Syslog "%CRYPTO-4-RECVD_PKT_MAC_ERR:" Messaggio di errore con risoluzione dei problemi del tunnel Ping Loss Over IPsec

Sommario

Introduzione

In questo documento viene descritto come risolvere la perdita di ping su un tunnel IPsec associato a messaggi "%CRYPTO-4-RECVD_PKT_MAC_ERR" nel syslog, come mostrato nella casella:

```
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
```

Una piccola percentuale di tali cadute è considerata normale. Tuttavia, un elevato tasso di caduta a causa di questo problema può avere un impatto sul servizio e potrebbe richiedere l'attenzione dell'operatore di rete. Si noti che questi messaggi riportati nei syslog sono limitati a intervalli di 30 secondi, quindi un singolo messaggio di log non sempre indica che è stato scartato un solo pacchetto. Per ottenere un conteggio accurato delle perdite, usare il comando **show crypto ipsec sa detail** e verificare l'associazione di sicurezza accanto all'ID di connessione visualizzato nei log. Tra i contatori SA, il contatore degli errori di **verifica PKTS non riuscita** tiene conto della perdita totale del pacchetto a causa dell'errore di verifica del codice di autenticazione del messaggio (MAC).

```
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
```

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni di questo documento si basano sui test eseguiti con Cisco IOS® versione 15.1(4)M4. Anche se non sono stati ancora testati, gli script e la configurazione devono essere compatibili con le versioni precedenti del software Cisco IOS, in quanto entrambe le applet utilizzano EEM versione 3.0 (supportata nella versione 12.4(22)T o successive).

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico

ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Informazioni sulle funzionalità

"%CRYPTO-4-RECVD_PKT_MAC_ERR: decrypt:" implica che è stato ricevuto un pacchetto crittografato che non ha superato la verifica MAC. Questa verifica è il risultato del set di trasformazioni di autenticazione configurato:

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

Nell'esempio precedente, *"esp-aes 256"* definisce l'algoritmo di crittografia come AES a 256 bit, mentre *"esp-md5"* definisce l'MD5 (variante HMAC) come l'algoritmo hash utilizzato per l'autenticazione. Gli algoritmi hash come MD5 vengono in genere utilizzati per fornire un'impronta digitale del contenuto di un file. L'impronta digitale viene spesso utilizzata per garantire che il file non sia stato alterato da un intruso o da un virus. Di conseguenza, il verificarsi di questo messaggio di errore implica in genere:

- Èstata utilizzata la chiave errata per crittografare o decrittografare il pacchetto. Questo errore è molto raro e potrebbe essere causato da un bug del software.

-OPPURE-

- Il pacchetto è stato manomesso durante il trasporto. Questo errore potrebbe essere dovuto a un circuito sporco o a un evento ostile.

Metodologia di risoluzione dei problemi

Poiché questo messaggio di errore è in genere causato dal danneggiamento dei pacchetti, l'unico modo per eseguire un'analisi della root cause è usare l'EPC per ottenere le acquisizioni complete dei pacchetti dal lato WAN su entrambi gli endpoint del tunnel e confrontarle. Prima di ottenere le clip, è meglio identificare il tipo di traffico che genera i log. In alcuni casi può trattarsi di un tipo specifico di traffico; in altri casi, potrebbe essere casuale ma facilmente riproducibile (come 5-7 gocce ogni 100 ping). In tali situazioni, il problema diventa leggermente più facile da identificare. Il modo migliore per identificare il trigger è contrassegnare il traffico di prova con contrassegni DSCP e acquisire i pacchetti. Il valore DSCP viene copiato nell'intestazione ESP e può quindi essere filtrato con Wireshark. Questa configurazione, che prevede un test con 100 ping, può essere utilizzata per contrassegnare i pacchetti ICMP:

```
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
```

A questo punto, è necessario applicare il criterio all'interfaccia in entrata che riceve il traffico sul router di crittografia:

```
interface GigabitEthernet0/0
```

```
service-policy MARKING in
```

In alternativa, è possibile eseguire questo test con il traffico generato dal router. Per questo motivo, non è possibile utilizzare QoS (Quality of Service) per contrassegnare i pacchetti, ma è possibile utilizzare PBR (Policy-Based Routing).

