Solución de problemas de errores RM-4-TX_BW_LIMIT en plataformas de router ISR

Contenido

Introducción

Este documento describe por qué puede encontrar el cifrado de la carga útil y los límites de sesión cifrados de túnel/seguridad de la capa de transporte (TLS) y qué hacer en tal situación. Debido a las fuertes restricciones de exportación de criptografía impuestas por el gobierno de Estados Unidos, una licencia de seguridad 90 solo permite el cifrado de carga útil hasta una velocidad cercana a los 90 Megabits por segundo (Mbps) y limita el número de túneles cifrados/sesiones TLS al dispositivo. Se aplican 85 Mbps en los dispositivos Cisco.

Antecedentes

La restricción de restricción de criptografía se aplica a los routers de la serie Cisco Integrated Service Router (ISR) con la implementación de Crypto Export Restrictions Manager (CERM). Con la implementación de CERM, antes de que el túnel de seguridad de protocolo de Internet (IPsec)/TLS entre en funcionamiento, solicita a CERM que reserve el túnel. Posteriormente, IPSec envía el número de bytes que se cifrarán/descifrarán como parámetros y consulta el CERM si puede continuar con el cifrado/descifrado. El CERM verifica el ancho de banda que permanece y responde con sí/no para procesar/descartar el paquete. IPSec no reserva el ancho de banda en absoluto. Según el ancho de banda que queda, para cada paquete, el CERM toma una decisión dinámica sobre si procesar o descartar el paquete.

Cuando IPSec debe terminar el túnel, debe liberar los túneles reservados anteriores para que el CERM pueda agregarlos al conjunto libre. Sin la licencia HSEC-K9, este límite de túnel se establece en 225 túneles. Esto se muestra en el resultado de **show platform cerm-information**:

```
router# show platform cerm-information
Crypto Export Restrictions Manager(CERM) Information:
CERM functionality: ENABLED
```

```
-------------------------------------------------------------
Resource Maximum Limit Available
-------------------------------------------------------------
Tx Bandwidth(in kbps) 85000 85000
Rx Bandwidth(in kbps) 85000 85000
Number of tunnels 225 221
Number of TLS sessions 1000 1000
```

> **Nota:** En los routers ISR serie 4400/ISR serie 4300 que ejecutan Cisco IOS-XE®, también se aplican las limitaciones del CERM, a diferencia de los routers de la serie Aggregation Services Router (ASR)1000. Se pueden ver con la salida de **show platform software cerm-information**.

¿Cómo se calculan los límites?

Para entender cómo se calculan los límites del túnel, debe entender qué es una identidad proxy. Si ya comprende la identidad de proxy, puede continuar con la siguiente sección. La identidad de proxy es el término utilizado en el contexto de IPSec que designa el tráfico protegido por una Asociación de Seguridad IPSec (SA). Existe una correspondencia uno a uno entre una entrada permit en una lista de acceso crypto y una identidad proxy (ID de proxy para short). Por ejemplo, cuando tiene una lista de acceso crypto definida de la siguiente manera:

```
permit ip 10.0.0.0 0.0.0.255 10.0.1.0 0.0.0.255
permit ip 10.0.0.0 0.0.0.255 10.10.10.0 0.0.0.255
```

Esto se traduce a exactamente dos ID de proxy. Cuando un túnel IPsec está activo, tiene un mínimo de un par de SA negociadas con el punto final. Si utiliza varias transformaciones, esto podría aumentar hasta tres pares de SA IPsec (un par para ESP, uno para AH y otro para PCP). Puede ver un ejemplo de esto en la salida del router. Aquí está el resultado **show crypto ipsec sa***:*

```
    protected vrf: (none)
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/6/0) |
remote ident (addr/mask/prot/port): (192.168.78.0/255.255.255.0/6/0) | =>
the proxy id: permit tcp any 192.168.78.0 0.0.255
current_peer 10.254.98.78 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 153557, #pkts encrypt: 153557, #pkts digest: 153557
#pkts decaps: 135959, #pkts decrypt: 135959, #pkts verify: 135959
#pkts compressed: 55197, #pkts decompressed: 50575
#pkts not compressed: 94681, #pkts compr. failed: 3691
#pkts not decompressed: 85384, #pkts decompress failed: 0
#send errors 5, #recv errors 62

local crypto endpt.: 10.254.98.2, remote crypto endpt.: 10.254.98.78
path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/0.1398
current outbound spi: 0xEE09AEA3(3993611939) <====== see below
for explanation.
PFS (Y/N): Y, DH group: group2
```

