Resolución de Problemas de IPSec para Túneles de Servicio en los Bordes con IKEv2

Contenido

Introducción

Este documento describe cómo resolver los problemas más comunes de los túneles de seguridad del protocolo de Internet (IPsec) a dispositivos de terceros con Intercambio de claves de Internet versión 2 (IKEv2) configurado. A menudo se hace referencia como Túneles de Transporte/Servicio en la documentación de Cisco SD-WAN. Este documento también explica cómo habilitar y leer las depuraciones IKE y asociarlas al intercambio de paquetes para comprender el punto de falla en una negociación IPSec.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- IKEv2
- negociación IPsec
- SD-WAN de Cisco

Componentes Utilizados

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

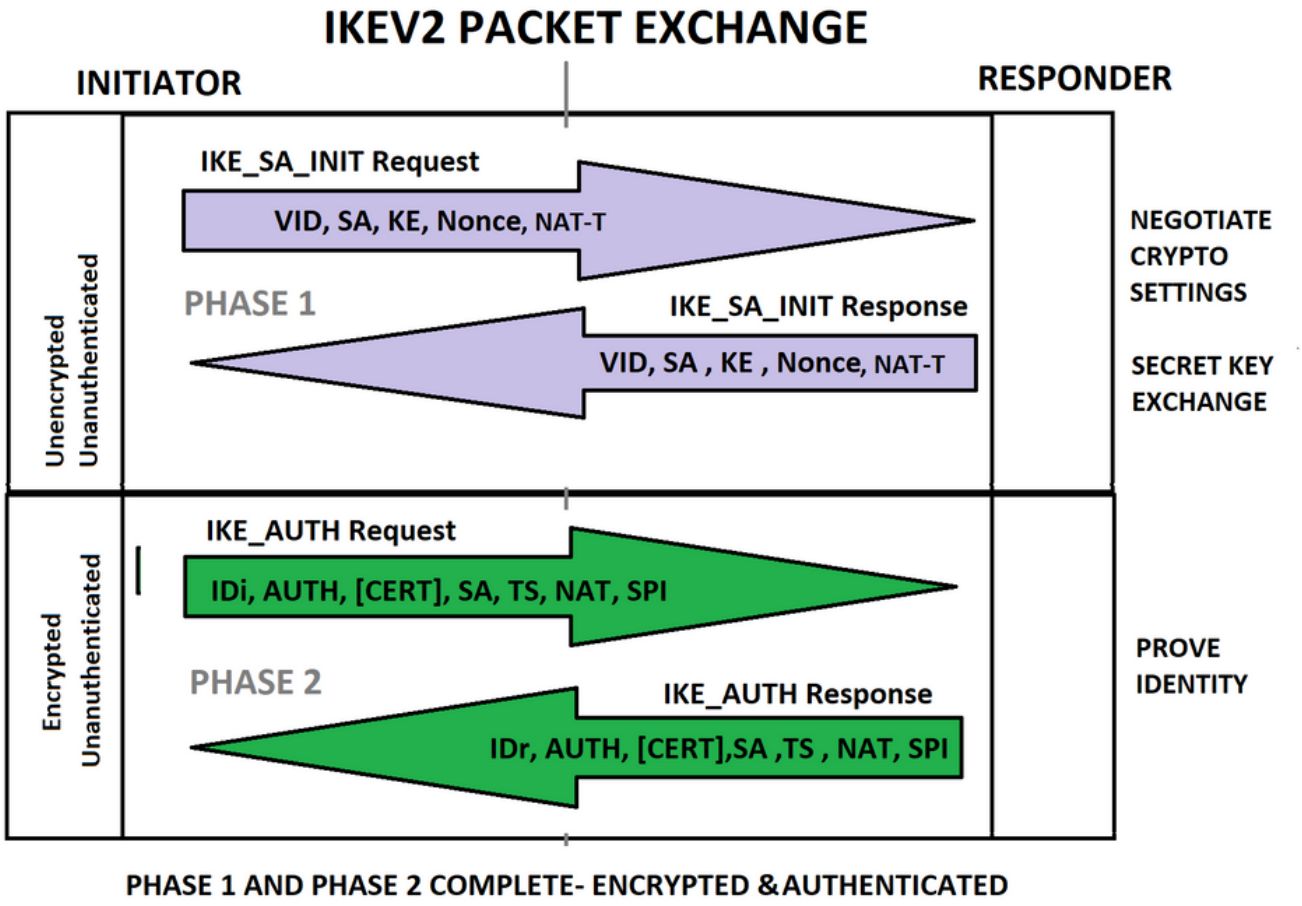
Antecedentes

Glosario IKE

- **Seguridad del protocolo de Internet (IPsec)** es un conjunto estándar de protocolos entre 2 puntos de comunicación a través de la red IP que proporcionan autenticación de datos, integridad y confidencialidad.
- **Internet Key Exchange versión 2 (IKEv2) es el protocolo utilizado para configurar una asociación de seguridad (SA) en el conjunto de protocolos IPsec.**
- Una **asociación de seguridad** (**SA**) es el establecimiento de atributos de seguridad compartidos entre dos entidades de red para soportar una comunicación segura. Una SA puede incluir atributos como el algoritmo criptográfico y el modo; clave de cifrado del tráfico; y parámetros para que los datos de red pasen a través de la conexión.
