Resolución de problemas de fallos de reproducción de bloqueo de IPsec de extremo SD-WAN

Contenido

Introducción

Este documento describe el comportamiento de IPsec Anti-Replay en SD-WAN IPsec para routers de Bordes y cómo resolver problemas de Anti-Replay.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Red de área extensa definida por software de Cisco (SD-WAN)
- Seguridad de protocolo de Internet (IPsec)

Componentes Utilizados

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

- C8000V Versión 17.06.01
- ASR1001-X versión 17.06.03a

- vManage versión 20.7.1

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.

Antecedentes

La autenticación IPSec proporciona protección anti-reproducción integrada contra paquetes IPSec antiguos o duplicados con el número de secuencia en el encabezado ESP verificado en el receptor. Las caídas de paquetes anti-reproducción es uno de los problemas más comunes del plano de datos con IPSec debido a que los paquetes entregados fuera de servicio fuera de la ventana anti-reproducción. Un enfoque general de solución de problemas para las caídas de IPsec anti-reproducción se puede encontrar en Fallas de Verificación de IPsec Anti-Replay, y la técnica general se aplica también a SD-WAN. Sin embargo, existen algunas diferencias de implementación entre IPsec tradicional e IPsec utilizado en la solución Cisco SD-WAN. En este artículo se pretende explicar estas diferencias y el enfoque en las plataformas cEdge con Cisco IOS ®XE.

Consideraciones sobre la detección de reproducción SD-WAN

Clave de grupo frente a clave en pares

A diferencia de IPsec tradicional, donde las SA IPsec se negocian entre dos peers con el uso del protocolo IKE, SD-WAN utiliza un concepto de clave de grupo. En este modelo, un dispositivo de extremo de SD-WAN genera periódicamente SA entrante de plano de datos por TLOC y envía estas SA al controlador vSmart, que a su vez propaga la SA al resto de los dispositivos de extremo de la red SD-WAN. Para obtener una descripción más detallada de las operaciones del plano de datos de SD-WAN, consulte Descripción general de la seguridad del plano de datos de SD-WAN.

> **Nota**: desde Cisco IOS ®XE. 6.12.1a/SD-WAN 19.2, se admiten claves IPsec en pares. Consulte Descripción General de Claves Pareadas IPSec. Con las teclas de par, la protección IPsec anti-replay funciona exactamente igual que IPsec tradicional. Este artículo se centra principalmente en la comprobación de la reproducción con el uso del modelo de clave de grupo.

SPI codificado

En el encabezado IPsec ESP, el SPI (Security Parameter Index) es un valor de 32 bits que el receptor utiliza para identificar la SA con la que se descifra un paquete entrante. Con SD-WAN, este SPI entrante se puede identificar con **show crypto ipsec sa**:

```
cedge-2#show crypto ipsec sa | se inbound
     inbound esp sas:
      spi: 0x123(291)
        transform: esp-gcm 256 ,
        in use settings ={Transport UDP-Encaps, esn}
        conn id: 2083, flow_id: CSR:83, sibling_flags FFFFFFFF80000008, crypto map: Tunnel1-
```

```
vesen-head-0
        sa timing: remaining key lifetime 9410 days, 4 hours, 6 mins
        Kilobyte Volume Rekey has been disabled
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)
```

Nota: Aunque el SPI entrante es el mismo para todos los túneles, el receptor tiene una SA diferente y el objeto de ventana de reproducción correspondiente asociado con la SA para cada dispositivo de borde par, ya que la SA es identificada por el origen, la dirección IP de destino, el origen, los puertos de destino 4-tupla y el número SPI. Así que, esencialmente, cada par tiene su propio objeto de ventana anti-reproducción.

En el paquete real enviado por el dispositivo par, observe que el valor SPI es diferente del resultado anterior. A continuación se muestra un ejemplo del resultado de seguimiento de paquetes con la opción de copia de paquetes habilitada:

```
Packet Copy In
  45000102 0cc64000 ff111c5e ac127cd0 ac127cd1 3062303a 00eea51b 04000123
  00000138 78014444 f40d7445 3308bf7a e2c2d4a3 73f05304 546871af 8d4e6b9f
```

El SPI real en el encabezado ESP es **0x04000123.** La razón de esto es que los primeros bits del SPI para SD-WAN están codificados con información adicional, y solo los bits bajos del campo SPI están asignados para el SPI real.

IPSec tradicional:

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|               Security Parameters Index (SPI)                 |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

SD-WAN:

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  CTR  | MSNS|         Security Parameters Index (SPI)         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Where:

- **CTR** (primeros 4 bits, bits 0-3) - Bits de control, utilizados para indicar el tipo específico de paquetes de control. Por ejemplo, el bit de control 0x80000000 se utiliza para BFD.
- **MSNS** (next 3 bits, bits 4-6) - Índice de espacio de número de secuencia múltiple. Esto se utiliza para localizar el contador de secuencia correcto en la matriz de contadores de secuencia para verificar la reproducción del paquete dado. Para SD-WAN, el 3-bit de MSNS permite que 8 clases de tráfico diferentes se mapeen en su propio espacio de número de secuencia. Esto implica que el valor SPI efectivo que se puede utilizar para la selección SA es el orden reducido de 25 bits a partir del valor completo de 32 bits del campo.

