# IPSec トンネルを介した PING 口スを含む Syslogs"%CRYPTO-4-RECVD_PKT_MAC_ERR:" エラー メッセージのトラブルシューティング

## 目次



## 概要

このドキュメントでは、ボックスに示すように、syslog の 「%CRYPTO-4-RECVD_PKT_MAC_ERR」メッセージと組み合わせて、IPSec トンネルでの ping の損失を解決する方法について説明しています。

```
May 23 11:41:38.139 GMT: %CRYPTO-4-RECVD_PKT_MAC_ERR:
decrypt: mac verify failed for connection
id=2989 local=172.16.200.18 remote=172.16.204.18 spi=999CD43B
seqno=00071328
```

このような廃棄のごく一部は、正常と見なされます。 ただし、この問題によりドロップ レートが高くなると、サービスに影響する可能性があるため、ネットワーク オペレータの注意が必要な場合があります。 syslog で報告されるこれらのメッセージは、30 秒間隔で限定された割合であるため、1 つのログ メッセージが、必ずしも 1 つのパケットのみが廃棄されたことを表すわけではないことに注意してください。 これらの廃棄の正確な数を取得するには、コマンド **show crypto ipsec sa detail** を発行し、ログに含まれる接続 ID の次の SA を確認してください。 SA カウンタでは、**pkts verify failed error** カウンタが、メッセージ認証コード（MAC）確認の失敗による廃棄パケットの総数を示します。

```
interface: GigabitEthernet0/1
Crypto map tag: MPLSWanGREVPN, local addr 172.16.204.18

protected vrf: (none)
local ident (addr/mask/prot/port): (172.16.204.18/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (172.16.205.18/255.255.255.255/47/0)
current_peer 172.16.205.18 port 500
PERMIT, flags={origin_is_acl,}
```

```
#pkts encaps: 51810, #pkts encrypt: 51810, #pkts digest: 51810
#pkts decaps: 44468, #pkts decrypt: 44468, #pkts verify: 44468
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#pkts no sa (send) 0, #pkts invalid sa (rcv) 0
#pkts encaps failed (send) 0, #pkts decaps failed (rcv) 0
#pkts invalid prot (recv) 0, #pkts verify failed: 8
#pkts invalid identity (recv) 0, #pkts invalid len (rcv) 0
#pkts replay rollover (send): 0, #pkts replay rollover (rcv) 0
#pkts replay failed (rcv): 0
#pkts internal err (send): 0, #pkts internal err (recv) 0

local crypto endpt.: 172.16.204.18, remote crypto endpt.: 172.16.205.18
path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/1
current outbound spi: 0xD660992C(3596654892)

inbound esp sas:
spi: 0x999CD43B(2577191995)
transform: esp-3des esp-sha-hmac ,
in use settings ={Transport, }
conn id: 2989, flow_id: AIM-VPN/SSL-3:2989, sibling_flags 80000006,
crypto map: MPLSWanGREVPN
sa timing: remaining key lifetime (k/sec): (4257518/24564)
IV size: 8 bytes
replay detection support: N
Status: ACTIVE

outbound esp sas:
spi: 0xD660992C(3596654892)
transform: esp-3des esp-sha-hmac ,
in use settings ={Transport, }
conn id: 2990, flow_id: AIM-VPN/SSL-3:2990, sibling_flags 80000006,
crypto map: MPLSWanGREVPN
sa timing: remaining key lifetime (k/sec): (4199729/24564)
IV size: 8 bytes
replay detection support: N
Status: ACTIVE
```

# 前提条件

## 要件

このドキュメントに関する固有の要件はありません。

## 使用するコンポーネント

このドキュメントの情報は、Cisco IOS® リリース 15.1(4)M4 で行われたテストに基づいています。 まだテストされていませんが、スクリプトおよび設定は、以前のバージョンの Cisco IOS ソフトウェアでも機能するはずです。これは、EEM バージョン 3.0（IOS バージョン 12.4(22) T 以降でサポート）が両方のアプレットで使用されるためです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

# 機能情報

「%CRYPTO-4-RECVD_PKT_MAC_ERR: decrypt: 」は、MAC 検証に失敗した暗号化パケットを受信したことを意味します。 この確認は、次のように設定された証明書トランスフォーム セットの結果です。

```
Router (config)# crypto ipsec transform transform-1 esp-aes 256 esp-md5-hmac
```

