ISR 라우터 플랫폼에서 ?RM-4-TX_BW_LIMIT 오류 문제 해결

목차

소개

이 문서에서는 페이로드 암호화 및 암호화된 터널/TLS(Transport Layer Security) 세션 제한이 발생할 수 있는 이유와 이러한 상황에서 수행할 작업에 대해 설명합니다.미국 정부가 시행하는 강력한 암호화 내보내기 제한 때문에 securityk9 라이센스는 페이로드 암호화를 최대 90Mbps(Mbps)까지 허용하고 암호화된 터널/TLS 세션 수를 디바이스에 제한합니다.85Mbps는 Cisco 장치에 적용됩니다.

배경 정보

암호화 제한 제한은 CERM(Crypto Export Restrictions Manager) 구현과 함께 Cisco ISR(Integrated Service Router) 시리즈 라우터에 적용됩니다.CERM이 구현된 상태에서 IPsec(Internet Protocol Security)/TLS 터널이 가동되기 전에 CERM에 터널을 예약하도록 요청합니다.나중에 IPsec은 암호화/암호 해독을 계속할 수 있는 경우 CERM을 쿼리하여 암호화/암호 해독할 바이트 수를 전송합니다.CERM은 패킷을 처리/삭제하기 위해 남아 있고 yes/no로 응답하는 대역폭을 확인합니다.IPsec에서 대역폭을 예약하지 않았습니다.남아 있는 대역폭을 기반으로, 각 패킷에 대해 CERM이 패킷을 처리할지 아니면 삭제할지를 동적으로 결정합니다.

IPsec에서 터널을 종료해야 하는 경우 CERM이 터널을 사용 가능한 풀에 추가할 수 있도록 이전에 예약된 터널을 해제해야 합니다.HSEC-K9 라이센스가 없으면 이 터널 제한은 225개의 터널에서 설정됩니다.다음은 **show platform cerm-information**의 출력에 **표시됩니다**.

```
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
```

> **참고:**Cisco IOS-XE®를 실행하는 ISR 4400/ISR 4300 Series 라우터에서는 ASR(Aggregation Services Router)1000 Series 라우터와는 달리 CERM 제한도 적용됩니다.**show platform software cerm-information**의 출력으로 볼 수 있습니다.

한도는 어떻게 계산됩니까?

터널 제한을 계산하는 방법을 이해하려면 프록시 ID가 무엇인지 이해해야 합니다.이미 프록시 ID를 알고 있는 경우 다음 섹션으로 진행할 수 있습니다.프록시 ID는 IPsec 컨텍스트에서 IPsec SA(Security Association)에서 보호하는 트래픽을 지정하는 데 사용되는 용어입니다. 암호화 액세스 목록의 허용 항목과 프록시 ID(프록시 ID(짧은 경우 프록시 ID) 사이에 일대일 대응이 있습니다. 예를 들어 다음과 같이 암호화 액세스 목록이 정의된 경우

```
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
```

이는 정확히 두 개의 프록시 ID로 변환됩니다.IPsec 터널이 활성화된 경우 엔드포인트와 협상된 SA 쌍이 최소 1개 이상 있습니다.다중 변환을 사용하는 경우 IPsec SA의 최대 3쌍(ESP의 경우 1쌍, AH의 경우 1쌍, PCP의 경우 1쌍)이 증가할 수 있습니다. 라우터의 출력에서 이 예시를 확인할 수 있습니다.다음은 **show crypto ipsec sa** 출력입니다.

```
    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
```

다음은 IPsec SA 쌍(인바운드-아웃바운드)입니다.

```
      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
```

이 경우에는 정확히 두 쌍의 SA가 있습니다.이 두 쌍은 트래픽이 프록시 ID와 일치하는 암호화 액세스 목록에 도달하자마자 생성됩니다.동일한 프록시 ID를 다른 피어에 사용할 수 있습니다.

> **참고:show cry ipsec sa**의 출력을 검사하면 비활성 항목에 대한 현재 아웃바운드 SPI(Security Parameter Index)가 0x0이고 터널이 가동 중일 때 기존 SPI가 있는 것을 확인할 수 있습니다.