Espacio de número de secuencia múltiple para QoS

Es común observar fallas de reproducción de IPsec en un entorno donde los paquetes se entregan fuera de servicio debido a QoS, por ejemplo, LLQ, ya que QoS siempre se ejecuta después del cifrado y la encapsulación de IPsec. La solución Multiple Sequence Number Space soluciona este problema con el uso de varios espacios de número de secuencia asignados a diferentes clases de tráfico de QoS para una asociación de seguridad determinada. El espacio de número de secuencia diferente se indexa mediante los bits MSNS codificados en el campo SPI de paquete ESP como se muestra. Para obtener una descripción más detallada, consulte Mecanismo de respuesta de bloqueo de IPSec para QoS.

Como se indicó anteriormente, esta implementación de número de secuencia múltiple implica que el valor SPI efectivo que se puede utilizar para la selección de SA es el orden reducido de 25 bits. Otra consideración práctica cuando el tamaño de la ventana de reproducción se configura con esta implementación es que el tamaño de la ventana de reproducción configurada es para la ventana de reproducción agregada, por lo que el tamaño efectivo de la ventana de reproducción para cada espacio de número de secuencia es 1/8 del total.

Ejemplo de configuración:

```
config-t
Security
IPsec
replay-window 1024
Commit
```

> **Nota**: El tamaño efectivo de la ventana de reproducción para cada espacio de número de secuencia es 1024/8 = 128.

> **Nota**: desde Cisco IOS ®XE. 17.2.1, el tamaño agregado de la ventana de reproducción se ha aumentado a 8192 de modo que cada espacio del número de secuencia pueda tener una ventana de reproducción máxima de 8192/8 = 1024 paquetes.

En un dispositivo cEdge, el último número de secuencia recibido para cada espacio de número de secuencia se puede obtener de la salida del plano de datos IPsec de la **plataforma show crypto ipsec sa peer x.x.x.x**:

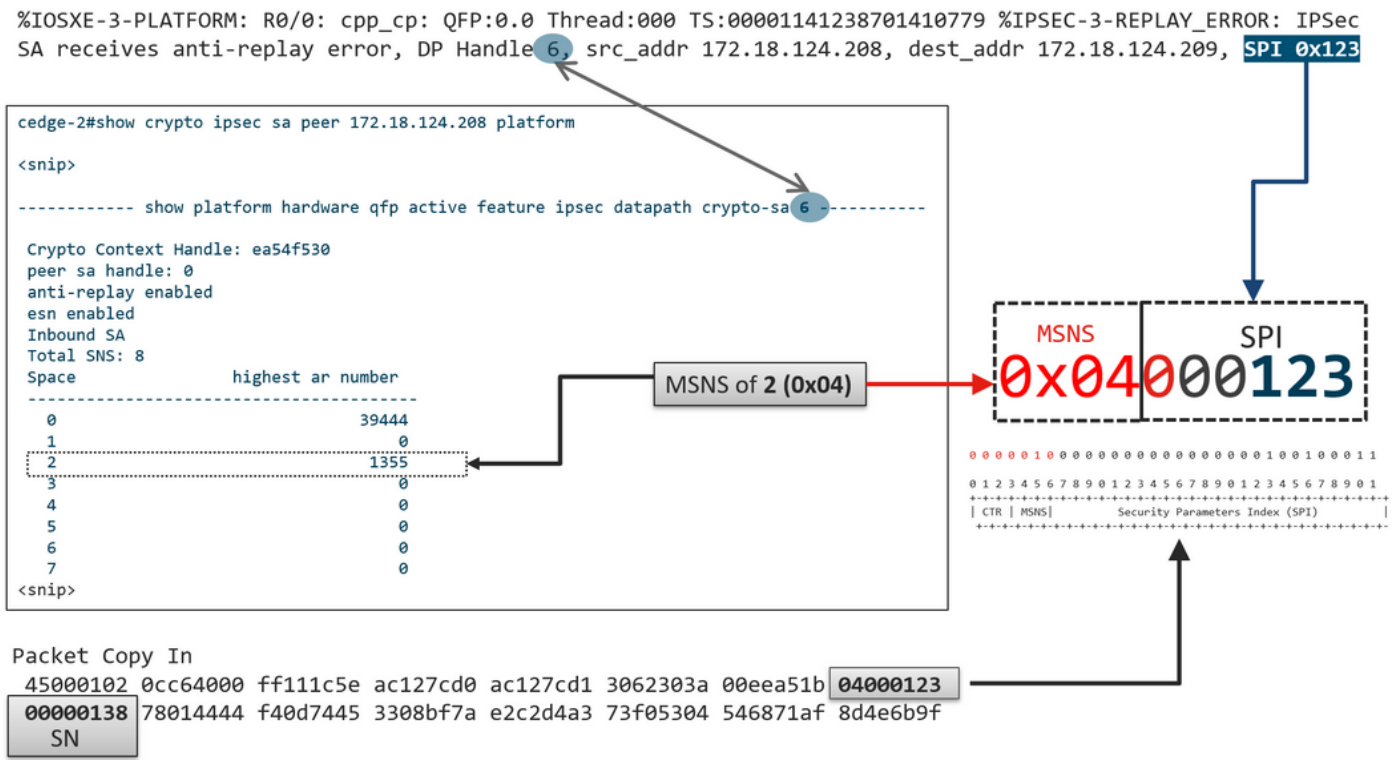
```
cedge-2#show crypto ipsec sa peer 172.18.124.208 platform

<snip>

------------------ show platform hardware qfp active feature ipsec datapath crypto-sa 5 --------
----------

 Crypto Context Handle: ea54f530
 peer sa handle: 0
 anti-replay enabled
 esn enabled
 Inbound SA
 Total SNS: 8
 Space                highest ar number
 ---------------------------------------
   0                              39444
   1                                  0
   2                               1355
   3                                  0
```

```
   4                                    0
   5                                    0
   6                                    0
   7                                    0
<snip>
```