- Las **IDs de proveedor** (**VID**) se utilizan para identificar dispositivos de peer con la misma implementación de proveedor para soportar las características específicas del proveedor.
- **Nonce**: valores aleatorios creados en el intercambio para agregar aleatoriedad y evitar ataques de repetición.
- Información **de intercambio de claves (KE)** para el proceso de intercambio seguro de claves Diffie-Hellman (DH).
- **Identity Initiator/respondedor (IDi/IDr.)** se utiliza para enviar información de autenticación al par. Esta información se transmite bajo la protección del secreto compartido común.
- La clave compartida IPSec se puede derivar de nuevo con el uso de DH para garantizar **Perfect Forward Secrecy (PFS)** o con una actualización del secreto compartido derivado del intercambio DH original.
- **El intercambio de claves Diffie-Hellman (DH) es un método de intercambio de algoritmos criptográficos seguros a través de un canal público.**
- **Los selectores de tráfico (TS)** son las identidades de proxy o el tráfico intercambiado en la negociación IPSec para pasar a través del túnel cifrado.

Intercambio de paquetes IKEv2

Cada paquete IKE contiene información de carga útil para el establecimiento del túnel. El glosario IKE explica las abreviaturas mostradas en esta imagen como parte del contenido de carga útil para el intercambio de paquetes.

