Risoluzione dei problemi relativi agli errori ?RM-4-TX_BW_LIMIT sulle piattaforme dei router ISR

Sommario

Introduzione

Questo documento descrive il motivo per cui potrebbe verificarsi la crittografia del payload e i limiti di sessione TLS (Transport Layer Security) crittografati e le operazioni da eseguire in una situazione di questo tipo. A causa delle forti restrizioni sull'esportazione delle funzioni di crittografia imposte dal governo degli Stati Uniti, una licenza securityk9 consente solo la crittografia del payload con velocità vicine a 90 Megabit al secondo (Mbps) e limita il numero di tunnel crittografati/sessioni TLS per il dispositivo. 85Mbps è imposto sui dispositivi Cisco.

Premesse

La restrizione della limitazione della crittografia viene applicata ai router Cisco serie ISR (Integrated Service Router) con l'implementazione di Crypto Export Restrictions Manager (CERM). Con l'implementazione di CERM, prima che il tunnel IPsec (Internet Protocol Security)/TLS diventi operativo, viene richiesto a CERM di riservare il tunnel. Successivamente, IPsec invia il numero di byte da crittografare/decrittografare come parametri ed esegue una query su CERM se è possibile procedere con la crittografia/decrittografia. CERM controlla la larghezza di banda rimanente e risponde con sì/no per elaborare/rilasciare il pacchetto. La larghezza di banda non è riservata da IPSec. In base alla larghezza di banda che rimane, per ogni pacchetto, il CERM decide in modo dinamico se elaborare o scartare il pacchetto.

Quando IPsec deve terminare il tunnel, deve liberare i tunnel riservati precedenti in modo che CERM possa aggiungerli al pool libero. Senza la licenza HSEC-K9, il limite del tunnel è impostato su 225 tunnel. Questo è mostrato nell'output di **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
```

> **Nota:** Sui router ISR serie 4400/ISR 4300 con Cisco IOS-XE®, si applicano anche le limitazioni CERM, a differenza dei router Aggregation Services Router (ASR)serie 1000. Possono essere visualizzati con l'output di **show platform software cerm-information**.

Come vengono calcolati i limiti?

Per comprendere come vengono calcolati i limiti del tunnel, è necessario capire cosa è un'identità proxy. Se si conosce già l'identità del proxy, è possibile passare alla sezione successiva. L'identità proxy è il termine utilizzato nel contesto di IPSec per indicare il traffico protetto da un'associazione di sicurezza (SA, Security Association) IPSec. Esiste una corrispondenza uno-a-uno tra una voce di autorizzazione in un elenco degli accessi crittografato e un'identità proxy (ID proxy abbreviato). Ad esempio, se si dispone di un elenco degli accessi crittografato definito come questo:

```
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
```

Ciò si traduce esattamente in due ID proxy. Quando è attivo un tunnel IPsec, si dispone di almeno una coppia di associazioni di protezione negoziate con l'endpoint. Se si utilizzano più trasformazioni, è possibile che vengano incrementate fino a tre coppie di associazioni di protezione IPsec, una per ESP, una per AH e una per PCP. Ciò si verifica in particolare nell'output del router. Di seguito è riportato l'output del comando **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
```