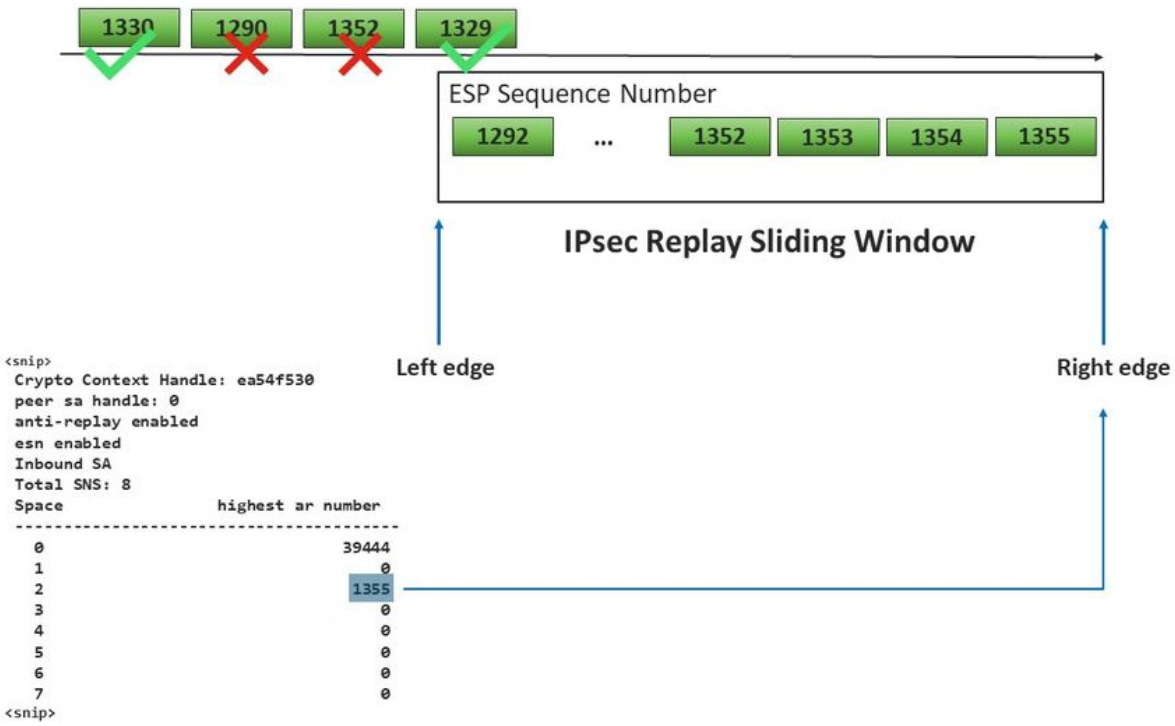
En el ejemplo, la ventana de anti-reproducción más alta (borde derecho de la ventana deslizante anti-reproducción) para MSNS de 0 **(0x00)** es **39444**, y para MSNS de **2 (0x04)** es **1335**, y estos contadores se utilizan para verificar si el número de secuencia está dentro de la ventana de reproducción para paquetes en el mismo espacio de número de secuencia.

> **Nota**: Existen diferencias de implementación entre la plataforma ASR1k y el resto de las plataformas de routing Cisco IOS ®XE (ISR4k, ISR1k, CSR1kv). Como resultado, existen algunas discrepancias en términos de los comandos show y su resultado para estas plataformas.

Es posible correlacionar los errores Anti-Replay y las salidas show para encontrar el SPI, y el índice de número de secuencia como se muestra en la imagen.



Con la información anterior obtenida, el borde derecho (ventana superior) y la ventana deslizante se ven como se muestra en la imagen.



Comandos para la Eficacia de la Ventana de Reproducción Configurada

A diferencia del IPSec normal (no SD-WAN), el comando rekey no tiene efecto para la ventana anti replay.

```
request platform software sdwan security ipsec-rekey
```

Estos comandos activan la ventana de reproducción configurada para que surta efecto:

> **Advertencia**: Asegúrese de comprender el impacto potencial de cualquier comando, ya que afecta a las conexiones de control y al plano de datos.

```
clear sdwan control connection
```

or

```
request platform software sdwan port_hop <color>
```

or

```
Interface Tunnelx
shutdown/ no shutdown
```

Resolución de problemas de fallos de reproducción

Solucionar problemas de recopilación de datos

Para las caídas de IPsec anti-replay, es importante entender las condiciones y los posibles desencadenantes del problema. Como mínimo, recopile el conjunto de información para proporcionar el contexto:

- La información del dispositivo para el emisor y el receptor de las caídas de paquetes de reproducción incluye el tipo de dispositivo, cEdge vs. vEdge, versión de software y configuración.
- Historial de problemas. ¿Cuánto tiempo lleva implantada la solución? ¿Cuándo comenzó el problema? Cualquier cambio reciente en la red o en las condiciones del tráfico.
- Cualquier patrón de la repetición cae, por ejemplo., ¿es esporádico o constante? Hora del problema y/o evento significativo, por ejemplo, ¿solo ocurre durante las horas pico de producción de tráfico elevado, o solo durante la regeneración de claves, y así sucesivamente?

