Troubleshooting de Fallas de Comprobación de Anti-Replay IPSec

Contenido

Introducción

Este documento describe un problema relacionado con las fallas de la comprobación de anti-reproducción del protocolo de seguridad de Internet (IPsec) y proporciona posibles soluciones.

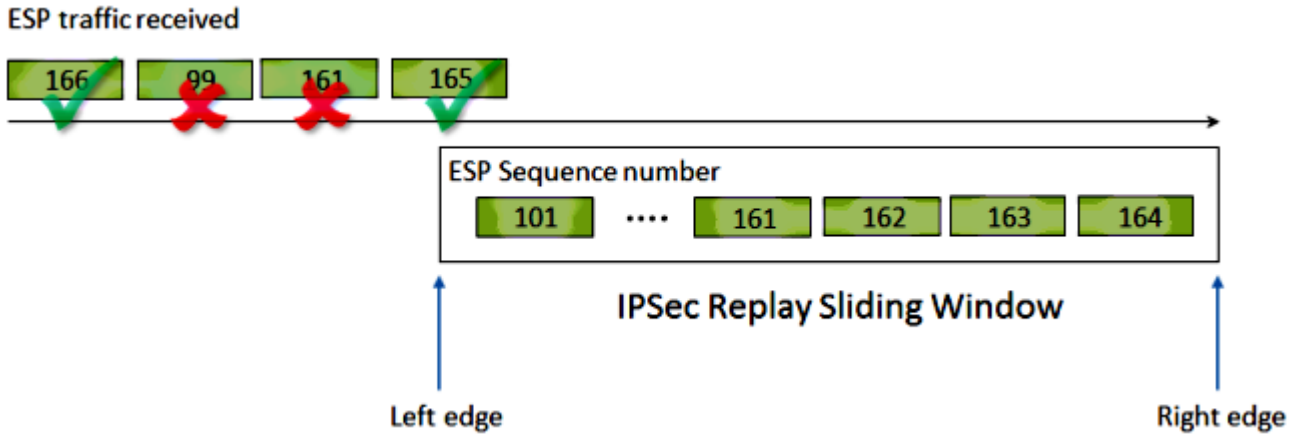
Antecedentes

Descripción general de los ataques de repetición

Un ataque de reproducción es una forma de ataque a la red en la que la transmisión de datos válidos se registra de forma malintencionada o fraudulenta y se repite posteriormente. Se trata de un intento de subvertir la seguridad por parte de alguien que registra las comunicaciones legítimas y las repite con el fin de hacerse pasar por un usuario válido e interrumpir o causar un impacto negativo en las conexiones legítimas.

Protección de verificación de reproducción IPSec

IPSec asigna a cada paquete cifrado un número de secuencia que aumenta monótonamente para proporcionar protección contra la reproducción frente a un atacante. El punto final de IPSec receptor realiza un seguimiento de los paquetes que ya ha procesado cuando utiliza estos números y una ventana deslizante de números de secuencia aceptables. El tamaño predeterminado de la ventana anti-reproducción en la implementación de Cisco IOS® es de 64 paquetes, como se muestra en esta imagen:



Cuando un extremo de túnel IPsec tiene habilitada la protección contra reproducción, el tráfico IPsec entrante se procesa de la siguiente manera:

- Si el número de secuencia se encuentra dentro de la ventana y no se ha recibido previamente, se comprueba la integridad del paquete. Si el paquete pasa la verificación de integridad, se acepta y el router marca que se ha recibido este número de secuencia. Por ejemplo, un paquete con el número de secuencia 162 de Carga de seguridad de encapsulación (ESP).
- Si el número de secuencia se encuentra dentro de la ventana pero se ha recibido previamente, el paquete se descarta. Este paquete duplicado se descarta y la caída se registra en el contador de reproducción.

- 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. Por ejemplo, si se recibe un paquete válido con un número de secuencia de 189, el nuevo borde derecho de la ventana se establece en 189 y el borde izquierdo es 125 (189 - 64 [tamaño de la ventana]).

- Si el número de secuencia es menor que el borde izquierdo, el paquete se descarta y se registra dentro del contador de reproducción. Esto se considera un paquete fuera de servicio.

