Probleemoplossing?RM-4-TX_BW_LIMIT fouten op ISR routerplatforms

Inhoud

Inleiding

Dit document beschrijft waarom u mogelijk te maken krijgt met payload-encryptie en versleutelde tunnel-/transportlaag security (TLS) sessielimieten en wat u in een dergelijke situatie kunt doen. Vanwege sterke crypto-exportbeperkingen die door de overheid van de Verenigde Staten worden opgelegd, staat een security k9 licentie alleen payload-encryptie toe tot snelheden van bijna 90 Megabits per seconde (Mbps) en beperkt het aantal versleutelde tunnels/TLS-sessies tot het apparaat. 85 Mbps wordt afgedwongen op Cisco-apparaten.

Achtergrondinformatie

De encryptie-beperking van de beperking wordt afgedwongen op Cisco Integrated Service Router (ISR) die routers met de Crypto Export Bepertions Manager (CERM) implementatie uitvoert. Met CERM wordt geïmplementeerd, voordat de Internet Protocol Security (IPsec)/TLS-tunnel levend wordt gehouden, vraagt het CERM om de tunnel te reserveren. Later, stuurt IPsec het aantal bytes dat moet worden versleuteld/gedecrypteerd als parameters en vraagt CERM als het kan doorgaan met encryptie/decryptie. CERM controleert tegen de bandbreedte die blijft en reageert met ja/nee om het pakket te verwerken/te laten vallen. Bandbreedte is helemaal niet door IPsec voorbehouden. Gebaseerd op de bandbreedte die, voor elk pakket, blijft, wordt een dynamisch besluit genomen door CERM of om het pakket te verwerken of te laten vallen.

Wanneer IPsec de tunnel moet afsluiten, moet deze de eerder gereserveerde tunnels opheffen zodat CERM ze aan de gratis pool kan toevoegen. Zonder de HSEC-K9 licentie is deze tunnellimiet ingesteld op 225 tunnels. Dit wordt getoond in de output van **show platform cerm-informatie**:

```
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
```

> Opmerking: Op de ISR 4400/ISR 4300 Series routers die Cisco IOS-XE® uitvoeren, zijn de CERM-beperkingen ook van toepassing, in tegenstelling tot de Aggregation Services Router (ASR) 1000 Series routers. Ze kunnen worden bekeken met de output van **show platform software cerm-informatie**.

Hoe worden de limieten berekend?

Om te begrijpen hoe de tunnelgrenzen worden berekend moet je begrijpen wat een proxy-identiteit is. Als u al een proxy-identiteit begrijpt, kunt u doorgaan met de volgende sectie. De proxy-identiteit is de term die wordt gebruikt in de context van IPsec, waarin het verkeer wordt aangeduid dat is beschermd door een IPsec Security Association (SA). Er is een één-op-één verband tussen een vergunningvermelding op een cryptotoegangslijst en een volmachthoudentiteit (proxy-ID voor short). Bijvoorbeeld, wanneer u een crypto toegangslijst hebt die als dit wordt gedefinieerd:

```
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
```

Dit vertaalt zich naar precies twee proxy-ID's. Wanneer een IPsec-tunnel actief is, hebt u minimaal één paar SA's onderhandeld met het eindpunt. Als u meerdere transformaties gebruikt, kan dit tot drie paren IPsec SA's (één paar voor ESP, één voor AH en één voor PCP) verhogen. U kunt een voorbeeld hiervan zien vanuit de uitvoer van uw router. Hier is de **show crypto ipsec als** 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
```

Hier zijn de IPsec SA paren (inkomend):

```
      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 dit geval zijn er precies twee paren SA's. Deze twee paren worden gegenereerd zodra het verkeer de crypto access lijst raakt die de proxy-ID aanpast. Dezelfde proxy-ID kan voor verschillende peers worden gebruikt.

> Opmerking: Wanneer u de output van **show wenen ipsec** onderzoekt, zie je dat er een huidige uitgaande Security Parameter Index (SPI) van 0x0 is voor de inactieve ingangen en een bestaande SPI wanneer de tunnel omhoog is.