Con la información anterior recopilada, continúe con el flujo de trabajo de solución de problemas.

Solucionar problemas de flujo de trabajo

El enfoque general de solución de problemas para los problemas de reproducción de IPSec es exactamente igual a cómo se realiza para IPSec tradicional, tenga en cuenta el espacio de secuencia SA por par y el Espacio de Número de Secuencia Múltiple como se explicó. A continuación, siga estos pasos:

Paso 1. Primero identifique el par para la caída de la reproducción desde el syslog y la velocidad de caída. Para las estadísticas de borrado, recopile siempre varias instantáneas con marca de tiempo de la salida para poder cuantificar la velocidad de borrado:

```
*Feb 19 21:28:25.006: %IOSXE-3-PLATFORM: R0/0: cpp_cp: QFP:0.0 Thread:000
TS:00001141238701410779 %IPSEC-3-REPLAY_ERROR: IPSec SA receives anti-replay error, DP Handle 6,
src_addr 172.18.124.208, dest_addr 172.18.124.209, SPI 0x123

cedge-2#show platform hardware qfp active feature ipsec datapath drops
Load for five secs: 1%/0%; one minute: 1%; five minutes: 1%
No time source, *11:25:53.524 EDT Wed Feb 26 2020
----------------------------------------------------------------------
Drop Type  Name                                        Packets
----------------------------------------------------------------------
        4  IN_US_V4_PKT_SA_NOT_FOUND_SPI                          30
       19  IN_CD_SW_IPSEC_ANTI_REPLAY_FAIL                        41
```

> **Nota**: No es raro ver caídas de reproducción ocasionales debido a la reordenación de la entrega de paquetes en la red, pero las caídas de reproducción persistentes afectan al servicio y se pueden investigar.

Paso 2a. Para una velocidad de tráfico relativamente baja, tome un seguimiento de paquetes con la condición establecida para ser la dirección ipv4 del par con la opción **copy packet** y examine los números de secuencia del paquete descartado contra el borde derecho de la ventana de reproducción actual y los números de secuencia en los paquetes adyacentes para confirmar si están realmente duplicados o fuera de la ventana de reproducción.

Paso 2b. Para velocidades de tráfico altas sin desencadenadores predecibles, configure una captura EPC con búfer circular y EEM para detener la captura cuando se detecten errores de reproducción. Dado que actualmente EEM no es compatible con vManage a partir de la versión 19.3, esto implica que cEdge tendría que estar en modo CLI cuando se realice esta tarea de solución de problemas.

Paso 3. Recopile la plataforma **show crypto ipsec sa peer x.x.x.x** en el receptor idealmente al mismo tiempo que se recopila la captura de paquetes o el seguimiento de paquetes. Este comando incluye la información de la ventana de reproducción del plano de datos en tiempo real para la SA entrante y saliente.

Paso 4. Si el paquete descartado está realmente fuera de servicio, tome capturas simultáneas tanto del emisor como del receptor para identificar si el problema está con el origen o con la capa de entrega de red subyacente.

Paso 5. Si los paquetes se descartan aunque no estén duplicados ni fuera de la ventana de reproducción, generalmente es indicativo de un problema de software en el receptor.

Ejemplo de Troubleshooting de ASR1001-x

Descripción de problemas:

HW: ASR1001-X
SW: 17.06.03a.

Se reciben múltiples errores de Anti-replay para el peer de sesión 10.62.33.91, por lo tanto, la sesión BFD se inestabiliza constantemente y el tráfico entre estos dos sitios se ve afectado.

```
Jul 26 20:31:20.879: %IOSXE-3-PLATFORM: R0/0: cpp_cp: QFP:0.0 Thread:027 TS:00000093139972173042
%IPSEC-3-REPLAY_ERROR: IPSec SA receives anti-replay error, DP Handle 22, src_addr 10.62.33.91,
dest_addr 10.62.63.251, SPI 0x106
Jul 26 20:32:23.567: %IOSXE-3-PLATFORM: R0/0: cpp_cp: QFP:0.0 Thread:009 TS:00000093202660128696
%IPSEC-3-REPLAY_ERROR: IPSec SA receives anti-replay error, DP Handle 22, src_addr 10.62.33.91,
dest_addr 10.62.63.251, SPI 0x106
Jul 26 20:33:33.939: %IOSXE-3-PLATFORM: R0/0: cpp_cp: QFP:0.0 Thread:051 TS:00000093273031417384
%IPSEC-3-REPLAY_ERROR: IPSec SA receives anti-replay error, DP Handle 22, src_addr 10.62.33.91,
dest_addr 10.62.63.251, SPI 0x106
Jul 26 20:34:34.407: %IOSXE-3-PLATFORM: R0/0: cpp_cp: QFP:0.0 Thread:020 TS:00000093333499638628
%IPSEC-3-REPLAY_ERROR: IPSec SA receives anti-replay error, DP Handle 22, src_addr 10.62.33.91,
dest_addr 10.62.63.251, SPI 0x106
```

Paso 1. Verifique que la ventana Anti Replay Configurada sea 8192.

```
cEdge#sh sdwan security-info
security-info authentication-type deprecated
security-info rekey 86400
 security-info replay-window 8192
security-info encryption-supported "AES_GCM_256 (and AES_256_CBC for multicast)"
security-info fips-mode Disabled
security-info pairwise-keying Disabled
security-info pwk-sym-rekey Enabled
security-info extended-ar-window Disabled
```

```
security-info integrity-type "ip-udp-esp esp"
```

> **Nota**: El tamaño efectivo de la ventana de reproducción para cada espacio de número de secuencia debe ser 8192/8= 1024 en este ejemplo.