上の例では、「*esp-aes 256*」が暗号化アルゴリズムを 256 AES として定義し、「*esp-md5*」が MD5 ( HMAC のバリアント ) を、認証に使用するハッシュ アルゴリズムとして定義します。 MD5 などのハッシュ アルゴリズムは、通常、ファイルの内容のデジタル フィンガープリントを提供するために使用されます。 デジタル フィンガープリントは、ファイルが侵入者またはウイルスによって変更されていないことを保証するために、よく使用されます。 したがって、このエラー メッセージが表示されることは、通常、次のいずれかを意味します。

- パケットの暗号化または復号化に使用したキーが誤っています。 このエラーは非常にまれで、ソフトウェアの不具合が原因で発生することがあります。

または

- パケットが転送中に改竄されています。 このエラーは、ダーティ回線または不正なイベントが原因である可能性があります。

# トラブルシューティング方法

このエラー メッセージは、通常、パケットの破損によって発生するため、根本原因を分析する方法は、EPC を使用して、両方のトンネル エンドポイントの WAN 側の完全なパケットのキャプチャを取得し、比較することだけです。 キャプチャを取得する前に、これらのログをトリガーするトラフィックの種類を特定することを推奨します。 場合によっては、特定の種類のトラフィックである可能性があります。 また、トラフィックの種類に無関係だが、簡単に再現できる場合もあります ( 100 回の ping ごとに 5 ~ 7 回の廃棄など ) 。 このような場合は、問題の特定が、やや容易になります。 最も効率よくトリガーを特定する方法は、DSCP マーキングでテスト トラフィックをマークし、パケットをキャプチャすることです。 DSCP 値は、ESP ヘッダーにコピーされ、その後、Wireshark でフィルタリングできます。 100 回の ping によるテストを想定したこの設定を使用して、次のように ICMP パケットをマークできます。

```
Router (config)# crypto ipsec transform transform-1 esp-aes 256 esp-md5-hmac
```

今度は、このポリシーを、clear traffic が暗号化ルータで受信される入力インターフェイスに適用する必要があります。

```
Router (config)# crypto ipsec transform transform-1 esp-aes 256 esp-md5-hmac
```

また、このテストを、ルータが生成するトラフィックで実行するという方法もあります。 この場合は、Quality of Service ( QoS ) を使用してパケットをマークすることはできませんが、ポリシー ベース ルーティング ( PBR ) を使用できます。

> **注:** 重大な (5) DSCP マーキングを見つけるには、Wireshark フィルタ **ip.dsfield.dscp == 0x28** を使用します。

```
Router (config)# crypto ipsec transform transform-1 esp-aes 256 esp-md5-hmac
```

QoS マーキングを ICMP トラフィックに対して設定したら、埋め込みパケット キャプチャを設定できます。

```
Router(config)# ip access-list ext vpn_capo
Router(config)# permit ip host <local> <peer>
Router(config)# permit ip host <peer> <local>
Router(config)#  exit //the capture is only configured in enable mode.
Router# monitor capture buffer vpncap size 256 max-size 100 circular
Router# monitor capture buffer vpncap filter access-list vpn_capo
Router# monitor capture point ip cef capo fastEthernet 0/1 both
Router# monitor capture point associate capo vpncap
Router# monitor capture point start capo //starts the capture.
To stop replace the "start" keyword with "stop"
```

注： これは、Cisco IOS リリース 12.4(20)T で導入された機能です。 EPC に関する詳細については、「埋め込みパケット キャプチャ」を参照してください。

このタイプの問題のトラブルシューティングのためにパケット キャプチャを使用するには、パケットの一部だけでなく、全体をキャプチャする必要があります。 15.0(1)M より前の Cisco IOS リリースの EPC 機能には、512K のバッファ制限と 1024 バイトの最大パケット サイズ制限があります。 この制限を回避するには、15.0(1)M 以降のコードにアップグレードしてください。これで、100M のキャプチャ バッファ サイズと、9500 バイトの最大パケット サイズがサポートされます。

