Fehlerbehebung für Fehler RM-4-TX_BW_LIMIT auf ISR Router-Plattformen

Inhalt

Einführung

In diesem Dokument wird erläutert, warum Sie möglicherweise mit Einschränkungen für Payload-Verschlüsselung und verschlüsselte Tunnel-/Transport Layer Security (TLS)-Sitzungen konfrontiert werden und was in einer solchen Situation zu tun ist. Aufgrund der strengen Exportbeschränkungen der US-Regierung im Bereich Verschlüsselung erlaubt eine SecureK9-Lizenz nur eine Payload-Verschlüsselung bis zu einer Rate von fast 90 Megabit pro Sekunde (Mbit/s) und beschränkt die Anzahl der verschlüsselten Tunnel/TLS-Sitzungen auf das Gerät. 85 Mbit/s werden auf Cisco Geräten durchgesetzt.

Hintergrundinformationen

Die Einschränkung der Verschlüsselung wird bei Routern der Cisco Integrated Service Router (ISR)-Serie mit der CERM-Implementierung (Crypto Export Restrictions Manager) durchgesetzt. Wenn CERM implementiert ist und der Internet Protocol Security (IPsec)/TLS-Tunnel aktiv ist, fordert es CERM auf, den Tunnel zu reservieren. Später sendet IPsec die Anzahl der Byte, die verschlüsselt/entschlüsselt werden sollen, als Parameter und fragt CERM ab, wenn es mit Verschlüsselung/Entschlüsselung fortfahren kann. CERM vergleicht die verbleibende Bandbreite und antwortet mit "Ja/Nein", um das Paket zu verarbeiten/zu verwerfen. Die Bandbreite wird von IPsec überhaupt nicht reserviert. Je nach verbleibender Bandbreite wird vom CERM für jedes Paket eine dynamische Entscheidung getroffen, ob das Paket verarbeitet oder verworfen werden soll.

Wenn IPsec den Tunnel beenden muss, muss es die zuvor reservierten Tunnel freigeben, damit das CERM sie dem freien Pool hinzufügen kann. Ohne die HSEC-K9-Lizenz ist diese Tunnelgrenze auf 225 Tunnel festgelegt. Dies wird in der Ausgabe von **show platform cerm-information** angezeigt:

```
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
```

> **Hinweis**: Auf den ISR Routern der Serien 4400/ISR 4300, auf denen Cisco IOS-XE® ausgeführt wird, gelten im Gegensatz zu den Routern der Aggregation Services Router (ASR) der Serie 1000 auch die CERM-Beschränkungen. Sie können mit der Ausgabe von **show platform software cerm-information** angezeigt werden.

Wie werden die Grenzwerte berechnet?

Um zu verstehen, wie die Tunnelgrenzen berechnet werden, müssen Sie verstehen, was eine Proxy-Identität ist. Wenn Sie die Proxy-Identität bereits kennen, können Sie mit dem nächsten Abschnitt fortfahren. Die Proxyidentität ist der im Kontext von IPsec verwendete Begriff, der den durch eine IPsec Security Association (SA) geschützten Datenverkehr bezeichnet. Zwischen einem Genehmigungseintrag in einer Crypto-Zugriffsliste und einer Proxy-Identität (kurz Proxy-ID) besteht eine 1:1-Korrespondenz. Wenn Sie beispielsweise eine Crypto-Zugriffsliste wie folgt definiert haben:

```
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
```

Dies entspricht genau zwei Proxy-IDs. Wenn ein IPsec-Tunnel aktiv ist, wird mindestens ein Paar SAs mit dem Endpunkt ausgehandelt. Wenn Sie mehrere Transformationen verwenden, kann dies bis zu drei Paare von IPsec-SAs erhöhen (ein Paar für ESP, eines für AH und eines für PCP). Ein Beispiel hierfür finden Sie in der Ausgabe Ihres Routers. Hier ist die **show crypto ipsec sa** output*:*

```
    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
```

Die folgenden IPsec-SA-Paare (eingehender und ausgehender Datenverkehr) sind verfügbar:

```
      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
```

In diesem Fall gibt es genau zwei SA-Paare. Diese beiden Paare werden generiert, sobald der Datenverkehr die Crypto Access-Liste erreicht, die der Proxy-ID entspricht. Dieselbe Proxy-ID kann für verschiedene Peers verwendet werden.

> **Hinweis**: Wenn Sie die Ausgabe von **show cry ipsec sa** untersuchen, sehen Sie, dass der aktuelle ausgehende Security Parameter Index (SPI) von 0x0 für die inaktiven Einträge und ein vorhandener SPI vorhanden sind, wenn der Tunnel aktiv ist.