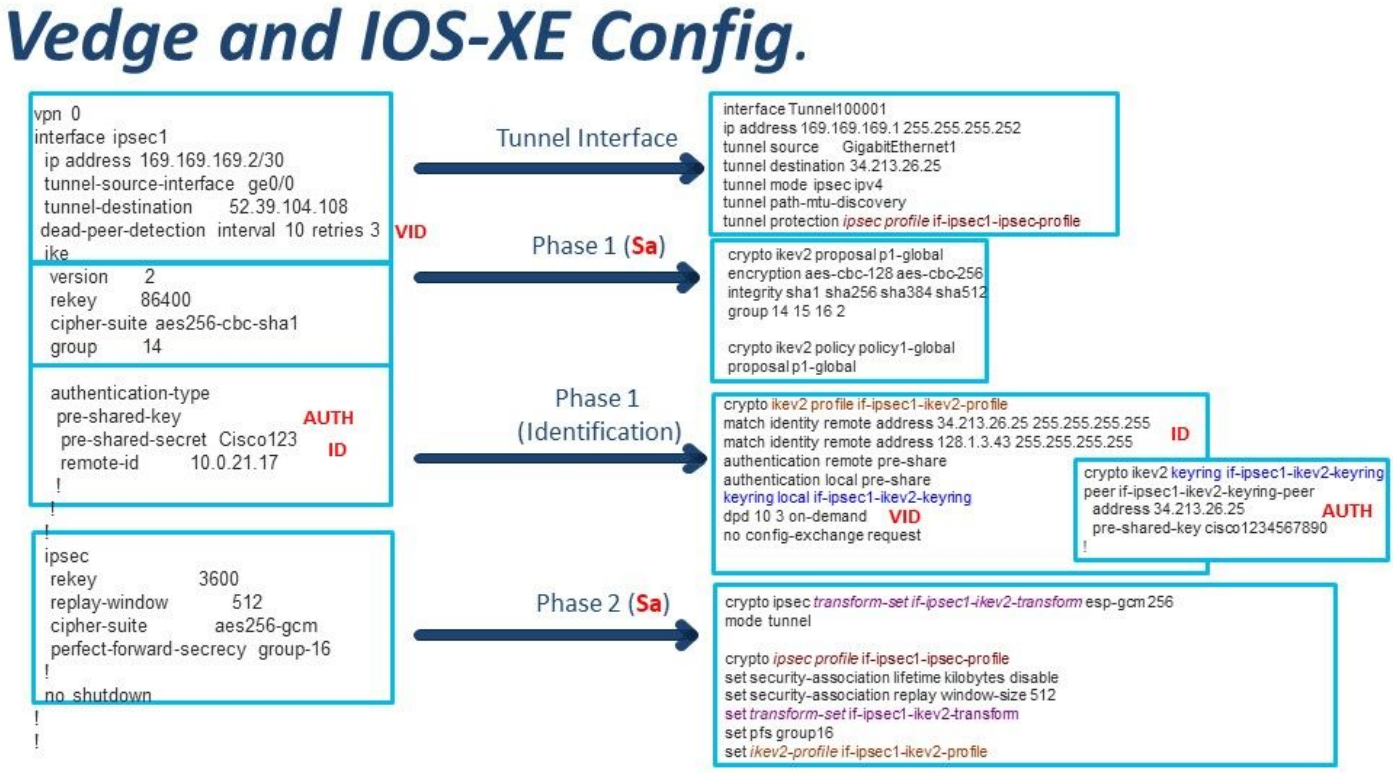


IKEV2-Exchange

> **Nota:** Es importante verificar en qué intercambio de paquetes de la negociación IKE el túnel IPSec no puede analizar rápidamente qué configuración está involucrada para abordar el problema de manera efectiva.

> **Nota:** Este documento no describe a fondo el intercambio de paquetes IKEv2. Para obtener más referencias, navegue hasta Intercambio de paquetes IKEv2 y Debugging de nivel de protocolo

Es necesario correlacionar la configuración de vEdge con la configuración de Cisco IOS® XE. Además, es útil para hacer coincidir los conceptos de IPSec y el contenido de carga útil para los intercambios de paquetes IKEv2 como se muestra en la imagen.



Nota: Cada parte de la configuración modifica un aspecto del intercambio de negociación IKE. Es importante correlacionar los comandos con la negociación de protocolo de IPSec.

Troubleshoot

Habilitar depuraciones IKE

En vEdges **debug iked** habilita la información de nivel de depuración IKEv1 o IKEv2.

```
debug iked misc high
debug iked event high
```

Es posible mostrar la información de depuración actual dentro de **vshell** y ejecutar el comando **tail -f <debug path>** .

```
vshell
tail -f /var/log/message
```

En CLI también es posible mostrar los registros/información de depuración actuales para la trayectoria especificada.

```
monitor start /var/log/messages
```

Sugerencias para Iniciar el Proceso de Troubleshooting para Problemas de IPSec

Es posible separar tres escenarios diferentes de IPSec. Es un buen punto de referencia identificar el síntoma para tener un mejor enfoque para saber cómo comenzar.

1. El túnel IPsec no se establece.

2. El túnel IPsec se cayó y se restableció por sí solo. (Desactivado)
3. El túnel IPsec se ha caído y permanece en estado descendente.

Para el túnel IPsec no establece síntomas, es necesario depurar en tiempo real para verificar cuál es el comportamiento actual en la negociación IKE.

Para el túnel IPsec se desactivó y se restableció por sus propios síntomas, más comúnmente conocidos como túnel Inundado y se necesita el análisis de la causa raíz (RCA). Es indispensable conocer la marca de tiempo cuando el túnel se cayó o tener un tiempo estimado para ver las depuraciones.

Para el túnel IPsec se apagó y permanece en los síntomas de estado descendente, significa que el túnel funcionó antes pero por cualquier motivo, se cayó y necesitamos saber el motivo de la caída y el comportamiento actual que impide que el túnel se establezca correctamente de nuevo.

Identifique los puntos antes de que comience la resolución de problemas:

1. Túnel IPsec (número) con problemas y configuración.
2. Marca de tiempo cuando el túnel se desactivó (si procede).
3. Dirección IP de peer IPsec (destino de túnel).