CERM의 컨텍스트에서 라우터는 활성 프록시 ID/피어 쌍의 수를 계산합니다.즉, 예를 들어 각 암호화 액세스 목록에 30개의 허용 항목이 있는 10개의 피어가 있고, 이러한 모든 액세스 목록과 일치하는 트래픽이 있는 경우 CERM에서 지정한 225개 제한 이상의 300개의 프록시 ID/피어 쌍으로 끝납니다.CERM에서 고려하는 터널의 수를 빠르게 계산하려면 **show crypto ipsec sa count** 명령을 사용하고 여기에 표시된 대로 IPsec SA 총 개수를 찾는 것입니다.

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

그런 다음 총 IPsec SA 수를 2로 나누어 터널 수를 쉽게 계산할 수 있습니다.

문제

증상

이러한 메시지는 암호화 통화 제한 제한을 초과할 경우 syslog에서 확인할 수 있습니다.

```
%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.
```

근본 원인

라우터가 기가비트 인터페이스를 통해 연결되는 경우가 드물지 않으며, 앞서 설명한 대로 라우터가 85Mbps 인바운드 또는 아웃바운드에 도달할 때 트래픽을 삭제하기 시작합니다.기가비트 인터페이스를 사용하지 않거나 평균 대역폭 사용률이 이 제한보다 훨씬 낮은 경우에도 전송 트래픽은 과부하가 발생할 수 있습니다.버스트가 몇 **밀리초**에 **해당하더라도**, 감소된 암호화 대역폭 제한을 트리거하는 데 충분합니다.이러한 경우 85Mbps를 초과하는 트래픽은 **show platform cerm-information** 출력에서 삭제되고 계산됩니다.

```
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
```

예를 들어 **Cisco 2911을 IPsec VTI**(Virtual Tunnel Interface)를 통해 **Cisco 2951**에 연결하고 패킷 생성기를 사용하여 평균 69mpbs의 트래픽을 전송하는 경우, **처리량 500Mbps**의 600**패킷**에서 **트래픽이** 폭발적으로 전달되는 경우 **syslog**에서 이를 확인할 수 있습니다.

```
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#
```

보시다시피 라우터는 버스트 트래픽을 지속적으로 삭제합니다.%CERM**-4-TX_BW_LIMIT** syslog 메시지는 분당 메시지 1개로 제한됩니다.

```
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.

문제 해결

대역폭 CERM 제한에 도달한 문제의 경우

다음 단계를 완료하십시오.

1. 연결된 스위치의 트래픽을 미러링합니다.
2. Wireshark를 사용하여 2~10msec의 시간 세분화로 다운하여 캡처된 추적을 분석합니다. 마이크로버스트가 85Mbps보다 큰 트래픽은 예상되는 동작입니다.

최대 터널 CERM 제한에 도달한 문제의 경우

다음 세 가지 조건 중 하나를 식별하기 위해 정기적으로 이 출력을 수집합니다.

- 터널 수가 CERM 제한을 초과했습니다.
- 터널 수 누수가 있습니다(암호화 통계에서 보고한 암호화 터널 수가 실제 터널 수를 초과합니다).
- CERM 수 누수가 있습니다(CERM 통계에서 보고한 CERM 터널 개수가 실제 터널 수를 초과합니다).

사용할 명령은 다음과 같습니다.

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

솔루션

영구 보안9 라이센스가 있는 사용자에게 이 문제가 발생하는 가장 적합한 솔루션은 **HSEC-K9** 라이센스를 구매하는 것입니다.이러한 라이센스에 대한 자세한 내용은 Cisco ISR G2 SEC 및 HSEC 라이센싱을 참조하십시오.

해결 방법

대역폭을 늘릴 필요가 없는 사용자에게 가능한 해결 방법 중 하나는 트래픽 버스트를 원활하게 처리하기 위해 양쪽의 인접 디바이스에 트래픽 쉐이퍼를 구현하는 것입니다.이 작업을 적용하려면 트래픽의 버스트림에 따라 큐 깊이를 조정해야 할 수 있습니다.

안타깝게도 이 해결 방법은 모든 구축 시나리오에서는 적용되지 않으며, 마이크로버스트에서 제대로 작동하지 않는 경우가 많습니다. 이는 매우 짧은 시간 간격으로 발생하는 트래픽 버스트입니다.