En los casos en que ocurre una falla de verificación de reproducción y se descarta el paquete, el router genera un mensaje de Syslog similar a este:

```
%IPSEC-3-REPLAY_ERROR: IPSec SA receives anti-replay error, DP Handle n, src_addr x.x.x.x, dest_addr y.y
```

Nota: La detección de repetición se basa en la suposición de que la asociación de seguridad (SA) IPsec existe sólo entre dos iguales. La VPN de transporte cifrado de grupo (GETVPN) utiliza una única SA IPsec entre varios pares. Como resultado, GETVPN utiliza un mecanismo de verificación anti-reproducción completamente diferente llamado Falla Anti-Reproducción Basada en Tiempo . Este documento sólo cubre la anti-reproducción basada en contadores para túneles IPsec punto a punto.

Nota: La protección contra reproducción es un importante servicio de seguridad que ofrece el protocolo IPsec. La función IPsec anti-replay inhabilitada tiene implicaciones de seguridad y se debe realizar con discreción.

Problemas que pueden causar caídas de reproducción de IPSec

Como se ha descrito anteriormente, el propósito de las comprobaciones de reproducción es proteger frente a repeticiones malintencionadas de paquetes. Sin embargo, hay algunas situaciones en las que una comprobación de reproducción errónea podría no deberse a un motivo malintencionado:

    - El error puede deberse a un paquete suficiente que se reordena en la ruta de red entre los extremos del túnel. Esto puede ocurrir si hay varias trayectorias de red entre los pares.

    - El error puede ser causado por trayectorias de procesamiento de paquetes desiguales dentro del IOS de Cisco. Por ejemplo, los paquetes IPSec fragmentados que requieren el reensamblado de IP antes del descifrado podrían retrasarse lo suficiente como para que queden fuera de la ventana de reproducción en el momento en que se procesen.
    - El error puede deberse a la calidad de servicio (QoS) habilitada en el extremo de IPsec de envío o en la ruta de red. Con la implementación de Cisco IOS, el cifrado IPsec se produce antes que QoS en la dirección de salida. Ciertas funciones de QoS, como la cola de latencia baja (LLQ), podrían provocar que la entrega de paquetes IPSec se desordene y el terminal receptor los descarte debido a un error en la comprobación de reproducción.

    - Un problema operativo o de configuración de red puede duplicar paquetes mientras transitan por la red.

- Un atacante (intermediario) podría retrasar, descartar y duplicar potencialmente el tráfico ESP.

Troubleshooting de IPsec Replay Drops

La clave para resolver problemas de caídas de reproducción IPSec es identificar qué paquetes se descartan debido a la reproducción y utilizar capturas de paquetes para determinar si estos paquetes son realmente paquetes reproducidos o paquetes que han llegado al router receptor fuera de la ventana de reproducción. Para hacer coincidir correctamente los paquetes descartados con lo que se captura en el rastreo del sabueso, el primer paso es identificar el par y el flujo IPSec al que pertenecen los paquetes descartados y el número de secuencia ESP del paquete.

Utilizar la Función de Seguimiento de Paquetes de Datapath de Cisco IOS XE

En las plataformas de router que ejecutan Cisco IOS® XE, la información sobre el peer y el Índice de Parámetros de Seguridad (SPI) IPSec se imprimen en el mensaje Syslog cuando se produce un descarte, para ayudar a resolver problemas de anti-reproducción. Sin embargo, un dato clave que aún no se ha obtenido es el número de secuencia de ESP. El número de secuencia ESP se utiliza para identificar de forma única un paquete IPSec dentro de un flujo IPSec determinado. Sin el número de secuencia, resulta difícil identificar exactamente qué paquete se descarta en una captura de paquetes.

