أستكشاف الأخطاء وإصلاحها ؟RM-4-TX_BW_LIMIT في الأنظمة الأساسية لموجهات ISR

المحتويات

[المقدمة](#)
[معلومات أساسية](#)
[كيف تحسب الحدود؟](#)
[المشكلة](#)
[الأعراض](#)
[سبب جذري](#)
[استكشاف الأخطاء وإصلاحها](#)
[للمشاكل التي تم الوصول إلى حد عرض النطاق CERM](#)
[للمشاكل التي تم الوصول فيها إلى الحد الأقصى ل CERM Tunnel](#)
[الحل](#)
[الحل](#)

المقدمة

يوضح هذا المستند لماذا قد تواجه تشفير الحمولة وحدود جلسات العمل المشفرة للنفق/طبقة النقل (TLS) وما يجب القيام به في مثل هذه الحالة. ارظن لقيود تصدير التشفير القوية التي تفرضها حكومة الولايات المتحدة، لا يسمح ترخيص SecurityTyk9 بتشفير الحمولة إلا بمعدل يصل إلى 90 ميجابت في الثانية (ميجابت في الثانية) ويحد من عدد الأنفاق المشفرة/جلسات عمل TLS على الجهاز. يتم فرض 85 ميجابت في الثانية على أجهزة Cisco.

معلومات أساسية

يتم فرض تقييد تقييد تقييد تقييد تقييد تقييد التشفير على موجهات سلسلة موجه الخدمة المتكاملة (ISR) من Cisco باستخدام مدير تنفيذ دووق تصدير التشفير (CERM). مع تنفيذ CERM، وقبل تشغيل نفق أمان بروتوكول الإنترنت (IPsec)/TLS، يطلب من CERM حجز النفق. فيما بعد، يرسل IPsec عدد وحدات البايت التي سيتم تشفيرهاو/فك تشفيرها كمعلمات واستعلامات CERM إذا كان يمكنه متابعة التشفير/فك التشفير. يتحقق CERM من النطاق الترددي المتبقي ويجيب بنعم/ال لمعالجة/إسقاط الحزمة. لم يتم حجز النطاق الترددي بواسطة IPsec على الإطلاق. استنادا إلى النطاق الترددي المتبقي، لكل حزمة، يتم إتخاذ قرار ديناميكي من قبل CERM حول ما إذا كان سيتم معالجة الحزمة أو إسقاطها.

عند وجود إنهاء النفق من قبل IPsec، يجب تحرير الأنفاق المحجوزة السابقة بحيث يمكن ل CERM إضافتها إلى التجمع الحر. بدون ترخيص HSEC-K9، يتم تعيين حد النفق هذا على 225 نفقا. وهذا موضح في مخرجات **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
```

ملاحظة: في موجهات سلسلة ISR 4400/ISR 4300 التي تشغل برنامج Cisco IOS-XE®، يتم تطبيق قيود CERM أيضا، بخلاف موجهات سلسلة خدمات التجميع (ASR)1000. ويمكن عرضها بمخرجات **show platform software cerm information**.

كيف تحسب الحدود؟

لفهم كيفية حساب حدود النفق، يجب أن تفهم ما هي هوية الوكيل. إذا كنت تفهم هوية الوكيل بالفعل، يمكنك المتابعة إلى القسم التالي. مصطلح الوكيل هو المعرف المستخدم في سياق IPsec الذي يعين حركة المرور المحمية بواسطة اقتران أمان IPsec (SA). هناك مراسلة مباشرة بين إدخال تصريح في قائمة الوصول المشفرة وهوية وكيل (معرف الوكيل للاختصار). على سبيل المثال، عندما يكون لديك قائمة وصول تشفير معرفة مثل هذه:

```
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
```

يترجم هذا إلى تأمين معرف وكيل. عندما يكون نفق IPsec نشطا، يكون لديك على الأقل زوج واحد من SAs تم التفاوض بشأنه مع نقطة النهاية. إذا كنت تستخدم توصيلات متعددة، فقد يزيد ذلك حتى ثلاثة أزواج من IPsec SAs (زوج واحد لـ ESP، وواحد لـ AH، وواحد لـ PCP). يمكنك رؤية مثال على ذلك من إخراج الموجه الخاص بك. فيما يلي إخراج **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
```

فيما يلي أزواج IPsec SA (الواردة-الصادرة):

```
      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
```

في هذه الحالة، هناك بالضبط زوجان من SAs. يتم إنشاء هذين الزوجين بمجرد وصول حركة الوكيل معرف مادختسإ نكمي .ليكولا فرعم قباطت يتلا ريفشتلا لوصو ةمئاق ىلإ رورملا نيفلتخم ءارظنل هسفن.

> **ةظحالم**: عند فحص إخراج **show cry ipSec**، تالحظ أن هناك فهرس معلمات أمان صادرة (SPI) نوكي امدنع ةدوجوم تاقيبطت ةجمرب ةهجاوو ةطشنلا ريغ تاالخدإلل 0x0 ةميقب يلاح النفق قيد التشغيل.

