Syslog「%CRYPTO-4-RECVD_PKT_MAC_ERR：」錯誤消息，其中包含Ping Loss Over IPsec隧道故障排除

目錄

[簡介](#)
[必要條件](#)
[需求](#)
[採用元件](#)
[功能資訊](#)
[故障排除方法](#)
[資料分析](#)
[常見問題](#)
[相關資訊](#)

簡介

本檔案介紹如何解決透過IPsec通道執行的ping損失問題，此通道與系統日誌中的「%CRYPTO-4-RECVD_PKT_MAC_ERR」訊息耦合在一起，如下方框所示：

```
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
```

這種下降中一小部分被認為是正常的。但是，由於此問題而導致的高丟棄率可能會影響服務，並可能需要網路運營商的注意。請注意，系統日誌中報告的這些消息以30秒的間隔進行速率限制，因此單個日誌消息並不總是表示只有單個資料包被丟棄。若要取得這些捨棄的準確計數，請發出**show crypto ipsec sa detail**指令，然後檢視記錄中看到的連線ID旁邊的SA。在SA計數器中，**pkts verify failed**錯誤計數器說明由於消息身份驗證代碼(MAC)驗證失敗而導致的總資料包丟棄。

```
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
```

必要條件

需求

本文件沒有特定需求。

採用元件

本檔案中的資訊是根據使用Cisco IOS®版本15.1(4)M4執行的測試。雖然尚未測試，但指令碼和組態應該適用於較舊的Cisco IOS軟體版本，因為兩個小程式都使用EEM版本3.0(IOS版本12.4(22)T或更新版本支援)。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

功能資訊

「%CRYPTO-4-RECVD_PKT_MAC_ERR:decrypt:""表示收到未通過MAC驗證的加密資料包。此驗

證是配置的身份驗證轉換集的結果：

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

在上方範例中，「*esp-aes 256」將加密演演算法定義*為256位AES，而「*esp-md5*」將MD5（HMAC變體）定義為用於驗證的雜湊演演算法。雜湊演算法（如MD5）通常用於提供檔案內容的數字指紋。數字指紋通常用於確保檔案未被入侵者或病毒篡改。因此出現此錯誤訊息通常意味著：

- 使用錯誤的金鑰加密或解密資料包。此錯誤非常罕見，可能是由軟體錯誤所導致。

— 或 —

- 傳輸過程中資料包被篡改。此錯誤可能是由於電路汙染或惡意事件所致。

故障排除方法

由於此錯誤訊息通常是由封包損毀引起的，因此進行根本原因分析的唯一方法是使用EPC，從兩個通道端點的WAN端取得完整的封包擷取，並進行比較。在獲取捕獲之前，最好確定觸發這些日誌的流量型別。在某些情況下，它可以是特定型別的流量；在其他情況下，它可能是隨機的，但很容易重現（例如每100次ping發生5-7次丟棄）。 在這種情況下，問題會變得容易一點點確定。識別觸發器的最佳方法是使用DSCP標籤來標籤測試流量並捕獲資料包。DSCP值將複製到ESP報頭，然後可以使用Wireshark進行過濾。此組態會假設使用100 ping進行測試，可用來標籤ICMP封包：

```
ip access-list extended VPN_TRAFFIC
 permit icmp <source> <destination>
class-map match-all MARK
 match access-group name VPN_TRAFFIC
policy-map MARKING
 class MARK
   set dscp af21
```

現在，此策略必須應用於加密路由器上接收清除流量的輸入介面：

```
interface GigabitEthernet0/0
service-policy MARKING in
```

或者，您可能要對路由器生成的流量運行此測試。因此，您不能使用服務品質(QoS)來標籤資料包，但可以使用基於策略的路由(PBR)。

附註：為了定位關鍵(5)DSCP標籤，請使用Wireshark過濾器**ip.dsfield.dscp == 0x28**。

```
ip access-list extended VPN_TRAFFIC
 permit icmp <source> <destination>
route-map markicmp permit 10
match ip address vpn
set ip precedence critical
ip local policy route-map markicmp
```