Im Zusammenhang mit CERM zählt der Router die Anzahl der aktiven Proxy-ID/Peer-Paare. Das bedeutet, wenn Sie z. B. zehn Peers hatten, für die Sie 30 Zugriffseinträge in jeder der Zugriffslisten für Krypto zulassen, und wenn Datenverkehr vorhanden ist, der mit all diesen Zugriffslisten übereinstimmt, haben Sie 300 Proxy-ID/Peer-Paare, die über dem vom CERM festgelegten Grenzwert von 225 liegen. Eine schnelle Möglichkeit, die Anzahl der Tunnel zu erfassen, die vom CERM berücksichtigt werden, besteht darin, den Befehl **show crypto ipsec als**

count zu verwenden und nach der Gesamtzahl der IPsec-SAs zu suchen, wie hier gezeigt:

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

Die Anzahl der Tunnel wird dann leicht berechnet, indem die gesamte IPsec-SA-Anzahl durch zwei dividiert wird.

Problem

Symptome

Diese Meldungen werden im Syslog angezeigt, wenn die Grenzwerte für die Verschlüsselungsreduzierung überschritten werden:

```
%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.
```

Ursache

Es ist nicht ungewöhnlich, dass Router über Gigabit-Schnittstellen angeschlossen werden. Wie bereits erläutert, beginnt der Router, den Datenverkehr zu verwerfen, wenn er 85 Mbit/s bei ein- oder ausgehenden Verbindungen erreicht. Selbst in Fällen, in denen Gigabit-Schnittstellen nicht verwendet werden oder die durchschnittliche Bandbreitennutzung deutlich unter diesem Grenzwert liegt, kann der Transitverkehr sprunghaft ansteigen. Auch wenn der Burst einige **Millisekunden** dauert, reicht es, die eingeschränkte Verschlüsselungsbandbreite auszulösen. In diesen Situationen wird der Datenverkehr, der 85 Mbit/s überschreitet, verworfen und in der Ausgabe der **Infoinformationen** der **Plattform** erfasst*:*

```
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
```

Wenn Sie beispielsweise einen **Cisco 2911** mit einem **Cisco 2951** über IPsec Virtual Tunnel Interface (VTI) verbinden und mit einem Paket-Generator durchschnittlich 69 mps Datenverkehr bereitstellen, wobei der Datenverkehr in Spitzen von **6000 Paketen** bei einem **Durchsatz von 500 Mbit/s** übertragen wird In Ihren Syslogs sehen Sie Folgendes:

```
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#
```

Wie Sie sehen können, verwirft der Router ständig den Datenverkehr durch Bursts. Beachten Sie, dass die Syslog-Rate von **%CERM-4-TX_BW_LIMIT** auf eine Nachricht pro Minute beschränkt ist.

```
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.
```

Fehlerbehebung

Bei Problemen, bei denen das Bandbreiten-CERM-Limit erreicht ist

Gehen Sie wie folgt vor:

1. Spiegeln Sie den Datenverkehr auf dem verbundenen Switch.
2. Verwenden Sie Wireshark, um die erfasste Ablaufverfolgung zu analysieren, indem Sie auf zwei bis 10 ms Zeitraum-Granularität herabgehen.
   Datenverkehr mit Microbursts über 85 Mbit/s ist ein erwartetes Verhalten.

Bei Problemen, bei denen der maximale Grenzwert für TunnelCERM erreicht ist

Erfassen Sie diese Ausgabe regelmäßig, um eine der folgenden drei Bedingungen zu identifizieren:

- Die Anzahl der Tunnel hat den CERM-Grenzwert überschritten.
- Es besteht ein Tunnelauslass (die Anzahl der Krypto-Tunnel überschreitet laut Kryptostatistik die tatsächliche Anzahl der Tunnel).
- Es liegt ein Leck der CERM-Anzahl vor (die Anzahl der CERM-Tunnel übersteigt laut CERM-Statistiken die tatsächliche Anzahl der Tunnel).

Die folgenden Befehle sollten verwendet werden:

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

Lösung

Die beste Lösung für Benutzer mit einer **permanenten** SecurityK9 Lizenz, die dieses Problem haben, ist der Erwerb der **HSEC-K9** Lizenz. Weitere Informationen zu diesen Lizenzen finden Sie unter Cisco ISR G2 SEC- und HSEC-Lizenzierung.

Problemumgehung

Eine mögliche Lösung für alle, die die erhöhte Bandbreite nicht benötigen, ist die Implementierung eines Traffic Shaper auf den benachbarten Geräten auf beiden Seiten, um Datenverkehrsspitzen auszugleichen. Die Warteschlangentiefe muss möglicherweise auf Basis der Datenverkehrsspitzen angepasst werden, damit dies wirksam ist.

Leider ist diese Problemumgehung nicht in allen Bereitstellungsszenarien anwendbar und funktioniert häufig nicht gut mit Microbursts, bei denen es sich um Datenverkehrsspitzen handelt, die in sehr kurzen Zeitintervallen auftreten.