Paso 2. Verifique el tamaño efectivo de la ventana de reproducción para el peer 10.62.33.91 para comparar y confirmar el valor configurado.

```
show crypto ipsec sa peer 10.62.33.91 platform
<snip>
------------------ show platform hardware qfp active feature ipsec sa 22 ------------------
<snip>
------------------ show platform software ipsec fp active encryption-processor 0 context
c441ff4c ------------------
<snip>
       window size: 64                  <-- Effective Window Size
window base(ESN): 0
Multi-SNS window_top
----------------------------------
index: 0, win_top: 0x00000000010dc0
index: 1, win_top: 0000000000000000
index: 2, win_top: 0x00000000b65f00
index: 3, win_top: 0000000000000000
index: 4, win_top: 0000000000000000
index: 5, win_top: 0000000000000000
index: 6, win_top: 0000000000000000
index: 7, win_top: 0000000000000000
traffic hard limit: 12876354284605669376
byte count: 0
packet count: 11378618
```

Tamaño de la ventana: 64 que se muestra en la salida no coincide con lo que la ventana de reproducción configurada **8192 (8192/8=1024)**, lo que significa que incluso si se configuró el comando no surtió efecto.

> **Nota**: La ventana de reproducción efectiva solo se muestra en las plataformas ASR. Para asegurarse de que el tamaño real de la ventana de reproducción anti es el mismo que el tamaño configurado, aplique uno de los comandos de la sección para tomar la efectividad de la ventana de reproducción configurada.

Paso 3. Configure y habilite el seguimiento de paquetes y supervise la captura (opcional) simultáneamente para el tráfico entrante desde el origen de la sesión: 10.62.33.91, destino: 10.62.63.251

```
cEdge#debug platform packet-trace packet 2048 circular fia-trace data-size 2048
cEdge#debug platform packet-trace copy packet both size 2048 L3
cEdge#debug platform condition ipv4 10.62.33.91/32 in
cEdge#debug plat cond start
```

Paso 4. Recopilar resumen de seguimiento de paquetes:

```
cEdge#show platform packet summay
```

Paso 5. Expanda algunos paquetes descartados (IpsecInput) capturados.

(IpsecInput) Paquetes descartados:

```
cEdge#sh platform pack pack 816
Packet: 816 CBUG ID: 973582
Summary
Input : TenGigabitEthernet0/0/0.972
Output : TenGigabitEthernet0/0/0.972
State : DROP 56 (IpsecInput)
Timestamp
Start : 97495234494754 ns (07/26/2022 21:43:56.25110 UTC)
Stop : 97495234610186 ns (07/26/2022 21:43:56.25225 UTC)
Path Trace
Feature: IPV4(Input)
Input : TenGigabitEthernet0/0/0.972
Output : <unknown>
Source : 10.62.33.91
Destination : 10.62.63.251
Protocol : 17 (UDP)
SrcPort : 12367
DstPort : 12347
<snip>

Packet Copy In
45000072 ab314000 fd115c77 0a3e215b 0a3e3ffb 304f303b 005e0000 04000106
00b6dfed 00000000 d0a60d5b 6161b06e 453d0e3d 5ab694ce 5311bbb6 640ecd68
7ceb2726 80e39efd 70e5549e 57b24820 fb963be5 76d01ff8 273559b0 32382ab4
c601d886 da1b3b94 7a2826e2 ead8f308 c464

817 DROP:
```

```
------------------------------
Packet: 817
<snip>
Packet Copy In
45000072 ab314000 fd115c77 0a3e215b 0a3e3ffb 304f303b 005e0000 04000106
00b6dfec 00000000 cc72d5dd ef73fe25 2440bed6 31378b78 3c506ee5 98e3dba4
bc9e6aa0 50ea98f6 7dee25c8 c1579ce0 1212290c 650f5947 57b9bc04 97c7996c
d4dbf3e6 25b33684 a7129b67 141a5e73 8736
```

SD-WAN utiliza ESP encapsulado UDP:

- El encabezado UDP es 304f303b 00770000,
- El siguiente es SPI (**0400106**)
- Por lo tanto, **00b6e00d** es el número de seguridad (SN).
- El índice MSNS es **2** (**x04**00106) debido a SPI de 32 bits (**0 0 0 0 0 0 1 0** 0 0 0 0 0 0 0 0 0 0 1 0 0 1 0 0 0 0 1 1.)

Paso 6. Verificar el índice MSNS

```
show crypto ipsec sa peer 10.62.33.91 platform
<snip>
------------------ show platform hardware qfp active feature ipsec sa 22 ------------------
<snip>
------------------ show platform software ipsec fp active encryption-processor 0 context
c441ff4c ------------------
<snip>
       window size: 64
window base(ESN): 0
Multi-SNS window_top
----------------------------------
index: 0, win_top: 0x00000000010dc0
index: 1, win_top: 0000000000000000
  index: 2, win_top: 0x00000000b65f00
index: 3, win_top: 0000000000000000
index: 4, win_top: 0000000000000000
index: 5, win_top: 0000000000000000
index: 6, win_top: 0000000000000000
index: 7, win_top: 0000000000000000
traffic hard limit: 12876354284605669376
byte count: 0
packet count: 11378618
```

La ventana antirreproducción más alta (borde derecho de la ventana deslizante antirreproducción) para MSNS de 2 (0x04) es **0b65f00.**

Paso 7. Expanda algunos paquetes capturados reenviados (FWD).

