トラブルシュートしますか。ISR ルータ プラットフォーム上の RM-4-TX_BW_LIMIT エラー

目次

概要

この資料はペイロード暗号化および暗号化されたトンネル/Transport Layer Security （ TLS ）セッション 限度になぜ出会うかもしれませんおよびそのような状況ではかするべきことを記述したものです。 米国 政府が適用する強い暗号 輸出制限が原因で securityk9 ライセンスは 90 メガビット/秒（ Mbps ）の近くのレートまでだけペイロード暗号化を可能にし、デバイスに暗号化された tunnels/TLS セッションの数を制限します。 85Mbps は実施された on Cisco デバイスです。

背景説明

暗号削減制約事項は暗号 輸出制限マネージャ（ CERM ）実装を用いる実施された on Cisco 統合サービス ルータ（ ISR ）シリーズ ルータです。 インターネット プロトコル セキュリティ（ IPsec ）/TLS トンネルの前に、設定されて CERM が生中継されます、トンネルを予約するように CERM を要求します。 以降は、IPsec 暗号化 復号化を続行できる場合パラメータとして暗号化されるべき/復号化されるバイト数を送信 し、CERM を問い合わせます。 CERM は yes/no/ドロップすると処理するためにパケット残り、応答する帯域幅に対してチェックします。 帯域幅は IPsec によってまったく予約されません。 、各パケットのために、ダイナミック デシジョンに残る帯域幅に基づいて CERM によってパケットを処理するか、または廃棄するためにかどうか作られます。

IPsec がトンネルを終える必要があるとき CERM がフリープールにそれらを追加できるようにより早い予約済みのトンネルを自由に使えるようにする必要があります。 HSEC-K9 ライセンスなしで、このトンネル 限界は 225 のトンネルで設定 されます。 これは出力での**示しますプラットフォーム cerm 情報を**示されています:

```
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 ® を実行する ISR 4400/ISR 4300 シリーズ ルータで、CERM 制限はまた集約でとは違って、保守しますルータを (ASR)1000 シリーズ ルータ適用されます。 それらは出力と**示しますプラットフォームソフトウェア cerm 情報を**の表示することができます。

制限はどのように計算されるか。

トンネル 限界がどのように計算されるか理解するために、プロキシの身元がであるもの理解して下さい。 既にプロキシの身元を理解している場合、次の セクションに進むことができます。 IPSecセキュリティアソシエーション結合 (SA) が保護するトラフィックを指定するプロキシの身元は IPsec という点において使用される用語です。 暗号 access-list の割り当てエントリとプロキシの身元 (短いのためのプロキシ ID) 間に 1対1の一致があります。 たとえば、これのように定義される暗号 access-list がある時:

```
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
```

これは丁度 2 プロキシ ID に変換します。 IPSecトンネルがアクティブなとき、エンドポイントによってネゴシエートされる SA の最低 1 つのペアがあります。 複数の変換を使用する場合、これは IPSec SA （ AH のための ESP、1、および PCP のための 1 のための 1 つのペア) の 3 つまでのペアを増加する可能性があります。 ルータの出力からのこれの例を表示できます。 出力される **show crypto ipsec sa はここにあります*:***

```
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
```

IPsec SA ペア (受信発信) はここにあります:

```
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
```
この場合、丁度 SA の 2 つのペアがあります。 これら二つのペアはトラフィックが暗号 access-list を見つけるとすぐ作成されますプロキシ ID と一致する。 同じプロキシ ID は別の同位に使用できます。

> **注:** 出力をの検査するときトンネルが稼働しているとき非アクティブ エントリおよび既存の SPI のための 0x0 の電流 送信 Security Parameter Index （ SPI ）があることが**叫び ipsec sa、わかります示して下さい。**

CERM という点において、ルータはアクティブなプロキシ ID/peer ペアの数を数えます。 これはたとえば 10 同位にそれらの access-list すべてと一致する暗号 access-list のそれぞれで 30 の割り当てエントリがある、およびトラフィックがあれば持っていたらことを意味します、CERM によって課される 225 制限の上にある 300 のプロキシ ID/peer ペアで終る。 CERM が考慮するトンネルの数を数える簡単は **show crypto ipsec sa 数**コマンドを使用し、ここに示されているとして IPsec SA 合計数を探すことです:

```
router#show crypto ipsec sa count
IPsec SA total: 6, active: 6, rekeying: 0, unused: 0, invalid: 0
```
トンネルの数はそれから容易に合計 IPsec SA 数が 2 で割ることによって求めたように計算されます。

問題

症状

これらのメッセージは syslog で暗号削減制限が超過するとき見られます:

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

受信か送信 85 Mbps に達するとき以前に説明されて、ルータがトラフィックを廃棄し始めるようにルータがギガビットインターフェイスによって接続されることは珍しくないし。 ギガビットインターフェイスが使用中ではないかまたは平均帯域幅 利用がこの制限よりずっと低く明確にあれば、トランジットトラフィックはバースト性である場合もあります。 バーストが少数の**ミリ秒**の間あっても、省略された暗号 帯域幅制限を引き起こす十分です。 そしてこの場合、トラフィックは 85Mbps を超過する**示します**出力される**プラットフォーム cerm 情報を**廃棄され、説明されます*:*

```
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、IPsec 仮想 な トンネルインターフェイス (VTI) によって syslog で Cisco 2911 に

Cisco 2951 を接続し、トラフィックが 500 Mbps のスループットの 6000 のパケットのバーストで渡されるパケット 生成機能とのトラフィックの 69 mps の平均を、見ればこれを渡せば:

```
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#
```

見てわかるように、ルータは絶えずバースト性トラフィックを廃棄します。 分毎に 1 つのメッセージにレートリミットされした %CERM-4-TX_BW_LIMIT syslog messageis に注意して下さい。


```
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#
```


トラブルシューティング

帯域幅 CERM 制限が達する問題に関しては

次の手順を実行します。

1. 接続されたスイッチのトラフィックを映して下さい。
2. 2 から 10 ミリ秒時間 細かさへダウン状態になることによってキャプチャされるトレースを分析するために Wireshark を使用して下さい。
   85Mbps より大きいマイクロ バーストのトラフィックは予期された動作です。

最大トンネル CERM 制限が達する問題に関しては

この 3 状態の 1 つの識別を助けるためにこの出力を定期的に集めて下さい:

- トンネルの数は CERM 制限を超過しました。
- トンネルカウント リークがあります（暗号統計情報によって報告されるように暗号化トンネルの数はトンネルの実際の数を超過します）。
- CERM 数リークがあります（CERM 統計情報によって報告されるとして CERM トンネルカウントの数はトンネルの実際の数を超過します）。

使用するコマンドはここにあります:

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

解決策

この問題に出会う**パーマネント** securityk9 ライセンスのユーザ向けの最もよいソリューションは **HSEC-K9** ライセンスを購入することです。 これらのライセンスの情報に関しては、Cisco ISR G2 SEC および HSEC 認可を参照して下さい。

回避策

絶対に高められた帯域幅を必要としない人のための 1 つの可能性のある回避策はトラフィックバーストをスムーズにするために両側の隣接デバイスのトラフィックシェイパーを設定することです。 キュー項目数はトラフィックのバースト性にこれが有効であることができるように基づいていました調整されなければならないかもしれません。

残念ながらこの回避策はすべてのデプロイメントシナリオの適用されないで、頻繁に短い時刻間隔に非常に発生するトラフィックバーストの microbursts とうまく作動しません。