHILD_R_DONE Evento: EV_START_DEL_NEG_TMR. *11 de noviembre 19:31:35.882: IKEv2:(ID de SA = 2):Acción: Action_Null *11 de noviembre 19:31:35.882: IKEv2:(SA ID = 2):SM Trace-> SA:	

	I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: EXIT Evento: EV_CHK_PENDING *11 de noviembre 19:31:35.882: IKEv2:(ID de SA = 2):Respuesta enviada con ID de mensaje 3, las solicitudes se pueden aceptar del intervalo 4 al 8 *11 de noviembre 19:31:35.882: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 0000003 **CurState: EXIT** Evento: EV_NO_EVENT	

Verificación del túnel

ISAKMP

Comando

<#root>

show crypto ikev2 sa detailed

Salida del router 1

<#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
```

Salida del router 2

<#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

Comando

<#root>

show crypto ipsec sa

> **Nota**: En esta salida, a diferencia de IKEv1, el valor del grupo PFS DH aparece como "PFS (Y/N): N, grupo DH: none" durante la primera negociación de túnel, pero, después de que se produzca una nueva clave, aparecen los valores correctos. No se trata de un error de funcionamiento, aunque el comportamiento se describe en el Id. de error de Cisco CSCug67056. (Sólo los usuarios registrados de Cisco pueden acceder a la información o las herramientas internas de Cisco).
> La diferencia entre IKEv1 e IKEv2 es que, en este último caso, las SA secundarias se crean como parte del intercambio AUTH. El grupo DH configurado bajo el mapa criptográfico se utilizaría solamente durante la regeneración de claves. Por lo tanto, verá 'PFS (Y/N): N, DH group: none' hasta la primera regeneración.

Con IKEv1, se ve un comportamiento diferente, porque la creación de SA secundaria se produce durante el modo rápido y el mensaje CREATE_CHILD_SA tiene una provisión para transportar la carga útil de intercambio de claves que especifica los parámetros DH para derivar un nuevo secreto compartido.

Salida del router 1

<#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:
```

Salida del router 2

<#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:
```

También puede verificar la salida del comando **show crypto session** en ambos routers; esta salida muestra el estado de la sesión del túnel como 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
```

Información Relacionada

- **Intercambio de paquetes IKEv2 y depuración a nivel de protocolo**

- **Asistencia técnica y descargas de Cisco**

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).