Paquetes reenviados:

```
Packet: 838
<snip>
Packet Copy In
4564008e ab044000 fd115c24 0a3e215b 0a3e3ffb 304f303b 007a0000 04000106
 00b6e015 00000000 088bbd6a f4e4b35f b131143f ef1f91eb 659149f7 dbe6b025
be7fbfd0 5fad1c71 014321f1 3e0d38f2 cc8d0e5f 1494e4fa 097c7723 dfc7ceef
```

```
4a14f444 abcc1777 0bb9337f cd70c1da 01fc5262 848b657c 3a834680 b07b7092
81f07310 4eacd656 ed36894a e468
```

Paquete: 837

```
Packet: 837
<snip>
Packet Copy In
4564008e ab044000 fd115c24 0a3e215b 0a3e3ffb 304f303b 007a0000 04000106
00b6e014 00000000 76b2a256 8e835507 13d14430 ae16d62c c152cdfd 2657c20c
01d7ce1d b3dfa451 a2cbf6e9 32f267f9 e10e9dec 395a0f9e 38589adb aad8dfb8
a3b72c8d a96f2dce 2a1557ab 67959b6e 94bbbb0a cfc4fc9e 391888da af0e492c
80bebb0e 9d7365a4 153117a6 4089
```

Paso 8. Recopile y obtenga la información del número de secuencia de varios paquetes reenviados (FWD) antes, después y después de las caídas.

```
FWD:
839 PKT: 00b6e003 FWD
838 PKT: 00b6e001 FWD
837 PKT: 00b6e000 FWD
815 PKT: 00b6e044 FWD
814 PKT: 00b6dfe8 FWD
813 PKT: 00b6e00d FWD

DROP:
816 PKT: 00b6dfed DROP
817 PKT: 00b6dfec DROP
818 PKT: 00b6dfeb DROP
819 PKT: 00b6dfe9 DROP
820 PKT: 00b6dfea DROP
```

Paso 9. Convierta a Decimal el SN y vuelva a ordenarlos para un cálculo simple:

```
REORDERED:
813 PKT: 00b6e00d FWD --- Decimal: 11984909
814 PKT: 00b6dfe8 FWD --- Decimal: 11984872
815 PKT: 00b6e044 FWD --- Decimal: 11984964 ***** Highest Value
816 PKT: 00b6dfed DROP--- Decimal: 11984877
817 PKT: 00b6dfec DROP--- Decimal: 11984876
818 PKT: 00b6dfeb DROP--- Decimal: 11984875
819 PKT: 00b6dfe9 DROP--- Decimal: 11984873
820 PKT: 00b6dfea DROP--- Decimal: 11984874
<snip>
837 PKT: 00b6e014 FWD --- Decimal: 11984916
838 PKT: 00b6e015 FWD --- Decimal: 11984917
839 PKT: 00b6e016 FWD --- Decimal: 11984918
```

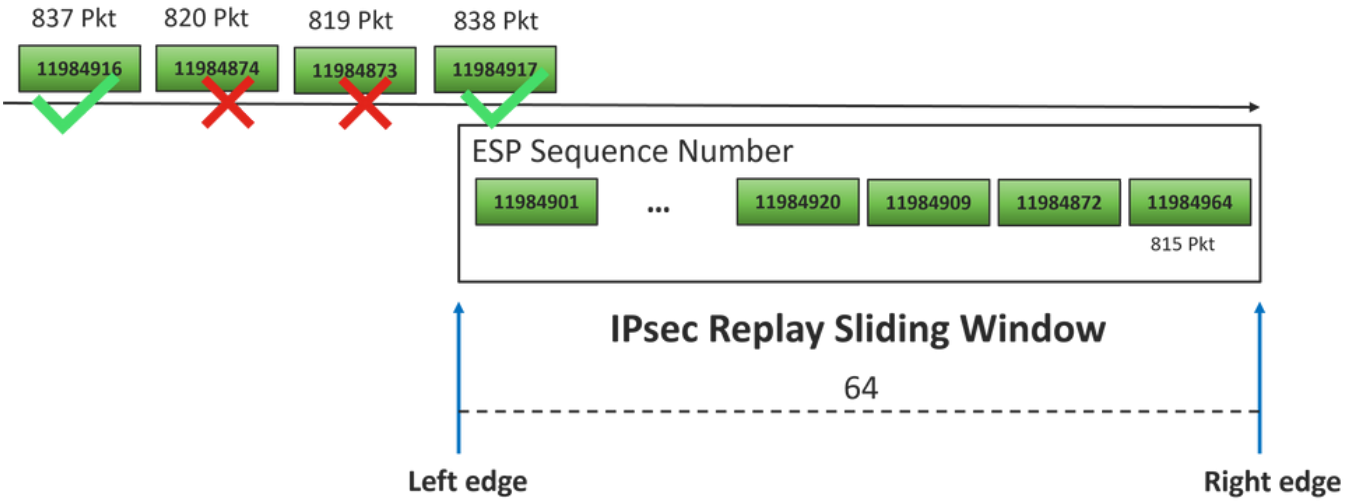
> **Nota**: Si el número de secuencia es mayor que el número de secuencia más alto de la ventana, se comprueba la integridad del paquete. Si el paquete pasa la verificación de integridad, la ventana deslizante se mueve a la derecha.