La función de seguimiento de paquetes de ruta de datos de Cisco IOS XE se puede utilizar en esta situación cuando se observa el descarte de reproducción, con este mensaje de Syslog:

```
%IOSXE-3-PLATFORM: F0: cpp_cp: QFP:0.0 Thread:060 TS:00000001132883828011
%IPSEC-3-REPLAY_ERROR: IPSec SA receives anti-replay error, DP Handle 3, src_addr 10.2.0.200, dest_addr
```

Para ayudar a identificar el número de secuencia ESP para el paquete descartado, complete estos pasos con la función de seguimiento de paquetes:

1. Configure el filtro de depuración condicional de la plataforma para hacer coincidir el tráfico del dispositivo par:

```
debug platform condition ipv4 10.2.0.200/32 ingress
debug platform condition start
```

1. Habilite el seguimiento de paquetes con la opción **copy** para copiar la información del encabezado del paquete:

```
debug platform packet enable
debug platform packet-trace packet 64
debug platform packet-trace copy packet input l3 size 100
```

1. Cuando se detectan errores de reproducción, utilice el buffer de seguimiento de paquetes para identificar el paquete descartado debido a la reproducción, y el número de secuencia ESP se puede encontrar en el paquete copiado:

<#root>

Router#

show platform packet-trace summary

```
Pkt   Input           Output          State  Reason
0     Gi4/0/0         Tu1             CONS   Packet Consumed
1     Gi4/0/0         Tu1             CONS   Packet Consumed
2     Gi4/0/0         Tu1             CONS   Packet Consumed
3     Gi4/0/0         Tu1             CONS   Packet Consumed
4     Gi4/0/0         Tu1             CONS   Packet Consumed
5     Gi4/0/0         Tu1             CONS   Packet Consumed
6     Gi4/0/0         Tu1             DROP   053 (IpsecInput)
7     Gi4/0/0         Tu1             DROP   053 (IpsecInput)
8     Gi4/0/0         Tu1             CONS   Packet Consumed
9     Gi4/0/0         Tu1             CONS   Packet Consumed
10    Gi4/0/0         Tu1             CONS   Packet Consumed
11    Gi4/0/0         Tu1             CONS   Packet Consumed
12    Gi4/0/0         Tu1             CONS   Packet Consumed
13    Gi4/0/0         Tu1             CONS   Packet Consumed
```

El resultado anterior muestra que los números de paquete 6 y 7 se descartan, por lo que se pueden examinar en detalle ahora:

```
<#root>

Router#

show platform packet-trace packet 6



/>Packet: 6           CBUG ID: 6
Summary
  Input     : GigabitEthernet4/0/0
  Output    : Tunnel1
  State     : DROP 053 (IpsecInput)
  Timestamp : 3233497953773
Path Trace
  Feature: IPV4
    Source      : 10.2.0.200
    Destination : 10.1.0.100
    Protocol    : 50 (ESP)
  Feature: IPSec
    Action    : DECRYPT
    SA Handle : 3
    SPI       :

0x4c1d1e90


    Peer Addr :

10.2.0.200


    Local Addr: 10.1.0.100
  Feature: IPSec
    Action    : DROP
    Sub-code  :

019 - CD_IN_ANTI_REPLAY_FAIL


Packet Copy In
  45000428 00110000 fc329575 0a0200c8 0a010064 4c1d1e90

00000006

 790aa252
  e9951cd9 57024433 d97c7cb8 58e0c869 2101f1ef 148c2a12 f309171d 1b7a4771
  d8868af7 7bae9967 7d880197 46c6a079 d0143e43 c9024c61 0045280a d57b2f5e
  23f06bc3 ab6b6b81 c1b17936 98939509 7aec966e 4dd848d2 60517162 9308ba5d
```

El número de secuencia ESP tiene un desplazamiento de 24 bytes que comienza desde el encabezado IP (o 4 bytes de los datos de carga útil del paquete IP), como se enfatizó en negrita en la salida anterior. En este ejemplo en particular, el número de secuencia ESP para el paquete descartado es 0x6.

