Устранение неполадок? Ошибки RM-4-TX_BW_LIMIT на платформах комплекта маршрутизаторов ISR

Содержание

Введение

Этот документ описывает, почему вы могли бы встретиться с шифрованием полезной нагрузки и зашифрованным туннелем / Transport Layer Security (TLS) пределы сеанса и что сделать в такой ситуации. Из-за сильных крипто-ограничений экспорта, принужденных Правительством США, securityk9 лицензия только позволяет шифрованию полезной нагрузки до скоростей близко к 90 мегабитам в секунду (Мбит/с) и ограничивает количество зашифрованных сеансов туннелей/TLS к устройству. Скорость 85 Мбит/с принудительно вводится на устройствах Cisco.

Общие сведения

Ограничениешифрования принудительно вводится на маршрутизаторах из серии маршрутизаторов с интегрированными сервисами (ISR) компании Cisco с реализацией диспетчера ограничений криптографического экспорта (CERM). Если реализован механизм CERM, то перед тем, как туннель с защитой Интернет-протоколов (IPSec) / TLS станет активным, выполняется запрос CERM для резервирования туннеля. Позднее IPSec отправляет определенное количество байтов, которые будут шифроваться/дешифроваться как параметры, и запрашивает CERM, если возможно продолжение с шифрованием/дешифрованием. CERM проверяет остаточную пропускную способность и отвечает да/нет для обработки/отбрасывания пакета. Пропускная способность не резервируется IPSec. На базе остаточной пропускной способности для каждого пакета модуль CERM принимает динамическое решение о том, следует ли обработать или отбросить пакет.

Когда механизм IPSec должен закрыть туннель, он должен освободить ранее зарезервированные туннели, чтобы модуль CERM мог добавить их в свободный пул. Без лицензии HSEC-K9 это туннельное ограничение установлено на уровне 225 туннелей. **Это отображается в выходных данных команды 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
```

> **Примечание:** На маршрутизаторах серии 4400/ISR 4300 , которые работают под управлением Cisco IOS-XE®, ограничения CERM также применяются в отличие от ограничений на маршрутизаторах серии 1000 на базе маршрутизатора агрегации сервисов (ASR). **Они могут быть просмотрены с использованием выходных данных команды show platform software cerm-information.**

Как рассчитываются ограничения?

Чтобы понять, как рассчитываются туннельные ограничения, необходимо понять, что представляет собой идентификатор прокси-сервера. Если вы уже понимаете, что такое идентификатор прокси-сервера, можно перейти к следующему разделу. Идентификатор прокси-сервера — это элемент, используемый в контексте IPSec, который делает трафик защищенным с помощью контекста безопасности (SA) IPsec. Есть однозначное соответствие между элементом разрешения в криптографическомсписке доступа и идентификатором прокси. Например, если есть криптографический список доступа, определенный следующим образом:

```
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
```

Эти данные транслируются в ровно два идентификатора прокси-сервера. Когда Туннель IPSec активен, у вас есть минимум одной пары SA, о которых выполняют согласование с оконечная точкой. При использовании множественных преобразований это могло бы увеличить до трех пар контекстов безопасности IPSec (одна пара для ESP, один для AH, и

один для PCP). Можно посмотреть пример из выходных данных своего маршрутизатора.
Выходные данные команды 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
```

Вот (входящие исходящие) пары контекста безопасности IPSec:

```
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
```

В этом случае существует точно две пары SA. Эти две пары генерируются, как только трафик пересекается с криптографическимсписком доступа, который соответствует идентификатору прокси-сервера. Один идентификатор прокси-сервера может использоваться для различных равноправных узлов.