問題が 100 回の ping ごとに確実に再生できる場合、最悪のシナリオは、制御されたテストとしてのみ ping トラフィックを許可し、キャプチャを取得するためにメンテナンス時間帯をスケジュールすることです。 このプロセスにかかる時間は数分だけですが、その時間の実稼働トラフィックが中断されます。 QoS マーキングを使用する場合は、パケットを ping のみに制限するために要件を排除する必要があります。 1 つのバッファのすべての ping パケットをキャプチャするには、ピーク時間帯にテストが行われないようにする必要があります。

問題が容易には再現されない場合は、EEM のスクリプトを使用してパケット キャプチャを自動化することができます。 この理論は、両側で循環バッファへとキャプチャを開始し、EEM を使用して片側でキャプチャを停止することです。 EEM でキャプチャを停止すると同時に、snmp トラップをピアに送信し、ピアでもキャプチャを停止します。 このプロセスは機能する可能性があります。 ただし、負荷が大きい場合は、2 番目のルータの反応が間に合わず、キャプチャが停止されない場合があります。 そのため、制御されたテストを推奨します。 プロセスを実行する EEM スクリプトを次に示します。

```
Router(config)# ip access-list ext vpn_capo
Router(config)# permit ip host <local> <peer>
Router(config)# permit ip host <peer> <local>
Router(config)#  exit //the capture is only configured in enable mode.
Router# monitor capture buffer vpncap size 256 max-size 100 circular
Router# monitor capture buffer vpncap filter access-list vpn_capo
Router# monitor capture point ip cef capo fastEthernet 0/1 both
Router# monitor capture point associate capo vpncap
Router# monitor capture point start capo //starts the capture.
To stop replace the "start" keyword with "stop"
```

```
Router(config)# ip access-list ext vpn_capo
Router(config)# permit ip host <local> <peer>
Router(config)# permit ip host <peer> <local>
Router(config)#  exit //the capture is only configured in enable mode.
Router# monitor capture buffer vpncap size 256 max-size 100 circular
Router# monitor capture buffer vpncap filter access-list vpn_capo
Router# monitor capture point ip cef capo fastEthernet 0/1 both
Router# monitor capture point associate capo vpncap
Router# monitor capture point start capo //starts the capture.
To stop replace the "start" keyword with "stop"
```

*前のボックスのコードは、15.0(1)M でテストされた設定であることに注意してください。 このコードをお客様の環境で実行する前に、お客様が使用する特定の Cisco IOS バージョンでテストすることをお勧めします。*