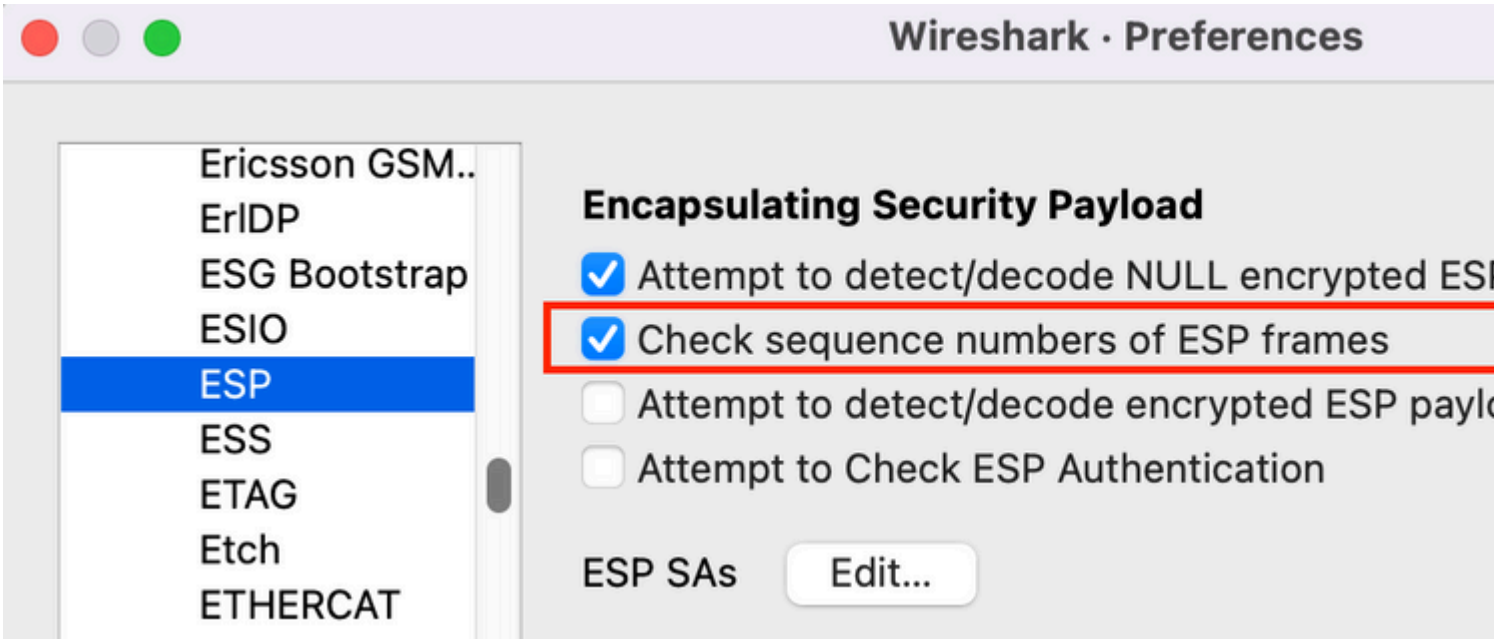
Recopilar capturas de paquetes

Además de la identificación de la información de paquete para el paquete descartado debido a una falla de verificación de reproducción, una captura de paquete para el flujo IPsec en cuestión debe recopilarse simultáneamente. Esto ayuda en el examen del patrón de número de secuencia ESP dentro del mismo flujo IPSec para ayudar a determinar la razón de la caída de la reproducción. Para obtener detalles sobre cómo

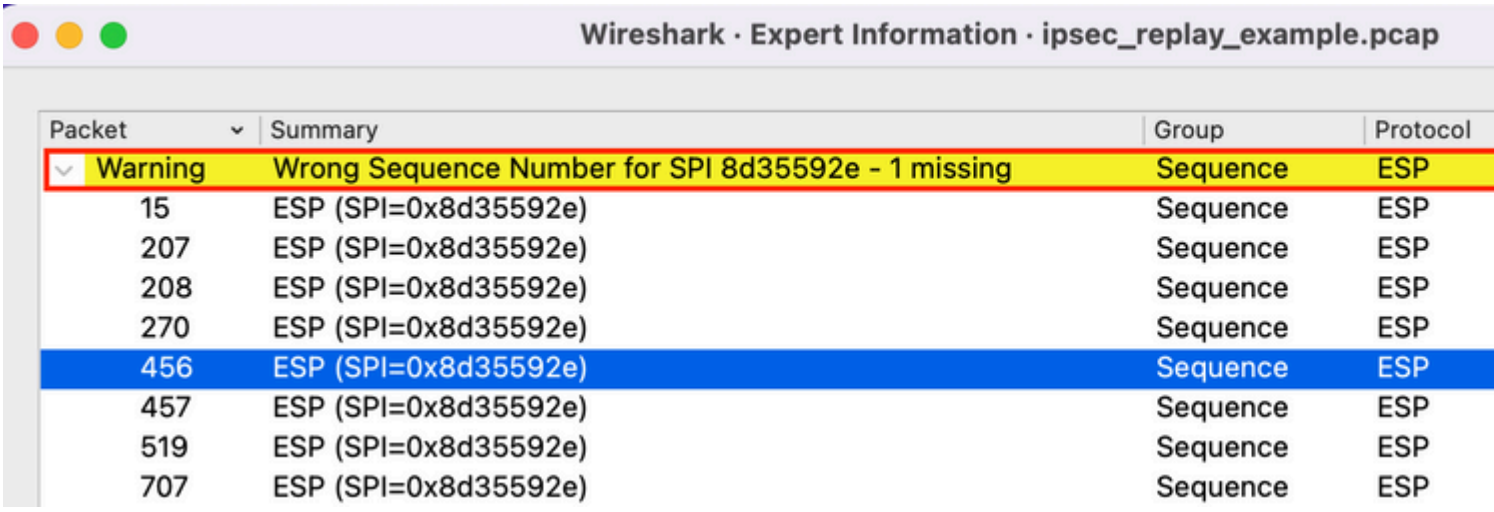
utilizar la captura de paquetes integrada (EPC) en los routers Cisco IOS XE, vea Ejemplo de Configuración de la Captura de Paquetes Integrada para Cisco IOS y Cisco IOS XE.

