Errores del control de la Anti-respuesta del IPSec

Contenido

Introducción

Este documento describe un problema que se refiera a un error del control de la anti-respuesta de la seguridad de protocolos en Internet (IPSec), y proporciona los procedimientos y las Soluciones posibles del Troubleshooting al problema.

> **Note**: La Protección Anti-Replay es un servicio de seguridad importante que el Protocolo IPSec ofrece. La incapacidad de la anti-respuesta del IPSec tiene consecuencias en la seguridad, y se debe utilizar solamente con cautela.

Antecedentes

Descripción del ataque con paquetes copiados

Un ataque con paquetes copiados es una forma de ataque a la red en la cual una transmisión de datos válida malévolo o fraudulento se relanza o retrasado. Es una tentativa derribar la Seguridad por alguien que registra las comunicaciones legítimas y las relanza para personificar a un usuario válido, e interrumpir o causar el impacto negativo para las conexiones legítimas.

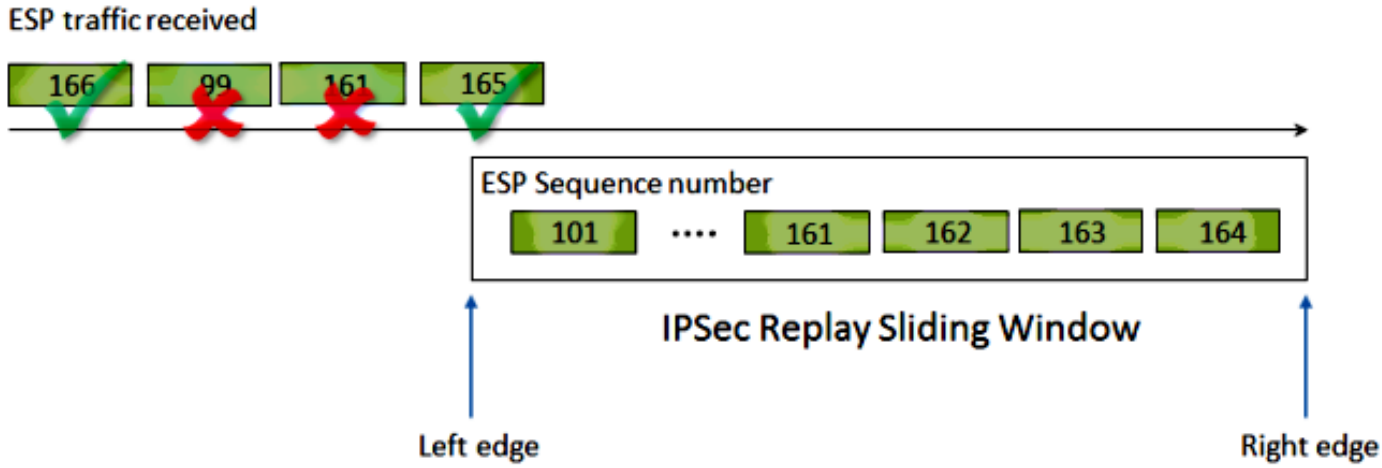
Descripción del error del control de la respuesta

El IPSec proporciona la Protección Anti-Replay contra un atacante que duplique los paquetes encriptados con la asignación de un número de secuencia monotónico cada vez mayor a cada paquete encriptado. El punto final de IPSec de recepción no pierde de vista que los paquetes él han procesado ya en base de estos números con el uso de una ventana de desplazamiento de todos los números de secuencia aceptables. Actualmente, el tamaño predeterminado de la

ventana contra repetición en la implementación del ® del Cisco IOS es 64 paquetes.

> **Note**: Se han clasifiado los pedidos de mejora CSCva65805 y CSCva65836 de aumentar el tamaño de la ventana predeterminado de la respuesta a 512 mientras que 64 se considera poco práctico pequeños para las redes modernas.

Esto se ilustra en esta figura:



Aquí están los pasos para procesar el tráfico IPSec entrante en que recibe el punto final del túnel con la anti-respuesta habilitada:

1. Cuando se recibe un paquete, si el número de secuencia cae dentro de la ventana y no fue recibido previamente, el paquete se valida, y se marca como recibido antes de que se envíe a la verificación de la integridad.