為ICMP流量配置QoS標籤後，可以配置嵌入式資料包捕獲：

```
Router(config)# ip access-list ext vpn_capo
Router(config)# permit ip host
```

```
Router(config)# permit ip host
```

```
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"
```

附註：此功能是在Cisco IOS版本12.4(20)T中匯入。有關EPC的詳細資訊，請參閱嵌入式資料包捕獲。

使用資料包捕獲解決此類問題需要捕獲整個資料包，而不僅僅是其中的一部分。15.0(1)M之前的Cisco IOS版本中的EPC功能具有512K的緩衝區限制和1024位元組的最大資料包大小限制。為了避免此限制，請升級到15.0(1)M或更新代碼，此代碼現在支援100M的捕獲緩衝區大小，最大資料包大小為9500位元組。

如果每隔100個計數ping能可靠地重現問題，則最糟糕的情況是計畫維護視窗，以便僅允許ping流量作為受控測試並執行捕獲。此過程只需幾分鐘時間，但確實會中斷該時間的生產流量。如果使用QoS標籤，則可以消除將資料包僅限製為ping的要求。為了在一個緩衝區中擷取所有ping封包，必須確保測試不會在高峰時間進行。

如果問題不易復發，可以使用EEM指令碼自動捕獲資料包。其原理是，將兩端的擷取啟動到一個循環緩衝區中，然後使用EEM在一端停止擷取。在EEM停止捕獲的同時，讓其向對等體傳送snmp陷阱，以停止其捕獲。這個過程可能奏效。但是如果負載過重，第二台路由器可能反應不夠快，無法停止捕獲。優選受控測試。以下是實施該過程的EEM指令碼：

```
Receiver
========
event manager applet detect_bad_packet
event syslog pattern "RECVD_PKT_MAC_ERR"
action 1.0 cli command "enable"
action 2.0 cli command "monitor capture point stop test"
action 3.0 syslog msg "Packet corruption detected and capture stopped!"
action 4.0 snmp-trap intdata1 123456 strdata ""
```

```
Sender
======
event manager applet detect_bad_packet
event snmp-notification oid 1.3.6.1.4.1.9.10.91.1.2.3.1.9.
oid-val "123456" op eq src-ip-address 20.1.1.1
action 1.0 cli command "enable"
action 2.0 cli command "monitor capture point stop test"
action 3.0 syslog msg "Packet corruption detected and capture stopped!"
```