Utilizar Análisis de número de secuencia de Wireshark

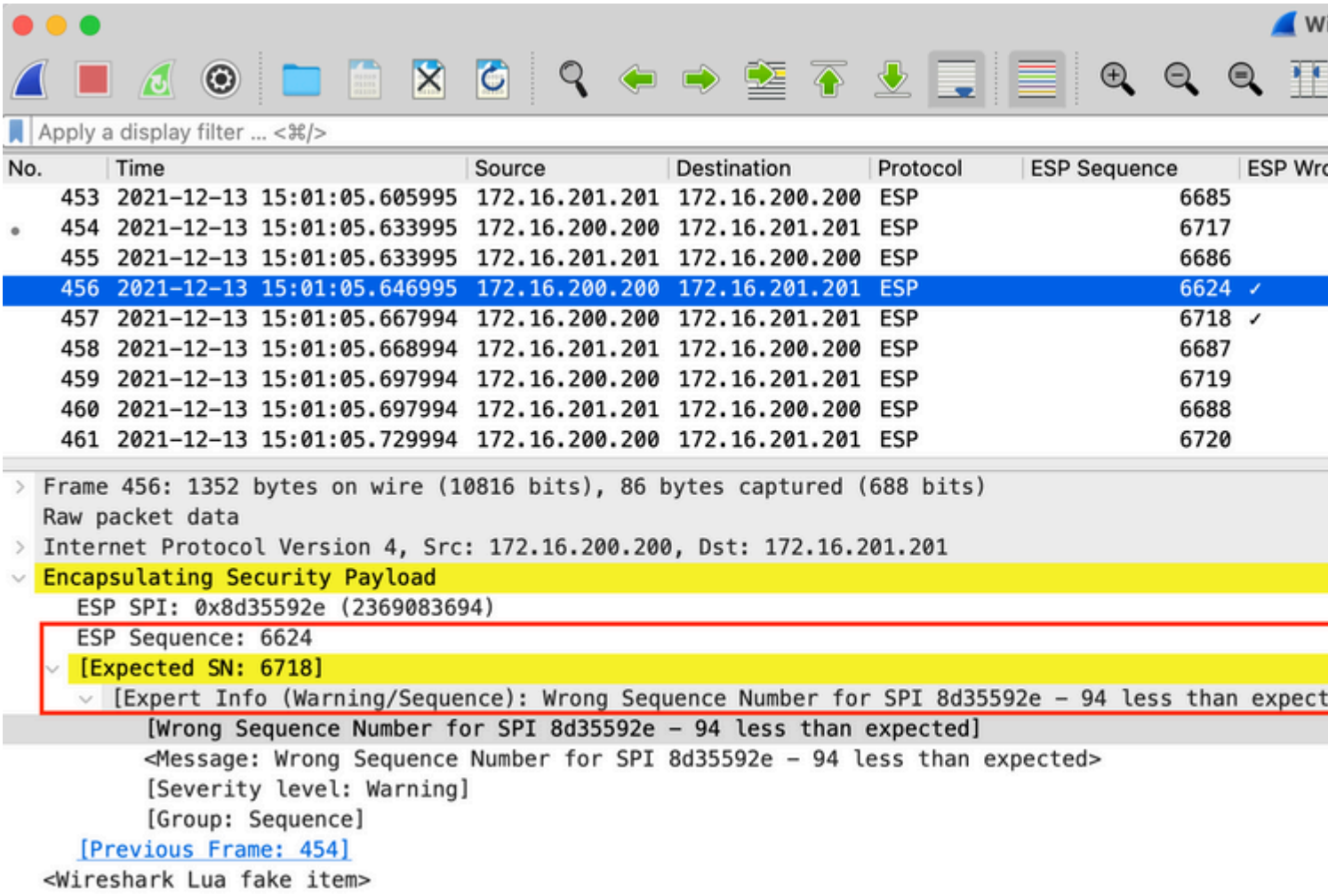
Una vez que se ha recopilado la captura de paquetes para los paquetes cifrados (ESP) en la interfaz WAN, Wireshark se puede utilizar para realizar un análisis de números de secuencia ESP para detectar cualquier anomalía en los números de secuencia. En primer lugar, asegúrese de que la Verificación del número de secuencia esté habilitada en **Preferencias** > **Protocolos** > **ESP** como se muestra en la imagen:



A continuación, verifique cualquier problema de número de secuencia de ESP en **Analizar** > **Información de experto** de la siguiente manera:



Haga clic en cualquiera de los paquetes con el número de secuencia incorrecto para obtener detalles adicionales de la siguiente manera:



Solución

Una vez que se identifica el peer y se recopila la captura de paquetes para las caídas de reproducción, tres escenarios posibles podrían explicar los fallos de reproducción:

1. Es un paquete válido que se ha retrasado:
   Las capturas de paquetes ayudan a confirmar si el paquete es realmente válido y si el problema es insignificante (debido a problemas de latencia de red o ruta de transmisión) o requiere una resolución de problemas más profunda. Por ejemplo, la captura muestra un paquete con un número de secuencia de X que llega fuera de orden, y el tamaño de la ventana de reproducción está actualmente establecido en 64. Si un paquete válido con el número de secuencia (X + 64) llega antes del paquete X, la ventana se desplaza hacia la derecha y luego el paquete X se descarta debido a una falla de reproducción.

   En tales escenarios, es posible aumentar el tamaño de la ventana de reproducción o inhabilitar la verificación de reproducción para asegurarse de que tales demoras se consideren aceptables y que los paquetes legítimos no sean descartados. De forma predeterminada, el tamaño de la ventana de reproducción es bastante pequeño (el tamaño de la ventana es 64). Si aumenta el tamaño, no aumenta en gran medida el riesgo de un ataque. Para obtener información sobre cómo configurar una Ventana Anti-Replay de IPSec, consulte el documento Cómo Configurar la Ventana Anti-Replay de IPSec: Expandir e Inhabilitar.

Sugerencia: si la ventana de reproducción está desactivada o alterada en el perfil IPSec utilizado en una interfaz de túnel virtual (VTI), los cambios no surtirán efecto hasta que se

---

elimine y vuelva a aplicar el perfil de protección o se restablezca la interfaz de túnel. Se trata de un comportamiento esperado, ya que los perfiles IPsec son una plantilla que se utiliza para crear un mapa de perfil de túnel cuando se activa la interfaz de túnel. Si la interfaz ya está activa, los cambios en el perfil no afectan al túnel hasta que se restablezca la interfaz.

Nota: los primeros modelos de Aggregation Services Router (ASR) 1000 (como ASR1000 con ESP5, ESP10, ESP20 y ESP40, junto con ASR1001) no admitían un tamaño de ventana de 1024, aunque la CLI permitía dicha configuración. Como resultado, es posible que el tamaño de la ventana que se informa en el resultado del comando **show crypto ipsec sa** no sea correcto. Utilice el comando **show crypto ipsec sa peer ip-address platform** para verificar el tamaño de la ventana anti-reproducción de hardware. El tamaño predeterminado de la ventana es de 64 paquetes en todas las plataformas. Para obtener más información, consulte el ID de bug de Cisco CSCso45946. Las plataformas de routing Cisco IOS XE más recientes (como ASR1K con ESP100 y ESP200, ASR1001-X y ASR1002-X, routers de la serie 4000 de router de servicio integrado (ISR) y routers de la serie Catalyst 8000) admiten un tamaño de ventana de 1024 paquetes en las versiones 15.2(2)S y posteriores.