Estos son los pares SA de IPSec (entrante-saliente):

```
      inbound esp sas:
spi: 0x12C37AFB(314800891)
transform: esp-aes ,
in use settings ={Tunnel, }
conn id: 2803, flow_id: Onboard VPN:803, sibling_flags 80000046, crypto
map: beograd
```

```
sa timing: remaining key lifetime (k/sec): (4561094/935)
IV size: 16 bytes
replay detection support: N
Status: ACTIVE

inbound ah sas:

inbound pcp sas:
spi: 0x8F6F(36719)
transform: comp-lzs ,
in use settings ={Tunnel, }
conn id: 2803, flow_id: Onboard VPN:803, sibling_flags 80000046, crypto
map: beograd
sa timing: remaining key lifetime (k/sec): (4561094/935)
replay detection support: N
Status: ACTIVE

outbound esp sas:
spi: 0xEE09AEA3(3993611939)
transform: esp-aes ,
in use settings ={Tunnel, }
conn id: 2804, flow_id: Onboard VPN:804, sibling_flags 80000046, crypto
map: beograd
sa timing: remaining key lifetime (k/sec): (4547825/935)
IV size: 16 bytes
replay detection support: N
Status: ACTIVE

outbound ah sas:

outbound pcp sas:
spi: 0x9A12(39442)
transform: comp-lzs ,
in use settings ={Tunnel, }
conn id: 2804, flow_id: Onboard VPN:804, sibling_flags 80000046, crypto
map: beograd
sa timing: remaining key lifetime (k/sec): (4547825/935)
replay detection support: N
Status: ACTIVE
```

En este caso, existen exactamente dos pares de SA. Estos dos pares se generan tan pronto como el tráfico llega a la lista de acceso crypto que coincide con la ID de proxy. Se puede utilizar el mismo ID de proxy para diferentes pares.

> **Nota:** Cuando examina el resultado de **show cry ipsec sa,** ve que hay un Índice de Parámetros de Seguridad de Salida (SPI) actual de 0x0 para las entradas inactivas y un SPI existente cuando el túnel está activo.

En el contexto del CERM, el router cuenta el número de pares de ID/peer proxy activos. Esto significa que si tiene, por ejemplo, diez pares para los que tiene 30 entradas de permiso en cada una de las listas de acceso crypto, y si hay tráfico que coincide con todas esas listas de acceso, termina con 300 pares de ID de proxy/peer que están por encima del límite de 225 impuesto por CERM. Una manera rápida de contar el número de túneles que el CERM considera es utilizar el comando **show crypto ipsec sa count** y buscar el conteo total de SA IPSec como se muestra aquí:

```
router#show crypto ipsec sa count
IPsec SA total: 6, active: 6, rekeying: 0, unused: 0, invalid: 0
```

A continuación, el número de túneles se calcula fácilmente como el recuento total de SA de IPsec dividido por dos.

Problema

Síntomas

Estos mensajes se ven en el syslog cuando se exceden los límites de restricción de criptografía:

```
%CERM-4-RX_BW_LIMIT : Maximum Rx Bandwidth limit of [dec] Kbps reached for Crypto
functionality with temporary license for securityk9 technology package.

%CERM-4-TLS_SESSION_LIMIT : Maximum TLS session limit of [dec] reached for Crypto
functionality with temporary license for securityk9 technology package.

%CERM-4-TUNNEL_LIMIT : Maximum tunnel limit of [dec] reached for Crypto functionality
with temporary license for securityk9 technology package.

%CERM-4-TX_BW_LIMIT : Maximum Tx Bandwidth limit of [dec] Kbps reached for Crypto
functionality with temporary license for securityk9 technology package.
```