請注意，上方的代碼是使用15.0(1)M測試的配置。在客戶環境中實施之前，您可能希望使用客戶使用的特定Cisco IOS版本對其進行測試。

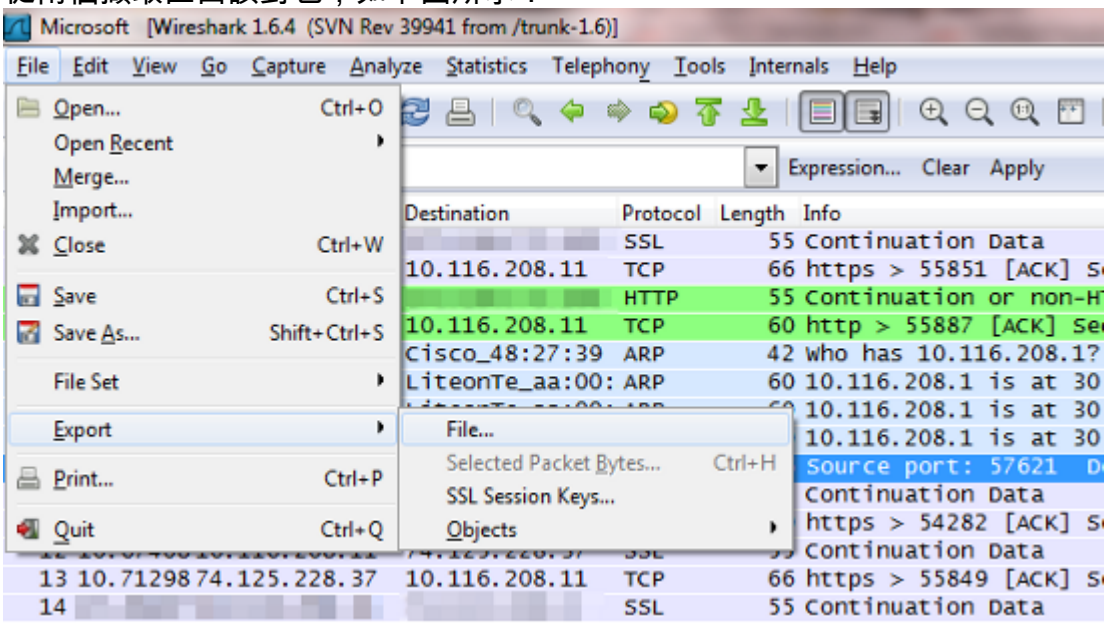
資料分析

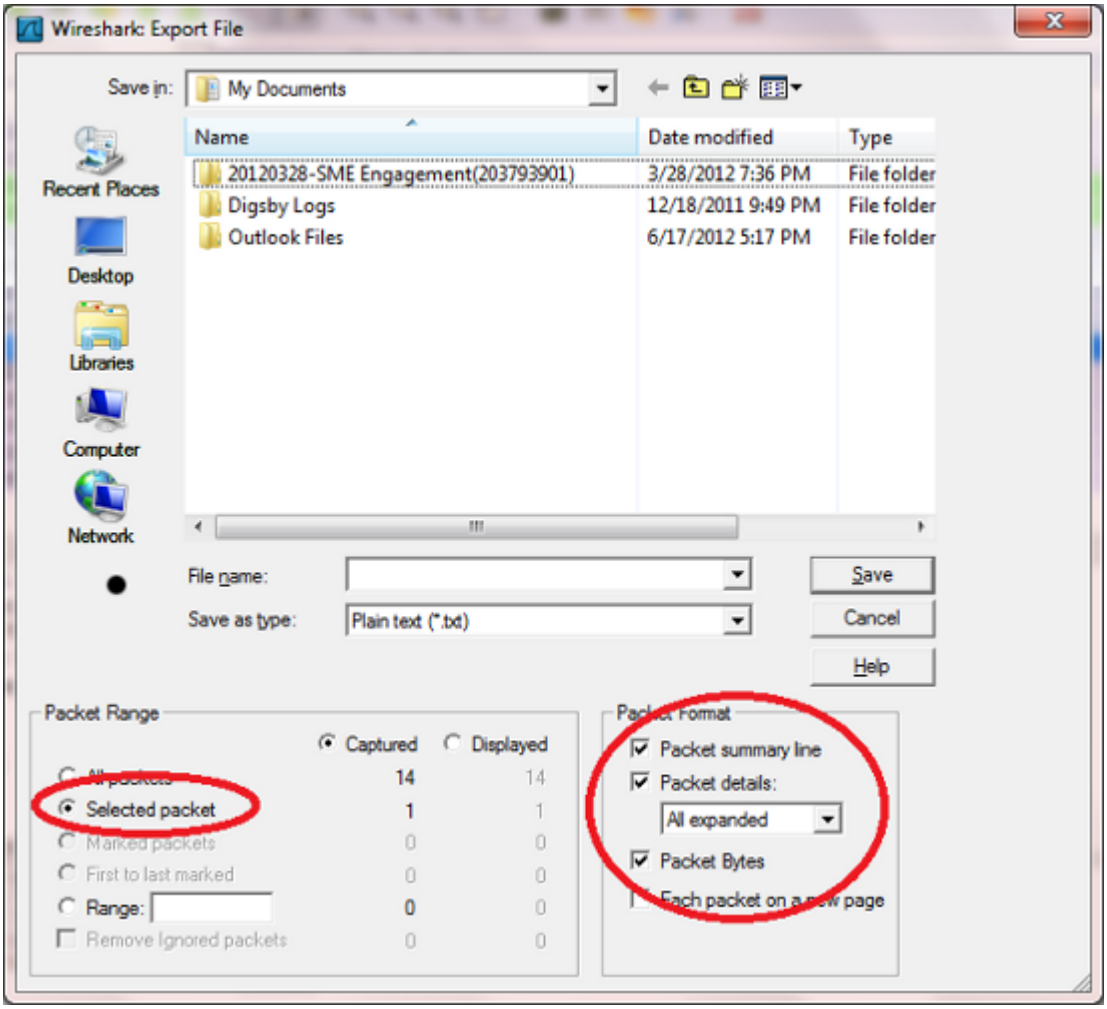
1. 捕獲完成後，使用TFTP將其匯出到PC。
2. 使用網路協定分析器（例如Wireshark）開啟捕獲。
3. 如果使用QoS標籤，請過濾掉各個資料包。

```
ip.dsfield.dscp==0x08
```