2. Se debe a la configuración de QoS en el terminal de envío:
   Esta situación requiere un examen cuidadoso y ajustar cierta QoS para mitigar la condición. Para obtener una descripción más detallada de este tema y una posible solución, consulte el artículo Consideraciones sobre la eliminación de reproducciones en una VPN IPSec (V3PN) con voz y vídeo.

3. Es un paquete duplicado que se recibió previamente:
   Si este es el caso, se pueden observar dos o más paquetes con el mismo número de secuencia ESP dentro del mismo flujo IPsec en la captura de paquetes. En este caso, se espera la caída de paquetes ya que la protección de reproducción IPSec funciona como se pretende para evitar ataques de reproducción en la red, y el registro del sistema es meramente informativo. Si esta condición persiste, debe investigarse como una amenaza de seguridad potencial.

Nota: Los errores de comprobación de reproducción sólo se ven cuando se habilita un algoritmo de autenticación en el conjunto de transformación IPsec. Otra forma de suprimir este mensaje de error es desactivar la autenticación y realizar el cifrado solamente; sin embargo, esto se desaconseja fuertemente debido a las implicaciones de seguridad de la autenticación desactivada.

Additional Information

Resolución de Problemas de Errores de Reproducción en Routers Heredados con Cisco IOS Classic

Las caídas de reproducción de IPSec en los routers de la serie ISR G2 heredada que utilizan el IOS de Cisco son diferentes de los routers que utilizan el IOS XE de Cisco, como se muestra aquí:

<#root>

```
%CRYPTO-4-PKT_REPLAY_ERR: decrypt: replay check failed
```

connection id=529, sequence number=13

Tenga en cuenta que la salida del mensaje no proporciona la dirección IP del par ni la información SPI. Para resolver problemas en esta plataforma, utilice el "conn-id" en el mensaje de error. Identifique el "conn-id" en el mensaje de error y búsquelo en el resultado de **show crypto ipsec sa**, ya que la reproducción es una verificación por SA (en lugar de una verificación por par). El mensaje Syslog también proporciona el número de secuencia ESP, que puede ayudar a identificar de manera única el paquete descartado en la captura de paquetes.

Nota: Con diferentes versiones de código, el "conn-id" es el **conn id** o el **flow_id** para la SA entrante.

Esto se ilustra aquí:

<#root>

```
%CRYPTO-4-PKT_REPLAY_ERR: decrypt: replay check failed
```

connection id=529, sequence number=13

```
Router#
```

show crypto ipsec sa | in peer|conn id

```
   current_peer 10.2.0.200 port 500
```

conn id: 529

```
, flow_id: SW:529, sibling_flags 80000046, crypto map: Tunnel0-head-0
        conn id: 530, flow_id: SW:530, sibling_flags 80000046, crypto map: Tunnel0-head-0
Router#

Router#
```

show crypto ipsec sa peer 10.2.0.200 detail

```
   interface: Tunnel0
    Crypto map tag: Tunnel0-head-0, local addr 10.1.0.100

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   current_peer 10.2.0.200 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 27, #pkts encrypt: 27, #pkts digest: 27
    #pkts decaps: 27, #pkts decrypt: 27, #pkts verify: 27
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #pkts no sa (send) 0, #pkts invalid sa (rcv) 0
    #pkts encaps failed (send) 0, #pkts decaps failed (rcv) 0
    #pkts invalid prot (recv) 0, #pkts verify failed: 0
    #pkts invalid identity (recv) 0, #pkts invalid len (rcv) 0
    #pkts replay rollover (send): 0, #pkts replay rollover (rcv) 0
```