Todas las depuraciones y registros se guardan en los archivos **/var/log/messages**, para los registros actuales, se guardan en el archivo de mensajes pero para este síntoma específico la inestabilidad se puede identificar horas/días después del problema, lo más probable es que las depuraciones relacionadas esten en mensajes1,2,3..etc. Es importante conocer la marca de tiempo para ver el archivo de mensaje correcto y analizar las depuraciones (charon) para la negociación IKE de la relación de túnel IPsec.

La mayoría de las depuraciones no imprimen el número del túnel IPsec. La manera más frecuente de identificar la negociación y los paquetes es con la dirección IP del par remoto y la dirección IP donde se origina el túnel en el puente. Algunos ejemplos de depuraciones IKE impresas:

```
Jun 18 00:31:22 vedge01 charon: 09[CFG] vici initiate 'child_IPsec2_1'
Jun 18 00:31:22 vedge01 charon: 16[IKE] initiating IKE_SA ipsec2_1[223798] to 10.10.10.1
Jun 18 00:31:22 vedge01 charon: 16[IKE] initiating IKE_SA ipsec2_1[223798] to 10.10.10.1
```

Los debugs para la negociación IKE INIT muestran el número de túnel IPsec. Sin embargo, la información subsiguiente para el intercambio de paquetes sólo utiliza las direcciones IP del túnel IPsec.

```
Jun 18 00:31:22 vedge01 charon: 09[CFG] vici initiate 'child_ipsec2_1'
Jun 18 00:31:22 vedge01 charon: 16[IKE] initiating IKE_SA ipsec2_1[223798] to 10.10.10.1
Jun 18 00:31:22 vedge01 charon: 16[IKE] initiating IKE_SA ipsec2_1[223798] to 10.10.10.1
Jun 18 00:31:22 vedge01 charon: 16[ENC] generating IKE_SA_INIT request 0 [ SA KE No N(NATD_S_IP)
N(NATD_D_IP) N(FRAG_SUP) N(HASH_ALG) N(REDIR_SUP) ]
Jun 18 00:31:22 vedge01 charon: 16[NET] sending packet: from 10.132.3.92[500] to 10.10.10.1[500]
(464 bytes)
Jun 18 00:31:22 vedge01 charon: 12[NET] received packet: from 10.10.10.1[500] to
10.132.3.92[500] (468 bytes)
Jun 18 00:31:22 vedge01 charon: 12[ENC] parsed IKE_SA_INIT response 0 [ SA KE No N(NATD_S_IP)
N(NATD_D_IP) N(HTTP_CERT_LOOK) N(FRAG_SUP) V ]
Jun 18 00:31:22 vedge01 charon: 12[ENC] received unknown vendor ID:
4f:85:58:17:1d:21:a0:8d:69:cb:5f:60:9b:3c:06:00
Jun 18 00:31:22 vedge01 charon: 12[IKE] local host is behind NAT, sending keep alives
```

Configuración del túnel IPsec:

```
interface ipsec2 ip address 192.168.1.9/30 tunnel-source 10.132.3.92 tunnel-destination
10.10.10.1 dead-peer-detection interval 30 ike version 2 rekey 86400 cipher-suite aes256-cbc-
sha1 group 14 authentication-type pre-shared-key pre-shared-secret
$8$wgrs/Cw6tX0na34yF4Fga0B62mGBpHFdOzFaRmoYfnBioWVO3s3efFPBbkaZqvoN ! ! ! ipsec rekey 3600
replay-window 512 cipher-suite aes256-gcm perfect-forward-secrecy group-14 !
```

Síntoma 1. El túnel IPsec no se establece

Como el problema puede ser la primera implementación para el túnel, no ha estado activo y las depuraciones IKE son la mejor opción.

Síntoma 2. El túnel IPsec se apagó y se restableció por sí solo

Como se mencionó anteriormente, generalmente este síntoma se dirige para saber la causa raíz de por qué el túnel se cayó. Con el análisis de la causa raíz conocido, a veces, el administrador de la red evita más problemas.

