Contenu

Introduction

En raison de cryptos restrictions à l'exportation fortes imposées par le gouvernement des États-Unis, un permis securityk9 permet seulement le cryptage de charge utile jusqu'aux débits de près de 90 mégabits par seconde (Mbits/s) et limite le nombre de tunnels chiffrés/de sessions de Transport Layer Security (TLS) au périphérique. 85Mbps est imposé sur des périphériques de Cisco. Ce document décrit pourquoi vous pourriez rencontrer ces limites et ce qui à faire dans une telle situation.

Contribué par Olivier Pelerin et Wen Zhang, ingénieurs TAC Cisco.

Informations générales

La crypto restriction de terminaison est imposée sur des routeurs de la gamme du routeur de service intégré de Cisco (ISR) avec la crypto implémentation du gestionnaire de restrictions à l'exportation (CERM). Le CERM étant mis en application, avant le tunnel d'IPSec (IPsec) /TLS devient disponible, il invite CERM à réserver le tunnel. Plus tard, IPSec envoie le nombre d'octets à chiffrer/être déchiffrés comme paramètres et questionne CERM s'il peut se poursuivre par le cryptage/déchiffrement. CERM vérifie contre la bande passante qui demeure et répond avec pour traiter oui/non/baisse le paquet. La bande passante n'est pas réservée par IPsec du tout. Basé sur la bande passante qui demeure, pour chaque paquet, une décision dynamique est fait par CERM si traiter ou relâcher le paquet.

Quand IPsec doit terminer le tunnel, il doit libérer les tunnels réservés plus tôt de sorte que CERM puisse les ajouter au pool libre. Sans permis HSEC-K9, cette limite de tunnel est fixée à 225 tunnels. Ceci est affiché dans la sortie des cerm-**informations de 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
```

> Remarque: Sur les Routeurs de gamme 4300 ISR 4400/ISR qui exécutent le ® de Cisco IOS XE, les limites CERM s'appliquent également, à la différence de sur l'agrégation entretient le routeur (routeurs de la gamme ASR)1000. Ils peuvent être visualisés avec la sortie des cerm-**informations de logiciel de show platform**.

Comment les limites sont-elles calculées ?

Afin de comprendre comment les limites de tunnel sont calculées, vous devez comprendre ce qu'est une identité de proxy. Si vous comprenez déjà l'identité de proxy, vous pouvez continuer à la section suivante. L'identité de proxy est le terme utilisé dans le cadre d'IPsec qui indique le trafic protégé par une association de sécurité IPSec (SA). Il y a une correspondance linéaire entre une entrée d'autorisation sur une crypto liste d'accès et une identité de proxy (ID de proxy pour faire court). Par exemple, quand vous avez une crypto liste d'accès définie comme ceci :

```
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
```

Ceci se traduit à exactement deux id de proxy. Quand un tunnel d'IPsec est en activité, vous avez un minimum d'une paire de SA étée en pourparlers avec le point final. Si vous utilisez le multiple transforme, ceci pourrait augmenter jusqu'à trois paires d'IPsec SA (une paire pour l'ESP, un pour oh, et un pour le pcp). Vous pouvez voir un exemple de ceci de la sortie de votre routeur. Voici le **show crypto ipsec sa** sorti *:*

```
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
```

Voici les paires d'IPsec SA (d'arrivée-sortantes) :

