Содержание

[Введение](#)
[Общие сведения](#)
[Как вычислены пределы?](#)
[Проблема](#)
[Признаки](#)
[Основная причина](#)
[Устранение неполадок](#)
[Для Проблем, Где Пропускная способность Достигнут Предел CERM](#)
[Для Проблем, Где Максимальный Туннель Достигнут Предел CERM](#)
[Решение](#)
[Обходной путь](#)

Введение

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/Transport Layer Security (TLS) к устройству. 85 Мбит/с принуждены на устройствах Cisco. Этот документ описывает, почему вы могли бы встретиться с этими пределами и что сделать в такой ситуации.

Внесенный Оливье Пелереном и Вэнь Чжаном, специалистами службы технической поддержки Cisco.

Общие сведения

Крипто-ограничение сокращения принуждено на series маршрутизаторах маршрутизатора с интеграцией служб (ISR) Cisco с реализацией Крипто-менеджера ограничений экспорта (CERM). С внедренным CERM, прежде чем протокол IPSEC (Internet Protocol Security) (IPsec) / туннель TLS идет оперативный, это запрашивает CERM резервировать туннель. Позже, IPSec передает количество байтов, которые будут шифроваться/дешифроваться как параметры, и делает запрос CERM, если это может продолжить в отличие от стандарта. Проверки CERM против пропускной способности, которая остается и отвечает да/нет для обработки пакета. Пропускная способность не зарезервирована IPsec вообще. На основе пропускной способности, которая остается для каждого пакета, динамическое решение принято CERM, обработать ли или отбрасывать пакет.

Когда IPsec должен завершить туннель, он должен освободить более ранние зарезервированные туннели так, чтобы CERM мог добавить их к свободному пулу. Без лицензии HSEC-K9 этот туннельный предел установлен в 225 туннелях. Это показывают в выходных данных **cerm-информации о show platform**:

```
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 ISR 4400/ISR 4300 series маршрутизаторов, которые выполняют Cisco IOS-XE®, ограничения CERM также, применяются, в отличие от этого на маршрутизаторах серии 1000 Маршрутизатора агрегации (ASR). Они могут быть просмотрены с выходными данными **cerm-информации о программном обеспечении show platform**.

Как вычислены пределы?

Чтобы понять, как туннельные пределы вычислены, необходимо понять, какова идентичность прокси. Если вы уже понимаете идентичность прокси, можно продолжить к следующему разделу. Идентичность прокси является термином, использованным в контексте IPsec, который называет трафик защищенным IPsec Security Association (SA). Существует однозначное соответствие между записью разрешения на крипто-access-list и идентичностью прокси (Proxy Id, если коротко). Например, когда вам определили крипто-access-list как это:

```
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
```

Это преобразовывает точно в два Proxy Id. Когда Туннель IPSec активен, у вас есть минимум одной пары SA, о котором выполняют согласование с оконечная точкой. При использовании множественных преобразований это могло бы увеличить до трех пар контекста безопасности IPSec (одна пара для ESP, один для ах, и один для PCP). Вы видите пример этого от выходных данных вашего маршрутизатора. Вот **выходные данные 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 поражает крипто-access-list, который совпадает с Proxy Id. Тот же Proxy Id мог использоваться для других узлов.

> **Примечание:** При исследовании выходных данных **ipsec крика показа sa** вы видите, что существует текущий исходящий индекс параметров безопасности (SPI) 0x0 для неактивных записей и существующего SPI, когда туннель подключен.

В контексте CERM маршрутизатор считает количество активного Proxy Id / одноранговыми парами. Это означает, что, если у вас были, например, десять узлов, для которых у вас есть 30 записей разрешения в каждом крипто-access-lists, и если существует трафик, который совпадает со всеми теми access-lists, вы заканчиваете с 300 Proxy Id / одноранговые пары, который является выше 225 ограничений, наложенных CERM. Быстрый способ для подсчета количества туннелей, которые рассматривает CERM, должен использовать команду **количества show crypto ipsec sa** и искать полный счет контекста безопасности IPSec как показано здесь:

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

Количество туннелей тогда легко вычислено как общее количество контекста безопасности IPSec, разделенное на два.

Проблема

Признаки

Это обменивается сообщениями, замечен в системном журнале, когда превышены крипто-пределы сокращения:

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

Основная причина

Маршрутизаторам весьма свойственно быть связанным через Гигабитные интерфейсы и, как объяснено ранее, маршрутизатор начинает отбрасывать трафик, когда это достигает 85 Мбит/с, входящих или исходящих. Даже в случаях, где Гигабитные интерфейсы не используются или использование средней пропускной способности ясно значительно ниже этого предела, транзитный трафик может быть пульсирующим. Даже если пакет для нескольких **миллисекунд**, достаточно инициировать сокращенный крипто-предел пропускной

способности. И в этих ситуациях, трафик, который превышает 85 Мбит/с, отбрасывается и считается в **cerm-выводе-информации show platform***:*

```
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, если вы подключаете **Cisco 2911** с **Cisco 2951** через интерфейс виртуальных туннелей IPsec (VTI) и отправляете среднее число 69 членов парламента трафика с мастером создания пакетов, куда трафик отправлен в пакетах **6000 пакетов** в **пропускной способности 500 Мбит/с**, вы видите это 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 вы можете видеть маршрутизатор постоянно отбрасывает пульсирующий трафик. Обратите внимание **, что %CERM-4-TX_BW_LIMIT** сообщение системного журнала с ограниченной скоростью к одному сообщению 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, Где Пропускная способность Достигнут Предел CERM

Выполните следующие действия:

1. Отразите трафик на связанном коммутаторе.

2. Используйте Wireshark для анализа перехваченной трассировки путем снижения два к 10 глубинам детализации периода времени мс.
   Трафик с микро пакетами, больше, чем 85 Мбит/с, является нормальным поведением.

Для Проблем, Где Максимальный Туннель Достигнут Предел CERM

Собирайте эти выходные данные периодически, чтобы помочь определять одно из этих трех условий:

- Количество туннелей превысило предел CERM.
- Существует туннельная утечка количества (количество зашифрованных туннелей, как сообщается крипто-статистикой превышает фактическое количество туннелей).
- Существует утечка количества CERM (количество туннельного количества CERM, как сообщается статистикой CERM превышает фактическое количество туннелей).

Вот 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** securityk9 лицензией, которые встречаются с этой проблемой, должно купить лицензию **HSEC-K9**. Для получения информации об этих лицензиях обратитесь к Cisco ISR G2 SEC и HSEC Лицензирование.

Обходной путь

Один возможный обходной путь для тех, кому абсолютно не нужно увеличение пропускной способности, должен внедрить регулировщика трафика на соседних устройствах с обеих сторон для сглаживания любых всплесков трафика. Глубину очереди, возможно, придется настроить на основе прерывистости трафика для этого, чтобы быть эффективной.

К сожалению, этот обходной путь не применим во всех сценариях развертывания, и часто не работает хорошо с микропакетами, которые являются всплесками трафика, которые происходят в очень кратковременных интервалах.