Identifique los puntos antes de que comience la resolución de problemas:

1. Túnel IPsec (número) con problemas y configuración.
2. Marca de tiempo cuando el túnel se cayó.
3. Dirección IP de peer IPsec (destino de túnel)

Retransmisiones DPD

En este ejemplo, el túnel cayó el 18 de junio a las 00:31:17.

```
Jun 18 00:31:17 vedge01 FTMD[1472]: %Viptela-vedge01-FTMD-6-INFO-1000001: VPN 1 Interface ipsec2
DOWN
Jun 18 00:31:17 vedge01 FTMD[1472]: %Viptela-vedge01-ftmd-6-INFO-1400002: Notification:
interface-state-change severity-level:major host-name:"vedge01" system-ip:4.0.5.1 vpn-id:1 if-
name:"ipsec2" new-state:down
```

> **Nota:** Los logs para el túnel IPSec down no son parte de los debugs iked, son registros *FTMD*. Por lo tanto, ni *charon* ni *IKE* se imprimirían.

> **Nota:** Los registros relacionados no suelen imprimirse juntos, hay más información entre ellos que no está relacionada con el mismo proceso.

Paso 1. Después de identificar la marca de tiempo y correlacionar la hora y los registros, comience a revisar los registros de abajo hacia arriba.

```
Jun 18 00:31:17 vedge01 charon: 11[IKE] giving up after 3 retransmits
```

```
Jun 18 00:28:22 vedge01 charon: 08[IKE] retransmit 3 of request with message ID 543 (tries=3,
timeout=30, exchange=37, state=2)
```

```
Jun 18 00:28:22 vedge01 charon: 08[NET] sending packet: from 10.132.3.92[4500] to
10.10.10.1[4500] (76 bytes)

Jun 18 00:26:45 vedge01 charon: 06[IKE] retransmit 2 of request with message ID 543 (tries=3,
timeout=30, exchange=37, state=2)
Jun 18 00:26:45 vedge01 charon: 06[NET] sending packet: from 10.132.3.92[4500] to
10.10.10.1[4500] (76 bytes)

Jun 18 00:25:21 vedge01 charon: 08[IKE] sending DPD request
Jun 18 00:25:21 vedge01 charon: 08[ENC] generating INFORMATIONAL request 543 [ ]
Jun 18 00:25:21 vedge01 charon: 08[NET] sending packet: from 10.132.3.92[4500] to
10.10.10.1[4500] (76 bytes)
Jun 18 00:25:51 vedge01 charon: 05[IKE] retransmit 1 of request with message ID 543 (tries=3,
timeout=30, exchange=37, state=2)
Jun 18 00:25:51 vedge01 charon: 05[NET] sending packet: from 10.132.3.92[4500] to
10.10.10.1[4500] (76 bytes)
```

El último intercambio exitoso de paquetes DPD se describe como solicitud nº 542.

```
Jun 18 00:24:08 vedge01 charon: 11[ENC] generating INFORMATIONAL request 542 [ ]
Jun 18 00:24:08 vedge01 charon: 11[NET] sending packet: from 10.132.3.92[4500] to
10.10.10.1[4500] (76 bytes)
Jun 18 00:24:08 vedge01 charon: 07[NET] received packet: from 13.51.17.190[4500] to
10.10.10.1[4500] (76 bytes)
Jun 18 00:24:08 vedge01 charon: 07[ENC] parsed INFORMATIONAL response 542 [ ]
```