Paso 10. Convierta a Decimal el SN y vuelva a ordenarlos para un cálculo simple:

```
Difference:

815 PKT: Decimal: 11984964 ***** Highest Value
```

```
-------------------------------------
815(Highest) - X PKT = Diff
-------------------------------------
816 PKT: 11984964 - 11984877 = 87 DROP
817 PKT: 11984964 - 11984876 = 88 DROP
818 PKT: 11984964 - 11984875 = 89 DROP
819 PKT: 11984964 - 11984873 = 91 DROP
820 PKT: 11984964 - 11984874 = 90 DROP
<snip>
837 PKT: 11984964 - 11984916 = 48 FWD
838 PKT: 11984964 - 11984917 = 47 FWD
839 PKT: 11984964 - 11984918 = 45 FWD
```

Para este ejemplo, es posible visualizar la ventana deslizante con el **tamaño de ventana 64** y el **borde derecho**11984964 como se muestra en la imagen.



El número de secuencia recibido para paquetes descartados está muy por delante del borde derecho de la ventana de reproducción para ese espacio de secuencia.

Solución

Dado que el tamaño de la ventana todavía está en el valor anterior 64, como se ve en el paso 2, uno de los comandos de la sección Comandos para la Eficacia de la Ventana de Reproducción Configurada debe aplicarse para que el tamaño de la ventana 1024 tenga efecto.

Herramienta de captura Wireshark adicional

Otra herramienta útil para ayudar a correlacionar el SPI ESP y el número de secuencia es el software Wireshark.

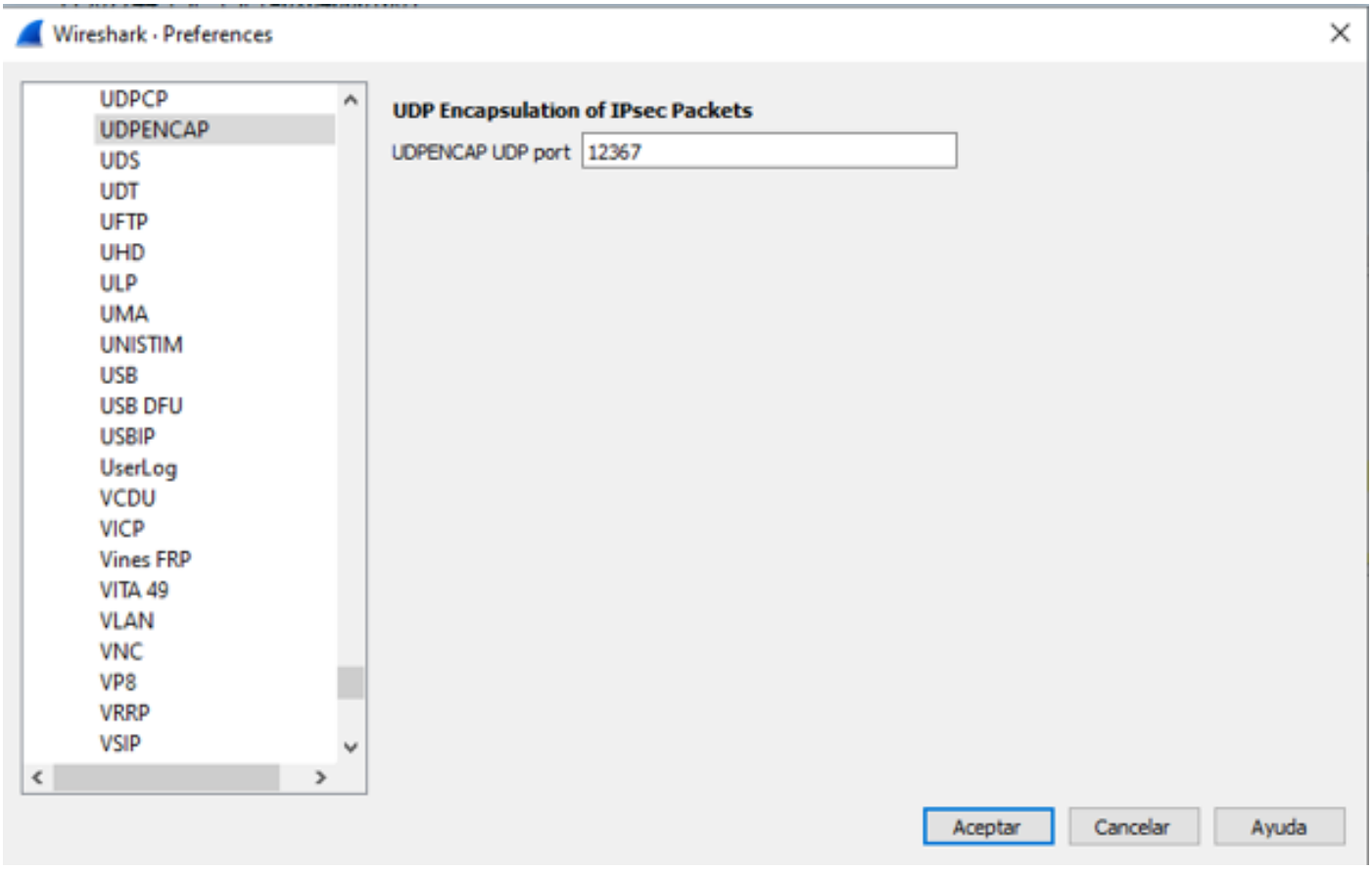
> **Nota**: Es importante recopilar la captura de paquetes cuando se produce el problema y, si es posible, al mismo tiempo, se recopila el seguimiento de fia como se ha descrito anteriormente

Configure la captura de paquetes para la dirección entrante y expórtela al archivo pcap.