##pkts replay failed (rcv): 21

```
    #pkts internal err (send): 0, #pkts internal err (recv) 0

     local crypto endpt.: 10.1.0.100, remote crypto endpt.: 10.2.0.200
     path mtu 2000, ip mtu 2000, ip mtu idb Serial2/0
     current outbound spi: 0x8B087377(2332586871)
     PFS (Y/N): N, DH group: none

               inbound esp sas:
```

spi: 0xE7EDE943(3891128643)

```
        transform: esp-gcm ,
        in use settings ={Tunnel, }
        conn id: 529, flow_id: SW:529, sibling_flags 80000046, crypto map:
        Tunnel0-head-0
        sa timing: remaining key lifetime (k/sec): (4509600/3223)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE

<SNIP>
```

Como se puede ver en esta salida, la caída de reproducción es de la dirección de peer 10.2.0.200 con un SPI SA ESP entrante de 0xE7EDE943. También se puede observar desde el propio mensaje de registro que el número de secuencia ESP para el paquete descartado es 13. La combinación de la dirección de peer, el número SPI y el número de secuencia ESP se puede utilizar para identificar de manera única el paquete descartado en la captura de paquetes.

> **Nota**: El mensaje Syslog de Cisco IOS está limitado por velocidad para el paquete del plano de datos que cae a uno por minuto. Para obtener un conteo exacto del número exacto de paquetes descartados, utilice el comando **show crypto ipsec sa detail** como se muestra anteriormente.

Uso con software Cisco IOS XE anterior

En los routers que ejecutan las versiones anteriores de Cisco IOS XE, es posible que el "REPLAY_ERROR" notificado en el Syslog no imprima el flujo IPsec real con la información del par donde se descarta el paquete reproducido, como se muestra aquí:

```
%IOSXE-3-PLATFORM: F0: cpp_cp: QFP:00 Thread: 095 TS:00000000240306197890
%IPSEC-3-REPLAY_ERROR: IPSec SA receives anti-replay error, DP Handle 3
```

Para identificar la información correcta de peer y flujo de IPSec, utilice el controlador de plano de datos (DP) impreso en el mensaje Syslog como el parámetro de entrada SA Handle en este comando, para recuperar la información de flujo de IPSec en el procesador de flujo cuántico (QFP):

<#root>

Router#

show platform hardware qfp active feature ipsec sa 3

```
QFP ipsec sa Information

         QFP sa  id: 3
          pal sa id: 2
         QFP spd id: 1
          QFP sp id: 2
            QFP spi:
```

0x4c1d1e90(1276976784)

```
         crypto ctx: 0x000000002e03bfff
              flags: 0xc000800
                   : src:IKE  valid:Yes  soft-life-expired:No  hard-life-expired:No
                   :
```

replay-check:Yes

```
  proto:0  mode:0  direction:0
                   : qos_preclassify:No  qos_group:No
                   : frag_type:BEFORE_ENCRYPT  df_bit_type:COPY
                   : sar_enable:No  getvpn_mode:SNDRCV_SA
                   : doing_translation:No  assigned_outside_rport:No
                   : inline_tagging_enabled:No
          qos_group: 0x0
                mtu: 0x0=0
          sar_delta: 0
         sar_window: 0x0
         sibling_sa: 0x0
             sp_ptr: 0x8c392000
            sbs_ptr: 0x8bfbf810
```

local endpoint: 10.1.0.100
remote endpoint: 10.2.0.200

```
   cgid.cid.fid.rid: 0.0.0.0
               ivrf: 0
               fvrf: 0
    trans udp sport: 0
    trans udp dport: 0
    first intf name: Tunnel1
  <SNIP>
```

También se puede utilizar un script Embedded Event Manager (EEM) para automatizar la recopilación de datos:

```
event manager applet Replay-Error
 event syslog pattern "%IPSEC-3-REPLAY_ERROR: IPSec SA receives anti-replay error"
 action 1.0 regexp "([0-9]+)$" "$_syslog_msg" dph
 action 2.0 cli command "enable"
 action 3.0 cli command "show platform hardware qfp active feature ipsec sa $dph |
 append bootflash:replay-error.txt"
```

En este ejemplo, la salida recolectada se redirige a la **memoria flash** de **inicialización.** Para ver este

resultado, utilice el comando **more bootflash:replay-error.txt**.

Información Relacionada

- Diseño de red de referencia de la solución VPN IPSec (V3PN) habilitada para voz y vídeo
- Cómo Configurar IPsec Anti-Replay Window: Expanding and Disabling.
- Soporte Técnico y Documentación - Cisco Systems

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).