Paso 2. Reúna toda la información en el orden adecuado:

```
Jun 18 00:24:08 vedge01 charon: 11[ENC] generating INFORMATIONAL request 542 [ ]
Jun 18 00:24:08 vedge01 charon: 11[NET] sending packet: from 10.132.3.92[4500] to
10.10.10.1[4500] (76 bytes)
Jun 18 00:24:08 vedge01 charon: 07[NET] received packet: from 10.10.10.1[4500] to
10.132.3.92[4500] (76 bytes)
Jun 18 00:24:08 vedge01 charon: 07[ENC] parsed INFORMATIONAL response 542 [ ]

Jun 18 00:25:21 vedge01 charon: 08[IKE] sending DPD request
Jun 18 00:25:21 vedge01 charon: 08[ENC] generating INFORMATIONAL request 543 [ ]
Jun 18 00:25:21 vedge01 charon: 08[NET] sending packet: from 10.132.3.92[4500] to
10.10.10.1[4500] (76 bytes)
Jun 18 00:25:51 vedge01 charon: 05[IKE] retransmit 1 of request with message ID 543 (tries=3,
timeout=30, exchange=37, state=2)
Jun 18 00:25:51 vedge01 charon: 05[NET] sending packet: from 10.132.3.92[4500] to
10.10.10.1[4500] (76 bytes)

Jun 18 00:26:45 vedge01 charon: 06[IKE] retransmit 2 of request with message ID 543 (tries=3,
timeout=30, exchange=37, state=2)
Jun 18 00:26:45 vedge01 charon: 06[NET] sending packet: from 10.132.3.92[4500] to
10.10.10.1[4500] (76 bytes)

Jun 18 00:28:22 vedge01 charon: 08[IKE] retransmit 3 of request with message ID 543 (tries=3,
timeout=30, exchange=37, state=2)
Jun 18 00:28:22 Lvedge01 charon: 08[NET] sending packet: from 10.132.3.92[4500] to
10.10.10.1[4500] (76 bytes)

Jun 18 00:31:17 vedge01 charon: 11[IKE] giving up after 3 retransmits
Jun 18 00:31:17 vedge01 FTMD[1472]: %Viptela-LONDSR01-FTMD-6-INFO-1000001: VPN 1 Interface
ipsec2 DOWN
Jun 18 00:31:17 vedge01 FTMD[1472]: %Viptela-LONDSR01-ftmd-6-INFO-1400002: Notification:
interface-state-change severity-level:major host-name:"LONDSR01" system-ip:4.0.5.1 vpn-id:1 if-
name:"ipsec2" new-state:down
```

Para el ejemplo descrito, el túnel se desactiva debido a que vEdge01 no recibe los paquetes DPD

de 10.10.10.1. Se espera que después de 3 retransmisiones DPD el peer IPSec se configure como "perdido" y el túnel se interrumpa. Hay múltiples razones para este comportamiento, generalmente, está relacionado con el ISP donde los paquetes se pierden o se descartan en la trayectoria. Si el problema ocurre una vez, no hay forma de hacer un seguimiento del tráfico perdido; sin embargo, si el problema persiste, se puede realizar un seguimiento del paquete con el uso de capturas en vEdge, el par IPSec remoto y el ISP.

Síntoma 3. El túnel IPsec se apagó y permanece en estado descendente

Como se mencionó anteriormente en este síntoma, el túnel funcionaba correctamente pero, por cualquier motivo, cayó y el túnel no ha podido establecerse de nuevo con éxito. En esta situación, la red se ve afectada.

identifique los puntos antes de que comience la resolución de problemas:

1. Túnel IPsec (número) con problemas y configuración.
2. Marca de tiempo cuando el túnel se cayó.
3. Dirección IP de peer IPsec (destino de túnel)

Discordancia de PFS

En este ejemplo, la resolución de problemas no comienza con la marca de tiempo cuando el túnel se desactiva. A medida que el problema persiste, las depuraciones IKE son la mejor opción.

```
interface ipsec1 description VWAN_VPN ip address 192.168.0.101/30 tunnel-source-interface ge0/0
tunnel-destination 10.10.10.1 ike version 2 rekey 28800 cipher-suite aes256-cbc-sha1 group 2
authentication-type pre-shared-key pre-shared-secret
"$8$njK2pLLjgKWNQu0KecNtY3+fo3hbTs0/7iJy6unNtersmCGjGB38kIPjsoqqXZdVmtizLu79\naQdjt2POM242Yw=="
! ! ! ipsec rekey 3600 replay-window 512 cipher-suite aes256-cbc-sha1 perfect-forward-secrecy
group-16 ! mtu 1400 no shutdown
```