> **Примечание: Изучая выходные данные команды show cry ipsec sa, можно увидеть, что текущий внеполосный индекс параметра безопасности (SPI) равен 0x0 для неактивных элементов и существующего SPI при активном состоянии туннеля.**

В контексте CERM маршрутизатор считывает количество активных пар идентификаторов прокси-сервера / равноправных узлов. Это означает, что если бы у вас были, например, десять равноправных узлов, для которых у вас есть 30 элементов разрешения в каждом из криптографическихсписков доступа и если существует трафик, который соответствует всем этим спискам доступа, вы заканчиваете работу с 300 парами идентификаторов прокси-сервера / равноправных узлов, что превышает ограничение (225), наложенное со стороны CERM. **Быстрый способ подсчета количества туннелей, которое учитывается CERM, должен использовать команду show crypto ipsec sa count и определять общее количество IPsec SA, как показано здесь:**

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

```
IPsec SA total: 6, active: 6, rekeying: 0, unused: 0, invalid: 0
```
Затем количество туннелей легко рассчитывается как общее количество контекста безопасности IPSec, разделенное на два.

Проблема

Признаки

Когда крипто-пределы сокращения превышены, эти сообщения замечены в системном журнале:

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

Основная причина

Маршрутизаторы часто подключаются через интерфейсы Gigabit и, как описано ранее, маршрутизатор начинает отбрасывать трафик, когда достигает скорости 85 Мбит/с для входящих или исходящих сообщений. Даже в тех случаях, когда интерфейсы Gigabit не используются или используемая средняя пропускная способность очевидно значительно ниже этого ограничения, транзитный трафик может быть пульсирующим. **Даже если пульсация длится всего несколько миллисекунд, это достаточно для достижения редуцированного ограничения пропускной способности шифрования. В этих ситуациях трафик, скорость которого превышает 85 Мбит/с, отбрасывается и оценивается по выходным данным команды show platform cerm-information:**

```
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
```
Например, при подключении Cisco 2911 к Cisco 2951 через интерфейс виртуального туннеля IPsec (VTI) и отправке трафика со средней скоростью 69 м/с трафика с помощью генератора пакетов, когда трафик отправляется пачками по 6000 пакетов при пропускной способности 500 Мбит/с, это можно видеть в своих системных журналах:

```
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#
```
Как можно видеть,маршрутизатор постоянно отбрасывает пульсирующий трафик. **Обратите внимание, что поток сообщений системного журнала %CERM-4-TX_BW_LIMIT ограничен по**

скорости до одного сообщения в минуту.

```
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#
```

Устранение неполадок

Для проблем, в которых достигается ограничение пропускной способности, заданное в CERM

Выполните следующие действия:

1. Зеркалирование трафика на подключенном коммутаторе.
2. Используйте Wireshark для анализа захваченной трассы посредством изменения гранулярности периода времени с 2 на 10 мсек.
   Трафик с микроимпульсами на скорости больше 85 Мбит/с является нормальным.

Для проблем, в которых достигается ограничение максимального количества туннелей, заданное в CERM

Периодически собирайте эти выходные данные для облегчения идентификации одного из этих трех условий:

- Количество туннелей превысило ограничение CERM.
- Существует утечка количества туннелей (количество криптографических туннелей в соответствии с переданной криптографической статистикой превышает фактическое количество туннелей).
- Существует утечка количества туннелей CERM (количество туннелей CERM в соответствии с переданной статистикой CERM превышает фактическое количество туннелей).

Команды для использования:

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

Решение

Лучшее решение для пользователей с постоянной лицензией securityk9, которые сталкиваются с этой проблемой — приобрести лицензию HSEC-K9. Для получения

информации об этих лицензиях см. Лицензирование Cisco ISR G2 SEC и HSEC.

Обходной путь

Один возможный обходной путь для тех, у кого нет никакой необходимости увеличения пропускной способности, заключается в подключении формирователя трафика к соседним устройствам с обеих сторон для сглаживания любых всплесков трафика. Для эффективности, возможно, придется настроить глубину очереди на базе пакетирования трафика.

К сожалению, этот обходной путь не применим во всех сценариях развертывания и часто не работает надлежащим образом с микровсплесками, которые являются всплесками трафика, возникающими на очень кратковременных интервалах.