排除ISR路由器平台上的？RM-4-TX_BW_LIMIT錯誤

目錄

簡介

本文說明為什麼您可能會遇到負載加密和加密隧道/傳輸層安全(TLS)會話限制，以及這種情況下的處理方式。由於美國政府強制實施嚴格的加密匯出限制，安全k9許可證僅允許負載加密速度接近每秒90兆位(Mbps)，並限制到裝置的加密隧道/TLS會話數量。85Mbps在思科裝置上實施。

背景資訊

透過密碼輸出限制管理員(CERM)實作，對思科整合服務路由器(ISR)系列路由器強制執行密碼輸出限制限制。實施CERM後，在Internet協定安全(IPsec)/TLS隧道啟動之前，它請求CERM保留隧道。之後，IPsec會將要加密/解密的位元組數作為引數傳送，如果可以繼續加密/解密，則查詢CERM。CERM會檢查剩餘的頻寬，並以yes/no作為響應處理/丟棄資料包。IPsec根本未保留頻寬。根據保留的頻寬，對於每個資料包，CERM會動態決定是處理還是丟棄資料包。

當IPsec必須終止隧道時，必須釋放較早的保留隧道，以便CERM可以將它們新增到空閒池。沒有HSEC-K9許可證，此隧道限制設定為225個隧道。**show platform cerm-information**的輸出中會顯示此資訊：

```
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
```

附註：在執行Cisco IOS-XE®的ISR 4400/ISR 4300系列路由器上，CERM限制也適用，與聚合服務路由器(ASR)1000系列路由器不同。可以通過**show platform software cerm-information**的輸出來檢視它們。

如何計算限制？

為了瞭解如何計算通道限制，您必須瞭解代理身份是什麼。如果您已瞭解代理身份，則可以繼續下一部分。代理身份是在IPsec上下文中使用的術語，用於指定受IPsec安全關聯(SA)保護的流量。 加密存取清單上的允許專案與代理身分之間是一對一對應關係（代表代理ID）。 例如，當您具有如下定義的加密訪問清單時：

```
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
```

這正好轉換為兩個代理ID。當IPsec通道處於使用中狀態時，您至少有一對與端點協商的SA。如果使用多個轉換，最多可以增加三對IPsec SA（一對ESP、一對AH和一對PCP）。 您可以從路由器的輸出中看到一個範例。以下是**show crypto ipsec sa**輸出*：*

```
    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
```

以下是IPsec SA對（傳入 — 傳出）：

```
      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
```

在這種情況下，只有兩對SA。當流量到達與代理ID相符的加密存取清單時，就會立即產生這兩個對。相同的代理ID可用於不同的對等體。

> **附註**：當您檢查**show cry ipsec sa的輸出**時，您會看到目前非活動專案的傳出安全引數索引(SPI)為0x0，且通道開啟時有一個現有的SPI。

在CERM的環境中，路由器會計算作用中代理ID/對等體對的數量。這表示如果您有10個對等點（每個加密存取清單中具有30個允許專案），且存在與所有這些存取清單相符的流量，您最終會產生300個代理ID/對等點對，超過CERM所設定的225個限制。計算CERM考慮的通道數的一種快速方法是使用**show crypto ipsec sa count**命令並查詢IPsec SA總計數，如下所示：

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

隧道數很容易計算為總IPsec SA數除以二。

問題

症狀

當超出密碼編譯限制限制時，系統日誌中會顯示以下訊息：

```
%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.
```

根本原因

路由器通過千兆介面連線的情況並不少見，如前所述，當流量達到85 Mbps入站或出站時，路由器開始丟棄流量。即使千兆介面未使用或者平均頻寬利用率明顯低於此限制，傳輸流量也可能出現突發情況。即使突發數毫秒，也足以觸發**縮短的加密**頻寬限制。在這些情況下，超過85Mbps的流量會被丟棄，並計入**show platform cerm-information**輸出*:*

```
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
```

例如，如果透過IPsec虛擬通道介面(VTI)將**Cisco 2911**連線到**Cisco 2951**，並使用封包產生器平均傳輸69 mps的流量(其中流量以**500 Mbps的輸送量以6000個封包的猝發**方式傳輸)，則會在系統日誌中看到以下情況：

```
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#
```

您可以看到，路由器不斷丟棄突發流量。請注意**%CERM-4-TX_BW_LIMIT** syslog messageis rate-limited to one message per minute。

```
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.
```

疑難排解

對於達到頻寬CERM限制的問題

請完成以下步驟：

1. 映象已連線交換機上的流量。
2. 使用Wireshark來分析捕獲的跟蹤，方法是將時間段粒度降為2到10毫秒。
   微突發大於85Mbps的流量是預期行為。

對於達到最大通道CERM限制的問題

定期收集此輸出，以幫助確定以下三種情況之一：

- 通道數已超過CERM限制。
- 存在通道計數洩漏（加密統計資訊報告的加密通道數超過實際通道數）。
- 存在CERM計數洩漏（CERM統計資訊報告的CERM隧道計數數超過實際隧道數）。

以下是要使用的命令：

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

解決方案

對於擁有永久安全**k9許**可證但遇到此問題的使用者，最佳解決方案是購買**HSEC-K9許**可證。有關這些許可證的資訊，請參閱Cisco ISR G2 SEC和HSEC許可。

因應措施

對於完全不需要增加頻寬的使用者而言，一種可能的解決方法是在兩端的相鄰裝置上實施流量整形器，以便平滑任何流量突發。隊列深度可能需要根據流量的突發性進行調整，才能使此過程有效。

遺憾的是，這種解決方法不適用於所有部署場景，而且通常不適用於微猝發（在極短的時間間隔內發生的流量猝發）。