في سياق CERM، يقوم الموجه بحساب عدد أزواج معرف/ناظر الوكيل النشط. هذا يعني أنه صيخرتلا تاالخدإ نم الاخدإ 30 كيدل رفوتي ءارظن ةرشع ،لاثملا ليبس ىلع ،كيدل ناك اذإ مئاوق عيمج قباطت رورم ةكرح كانه تناك اذإو ،ريفشتلاب ةصاخلا لوصولا مئاوق نم لك يف يذلا 225 حد نع ديزي ام وهو ريظن/ليكو فرعم جوز 300 عم رمألا كب يهتنيسف ،هذه لوصولا هضرف CERM. إحدى الطرق السريعة لعد عدد األنفاق التي اهاري CERM يه مادختسإ رمألا **show crypto ip sa count** والبحث عن العدد اإلجمالي ل IPsec SA كما هو موضح هنا:

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

وبعد ذلك، يتم حساب عدد الأنفاق بسهولة كإجمالي عدد عمليات sa الخاصة ب IPsec مقسوما على إثنين.

المشكلة

الأعراض

تظهر هذه الرسالة في ال syslog عندما يكون حد خفض ال crypto متجاوزا:

```
%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.
```

سبب جذري

ليس من غير الشائع أن تكون الموجهات متصلة عبر واجهات Gigabit، وكما هو موضح مسبقا، يبدأ الموجه في إسقاط حركة المرور عندما تصل إلى 85 ميجابت في الثانية واردة أو صادرة. حتى في الحالات التي لا تكون فيها واجهات جيجابت قيد الاستخدام أو يكون متوسط إستخدام النطاق الترددي أقل بكثير من هذا الحد، يمكن أن تكون حركة مرور البيانات العابرة متقطعة. حتى إذا كان الاندفاع عبارة عن بضع **مللي ثانية**، فإنه يكفي لتشغيل حد النطاق الترددي للتشفير المقيد. وفي هذه الحالات، يتم إسقاط حركة المرور التي تتجاوز 85 ميجابت في الثانية وحسابها في إخراج **معلومات** قاعدة بيانات **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
```

على سبيل المثال، إذا قمت بتوصيل **Cisco 2911** بواجهة النفق الظاهرية (VTI) من **Cisco 2951** عبر IPsec وتدفق متوسط حركة مرور بسرعة 69 ميجابت في الثانية بمعدل استخدام 6000 **من** دفعات في المرور حركة مرور يتم تسليمها، حيث يتم إسقاط **500 غلبت حزمة بسرعة ميجابت في الثانية**، فأنت ترى هذا في syslog لديك:

```
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#
```

كما يمكن رؤية ذلك، يقوم الموجه بشكل مستمر بإسقاط حركة المرور المتقطعة. لاحظ أن رسائل syslog CERM-4-TX_BW_LIMIT% محدودة بمعدل رسالة واحدة في الدقيقة.

```
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.
```

استكشاف الأخطاء وإصلاحها

للمشاكل التي تم الوصول إلى حد عرض النطاق CERM

أكمل الخطوات التالية:

1. انسخ حركة مرور البيانات على المحول المتصل.
2. أستخدم Wireshark لتحليل التتبع المأخوذ عن طريق الانتقال إلى دقة الفترة الزمنية التي تتراوح بين 2 و 10 ملي ثانية.
   ومن المتوقع أن يكون المرور بهارات صغيرة تزيد عن 85 ميجابت في الثانية.

للمشاكل التي تم الوصول فيها إلى الحد الأقصى لـ CERM Tunnel

قم بجمع هذا الإخراج بشكل دوري للمساعدة في تحديد أحد هذه الشروط الثلاثة:

- تجاوز عدد الأنفاق حد CERM.
- هناك تسرب في عدد الأنفاق (يتجاوز عدد أنفاق التشفير كما هو موضح بواسطة إحصائيات التشفير العدد الفعلي للأنفاق).
- يوجد تسرب في عدد CERM (يتجاوز عدد أرقام نفق CERM كما تم الإبلاغ عنها بواسطة إحصائيات CERM العدد الفعلي للأنفاق).

هنا الأمر أن يستعمل:

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

الحل

أفضل حل للمستخدمين الذين لديهم ترخيص SecurityTYK9 **مرتاد** الذين يواجهون هذه المشكلة هو شراء ترخيص **HSEC-K9**. للحصول على معلومات حول هذه التراخيص، ارجع إلى ترخيص Cisco ISR G2 SEC و HSEC.

الحل

أحد الحلول الممكنة للأشخاص الذين لا يحتاجون إطلاقا إلى زيادة النطاق الترددي هي

تطبيق ميزة تغيير حركة المرور على الأجهزة المجاورة على كل الجانبين من أجل تخفيف أي انفجارات مرور. ربما يجب ضبط عمق قائمة الانتظار استنادا إلى كثافة حركة المرور لكي يكون هذا فعالا.

ولسوء الحظ لا يمكن تطبيق هذا الحل البديل في جميع سيناريوهات النشر، وغالبا ما لا يعمل بشكل جيد مع البروتوكولات الدقيقة، وهي دفعات في حركة المرور تحدث في فترات زمنية قصيرة جدا.

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).