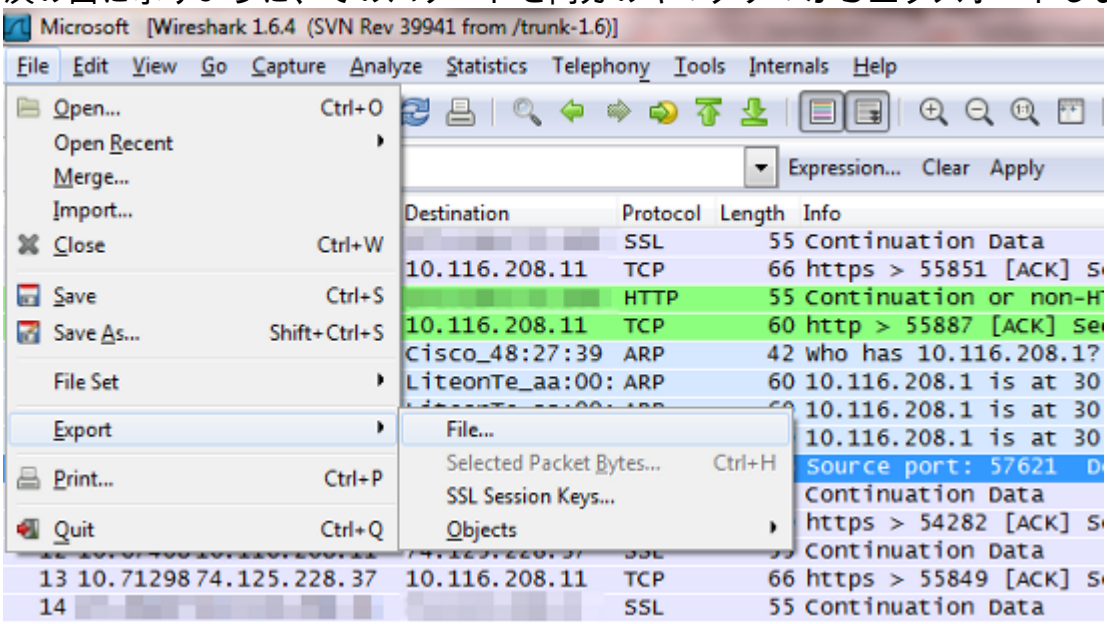
# データ分析

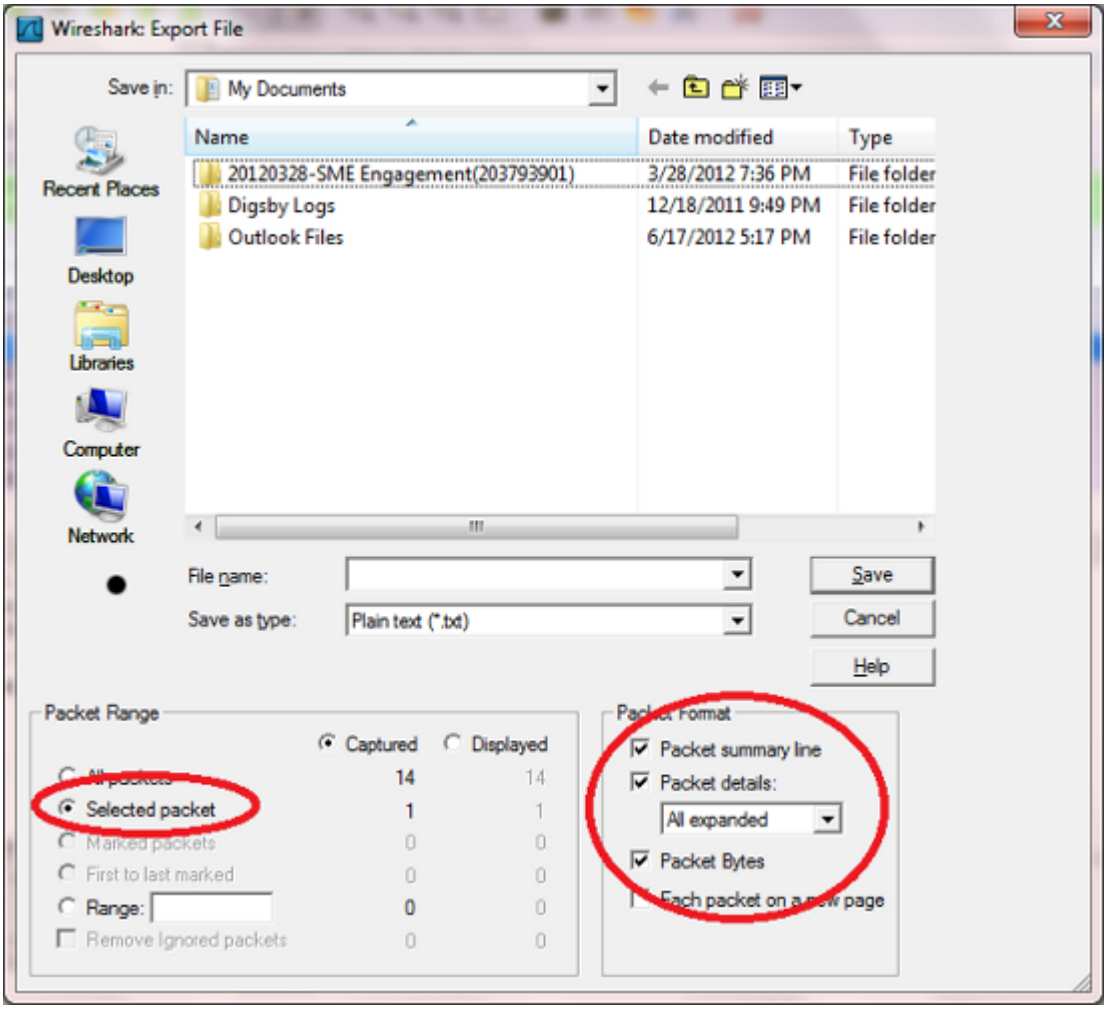
1. キャプチャが完了したら、TFTP を使用して PC にエクスポートします。
2. ネットワーク プロトコル アナライザ ( Wireshark など ) を使用してキャプチャを開きます。
3. QoS マーキングを使用した場合は、各パケットをフィルタリングします。

```
Router(config)# ip access-list ext vpn_capo
Router(config)# permit ip host <local> <peer>
Router(config)# permit ip host <peer> <local>
Router(config)#  exit //the capture is only configured in enable mode.
Router# monitor capture buffer vpncap size 256 max-size 100 circular
Router# monitor capture buffer vpncap filter access-list vpn_capo
Router# monitor capture point ip cef capo fastEthernet 0/1 both
Router# monitor capture point associate capo vpncap
Router# monitor capture point start capo //starts the capture.
To stop replace the "start" keyword with "stop"
```