Causa raíz

No es raro que los routers se conecten a través de interfaces Gigabit, y como se explicó anteriormente, el router comienza a descartar tráfico cuando alcanza 85 Mbps de entrada o de salida. Incluso en los casos en los que las interfaces Gigabit no están en uso o la utilización media del ancho de banda está claramente muy por debajo de este límite, el tráfico de tránsito puede estar saturado. Incluso si la ráfaga es por unos pocos **milisegundos**, es suficiente para activar el límite de ancho de banda crypto restringido. Y en estas situaciones, el tráfico que excede los 85 Mbps se descarta y se contabiliza en el resultado **show platform cerm-information***:*

```
router#show platform cerm-information | include pkt
Failed encrypt pkts: 42159817
Failed decrypt pkts: 0
Failed encrypt pkt bytes: 62733807696
Failed decrypt pkt bytes: 0
Passed encrypt pkts: 506123671
Passed decrypt pkts: 2452439
Passed encrypt pkt bytes: 744753142576
Passed decrypt pkt bytes: 1402795108
```

Por ejemplo, si conecta un **Cisco 2911** a un **Cisco 2951** a través de la interfaz de túnel virtual (VTI) IPsec y proporciona un promedio de 69 TB de tráfico con un generador de paquetes, donde el tráfico se entrega en ráfagas de **6000 paquetes** a un **rendimiento de 500 Mbps, ve esto en sus syslogs:**

```
router#
Apr 2 11:52:30.028: %CERM-4-TX_BW_LIMIT: Maximum Tx Bandwidth limit of 85000 Kbps
reached for Crypto functionality with securityk9 technology package license.
router#show platform cerm-information | include pkt
Failed encrypt pkt bytes: 62930990016
Failed decrypt pkt bytes: 0
Passed encrypt pkt bytes: 747197374528
Passed decrypt pkt bytes: 1402795108
router#show platform cerm-information | include pkt
Failed encrypt pkt bytes: 62931497424
Failed decrypt pkt bytes: 0
Passed encrypt pkt bytes: 747203749120
```

```
Passed decrypt pkt bytes: 1402795108
router#
```

Como puede ver, el router descarta constantemente el tráfico saturado. Tenga en cuenta que el mensaje syslog **%CERM-4-TX_BW_LIMIT** se limita a un mensaje por minuto.

```
Router#
Apr 2 11:53:30.396: %CERM-4-TX_BW_LIMIT: Maximum Tx Bandwidth limit of 85000 Kbps
reached for Crypto functionality with securityk9 technology package license.
BIOS#
Apr 2 11:54:30.768: %CERM-4-TX_BW_LIMIT: Maximum Tx Bandwidth limit of 85000 Kbps
reached for Crypto functionality with securityk9 technology package license.
```

Troubleshoot

Para problemas en los que se alcanza el límite CERM de ancho de banda

Complete estos pasos:

1. Refleje el tráfico en el switch conectado.
2. Utilice Wireshark para analizar el seguimiento capturado mediante una granularidad de dos a 10 milisegundos.
   El tráfico con microrráfagas superiores a 85 Mbps es un comportamiento esperado.

Para problemas en los que se alcanza el límite máximo de CERM de túnel

Recopile esta salida periódicamente para ayudar a identificar una de estas tres condiciones:

- El número de túneles ha superado el límite del CERM.
- Hay una fuga de recuento de túneles (el número de túneles criptográficos según las estadísticas criptográficas excede el número real de túneles).
- Hay una fuga de conteo CERM (el número de recuentos de túnel CERM según las estadísticas CERM excede el número real de túneles).

Estos son los comandos que se deben utilizar:

```
show crypto eli detail
show crypto isa sa count
show crypto ipsec sa count
show platform cerm-information
```

Solución

La mejor solución para los usuarios con una licencia **permanente** de seguridad9 que se enfrentan a este problema es comprar la **licencia HSEC-K9**. Para obtener información sobre estas licencias, consulte Cisco ISR G2 SEC y HSEC Licensing.

Solución Aternativa

Una solución alternativa posible para aquellos que absolutamente no necesitan el mayor ancho de banda es implementar un modelador de tráfico en los dispositivos vecinos en ambos lados para suavizar cualquier ráfaga de tráfico. La profundidad de la cola puede tener que ajustarse en

función de la saturación del tráfico para que esto sea efectivo.

Desafortunadamente, esta solución alternativa no se aplica en todos los escenarios de implementación, y a menudo no funciona bien con microrráfagas, que son ráfagas de tráfico que se producen en intervalos de tiempo muy cortos.