Di seguito sono riportate le coppie di SA IPsec (in entrata-in uscita):

```
      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 questo caso, sono presenti esattamente due coppie di associazioni di protezione. Queste due coppie vengono generate non appena il traffico raggiunge l'elenco degli accessi crittografati che corrisponde all'ID proxy. È possibile utilizzare lo stesso ID proxy per peer diversi.

> **Nota:** Quando si esamina l'output di **show cry ipsec sa,** si osserverà che esiste un indice dei parametri di sicurezza (SPI) in uscita corrente di 0x0 per le voci inattive e un indice SPI esistente quando il tunnel è attivo.

Nel contesto di CERM, il router conta il numero di coppie di ID proxy/peer attive. Ciò significa che se si hanno, ad esempio, dieci peer per i quali si hanno 30 voci di permesso in ciascuno degli elenchi degli accessi crittografici e se c'è traffico che corrisponde a tutti quegli elenchi degli accessi, si finisce con 300 coppie di ID proxy/peer, che sono al di sopra del limite di 225 imposto da CERM. Per contare rapidamente il numero di tunnel presi in considerazione dal CERM, usare il comando **show crypto ipsec sa count** e cercare il conteggio totale delle SA IPsec, come mostrato di seguito:

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

Il numero di tunnel viene quindi facilmente calcolato dividendo il conteggio SA IPsec totale per

due.

Problema

Sintomi

Questi messaggi vengono visualizzati nel syslog quando i limiti di riduzione della crittografia vengono superati:

```
%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.
```

Causa principale

Non è raro che i router siano connessi tramite interfacce Gigabit e, come spiegato in precedenza, il router inizia a perdere traffico quando raggiunge gli 85 Mbps in entrata o in uscita. Anche nei casi in cui le interfacce Gigabit non siano in uso o l'utilizzo medio della larghezza di banda sia chiaramente al di sotto di questo limite, il traffico di transito può essere bursty. Anche se lo burst è di pochi **millisecondi**, è sufficiente per attivare il limite ridotto della larghezza di banda crittografica. In questi casi, il traffico che supera gli 85 Mbps viene scartato e preso in considerazione nell'output **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
```

Ad esempio, se si collega una **scheda Cisco 2911** a una **scheda Cisco 2951** tramite l'interfaccia VTI (Virtual Tunnel Interface) IPsec e si invia una media di 69 mps di traffico con un generatore di pacchetti, in cui il traffico viene inviato in modo frammentato a **6000 pacchetti** a un **throughput di 500 Mbps**, nei syslog viene visualizzato quanto segue:

```
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#
```

Come si può vedere, il router scarta continuamente il traffico che scoppia. Si noti che la velocità dei messaggi syslog **%CERM-4-TX_BW_LIMIT** è limitata a un messaggio al minuto.

```
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.
```

Risoluzione dei problemi

Per i problemi in cui viene raggiunto il limite CERM della larghezza di banda

Attenersi alla seguente procedura:

1. Eseguire il mirroring del traffico sullo switch connesso.
2. Usare Wireshark per analizzare la traccia acquisita riducendo la granularità a due o 10 msec. Il traffico con micro burst superiori a 85 Mbps è un comportamento previsto.

Per i problemi in cui viene raggiunto il limite massimo del CERM del tunnel

Raccogli questo output periodicamente per identificare una delle tre condizioni seguenti:

- Il numero di tunnel ha superato il limite CERM.
- Si è verificata una perdita nel numero di tunnel (il numero di tunnel crittografici segnalato dalle statistiche crittografiche supera il numero effettivo di tunnel).
- Si è verificata una perdita nel conteggio CERM (il numero di tunnel CERM come riportato dalle statistiche CERM supera il numero effettivo di tunnel).

Di seguito sono riportati i comandi da utilizzare:

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

Soluzione

La soluzione migliore per gli utenti con una licenza **perpetua** security9 che incontrano questo problema è acquistare la licenza **HSEC-K9**. Per informazioni su queste licenze, fare riferimento a Cisco ISR G2 SEC e alle licenze HSEC.

Soluzione alternativa

Per coloro che non hanno assolutamente bisogno di una larghezza di banda maggiore, è possibile implementare uno shaper del traffico sui dispositivi adiacenti su entrambi i lati, al fine di attenuare

eventuali picchi di traffico. Affinché la coda sia efficace, potrebbe essere necessario sintonizzare la profondità in base alla frammentazione del traffico.

Purtroppo questa soluzione non è applicabile in tutti gli scenari di distribuzione e spesso non funziona bene con i microscopi, ovvero i picchi di traffico che si verificano a intervalli di tempo molto brevi.