2. Si el número de secuencia cae dentro de la ventana y fue recibido previamente, se cae el paquete, y se incrementa el contador de la respuesta.

3. Si el número de secuencia es mayor que el número de secuencia más alto de la ventana, el paquete se valida, y se marca como recibido. La ventana de desplazamiento entonces se mueve a la derecha.
   Note: Esto ocurre si el paquete es válido y pasa solamente las verificaciones de la integridad.
4. Si el número de secuencia es menos que la secuencia más baja de la ventana, se cae el paquete, y se incrementa el contador de la respuesta.

En los segundos y cuartos escenarios, un error del control de la respuesta ocurre, y el router visualiza un mensaje de error similar a esto:

```
%CRYPTO-4-PKT_REPLAY_ERR: decrypt: replay check failed connection id=#, sequence
number=#
```

> **Note**: El transporte cifrado grupo VPN (GETVPN) tiene un error basado totalmente diverso de la Anti-respuesta del tiempo llamado del control de la anti-respuesta. Este documento cubre solamente la anti-respuesta contador-basada.

Problema

Según lo descrito previamente, el propósito de los controles de la respuesta es proteger contra las repeticiones malévolas de los paquetes. Sin embargo, hay algunos escenarios donde un control fallado de la respuesta no pudo ser debido a una razón malévola:

- El error pudo resultar de un paquete reordena en el medio de transmisión. Esto es especialmente verdad si existen los trayectos paralelos.
- El error se pudo causar por las trayectorias de proceso desiguales del paquete dentro del Cisco IOS. Por ejemplo, paquetes IPsec grandes que requieren el nuevo ensamble IP antes de que el desciframiento se pudiera retrasar bastantes, en un sistema bajo carga, para caer fuera de la ventana de la respuesta para el momento en que él se procese.
- El error se pudo causar por el Calidad de Servicio (QoS) habilitado en el punto final de IPSec de envío. Con el Cisco IOS implementación, la encripción de IPSec sucede antes de QoS en la dirección de salida. Ciertas características de QoS, tales como low latency queueing (LLQ), pueden hacer la salida del paquete IPsec fuera de servicio y caerse por el punto final de recepción debido a un error del control de la respuesta.

Descensos de la respuesta del IPSec del Troubleshooting

La clave para resolver problemas los descensos de la respuesta del IPSec es identificar las caídas de paquetes debidas jugar de nuevo, y a las capturas de paquetes del uso para confirmar si estos paquetes son de hecho los paquetes jugados de nuevo o los paquetes que han llegado en el router de recepción fuera de la ventana de la respuesta. Para hacer juego correctamente los paquetes perdidos a qué se capturan en la traza de sniffer, el primer paso es identificar el par y el flujo del IPSec a quienes los paquetes perdidos pertenecen. Esto se hace diferentemente basó en la plataforma del router.

Plataforma del router de los Servicios integrados de Cisco (ISR) /ISR G2 que funciona con el Cisco IOS clásico

Para resolver problemas en esta plataforma, utilice la CONN-**identificación** en el mensaje de error. Identifique la CONN-**identificación** en el mensaje de error, y busqúela en la salida **crypto IPSec sa de la demostración**, puesto que la respuesta es un control por-**SA** (asociación de seguridad) (en comparación con un por-**par**). El mensaje de Syslog también proporciona el número de secuencia del Encapsulating Security Payload (ESP), que puede ayudar únicamente a identificar el paquete perdidos en la captura de paquetes.

> **Note**: Con diversas versiones del código, la CONN-**identificación** es la **identificación conec** o **flow_id** para el SA entrante.

