目录

简介

由于美国政府强制执行的强crypto出口限制， securityk9许可证只允许有效载荷加密至速率近90个兆比特每秒(Mbps)并且对设备限制加密隧道/传输层安全(TLS)会话数量。85Mbps在Cisco设备被强制执行。本文描述您要执行为什么也许遇到这些限额，并且什么在这种情况下。

贡献用奥利维尔Pelerin和温张， Cisco TAC工程师。

背景信息

crypto削减限制在思科集成多业务有crypto出口限制管理器(CERM)实施的路由器(ISR)系列路由器被强制执行。使用在Internet协议安全性(IPsec) /TLS通道前实现的， CERM现场，它请求CERM保留通道。如果能继续进行加密/解密，以后， IPSec发送作为参数将加密/解密的字节数并且查询CERM。CERM检查依然是并且响应与是或不是处理/丢弃数据包的带宽。带宽没有由IPsec根本保留。基于为每数据包依然存在，一个动态决策的带宽是否由CERM做处理或丢弃数据包。

当IPsec必须终止通道时，必须释放更加早期的保留通道，以便CERM能添加他们到空闲池。没有HSEC-K9许可证，此隧道限制定在225个通道。这在输出中显示**显示平台cerm信息**：

```
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，不同于在聚合服务路由器(ASR)1000系列路由器。他们可以查看与输出**显示平台软件cerm信息**。

限额如何计算？

为了知道隧道限制如何计算，您必须了解什么代理身分是。如果已经了解代理身分，您能继续到下一部分。指派IPSec安全关联保护的流量的代理身分是此术语用于在IPsec中(SA)。有在一个permit条目在crypto access-list和代理身分(代理ID之间的一一对应简称)。例如，当您有一crypto access-list定义象这样：

```
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
```

这翻译对正确地两代理ID。当IPSec隧道是活跃的时，您有用端点SA协商的至少一个对。如果使用多次转换，这可能增加三个对SA (特别是的一个对，一为啊和一IPsec pcp的)。您能参见此的示例从您的路由器输出。这是输出的**show crypto ipsec sa** *：*

```
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
```

这是SA IPsec对(入站出站) ：

```
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
```

在这种情况下，正确地有两个对SA。这两个对生成，当匹配代理ID的流量点击crypto access-list。同一个代理ID能用于不同的对等体。

> **注意**：当您检查输出时请**显示啼声sa ipsec，**您看到有一个当前出站安全参数索引(SPI)非激活条目和一个现有SPI的0x0，当通道是UP时。

在CERM中，路由器计数活动代理ID/peer对数量。这意味着，如果有，例如，十对等体，您有30个permit条目在其中每一crypto访问列表，并且，如果有匹配所有那些访问列表的流量，您最终获得300个代理ID/peer对，是在CERM实施的225限制上。快速方式计数CERM考虑通道的数量将使用**count命令的show crypto ipsec sa**和寻找SA IPsec总数显示此处：

```
router#show crypto ipsec sa count
IPsec SA total: 6, active: 6, rekeying: 0, unused: 0, invalid: 0
```
通道数量容易地然后计算，总计SA IPsec计数除了两。

问题

症状

当crypto削减限额超过时，此消息在Syslog被看到：

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

根本原因

连接通过千兆接口和路由器是不不常见的如以前解释，路由器启动降低流量，当到达出站时的85 Mbps入站或。在千兆接口不是在使用中的处或平均带宽利用率清楚地低于此限制，中转流量可以突变性。即使突发流量是在一些**毫秒**，是触发被削减的crypto带宽限制的足够。并且在这些情况下，超出85Mbps的流量丢弃并且认为**显示**输出的**平台cerm信息*：***

```
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，如果在您的Syslog连接**Cisco 2911**对**Cisco 2951**通过IPsec虚拟隧道接口(VTI)并且传送流量69 mps平均值用信息包生成器，流量在**6000数据包**突发流量传送在一**吞吐量的500 Mbps**，您看到此：

```
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#
```
正如你看到的路由器经常降低突发数据流。注释**%CERM-4-TX_BW_LIMIT**系统消息是速率限制对每分钟一个消息。

```
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#
```

故障排除

带宽CERM限制达到的问题

完成这些步骤：

1. 反映在连接的交换机的流量。
2. 请使用Wireshark为了通过断开分析获取trace两到10毫秒时间粒度。
   与微突发流量的流量极大比85Mbps是预料之中的行为。

最大通道CERM限制达到的问题

收集周期地此输出为了帮助识别这三个情况之一：

- 通道数量超过了CERM限制。
- 有隧道计数泄漏(加密隧道编号如报告由crypto统计信息超出通道实际数量)。
- 有CERM计数泄漏(CERM隧道计数编号报告由CERM统计信息超出通道实际数量)。

这是命令使用：

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

解决方案

遇到此问题的用户的佳解决方案有**永久性**securityk9许可证的是采购**HSEC-K9**许可证。关于这些许可证的信息，参考的Cisco ISR G2 SEC和HSEC许可授权。

解决方法

绝对不需要增加的带宽的那些人的一可能的应急方案是实现相邻设备的一台流量整形器在两边为了使所有流量突发平滑。队列深度也许必须被调整根据流量的突变为了此能有效。

不幸地此应急方案不是可适用的在所有部署方案和经常不工作良好与微下击暴流，是流量突发在非常短时间时间间隔发生。