```
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
```

Dans ce cas, il y a exactement deux paires de SA. Ces deux paires sont générées dès que le trafic frappera la crypto liste d'accès qui apparie l'ID de proxy. Le même ID de proxy a pu être utilisé pour différents pairs.

> Remarque: Quand vous examinez la sortie d'**ipsec SA de cri d'exposition,** vous voyez qu'il y a un index sortant en cours de paramètre de Sécurité (SPI) de 0x0 pour les entrées inactives et un SPI existant quand le tunnel est.

Dans le cadre de CERM, le routeur compte le nombre de paires actives du proxy ID/peer. Ceci signifie que si vous aviez, par exemple, dix pairs, pour lesquels vous prenez 30 entrées d'autorisation dans chacune des cryptos Listes d'accès, et s'il y a du trafic qui apparie toutes ces Listes d'accès, vous finissez par avec 300 paires du proxy ID/peer, qui est au-dessus de la limite 225 imposée par CERM. Un moyen rapide de compter le nombre de tunnels que CERM considère est d'utiliser la commande de **compte de show crypto ipsec sa** et de rechercher le comptage total d'IPsec SA comme affiché ici :

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

Le nombre de tunnels alors est facilement calculé comme le compte d'IPsec SA de total s'est divisé par deux.

Problème

Symptômes

Ce des messages est vus dans le Syslog quand les cryptos limites de terminaison sont dépassées :

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

Cause principale

Il n'est pas rare que des Routeurs soient connectés par l'intermédiaire des interfaces de gigabit et comme expliqué précédemment, les débuts de routeur pour relâcher le trafic quand il atteint 85 Mbits/s d'arrivée ou sortants. Même dans les cas où les interfaces de gigabit sont non utilisables ou l'utilisation de bande passante moyenne est clairement bien au-dessous de cette limite, le trafic de transit peut être bursty. Même si la rafale a lieu pendant quelques **millisecondes**, elle est assez pour déclencher la crypto limite raccourcie de bande passante. Et dans ces situations, le trafic qui dépasse 85Mbps est abandonné et rendu compte dans les cerm-**informations de show platform** sorties ***:***

```
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
```

Par exemple, si vous connectez **Cisco 2911 à Cisco 2951** par l'intermédiaire de l'interface de tunnel virtuelle d'IPsec (VTI) et fournissez une moyenne de 69 MP du trafic avec un générateur de paquet, où le trafic est fourni dans les rafales de **6000 paquets à un débit de 500 Mbits/s**, vous voyez ceci dans vos Syslog :

```
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#
```

Comme vous pouvez voir, le routeur relâche constamment le trafic bursty. Notez le message de Syslog **%CERM-4-TX_BW_LIMIT** est débit-limité à un message par minute.


```
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#
```


Dépannez

Pour des questions où la limite de la bande passante CERM est atteinte

Procédez comme suit :

1. Reflétez le trafic sur le commutateur connecté.
2. Utilisation Wireshark afin d'analyser le suivi capturé en allant vers le bas à la finesse de délai prévu deux à 10 millisecondes.
   Le trafic avec des rafales micro plus grandes que 85Mbps est un comportement prévu.

Pour des questions où la limite maximum du tunnel CERM est atteinte

Collectez cette sortie périodiquement afin d'aider à identifier une de ces trois conditions :

- Le nombre de tunnels a dépassé la limite CERM.

- Il y a une fuite de compte de tunnel (le nombre de tunnels du chiffrement comme signalé par de cryptos statistiques dépasse le nombre réel de tunnels).
- Il y a une fuite de compte CERM (le nombre de compte de tunnel CERM comme signalé par des statistiques CERM dépasse le nombre réel de tunnels).

Voici les commandes de utiliser :

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

Solution

La meilleure solution pour les utilisateurs avec un permis securityk9 **permanent** qui rencontrent cette question est d'acheter le permis **HSEC-K9**. Pour les informations sur ces permis, référez-vous à l'autorisation sec et HSEC d'ISR G2 de Cisco.

Contournement

Un contournement possible pour ceux qui absolument n'a pas besoin de la bande passante accrue est d'implémenter un régulateur de trafic sur les périphériques voisins des deux côtés afin de lisser toutes les rafales du trafic. La profondeur de la file d'attente pourrait devoir être accordée a basé sur les rafales du trafic pour que ceci soit efficace.

Malheureusement ce contournement s'applique pas applicable dans tous les scénarios de déploiement, et souvent ne fonctionne pas bien avec les microbursts, qui sont des rafales du trafic qui se produisent dans très des intervalles de courte durée.