Esto se ilustra aquí:

```
%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 puede ser visto de esta salida, el descenso de la respuesta es de la dirección de peer de **10.2.0.200** con un Security Parameter Index entrante ESP SA (SPI) de **0xE7EDE943**. Puede también ser observado del mensaje del registro sí mismo que el número de secuencia ESP para el paquete perdidos es **13**. Así pues, la combinación de dirección de peer, de número de SPI, y del número de secuencia ESP se puede utilizar para identificar únicamente el paquete caído en la captura de paquetes.

> **Note**: El mensaje de Syslog del Cisco IOS es tarifa limitada para las caídas de paquetes del dataplane. Para conseguir una cuenta exacta de la cantidad exacta de paquetes cayó, utiliza el **comando show crypto ipsec sa detail** como se muestra previamente. También, la nota en el código anterior que la versión deL Cisco IOS 12.4(4)T, los contadores se pudo poner al día incorrectamente. Esto se repara en el Id. de bug Cisco CSCsa90034.

La agregación de Cisco mantiene al router (ASR) ese Cisco IOS XE de los funcionamientos

En la plataforma ASR, el REPLAY_ERROR señalado en algunas de las versiones anteriores del Cisco IOS XE no pudo imprimir el flujo real del IPSec donde se cae el paquete jugado de nuevo, como se muestra aquí:

```
%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>
```

Para identificar el peer IPSec y la información de flujo correctos, utilice la manija del avión de los

datos (DP) impresa en el mensaje de Syslog como la **manija** parámetro de entrada **SA** en este comando para extraer la información de flujo del IPSec en el procesador del flujo de Quantum (QFP):

```
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 (Details below)
: 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>
```

Si la versión deL Cisco IOS en el ASR es la versión 3.7 PRE-XE, después el mensaje de error registra simplemente el mensaje con la **manija DP** y ninguna información sobre el peer/SPI al cual el paquete del culpable pertenece. Aquí es donde el Id. de bug Cisco CSCtw69096 llega a ser relevante:

```
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 (Details below)
: 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>
```

En estos casos, este script integrado del administrador del evento (EEM) se puede utilizar para ver qué par y acciona SPI los mensajes de la anti-respuesta:

```
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 (Details below)
: 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>
```

Para ver la salida en el ASR sí mismo, ingrese el **más bootflash: comando replay-error.txt** periódicamente.

Trabajo con la característica del seguimiento del paquete ASR Datapath

Con el Software Cisco IOS XE más reciente para el ASR1000, la información sobre el par así como el IPSec SPI también se imprimen para ayudar a resolver problemas los problemas de la

anti-respuesta. Sin embargo, una información clave que sigue siendo falta comparada a qué se imprime en las Plataformas ISR G2 que funcionan con la obra clásica del Cisco IOS es el número de secuencia ESP. El número de secuencia ESP se utiliza para identificar únicamente un paquete IPsec dentro de un flujo dado del IPSec. Sin el número de secuencia, llega a ser difícil identificar exactamente que el paquete consigue caído en una captura de paquetes.

En la versión 3.10 (15.3(3)S) del Cisco IOS XE, una nueva infraestructura del seguimiento del paquete fue introducida para ayudar a resolver problemas el problema del reenvío de paquete del dataplane, y puede ser utilizada en esta situación de Troubleshooting determinada en donde este descenso de la respuesta se observa en el ASR:

```
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 (Details below)
: 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>
```

Para ayudar a identificar el número de secuencia ESP para el paquete caído, complete estos pasos con la característica del seguimiento del paquete:

1. Configure el filtro del debugging condicional de la plataforma para hacer juego el tráfico del dispositivo de peer:

```
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 (Details below)
: 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>
```

2. Permita al seguimiento del paquete con la **opción Copy (Copiar)** para copiar la información de encabezado de paquete:

```
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 (Details below)
: 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>
```

3. Cuando se detectan los errores de la respuesta, utilice el buffer de la traza del paquete para identificar el debido caída paquete jugar de nuevo, y el número de secuencia ESP se puede encontrar en el paquete copiado:

```
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
```

La salida anterior muestra que los números **6** y **7 del** paquete están caídos, así que pueden ahora ser examinados detalladamente:

```
Router#show platform packet-trace  pac 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** que empiece con el encabezado IP, según lo acentuado en intrépido y los itálicos en la salida anterior. En este ejemplo en particular, el número de secuencia ESP para el paquete perdidos es **0x6**.

