Solucione problemas de erros ?RM-4-TX_BW_LIMIT em plataformas de roteador ISR

Contents

Introduction

Este documento descreve por que você pode encontrar a criptografia de payload e os limites de sessão TLS (Transport Layer Security) de túnel/camada de transporte criptografados e o que fazer em tal situação. Devido às fortes restrições de exportação de criptografia impostas pelo governo dos Estados Unidos, uma licença securityk9 permite somente criptografia de payload a taxas próximas a 90 Megabits por segundo (Mbps) e limita o número de túneis/sessões TLS criptografadas ao dispositivo. 85 Mbps é aplicada em dispositivos Cisco.

Informações de Apoio

A restrição de criptografia é aplicada nos roteadores da série Cisco Integrated Service Router (ISR) com a implementação do Crypto Export Restrictions Manager (CERM). Com o CERM implementado, antes que o túnel IPsec (Internet Protocol Security)/TLS entre em funcionamento, ele solicita que o CERM reserve o túnel. Mais tarde, o IPsec envia o número de bytes a serem criptografados/descriptografados como parâmetros e consulta CERM se puder prosseguir com a criptografia/descriptografia. O CERM verifica a largura de banda restante e responde com sim/não para processar/descartar o pacote. A largura de banda não é reservada pelo IPsec. Com base na largura de banda que permanece, para cada pacote, uma decisão dinâmica é tomada pelo CERM para processar ou descartar o pacote.

Quando o IPsec deve encerrar o túnel, ele deve liberar os túneis reservados anteriores para que o CERM possa adicioná-los ao pool livre. Sem a licença HSEC-K9, esse limite de túnel é definido em 225 túneis. Isso é mostrado na saída 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
```

> **Note**: Nos roteadores ISR 4400/ISR 4300 Series que executam o Cisco IOS-XE®, as limitações do CERM também se aplicam, ao contrário dos roteadores Aggregation Services Router (ASR)1000 Series. Elas podem ser visualizadas com a saída de **show platform software cerm-information**.

Como se calculam os limites?

Para entender como os limites de túnel são calculados, você deve entender o que é uma identidade de proxy. Se você já entender a identidade do proxy, poderá continuar para a próxima seção. A identidade do proxy é o termo usado no contexto do IPsec que designa o tráfego protegido por uma associação de segurança (SA) IPsec. Há uma correspondência um-para-um entre uma entrada de permissão em uma lista de acesso de criptografia e uma identidade de proxy (ID de proxy para abreviação). Por exemplo, quando você tem uma lista de acesso de criptografia definida como:

```
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
```

Isso se traduz em exatamente duas IDs de proxy. Quando um túnel IPsec está ativo, você tem no mínimo um par de SAs negociados com o ponto final. Se você usar várias transformações, isso pode aumentar até três pares de SAs IPsec (um par para ESP, um para AH e um para PCP). Você pode ver um exemplo disso na saída do roteador. Esta é a saída **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
```

Aqui estão os pares SA IPsec (entrada e saída):

```
      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
```

Neste caso, há exatamente dois pares de SAs. Esses dois pares são gerados assim que o tráfego atinge a lista de acesso de criptografia que corresponde à ID do proxy. A mesma ID de proxy pode ser usada para diferentes peers.

> **Note**: Ao examinar a saída de **show cry ipsec sa,** você verá que há um Índice de Parâmetro de Segurança (SPI) de saída atual de 0x0 para as entradas inativas e um SPI existente quando o túnel está ativo.

No contexto do CERM, o roteador conta o número de pares de ID/peer de proxy ativos. Isso significa que se você tiver, por exemplo, dez peers para os quais você tem 30 entradas de permissão em cada uma das listas de acesso de criptografia e se houver tráfego que corresponda a todas essas listas de acesso, você terminará com 300 pares de ID/peer de proxy acima do limite de 225 imposto pelo CERM. Uma maneira rápida de contar o número de túneis que o CERM considera é usar o comando **show crypto ipsec sa count** e procurar a contagem total de SA IPsec como mostrado aqui:

```
router#show crypto ipsec sa count
```

```
IPsec SA total: 6, active: 6, rekeying: 0, unused: 0, invalid: 0
```

O número de túneis é então facilmente calculado como a contagem de SAs IPsec total dividida por dois.

Problema

Sintomas

Essas mensagens são vistas no syslog quando os limites de redução de criptografia são excedidos:

```
%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 raiz

Não é incomum que os roteadores sejam conectados através de interfaces Gigabit e, como explicado anteriormente, o roteador começa a descartar o tráfego quando chega a 85 Mbps de entrada ou saída. Mesmo nos casos em que as interfaces Gigabit não estão em uso ou a utilização média da largura de banda está claramente abaixo desse limite, o tráfego de trânsito pode ser intermitente. Mesmo se a intermitência for por alguns **milissegundos**, basta disparar o limite de largura de banda criptografada. E nessas situações, o tráfego que excede 85 Mbps é descartado e contabilizado na saída **cerm-information da plataforma***:*

```
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 conectar um **Cisco 2911** a um **Cisco 2951** via Interface de Túnel Virtual (VTI - Virtual Tunnel Interface) IPsec e fornecer uma média de 69 mps de tráfego com um gerador de pacotes, onde o tráfego é entregue em rajadas de **6000 pacotes** a uma **taxa de transferência de 500 Mbps bps**, você vê isso em seus 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 você pode ver, o roteador constantemente descarta o tráfego intermitente. Observe que a mensagem de syslog **%CERM-4-TX_BW_LIMIT** é limitada a uma mensagem 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 em que o limite de largura de banda CERM é atingido

Conclua estes passos:

1. Espelhe o tráfego no switch conectado.
2. Use o Wireshark para analisar o rastreamento capturado diminuindo para 2 a 10 ms de granularidade do período de tempo.
   O tráfego com microsurtos superiores a 85 Mbps é um comportamento esperado.

Para problemas em que o limite máximo de CERM do túnel é atingido

Colete essa saída periodicamente para ajudar a identificar uma destas três condições:

- O número de túneis excedeu o limite CERM.
- Há um vazamento de contagem de túnel (o número de túneis criptografados conforme relatado pelas estatísticas de criptografia excede o número real de túneis).
- Há um vazamento de contagem de CERM (o número de contagens de túneis CERM conforme relatado pelas estatísticas CERM excede o número real de túneis).

Estes são os comandos a serem usados:

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

Solução

A melhor solução para os usuários com uma licença **permanente** securityk9 que encontram esse problema é comprar a licença **HSEC-K9**. Para obter informações sobre essas licenças, consulte Cisco ISR G2 SEC e HSEC Licensing.

Solução

Uma solução possível para aqueles que não precisam absolutamente da largura de banda ampliada é implementar um modelador de tráfego nos dispositivos vizinhos em ambos os lados para suavizar qualquer surto de tráfego. A profundidade da fila pode ter que ser ajustada com base na intermitência do tráfego para que isso seja eficaz.

Infelizmente, essa solução alternativa não é aplicável em todos os cenários de implantação e geralmente não funciona bem com microsurtos, que são surtos de tráfego que ocorrem em intervalos de tempo muito curtos.