El comando debug iked está activado y se muestra la negociación.

```
daemon.info: Apr 27 05:12:56 vedge01 charon: 16[NET] received packet: from 10.10.10.1[4500] to
172.28.0.36[4500] (508 bytes)
daemon.info: Apr 27 05:12:56 vedge01 charon: 16[ENC] parsed CREATE_CHILD_SA request 557 [ SA No
TSi TSr ]
daemon.info: Apr 27 05:12:56 vedge01 charon: 16[CFG] received proposals:
ESP:AES_GCM_16_256/NO_EXT_SEQ, ESP:AES_CBC_256/HMAC_SHA1_96/NO_EXT_SEQ,
ESP:3DES_CBC/HMAC_SHA1_96/NO_EXT_SEQ, ESP:AES_CBC_256/HMAC_SHA2_256_128/NO_EXT_SEQ,
ESP:AES_CBC_128/HMAC_SHA1_96/NO_EXT_SEQ, ESP:3DES_CBC/HMAC_SHA2_256_128/NO_EXT_SEQ
daemon.info: Apr 27 05:12:56 vedge01 charon: 16[CFG] configured proposals:
ESP:AES_CBC_256/HMAC_SHA1_96/MODP_4096/NO_EXT_SEQ
daemon.info: Apr 27 05:12:56 vedge01 charon: 16[IKE] no acceptable proposal found
daemon.info: Apr 27 05:12:56 vedge01 charon: 16[IKE] failed to establish CHILD_SA, keeping
IKE_SA
daemon.info: Apr 27 05:12:56 vedge01 charon: 16[ENC] generating CREATE_CHILD_SA response 557 [
N(NO_PROP) ]
daemon.info: Apr 27 05:12:56 vedge01 charon: 16[NET] sending packet: from 172.28.0.36[4500] to
10.10.10.1[4500] (76 bytes)

daemon.info: Apr 27 05:12:57 vedge01 charon: 08[NET] received packet: from 10.10.10.1[4500] to
172.28.0.36[4500] (76 bytes)
daemon.info: Apr 27 05:12:57 vedge01 charon: 08[ENC] parsed INFORMATIONAL request 558 [ ]
daemon.info: Apr 27 05:12:57 vedge01 charon: 08[ENC] generating INFORMATIONAL response 558 [ ]
```

```
daemon.info: Apr 27 05:12:57 vedge01 charon: 08[NET] sending packet: from 172.28.0.36[4500] to
10.10.10.1[4500] (76 bytes)
daemon.info: Apr 27 05:12:58 vedge01 charon: 07[NET] received packet: from 10.10.10.1[4500] to
172.28.0.36[4500] (396 bytes)
daemon.info: Apr 27 05:12:58 vedge01 charon: 07[ENC] parsed CREATE_CHILD_SA request 559 [ SA No
TSi TSr ]
daemon.info: Apr 27 05:12:58 vedge01 charon: 07[CFG] received proposals:
ESP:AES_GCM_16_256/NO_EXT_SEQ, ESP:AES_CBC_256/HMAC_SHA1_96/NO_EXT_SEQ,
ESP:3DES_CBC/HMAC_SHA1_96/NO_EXT_SEQ, ESP:AES_CBC_256/HMAC_SHA2_256_128/NO_EXT_SEQ,
ESP:AES_CBC_128/HMAC_SHA1_96/NO_EXT_SEQ, ESP:3DES_CBC/HMAC_SHA2_256_128/NO_EXT_SEQ
daemon.info: Apr 27 05:12:58 vedge01 charon: 07[CFG] configured proposals:
ESP:AES_CBC_256/HMAC_SHA1_96/MODP_4096/NO_EXT_SEQ
daemon.info: Apr 27 05:12:58 Avedge01 charon: 07[IKE] no acceptable proposal found
daemon.info: Apr 27 05:12:58 vedge01 charon: 07[IKE] failed to establish CHILD_SA, keeping
IKE_SA
```

> **Nota:** Los paquetes CREATE_CHILD_SA se intercambian por cada SA nueva o nueva. Para obtener más referencias, navegue hasta Comprensión del Intercambio de Paquetes IKEv2

Las depuraciones IKE muestran el mismo comportamiento y se repite constantemente, por lo que es posible tomar parte de la información y analizarla:

CREATE_CHILD_SA significa una nueva clave, con el propósito de que el nuevo SPIS se genere e intercambie entre los terminales IPsec.

- El puente recibe el paquete de solicitud CREATE_CHILD_SA desde 10.10.10.1.
- El proveedor procesa la solicitud y verifica las propuestas (SA) enviadas por el peer 10.10.10.1
- El proveedor compara la propuesta recibida enviada por el par con sus propuestas configuradas.
- El intercambio CREATE_CHILD_SA falla con "no se encontraron propuestas aceptables".