Solución

Después de que identifiquen al par, hay tres escenarios posibles:

1. **Es un paquete válido:** Las capturas de paquetes ayudan a confirmar si el paquete es realmente válido, y si el problema es insignificante (debido a los problemas de la latencia de red o del trayecto de transmisión) o requiere un Troubleshooting más profundizado. Por ejemplo, la captura muestra un paquete con un número de secuencia de **X** que llegue fuera de servicio, y el tamaño de la ventana se fija a **64**. Si **X + 64** paquetes llega antes del paquete **X**, después consigue caída debido a un error de la respuesta (no es realmente un ataque).

   En tales escenarios, aumente el tamaño de la ventana de la respuesta para asegurarse de que tales retardos están explicados y evitar que los paquetes legítimos sean caídos. Por abandono, el tamaño de la ventana es bastante pequeño (tamaño de la ventana de **64**). Si usted aumenta el tamaño, no aumenta grandemente el riesgo de un ataque. Para la información sobre cómo configurar una ventana contra repetición del IPSec, refiera a cómo configurar la ventana contra repetición del IPSec: Ampliando y inhabilitando el artículo.
   Tip: Si se inhabilita la ventana de la respuesta o alterado en el perfil de ipsec y el perfil de ipsec se utiliza con la protección del túnel en una interfaz del túnel virtual (VTI), los cambios no tomarán el efecto hasta que se quite y se reaplique el perfil de la protección u o se reajusta la interfaz del túnel. Ésta es conducta esperada porque los perfiles de ipsec son apenas una plantilla para crear la correspondencia del perfil del túnel cuando se habilita la interfaz del túnel (no cerrado). La interfaz está una vez ya para arriba, los cambios al perfil no afectan el túnel hasta reaplicado o se reajusta la interfaz.**Note**: Un problema comúnmente encontrado en los ASR, en cuanto al tamaño de la ventana contra repetición, es que los modelos clásicos ASR1K (tales como el ASR1K con ESP5, ESP10, ESP20, y ESP40, junto con el ASR1001) no soportan realmente un tamaño de la ventana de 1024. Aunque el comando permite que usted establezca este límite a 1024, el tamaño de la ventana es reajustado a 512 por el hardware. Debido a esto, el tamaño de la ventana que está señalado en la salida del **comando show crypto ipsec sa** no pudo estar correcto. Ingrese el comando **crypto de la plataforma del IP Address de Peer IPSec sa de la demostración** para verificar el tamaño de la ventana contra repetición del hardware. El tamaño predeterminado de la ventana es 64 paquetes en todas las Plataformas. Para más información, refiera al Id. de bug Cisco CSCso45946. Más nuevos modelos ASR1K (tales como el ASR1K con ESP100 y ESP200, el ASR1001-X y el ASR1002-X, y también el ISR-4400) soportan un tamaño de la ventana de 1024 paquetes en las versiones 15.2(2)S y posterior.
2. **Es un paquete que cae fuera de la ventana contra repetición del receptor:** En caso de que el punto final de IPSec de recepción caiga los paquetes jugados de nuevo (mientras que se supone a), el sniffer simultáneo captura en el lado de WAN del remitente y de la ayuda del receptor para rastrear si esto es causada por el misbehavior del remitente, o por los paquetes jugado de nuevo en el transit network.

3. **Es debido a la configuración de QoS en el extremo del remitente:** Esta situación requiere el examen cuidadoso y algún a QoS que ajustan para atenuar la condición. Para una descripción más profundizada de este tema y de una solución potencial, refiera a las consideraciones de la Anti-respuesta en una Voz y un artículo habilitado vídeo del IPSec

VPN (V3PN).

Note: Consideran a los errores del control de la respuesta solamente cuando un algoritmo de autenticación se habilita en el IPSec transforma el conjunto. Otra manera de suprimir este mensaje de error es inhabilitar la autenticación y realizar el cifrado solamente; sin embargo, esto es fuertemente desalientador debido a las consecuencias en la seguridad de la autenticación discapacitada.

Información Relacionada

- **Diseño de red habilitado de la referencia de la solución del IPSec VPN de la Voz y del vídeo (V3PN)**
- **Cómo Configurar IPsec Anti-Replay Window:** Extensión e Inhabilitación.
- **Soporte Técnico y Documentación - Cisco Systems**