Dépannage des erreurs RM-4-TX_BW_LIMIT sur les plates-formes de routeur ISR

Contenu

Introduction

Ce document décrit pourquoi vous pourriez rencontrer des limites de session de chiffrement de données utiles et de sécurité de la couche de transport (TLS) et ce que vous devez faire dans une telle situation. En raison de fortes restrictions à l'exportation de crypto appliquées par le gouvernement des États-Unis, une licence securityyk9 autorise uniquement le cryptage de charge utile jusqu'à des débits proches de 90 mégabits par seconde (Mbits/s) et limite le nombre de tunnels/sessions TLS cryptés au périphérique. 85 Mbits/s sont appliqués aux périphériques Cisco.

Informations générales

La restriction de restriction de chiffrement est appliquée aux routeurs de la gamme Cisco Integrated Service Router (ISR) avec l'implémentation du Crypto Export Restrictions Manager (CERM). Une fois le CERM mis en oeuvre, avant que le tunnel IPsec (Internet Protocol Security)/TLS ne soit mis en service, il demande au CERM de réserver le tunnel. Par la suite, IPsec envoie le nombre d'octets à chiffrer/décrypter en tant que paramètres et interroge le CERM s'il peut continuer avec le chiffrement/déchiffrement. Le CERM vérifie la bande passante qui reste et répond par oui/non pour traiter/abandonner le paquet. La bande passante n'est pas du tout réservée par IPsec. En fonction de la bande passante qui reste, pour chaque paquet, une décision dynamique est prise par le CERM, que le paquet soit traité ou abandonné.

Quand IPsec doit terminer le tunnel, il doit libérer les tunnels réservés précédents afin que le CERM puisse les ajouter au pool libre. Sans la licence HSEC-K9, cette limite de tunnel est fixée à 225 tunnels. Ceci est montré dans le résultat de **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
```

> **Note**: Sur les routeurs de la gamme ISR 4400/ISR 4300 qui exécutent Cisco IOS-XE®, les limites CERM s'appliquent également, contrairement aux routeurs de la gamme ASR (Aggregation Services Router) 1000. Ils peuvent être affichés avec la sortie de **show platform software cerm-information**.

Comment les limites sont-elles calculées ?

Pour comprendre comment les limites de tunnel sont calculées, vous devez comprendre ce qu'est une identité proxy. Si vous comprenez déjà l'identité du proxy, vous pouvez passer à la section suivante. L'identité du proxy est le terme utilisé dans le contexte d'IPsec qui désigne le trafic protégé par une association de sécurité (SA) IPsec. Il existe une correspondance un-à-un entre une entrée de permis sur une liste d'accès de chiffrement et une identité de proxy (ID de proxy pour abréger). Par exemple, lorsque vous avez une liste d'accès de chiffrement définie comme ceci :

```
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
```

Cela signifie exactement deux ID de proxy. Lorsqu'un tunnel IPsec est actif, vous avez négocié au moins une paire de SA avec le point d'extrémité. Si vous utilisez plusieurs transformations, cela peut augmenter jusqu'à trois paires de SA IPsec (une paire pour ESP, une pour AH et une pour PCP). Vous pouvez en voir un exemple à partir du résultat de votre routeur. Voici la sortie **show crypto ipsec sa** *:*

```
    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
```

Voici les paires de SA IPsec (entrante-sortante) :

```
      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
```

Dans ce cas, il y a exactement deux paires de SA. Ces deux paires sont générées dès que le trafic atteint la crypto access-list qui correspond à l'ID du proxy. Le même ID proxy peut être utilisé pour différents homologues.

> **Note**: Lorsque vous examinez le résultat de **show cry ipsec sa,** vous voyez qu'il existe un SPI (Security Parameter Index) sortant actuel de 0x0 pour les entrées inactives et un SPI existant lorsque le tunnel est actif.

Dans le contexte du CERM, le routeur compte le nombre de paires d'ID/homologues de proxy actives. Cela signifie que si vous aviez, par exemple, dix homologues pour lesquels vous avez 30 entrées d'autorisation dans chacune des listes d'accès cryptographiques, et si le trafic correspond à toutes ces listes d'accès, vous finissez avec 300 paires d'ID proxy/homologue qui est au-dessus de la limite de 225 imposée par le CERM. Une façon rapide de compter le nombre de tunnels que CERM considère est d'utiliser la commande **show crypto ipsec sa count** et de rechercher le nombre total de SA IPsec comme indiqué ici :

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

Le nombre de tunnels est ensuite facilement calculé comme le nombre total de SA IPsec divisé par deux.

Problème

Symptômes

Ces messages sont affichés dans le syslog lorsque les limites de restriction de chiffrement sont dépassées :

```
%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.
```

Cause première

Il n'est pas rare que les routeurs soient connectés via des interfaces Gigabit. Comme expliqué précédemment, le routeur commence à abandonner le trafic lorsqu'il atteint 85 Mbits/s en entrée ou en sortie. Même dans les cas où les interfaces Gigabit ne sont pas utilisées ou où l'utilisation moyenne de la bande passante est nettement inférieure à cette limite, le trafic de transit peut être en rafale. Même si la rafale est de quelques **millisecondes**, elle suffit à déclencher la limite de bande passante de chiffrement réduite. Et dans ces situations, le trafic qui dépasse 85 Mbits/s est abandonné et comptabilisé dans la sortie **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
```

Par exemple, si vous connectez un **Cisco 2911** à un **Cisco 2951** via l'interface de tunnel virtuel IPsec (VTI) et que vous fournissez en moyenne 69 mps de trafic avec un générateur de paquets, où le trafic est livré en rafales de **6000 paquets** à un **débit de 50Mbits ps**, vous voyez ceci dans vos syslogs :

```
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 le voir, le routeur abandonne constamment le trafic en rafale. Notez que le message syslog **%CERM-4-TX_BW_LIMIT** est limité à un message par minute.

```
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.
```

Dépannage

Pour les problèmes où la limite CERM de bande passante est atteinte

Procédez comme suit :

1. Mettre en miroir le trafic sur le commutateur connecté.
2. Utilisez Wireshark afin d'analyser la trace capturée en descendant jusqu'à une granularité de période de deux à dix ms.
   Le trafic avec des microrafales supérieures à 85 Mbits/s est un comportement attendu.

Pour les problèmes où la limite CERM de tunnel maximale est atteinte

Collectez périodiquement ce résultat afin d'identifier l'une de ces trois conditions :

- Le nombre de tunnels a dépassé la limite CERM.
- Il y a une fuite de nombre de tunnels (le nombre de tunnels de chiffrement signalé par les statistiques de chiffrement dépasse le nombre réel de tunnels).
- Il y a une fuite du nombre CERM (le nombre de tunnels CERM indiqué par les statistiques CERM dépasse le nombre réel de tunnels).

Voici les commandes à 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 disposant d'une licence **permanente** security9 qui rencontre ce problème est d'acheter la licence **HSEC-K9**. Pour plus d'informations sur ces licences, consultez Cisco ISR G2 SEC et HSEC Licensing.

Solution de contournement

Une solution de contournement possible pour ceux qui n'ont absolument pas besoin de la bande passante accrue consiste à mettre en oeuvre un formateur de trafic sur les périphériques voisins des deux côtés afin de lisser les rafales de trafic. La profondeur de la file d'attente doit peut-être être ajustée en fonction de l'intensité du trafic pour que cela soit efficace.

Malheureusement, cette solution de contournement n'est pas applicable dans tous les scénarios de déploiement et ne fonctionne souvent pas bien avec les microrafales, qui sont des rafales de trafic qui se produisent à des intervalles très courts.