排除ISR路由器平台上的“RM-4-TX_BW_LIMIT”错误

目录

简介

本文档介绍为什么可能会遇到负载加密和加密隧道/传输层安全(TLS)会话限制，以及在这种情况下应如何操作。由于美国政府强制实施加密出口限制，securityk9许可证仅允许负载加密速率接近每秒90兆位(Mbps)，并限制到设备的加密隧道/TLS会话数。85Mbps在思科设备上实施。

背景信息

加密限制在采用加密出口限制管理器(CERM)实施的思科集成多业务路由器(ISR)系列路由器上实施。实施CERM后，在Internet协议安全(IPsec)/TLS隧道生效之前，它会请求CERM保留隧道。之后，IPsec将要加密/解密的字节数作为参数发送，并查询CERM（如果它可以继续加密/解密）。CERM根据保留的带宽进行检查，并以是/否响应以处理/丢弃数据包。带宽完全不由IPsec保留。CERM根据每个数据包的保留带宽做出是处理还是丢弃数据包的动态决策。

当IPsec必须终止隧道时，它必须释放之前保留的隧道，以便CERM可以将它们添加到空闲池。如果没有HSEC-K9许可证，此隧道限制设置为225个隧道。如show platform cerm-information的输**出所示**:

```
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
```

注意：在运行Cisco IOS-XE®的ISR 4400/ISR 4300系列路由器上，CERM限制也适用，这与聚合服务路由器(ASR)1000系列路由器不同。通过show platform software cerm-information的输出可以查看它们。

如何计算限制？

要了解如何计算隧道限制，您必须了解代理身份。如果您已经了解代理身份，可以继续下一节。代理身份是IPsec环境中使用的术语，用于指定受IPsec安全关联(SA)保护的流量。 加密访问列表上的允许条目与代理身份（简称代理ID）之间有一对一的对应关系。 例如，当您定义了如下加密访问列表时：

```
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
```

这将转换为恰好两个代理ID。当IPsec隧道处于活动状态时，您至少有一对SA与终端协商。如果使用多个转换，这最多可增加三对IPsec SA（一对用于ESP，一对用于AH，一对用于PCP）。 从路由器的输出中可以看到此示例。以下是**show crypto ipsec sa**输出*:*

```
    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对（入站 — 出站）：

```
      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
```

在本例中，正好有两对SA。当流量到达与代理ID匹配的加密访问列表时，会立即生成这两对。同一代理ID可用于不同的对等体。

> **注意**：当您检查**show cry ipsec sa的输**出时，您会看到当前的出站安全参数索引(SPI)为0x0，当隧道启动时为现有SPI。

在CERM环境中，路由器计算活动代理ID/对等体对的数量。这意味着，例如，如果您有十个对等体，每个加密访问列表中有30个permit条目，并且如果有与所有这些访问列表匹配的流量，则最终会有300个代理ID/对等体对，超过CERM施加的225个限制。计数CERM考虑的隧道数的快速方法是使用**show crypto ipsec sa count**命令并查找IPsec SA总计，如下所示：

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

然后，可以轻松地将隧道数计算为IPsec SA总计数除以2。

问题

症状

超过加密限制限制时，系统日志中会显示以下消息：

```
%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

路由器通过千兆接口连接的情况并不罕见，如前所述，当流量达到85 Mbps的入站或出站时，路由器开始丢弃流量。即使千兆接口未在使用或平均带宽利用率明显低于此限制，中转流量也可能是突发流量。即使突发数为几毫**秒**，也足以触发缩减的加密带宽限制。在这些情况下，超过85Mbps的流量会被丢弃并计入**show platform cerm-information输**出中*:*

```
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，如果您通过IPsec虚拟隧道接口(VTI)将**Cisco 2911**连接到**Cisco 2951**，并通过数据包生成器平均传输69 mps的流量，其中流量以5个吞吐量的**6000个数据包的突发传输00 Mbps**，您在系统日志中看到：

```
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#
```

如您所见，路由器会不断丢弃突发流量。请注意**%CERM-4-TX_BW_LIMIT系**统日志消息速率限制为每分钟一条消息。

```
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.
```

故障排除

对于达到带宽CERM限制的问题

请完成以下步骤：

1. 镜像所连接交换机上的流量。
2. 使用Wireshark，通过向下到2至10毫秒的时间段粒度分析捕获的跟踪。
   微爆发大于85Mbps的流量是预期行为。

对于达到最大隧道CERM限制的问题

定期收集此输出，以帮助确定以下三种情况之一：

- 隧道数已超出CERM限制。
- 存在隧道计数泄漏（加密统计报告的加密隧道数超过实际隧道数）。
- 存在CERM计数泄漏（CERM统计数据报告的CERM隧道计数超过实际隧道数）。

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
```

解决方案

对于拥有永久性securityk9许可证**但遇**到此问题的用户，最佳解决方案是购买**HSEC-K9许**可证。有关这些许可证的信息，请参阅Cisco ISR G2 SEC和HSEC许可。

解决方法

对于完全不需要增加带宽的用户，一个可能的解决方法是在两端的相邻设备上实施流量整形器，以便消除任何流量突发。为使此有效，可能必须根据流量的突发性调整队列深度。

遗憾的是，此解决方法并不适用于所有部署方案，并且通常不适用于微爆发，微爆发是指在非常短的时间间隔内发生的流量突发。