En este punto, la pregunta es: **¿Por qué hay una discordancia de configuración si el túnel funcionó anteriormente y no se realizaron cambios?**

Analice en profundidad, hay un campo adicional en las propuestas configuradas que el par no está enviando.

propuestas configuradas: ESP:AES_CBC_256/HMAC_SHA1_96/MODP_4096/NO_EXT_SEQ

Propuestas recibidas:
ESP:AES_GCM_16_256/NO_EXT_SEQ,
ESP:AES_CBC_256/HMAC_SHA1_96/NO_EXT_SEQ,
ESP:3DES_CBC/HMAC_SHA1_96/NO_EXT_SEQ,
ESP:AES_CBC_256/HMAC_SHA2_256_128/NO_EXT_SEQ,
ESP:AES_CBC_128/HMAC_SHA1_96/NO_EXT_SEQ,
ESP:3DES_CBC/HMAC_SHA2_256_128/NO_EXT_SEQ

MODP_4096 es el grupo DH 16, que los vectores han configurado para PFS (perfecto-avance-secreto) en la fase 2 (sección IPSec).

PFS es la única configuración de discordancia en la que el túnel puede establecerse correctamente o no según quién es el iniciador o el respondedor en la negociación IKE. Sin embargo, cuando se inicia el reinicio, el túnel no puede continuar y este síntoma puede presentarse o relacionarse con.

El túnel IPSec/Ikev2 de vEdge no se reinicia después de ser desmontado debido a un evento DELETE

Consulte Cisco bug ID CSCvx86427 para obtener más información sobre este comportamiento.

A medida que el problema persiste, las depuraciones IKE son las mejores opciones. Sin embargo, para este bug en particular si las depuraciones están habilitadas, no se muestra información ni el terminal ni el archivo de mensaje.

Para reducir este problema y verificar si vEdge llega al Id. de error de Cisco CSCvx86427, es necesario encontrar el momento en que el túnel se interrumpe.

identifique los puntos antes de que comience la resolución de problemas:

1. Túnel IPsec (número) con problemas y configuración.
2. Marca de tiempo cuando el túnel se cayó.
3. Dirección IP de peer IPsec (destino de túnel)

Después de identificar la marca de tiempo y de correlacionar la hora y los registros, revise los registros justo antes de que el túnel se desactive.

```
Apr 13 22:05:21 vedge01 charon: 12[IKE] received DELETE for IKE_SA ipsec1_1[217]
Apr 13 22:05:21 vedge01 charon: 12[IKE] deleting IKE_SA ipsec1_1[217] between
10.16.0.5[10.16.0.5]...10.10.10.1[10.10.10.1]
Apr 13 22:05:21 vedge01 charon: 12[IKE] deleting IKE_SA ipsec1_1[217] between
10.16.0.5[10.16.0.5]...10.10.10.1[10.10.10.1]
Apr 13 22:05:21 vedge01 charon: 12[IKE] IKE_SA deleted
Apr 13 22:05:21 vedge01 charon: 12[IKE] IKE_SA deleted
Apr 13 22:05:21 vedge01 charon: 12[ENC] generating INFORMATIONAL response 4586 [ ]
Apr 13 22:05:21 vedge01 charon: 12[NET] sending packet: from 10.16.0.5[4500] to 10.10.10.1[4500]
(80 bytes)
Apr 13 22:05:21 vedge01 charon: 12[KNL] Deleting SAD entry with SPI 00000e77
Apr 13 22:05:21 vedge01 FTMD[1269]: %Viptela-AZGDSR01-FTMD-6-INFO-1000001: VPN 1 Interface
ipsec1 DOWN
Apr 13 22:05:21 vedge01 FTMD[1269]: %Viptela-AZGDSR01-ftmd-6-INFO-1400002: Notification:
interface-state-change severity-level:major host-name:"vedge01" system-ip:4.1.0.1 vpn-id:1 if-
name:"ipsec1" new-state:down
```

> **Nota:** Hay varios paquetes DELETES en una negociación IPSec, y DELETE para CHILD_SA es un valor esperado DELETE para un proceso REKEY, este problema se ve cuando se recibe un paquete IKE_SA DELETE puro sin ninguna negociación IPSec particular. Ese DELETE elimina todo el túnel IPsec/IKE.

Información Relacionada

- Depuración de Nivel de Protocolo y de Intercambio de Paquetes KEv2
- Intercambio de claves de Internet (IKE): RFC 2409
- IKEv2 - RFC 7296
- IPSec de LAN a LAN de sitio a sitio entre vEdge y Cisco IOS
- Soporte Técnico y Documentación - Cisco Systems