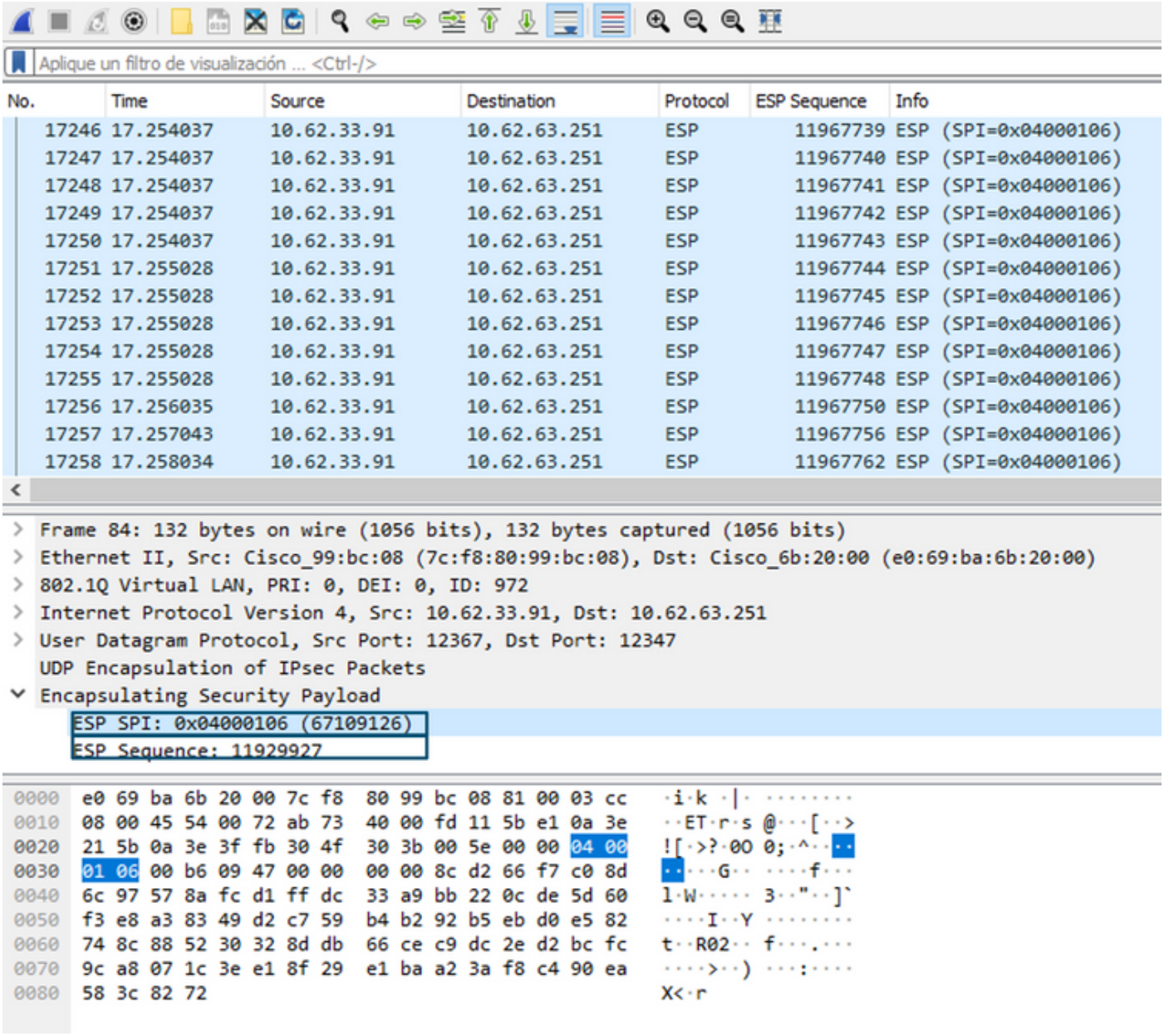
```
monitor caputure CAP match ipv4 host 10.62.33.91 host 10.62.63.251 buffer size 20 inter
TenGigabitEthernet0/0/0 in
monitor caputure CAP star
```

```
monitor caputure CAP stop
monitor caputure CAP export bootflash:Anti-replay.pca
```

Cuando se abre la captura pcap en Wireshark, para poder ver el SPI ESP y el número de secuencia, expanda un paquete, haga clic con el botón derecho y seleccione las **preferencias de protocolo**, busque **UDPENCAP** y cambie el puerto predeterminado al puerto SD-WAN (puerto de origen) como se muestra en la imagen.



Una vez que UDPENCAP está en su lugar con el puerto correcto, la información ESP se muestra como se muestra en la imagen.



Información Relacionada

- [Artículo de TechZone sobre Fallas de Comprobación de Anti-Replay de IPsec]
- [Expansión e Inhabilitación de la Ventana IPsec Anti-Replay]
- [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).