Pesquise defeitos? Erros RM-4-TX_BW_LIMIT em plataformas de roteador ISR

Índice

Introdução

Este documento descreve porque você pôde encontrar a criptografia de payload e o túnel criptografado/limites de sessão do Transport Layer Security (TLS) e que a fazer em tal situação. Devido às restrições de exportação criptos fortes reforçadas pelo governo dos estados unidos, uma licença securityk9 permite somente a criptografia de payload até taxas perto de 90 megabits por segundo (Mbps) e limita o número de sessões cifradas tunnels/TLS ao dispositivo. 85Mbps é reforçado em dispositivos Cisco.

Informações de Apoio

A limitação cripto da restrição é reforçada em Series Router do roteador do serviço integrado de Cisco (ISR) com a aplicação cripto do gerente das restrições de exportação (CERM). Com o CERM executado, antes do túnel da segurança de protocolo do Internet (IPsec) /TLS vai vivo, pede CERM para reservar o túnel. Mais tarde, o IPsec envia o número de bytes a ser cifrado/decifrado como parâmetros e pergunta CERM se pode continuar com criptografia /descriptografia. CERM verifica contra a largura de banda que permanece e responde com processar sim/não/gota o pacote. A largura de banda não é reservada pelo IPsec de todo. Baseado na largura de banda que permanece, para cada pacote, uma decisão dinâmica é feito por CERM se processar ou deixar cair o pacote.

Quando o IPsec deve terminar o túnel, deve livrar acima os túneis reservados mais adiantados de modo que CERM possa os adicionar ao conjunto livre. Sem a licença HSEC-K9, este limite do túnel é ajustado em 225 túneis. Isto é mostrado na saída da cerm-**informação da plataforma da mostra**:

```
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: Nos 4300 Series Router ISR 4400/ISR que executam o ® do Cisco IOS XE, as limitações CERM igualmente aplicam-se, ao contrário na agregação prestam serviços de manutenção ao roteador (Series Router ASR)1000. Podem ser vistos com a saída da cerm-**informação do software de plataforma da mostra**.

Como os limites são calculados?

A fim compreender como os limites do túnel são calculados, você deve compreender o que uma identidade de proxy é. Se você já compreende a identidade de proxy, você pode continuar à próxima seção. A identidade de proxy é o termo usado no contexto do IPsec que designa o tráfego protegido por uma associação de segurança IPSec (SA). Há uma correspondência de um para um entre uma entrada da licença em uma lista de acesso cripto e uma identidade de proxy (ID de proxy para breve). Por exemplo, quando você tiver uma lista de acesso cripto definida como esta:

```
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
```

Isto traduz a exatamente dois proxy ID. Quando um túnel de IPsec é ativo, você tem um mínimo de um par de SA negociado com o ponto final. Se você se usa o múltiplo transforma, isto poderia aumentar até três pares do sas de IPSec (um par para o ESP, o um para o AH, e o um para PCP). Você pode ver um exemplo deste da saída de seu roteador. Está aqui **IPsec cripto sa da mostra** output*:*

```
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
```

Estão aqui os pares IPsec SA (de entrada-de partida):

```
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
```

Neste caso, há exatamente dois pares de SA. Estes dois pares são gerados assim que o tráfego bater a lista de acesso cripto que combina o ID de proxy. O mesmo ID de proxy podia ser usado para pares diferentes.

> Nota: Quando você examina a saída **IPsec sa do grito da mostra,** você vê que há um Security Parameter Index de partida atual (SPI) de 0x0 para as entradas inativas e um SPI existente quando o túnel está acima.

No contexto de CERM, o roteador conta o número de pares ativos do proxy ID/peer. Isto significa que se você teve, por exemplo, dez pares para que você têm 30 entradas da licença em cada um das listas de acesso criptos, e se há o tráfego que combina todas aquelas listas de acesso, você termina acima com 300 pares do proxy ID/peer que está acima do limite 225 imposto por CERM. Uma maneira rápida contar o número de túneis que CERM considera é usar o **comando count cripto IPsec sa da mostra** e procurar como mostrado o contagem total IPsec SA aqui:

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

O número de túneis é calculado então facilmente como a contagem total IPsec SA se dividiu por dois.

Problema

Sintomas

Estas mensagens estão consideradas no Syslog quando os limites criptos da restrição são excedidos:

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

Causa de raiz

Não é raro para o Roteadores ser conectado através das interfaces de gigabit, e como explicado previamente, os começos do roteador para deixar cair o tráfego quando alcança o 85 Mbps de entrada ou de partida. Mesmo nos casos onde as interfaces de gigabit não são dentro uso ou a utilização da largura de banda média está claramente bem abaixo deste limite, o tráfego de trânsito pode ser intermitência. Mesmo se a explosão se realiza por alguns **milissegundos**, é bastante para provocar o limite cripto reduzido da largura de banda. E nestas situações, o tráfego que excede 85Mbps é deixado cair e explicado na cerm-**informação da plataforma da mostra** output*:*

```
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 exemplo, se você conecta **Cisco 2911 a Cisco 2951** através da interface de túnel virtual do IPsec (VTI) e entrega uma média de 69 PM do tráfego com um gerador de pacote, onde o tráfego esteja entregado nas explosões de **6000 pacotes em uma taxa de transferência de 500 Mbps**, você vê isto em seus 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 você pode ver, o roteador deixa cair constantemente o tráfego intermitente. Note o limite de taxa dos messageis do Syslog **%CERM-4-TX_BW_LIMIT a** uma mensagem pelo 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 as edições onde o limite da largura de banda CERM é alcançado

Conclua estes passos:

1. Espelhe o tráfego no switch conectado.
2. Use Wireshark a fim analisar o traço capturado indo para baixo a dois à granularidade do período de tempo 10 milissegundo.
   O tráfego com as micro explosões maiores do que 85Mbps é um comportamento esperado.

Para as edições onde o limite máximo do túnel CERM é alcançado

Recolha esta saída periodicamente a fim ajudar a identificar uma destas três circunstâncias:

- O número de túneis excedeu o limite CERM.
- Há um escape da contagem do túnel (o número de criptos túnel como relatado por

estatísticas criptos excede o número real de túneis).
- Há um escape da contagem CERM (o número de contagem do túnel CERM como relatado por estatísticas CERM excede o número real de túneis).

Estão aqui os comandos usar-se:

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

Solução

A melhor solução para usuários com uma licença securityk9 **permanente** que encontra esta edição é comprar a licença **HSEC-K9**. Para obter informações sobre destas licenças, refira Cisco ISR G2 SEC e licenciar HSEC.

Solução

Uma alternativa possível para aquelas que absolutamente não precisam o aumento de largura de banda é executar um formador de tráfego nos dispositivos confinante em ambos os lados a fim alisar para fora todas as intermitências de tráfego. A profundidade de fila pôde ter que ser ajustado baseou na intermitência do tráfego para que esta seja eficaz.

Infelizmente esta ação alternativa não é aplicável em todos os cenários de distribuição, e frequentemente não trabalha bem com microbursts, que são as intermitências de tráfego que ocorrem muito em intervalos de curto período de tempo.