「0x08」專用於DSCP值AF21。如果使用不同的DSCP值，則可以從資料包捕獲本身或從DSCP值轉換圖表清單獲取正確的值。有關詳細資訊，請參閱DSCP和優先順序值。

4. 識別來自傳送者的擷取上已捨棄的ping，並在接收端和傳送端上的擷取上找到該封包。
5. 從兩個擷取匯出該封包，如下圖所示：





6. 將兩者進行二進位制比較。如果兩者相同，則在傳輸過程中沒有錯誤，Cisco IOS會在接收端拋出假陰性，或在傳送端使用錯誤的金鑰。在這兩種情況下，問題都是Cisco IOS錯誤。如果資料包不同，則在傳輸過程中資料包會被篡改。

以下封包離開FC上的密碼編譯引擎時出現：

```
*Mar  1 00:01:38.923: After encryption:
05F032D0: 45000088 00000000 E.......
05F032E0: FF3266F7 0A01201A 0A012031 7814619F .2fw.. ... 1x.a.
05F032F0: 00000001 DE9B4CEF ECD9178C 3E7A7F24 ....^.LolY..>z.$
05F03300: 83DCF16E 7FD64265 79F624FB 74D5AEF2 .\qn.VBeyv${tU.r
05F03310: 5EC0AC16 B1F9F3AB 89524205 A20C4E58 ^@,.1ys+.RB.".NX
05F03320: 09CE001B 70CC56AB 746D6A3A 63C2652B .N..pLV+tmj:cBe+
05F03330: 1992E8AF 2CE2A279 46367BDB 660854ED ..h/,b"yF6{[f.Tm
05F03340: 77B69453 83E47778 1470021F 09436285 w6.S.dwx.p...Cb.
05F03350: CB94AEF5 20A65B1F 480D86F6 125BA12E K..u &[.H..v.[!.
```

以下是對等體上接收的相同封包：

```
4F402C90:                   45000088 00000000          E.......
4F402CA0: FF3266F7 0A01201A 0A012031 7814619F .2fw.. ... 1x.a.
4F402CB0: 00000001 DE9B4CEF ECD9178C 3E7A7F24 ....^.LolY..>z.$
4F402CC0: 83DCF16E 7FD64265 79F624FB 74D5AEF2 .\qn.VBeyv${tU.r
4F402CD0: 5EC0AC16 B1F9F3AB 89524205 A20C4E58 ^@,.1ys+.RB.".NX
4F402CE0: 09CE001B 70CC56AB 00000000 00000000 .N..pLV+........
4F402CF0: 00000000 00000000 00000000 00000000 ................
4F402D00: 00000000 00000000 00000000 00000000 ................
4F402D10: 00000000 00000000 00000000 00000000 ................
```

此時，很可能是ISP的問題，該組應參與故障排除。

常見問題

- 思科錯誤ID CSCed87408說明83xs上的加密引擎出現硬體問題，加密期間隨機傳出封包損毀，導致接收端發生驗證錯誤（在使用驗證的情況下）和封包捨棄。務必認識到，在83x上不會看到這些錯誤，而是在接收裝置上。

- 有時運行舊代碼的路由器會顯示此錯誤。您可以升級到更新的代碼版本(例如15.1(4)M4)以解決此問題。

- 要驗證問題是否由硬體或軟體引起，請禁用硬體加密。如果日誌消息繼續，則說明存在軟體問題。如果不是，則RMA應解決問題。
  請記住，如果禁用硬體加密，則可能導致過載VPN隧道的嚴重網路降級。因此，思科建議您在維護期間嘗試本文檔中介紹的步驟。

相關資訊

- 技術支援與文件 - Cisco Systems