ISRルータプラットフォームでの「RM-4-TX_BW_LIMIT」エラーのトラブルシューティング

内容

概要

このドキュメントでは、ペイロードの暗号化と暗号化されたトンネル/Transport Layer Security(TLS)セッションの制限が発生する理由と、このような状況での対処方法について説明します。米国政府によって強化された強力な暗号化エクスポートの制限により、securityk9ライセンスでは、最大90 Mbps（メガビット/秒）近くのレートでのペイロード暗号化のみが許可され、デバイスへの暗号化トンネル/TLSセッションの数が制限されます。85 Mbpsがシスコデバイスに適用されます。

背景説明

暗号化の制限は、Crypto Export Restrictions Manager(CERM)実装のCisco Integrated Service Router(ISR)シリーズルータに適用されます。CERMを実装すると、Internet Protocol Security(IPsec)/TLSトンネルが稼働する前に、CERMにトンネルの予約を要求します。その後、IPsecは暗号化/復号化するバイト数をパラメータとして送信し、暗号化/復号化を続行できる場合はCERMに照会します。CERMは残っている帯域幅をチェックし、パケットを処理/ドロップするためにyes/noで応答します。帯域幅はIPSecによってまったく予約されていません。パケットごとに残っている帯域幅に基づいて、パケットを処理するか廃棄するかをCERMが動的に決定します。

IPsecがトンネルを終端する必要がある場合、CERMがトンネルを空きプールに追加できるように、以前に予約されていたトンネルを解放する必要があります。HSEC-K9ライセンスがないと、このトンネル制限は225トンネルに設定されます。**show platform cerm-information**の出力に次のように表示されます。

```
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
```

> **注**：Cisco IOS-XE®が稼働するISR 4400/ISR 4300シリーズルータでは、アグリゲーションサービスルータ(ASR)1000シリーズルータとは異なり、CERMの制限も適用されます。これらは、**show platform software cerm-information**の出力で**確認できます**。

制限はどのように計算されますか。

トンネル制限の計算方法を理解するには、プロキシIDを理解する必要があります。プロキシIDをすでに理解している場合は、次のセクションに進むことができます。プロキシIDは、IPSecセキュリティアソシエーション(SA)によって保護されるトラフィックを指定するIPSecのコンテキストで使用される用語です。 暗号化アクセスリストの許可エントリとプロキシID（短い場合はプロキシID）の間には1対1の対応があります。 たとえば、次のように定義された暗号アクセスリストがある場合、

```
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
```

これは、2つのプロキシIDに変換されます。IPSecトンネルがアクティブな場合、エンドポイントとネゴシエートされるSAのペアが少なくとも1つ存在します。複数のトランスフォームを使用すると、IPsec SAのペア（ESP用に1ペア、AH用に1ペア、PCP用に1ペア）が最大3ペアまで増加する可能性があります。 この例は、ルータの出力から確認できます。**show crypto ipsec sa**の出力**を次に示**します。

```
    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
```

IPsec SAペア（着信と発信）は次のとおりです。

```
      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
```

この例では、SAのペアは2つのみです。これらの2つのペアは、プロキシIDに一致する暗号アクセスリストにトラフィックが到達するとすぐに生成されます。同じプロキシIDを異なるピアに使用できます。

> **注：show cry ipsec sa**の出力を調べると、非アクティブなエントリに対する現在の発信セキュリティパラメータインデックス(SPI)が0x0であり、トンネルが稼働している場合は既存のSPIであることがわかります。

CERMのコンテキストでは、ルータはアクティブなプロキシID/ピアペアの数をカウントします。これは、たとえば、暗号アクセスリストごとに30個の許可エントリがあるピアが10個あり、これらすべてのアクセスリストに一致するトラフィックがある場合、CERMによって課された225の制限を超える300のプロキシIDとピアペアが発生することを意味します。CERMが考慮するトンネルの数を簡単にカウントするには、**show crypto ipsec sa count**コマンドを使用して、次に示すようにIPsec SAの総数を検索します。

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

その後、トンネルの数は、IPsec SAの総数を2で割って簡単に計算できます。

問題

症状

次のメッセージは、暗号化の制限を超えたときにsyslogに表示されます。

```
%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.
```

根本原因

ルータがギガビットインターフェイスを介して接続されることは珍しくありません。前述したように、ルータは85 Mbpsの着信または発信に達すると、トラフィックのドロップを開始します。ギガビットインターフェイスが使用されていない場合や、帯域幅の平均使用率がこの制限を明確に下回っている場合でも、通過トラフィックがバースト性を持つ可能性があります。バーストが数ミリ秒の場合でも、暗号化の帯域幅制限の縮小をトリガーするのに十分です。このような状況では、85 Mbpsを超えるトラフィックはドロップされ、**show platform cerm-informationの出力に含まれます。**

```
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
```

たとえば、**Cisco 2911をIPsec Virtual Tunnel Interface(VTI)経由でCisco 2951に接続**し、パケットジェネレータを使用して平均69 mbpsのトラフィックを配信する場合は、6000パケットの**5のバーストででトラフィックがを配信**送信されます00 Mbpsの場合、syslogに次のように表示されます。

```
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#
```

ルータはバーストトラフィックを絶えずドロップしています。%CERM-4-TX_BW_LIMIT syslogメッセージは、1分あたり1メッセージに制限されています。

```
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.
```

トラブルシュート

帯域幅CERMの制限に達した問題

次のステップを実行します。

1. 接続されたスイッチのトラフィックをミラーリングします。
2. Wiresharkを使用して、キャプチャされたトレースを2 ~ 10ミリ秒の時間間隔の精度まで下げて分析します。
   85 Mbpsを超えるマイクロバーストを持つトラフィックは、想定される動作です。

トンネルCERMの最大限度に達した問題

次の3つの条件のいずれかを特定するために、この出力を定期的に収集します。

- トンネルの数がCERMの制限を超えています。
- トンネルカウントリークが発生しています（暗号統計情報によって報告される暗号化トンネルの数が、実際のトンネルの数を超えています）。
- CERMカウントリーク（CERM統計情報で報告されるCERMトンネル数が実際のトンネル数を超えている）が発生しています。

使用するコマンドを次に示します。

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

解決方法

この問題が発生した永久セキュリティK9ライセンスを持つユーザに最適なソリューションは、HSEC-K9ライセンスを購入します。これらのライセンスの詳細については、『Cisco ISR G2 SECおよびHSECのライセンス』を参照してください。

回避策

帯域幅の増加を絶対に必要としない場合の1つの回避策として、トラフィックバーストを円滑に処

理するために、両側の隣接デバイスにトラフィックシェーパーを実装します。これを有効にするには、トラフィックのバースト性に基づいてキュー項目数を調整する必要がある場合があります。

残念ながら、この回避策はすべての導入シナリオに適用できるわけではなく、非常に短い時間間隔で発生するトラフィックのバーストであるマイクロバーストでは適切に動作しません。