「0x08」は DSCP 値 AF21 に固有です。 別の DSCP 値を使用している場合は、正しい値をパケット キャプチャ自体から、または DSCP 値の変換表のリストから取得できます。 詳細については、「DSCP 値と優先値」を参照してください。

4. 送信者からのキャプチャの廃棄 ping を特定し、そのパケットを、受信側と送信側の両方のキャプチャで見つけます。
5. 次の図に示すように、そのパケットを両方のキャプチャから工クスポートします。






6. その 2 つのバイナリ比較を実行します。 これらが同じである場合、転送中のエラーはありません。Cisco IOS が受信側で検出漏れをスローしたか、送信側で誤ったキーを使用しています。 いずれの場合も、問題は Cisco IOS の不具合です。 パケットが異なっている場合は、パケットが転送中に改竄されています。

FC の暗号化エンジンから送信されるパケットを次に示します。

```
Router(config)# ip access-list ext vpn_capo
Router(config)# permit ip host <local> <peer>
Router(config)# permit ip host <peer> <local>
Router(config)#  exit //the capture is only configured in enable mode.
Router# monitor capture buffer vpncap size 256 max-size 100 circular
Router# monitor capture buffer vpncap filter access-list vpn_capo
Router# monitor capture point ip cef capo fastEthernet 0/1 both
Router# monitor capture point associate capo vpncap
Router# monitor capture point start capo //starts the capture.
To stop replace the "start" keyword with "stop"
```

ピアで受信した、同じパケットを次に示します。

```
Router(config)# ip access-list ext vpn_capo
Router(config)# permit ip host <local> <peer>
Router(config)# permit ip host <peer> <local>
Router(config)#  exit //the capture is only configured in enable mode.
Router# monitor capture buffer vpncap size 256 max-size 100 circular
Router# monitor capture buffer vpncap filter access-list vpn_capo
Router# monitor capture point ip cef capo fastEthernet 0/1 both
Router# monitor capture point associate capo vpncap
Router# monitor capture point start capo //starts the capture.
```

```
To stop replace the "start" keyword with "stop"
```

この時点では、最も可能性が高いのが ISP の問題で、そのグループをトラブルシューティングに使用する必要があります。

# 一般的な問題

- Cisco Bug ID CSCed87408 は、83xs の暗号化エンジンのハードウェア問題について説明しています。これは、任意の発信パケットが暗号化時に破損したために認証エラーが発生し（認証が使用されている場合）、受信側でパケットがドロップされるという問題です。 ここで重要なのは、これらのエラーが表示されるのが 83x 自体ではなく、着信側デバイスであることを認識することです。

- また、このエラーが、古いコード ショーを実行するルータで表示される場合もあります。15.1(4)M4 などの最新バージョンのコードにアップグレードすると、問題を解決できます。

- ハードウェアとソフトウェアのどちらの問題であるかを確認するには、ハードウェア暗号化を無効にします。 引き続きログ メッセージが表示される場合は、ソフトウェアの問題です。そうでない場合は、RMA で問題を解できます。
ハードウェア暗号化を無効にすると、負荷の大きい VPN トンネルの重大なネットワーク劣化を引き起こす場合があることに注意してください。 そのため、このドキュメントで説明したプロシージャはメンテナンス時間帯に実行することをお勧めします。

# 関連情報

- テクニカルサポートとドキュメント - Cisco Systems