¿Troubleshooting? Errores RM-4-TX_BW_LIMIT en las plataformas del router ISR

Contenido

Introducción

Este documento describe porqué usted puede ser que encuentre la encripción de carga útil y el túnel encriptado/los límites de sesión de Transport Layer Security (TLS) y lo que a hacer en una situación semejante. Debido a las limitaciones de exportación crypto fuertes aplicadas por el gobierno de los Estados Unidos, una licencia securityk9 permite solamente la encripción de carga útil hasta las tarifas cerca de 90 megabits por segundo (Mbps) y limita el número de sesiones cifradas tunnels/TLS al dispositivo. 85Mbps se aplica en los dispositivos de Cisco.

Antecedentes

La restricción crypto del acortamiento se aplica en los routeres de la serie del router del servicio integrado de Cisco (ISR) con la implementación Crypto del administrador de las limitaciones de exportación (CERM). Con CERM implementado, antes del túnel de la seguridad de protocolos en Internet (IPSec) /TLS resulta útil, solicita CERM para reservar el túnel. Más adelante, el IPSec envía la cantidad de bytes que se cifrará/desencriptada como parámetros y pregunta CERM si puede proceder con encripción/desencripción. CERM marca contra el ancho de banda que sigue habiendo y responde con procesar sí/no/descenso el paquete. El ancho de banda no es reservado por el IPSec en absoluto. De acuerdo con el ancho de banda que sigue habiendo, para cada paquete, una decisión dinámica es hecho por CERM si procesar o caer el paquete.

Cuando el IPSec debe terminar el túnel, debe liberar para arriba los túneles reservados anteriores de modo que CERM pueda agregarlos a la agrupación disponible. Sin la licencia HSEC-K9, este límite del túnel se establece en 225 túneles. Esto se muestra en la salida de la cerm-**información de la plataforma de la demostración**:

```
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 4300 Series Router ISR 4400/ISR que ejecutan el ® del Cisco IOS XE, las limitaciones CERM también se aplican, a diferencia en de la agregación mantienen al router (routeres de la serie ASR)1000. Pueden ser vistas con la salida de la cerm-**información del software de plataforma de la demostración**.

¿Cómo se calculan los límites?

Para entender cómo se calculan los límites del túnel, usted debe entender cuáles es una identidad de representación. Si usted entiende ya la identidad de representación, usted puede continuar a la siguiente sección. La identidad de representación es el término usado en el contexto del IPSec que señala el tráfico protegido por una asociación de seguridad IPSec (SA). Hay una correspondencia de uno a uno entre una entrada del permiso en una lista de acceso crypto y una identidad de representación (ID de proxy para el cortocircuito). Por ejemplo, cuando usted tiene una lista de acceso crypto definida como esto:

```
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
```

Esto traduce a exactamente dos ID de proxy. Cuando un túnel IPsec es activo, usted tiene un mínimo de un par de SA negociado con el punto extremo. Si usted utiliza el múltiplo transforma, esto podría aumentar hasta tres pares del SA de IPSec (un par para el ESP, uno para AH, y uno para PCP). Usted puede ver un ejemplo de esto de la salida de su router. Aquí está **IPSec crypto sa de la demostración** hecho salir*:*

```
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
```

Aquí están los pares IPSec SA (entrante-salientes):

```
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
```

En este caso, hay exactamente dos pares de SA. Se generan estos dos pares tan pronto como el tráfico golpee la lista de acceso crypto que hace juego el ID de proxy. El mismo ID de proxy se podía utilizar para diversos pares.

> Nota: Cuando usted examina la salida **IPSec sa del grito de la demostración,** usted ve que hay un Security Parameter Index saliente actual (SPI) de 0x0 para las entradas inactivas y SPI existente cuando el túnel está para arriba.

En el contexto de CERM, el router cuenta el número de pares activos del proxy ID/peer. Esto significa que si usted tenía, por ejemplo, diez pares para quien usted tienen 30 entradas del permiso en cada uno de las listas de acceso crypto, y si hay el tráfico que hace juego todas esas listas de acceso, usted termina para arriba con 300 pares del proxy ID/peer que está sobre el límite 225 impuesto por CERM. Un modo rápido de contar el número de túneles que CERM considere es utilizar el **comando count crypto IPSec sa de la demostración** y buscar el recuento total IPSec SA como se muestra aquí:

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

El número de túneles entonces se calcula fácilmente como la cuenta total IPSec SA dividió por dos.

Problema

Síntomas

Estos mensajes se consideran en el Syslog cuando se exceden los límites crypto del acortamiento:

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

Causa raíz

No es infrecuente que el Routers sea conectado vía las interfaces Gigabit, y según lo explicado previamente, el comienzo del router para caer el tráfico cuando alcanza el 85 Mbps entrante o saliente. Incluso en caso de que las interfaces Gigabit son paradas o la utilización del ancho de banda promedio está claramente bien debajo de este límite, el tráfico de tránsito puede ser bursty. Incluso si la explosión es por algunos **milisegundos**, es bastante para accionar el límite crypto acortado del ancho de banda. Y en estas situaciones, el tráfico que se excede 85Mbps se cae y se considera en la cerm-**información de la plataforma de la demostración** hecha salir*:*

```
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 usted conecta **Cisco 2911** con **Cisco 2951** vía la interfaz del túnel virtual del IPSec (VTI) y entrega a una media de 69 P.M. de tráfico con un generador de paquete, donde el tráfico se entrega en las explosiones de **6000 paquetes** en una **producción del 500 Mbps**, usted ve esto en sus Syslog:

```
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 usted puede ver, el router cae constantemente el tráfico congestionado. Observe la tarifa limitada de los messageis del Syslog **%CERM-4-TX_BW_LIMIT a** un mensaje por el minuto.


```
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#
```


Troubleshooting

Para los problemas donde se alcanza el límite del ancho de banda CERM

Complete estos pasos:

1. Duplique el tráfico en el switch conectado.
2. Utilice Wireshark para analizar la traza capturada yendo abajo a dos a 10 granularity del período de tiempo milisegundo.
   El tráfico con las explosiones micro mayores que 85Mbps es una conducta esperada.

Para los problemas donde se alcanza el límite máximo del túnel CERM

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

- El número de túneles ha excedido el límite CERM.
- Hay un escape de la cuenta del túnel (el número de túneles de criptografía según lo señalado

por las estadísticas crypto excede el número real de túneles).
- Hay un escape de la cuenta CERM (el número de cuenta del túnel CERM según lo señalado por las estadísticas CERM excede el número real de túneles).

Aquí están los comandos de 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** securityk9 que encuentra este problema es comprar la licencia **HSEC-K9**. Para la información sobre estas licencias, refiera a Cisco ISR G2 SEC y a autorización HSEC.

Solución Aternativa

Una solución alternativa posible para las que no necesiten absolutamente el mayor ancho de banda es implementar a un modelador de tráfico en los dispositivos de vecindad en los ambos lados para allanar cualquier ráfaga de tráfico. La profundidad de espera en cola pudo tener que ser ajustado basó en el burstiness del tráfico para que esto sea eficaz.

Desafortunadamente esta solución alternativa es no corresponde en todos los escenarios de instrumentación, y no trabaja a menudo bien con los microbursts, que son las ráfagas de tráfico que ocurren en mismo los intervalos de breve periodo de tiempo.