In de context van CERM, telt de router het aantal actieve proxy ID/peer paren. Dit betekent dat als je, bijvoorbeeld, tien peers had waarvoor je 30 vergunningsingangen hebt in elk van de cryptotoegangslijsten, en als er verkeer is dat overeenkomt met al die toegangslijsten, dan eindig je met 300 proxy-ID/peer paren die boven de 225-limiet liggen die door CERM wordt opgelegd. Een snelle manier om het aantal tunnels te tellen dat CERM van mening is, is het gebruik van de **show crypto ipsec als tellingsopdracht** en zoek de totale telling van IPsec SA zoals hier getoond:

```
router#show crypto ipsec sa count
```

```
IPsec SA total: 6, active: 6, rekeying: 0, unused: 0, invalid: 0
```

Het aantal tunnels wordt dan gemakkelijk berekend zoals het totale aantal IPsec SA dat door twee wordt gedeeld.

Probleem

Symptomen

Deze berichten worden in de slang gezien wanneer de limieten voor crypto-reductie worden overschreden:

```
%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.
```

Root-oorzaak

Het is niet ongebruikelijk dat routers via Gigabit-interfaces worden aangesloten, en zoals eerder is uitgelegd, start de router om verkeer te laten vallen wanneer deze 85 Mbps binnenkomend of uitgaande bereikt. Zelfs in gevallen waar Gigabit interfaces niet in gebruik zijn of het gemiddelde bandbreedte gebruik duidelijk onder deze limiet is, kan het transitoverkeer zwaar zijn. Zelfs als de uitbarsting een paar **milliseconden** is, is het genoeg om de ingeperkte bandbreedte van crypto te activeren. En in deze situaties, wordt het verkeer dat meer dan 85 Mbps is gedaald en geregistreerd in **de** uitvoer **van platform cerm-informatie*:***

```
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
```

Als u bijvoorbeeld **Cisco 2911** aansluit op een **Cisco 2951** via IPsec Virtual Tunnel Interface (VTI) en een gemiddelde van 69 Mbps van verkeer met een pakketgenerator levert, waar het verkeer wordt geleverd in bursts van **6000 pakketten** bij een **doorvoersnelheid van 500** Mbps zie je dit in je weblog :

```
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#
```

Zoals je kunt zien, laat de router constant het bursty verkeer vallen. Merk op dat het **%CERM-4-TX_BW_LIMIT** syslg bericht aan de snelheid is beperkt tot één bericht per minuut.

```
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.
```

Problemen oplossen

Voor emissies waarbij de Bandbreedtecertificeringsgrens wordt bereikt

Voer de volgende stappen uit:

1. Spiegelen het verkeer op de aangesloten schakelaar.
2. Gebruik Wireshark om het opgenomen spoor te analyseren door het te beperken tot 2 tot 10 msec tijdgranulariteit.
   Verkeer met microbosten groter dan 85 Mbps is een verwacht gedrag.

Voor kwesties waarbij de maximumgrenswaarde voor tunnels wordt bereikt

Verzamel deze uitvoer regelmatig om een van deze drie voorwaarden te helpen identificeren:

- Het aantal tunnels is de CERM-grens overschreden.
- Er is een lek in tunnels (het aantal cryptotunnels zoals gerapporteerd door cryptostatistieken overschrijdt het aantal tunnels).
- Er is een lek aan CERM-tellingen (het aantal CERM-tunneltellingen zoals gerapporteerd door CERM-statistieken overschrijdt het werkelijke aantal tunnels).

Hier zijn de opdrachten die moeten worden gebruikt:

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

Oplossing

De beste oplossing voor gebruikers met een **permanente** security, k9 licentie die deze emissie tegenkomt is de **HSEC-K9** licentie te kopen. Raadpleeg voor informatie over deze licenties Cisco ISR G2 SEC en HSEC Licensing.

Werken

Een mogelijke workround voor degenen die de verhoogde bandbreedte absoluut niet nodig hebben is het implementeren van een traffic shaper op de aangrenzende apparaten aan beide zijden om alle files glad te strijken. De wachtrijdiepte moet misschien worden aangepast op basis van de last van het verkeer, zodat dit effectief kan zijn.

Helaas is deze tijdelijke oplossing niet van toepassing in alle uitzettingsscenario's en werkt het vaak niet goed met microbosten, die verkeersuitbarstingen zijn die zich in zeer korte periodes voordoen.