> **Nota:** Per individuare i contrassegni DSCP critici (5), utilizzare il filtro Wireshark **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
```

Dopo aver configurato il contrassegno QoS per il traffico ICMP, è possibile configurare l'acquisizione pacchetti incorporata:

```
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"
```

Nota: questa funzione è stata introdotta in Cisco IOS versione 12.4(20)T. per ulteriori informazioni sugli EPC, fare riferimento a Embedded Packet Capture.

Per risolvere questo tipo di problema, è necessario che l'intero pacchetto venga acquisito, non solo una parte. La funzione EPC nelle versioni Cisco IOS precedenti alla 15.0(1)M ha un limite di buffer di 512K e un limite massimo per le dimensioni del pacchetto di 1024 byte. Per evitare questo limite, aggiornare il codice a 15.0(1)M o versioni successive, che ora supporta una dimensione del buffer di acquisizione di 100M con una dimensione massima del pacchetto di 9500 byte.

Se il problema può essere riprodotto in modo affidabile ogni 100 ping, lo scenario peggiore è pianificare un intervallo di manutenzione in modo da consentire solo il traffico ping come test controllato e acquisire le immagini. Questo processo richiede solo pochi minuti, ma interrompe il traffico di produzione per tale periodo di tempo. Se si usa il contrassegno QoS, è possibile eliminare la necessità di limitare i pacchetti solo ai ping. Per acquisire tutti i pacchetti ping in un

buffer, accertarsi che il test non venga eseguito nelle ore di punta.

Se il problema non viene riprodotto facilmente, è possibile utilizzare uno script EEM per automatizzare l'acquisizione del pacchetto. La teoria è che si avviano le acquisizioni su entrambi i lati in un buffer circolare e si utilizza EEM per fermare la cattura su un lato. Allo stesso tempo, l'EEM interrompe l'acquisizione e invia una trap snmp al peer, che interrompe l'acquisizione. Questo processo potrebbe funzionare. Tuttavia, se il carico è pesante, il secondo router potrebbe non reagire abbastanza rapidamente da interrompere la cattura. È preferibile un test controllato. Di seguito sono riportati gli script EEM che implementeranno il processo:

```
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!"
```

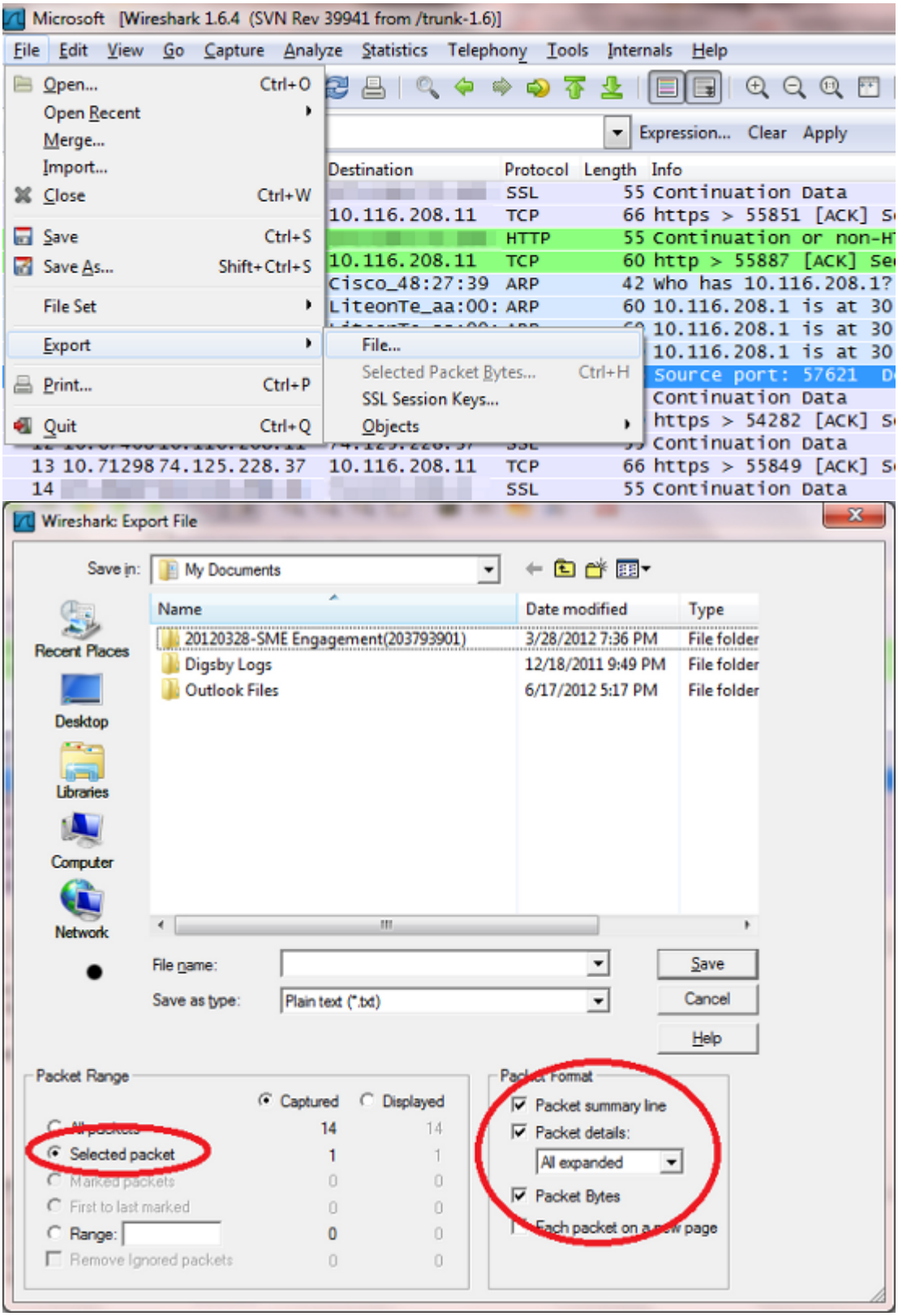
Il codice della casella precedente è una configurazione provata con 15.0(1)M. È possibile testarlo con la versione Cisco IOS specifica utilizzata dal cliente prima di implementarlo nell'ambiente del cliente.

Analisi dei dati

1. Una volta completate le clip, usare il protocollo TFTP per esportarle su un PC.
2. Aprire le clip con un analizzatore di protocolli di rete (ad esempio Wireshark).
3. Se è stato usato il contrassegno QoS, filtrare i rispettivi pacchetti.

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

   "0x08" è specifico per il valore DSCP AF21. Se si utilizza un valore DSCP diverso, è possibile ottenere il valore corretto dallo stesso packet capture o dall'elenco dei valori DSCP del grafico di conversione. per ulteriori informazioni, fare riferimento a DSCP e valori di precedenza.
4. Identificare il ping interrotto sulle clip provenienti dal mittente e individuare il pacchetto sulle clip sia dal lato ricevente che dal lato mittente.
5. Esporta il pacchetto da entrambe le clip come mostrato nell'immagine:



6. Effettuare un confronto binario tra i due. Se sono identici, non vi sono errori in transito e Cisco IOS ha generato un falso negativo sul lato ricevente o ha utilizzato la chiave errata sul lato mittente. In entrambi i casi, il problema è un bug di Cisco IOS. Se i pacchetti sono diversi, sono stati manomessi durante la trasmissione.

   Di seguito è riportato il pacchetto che ha lasciato il motore di crittografia sull'FC:

```
*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.[!.
```

Di seguito è riportato lo stesso pacchetto ricevuto sul peer:

```
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 ................
```

A questo punto, è molto probabile che si tratti di un problema dell'ISP e che il gruppo sia coinvolto nella risoluzione del problema.

Problemi comuni

- L'ID bug Cisco CSCed87408 descrive un problema hardware con il motore di crittografia degli switch 83x, in cui i pacchetti in uscita casuali vengono danneggiati durante la crittografia, il che porta a errori di autenticazione (nei casi in cui viene utilizzata l'autenticazione) e a perdite di pacchetti sull'estremità ricevente. È importante notare che questi errori non verranno visualizzati sul dispositivo 83x ma sul dispositivo ricevente.

- A volte questo errore viene visualizzato nei router che eseguono il codice precedente. Per risolvere il problema, è possibile eseguire l'aggiornamento alle versioni più recenti del codice, ad esempio 15.1(4) M4.

- Per verificare se il problema è di tipo hardware o software, disattivare la crittografia hardware. Se i messaggi di registro continuano, si tratta di un problema software. In caso contrario, un'autorizzazione al reso (RMA) dovrebbe risolvere il problema.
  Tenere presente che la disabilitazione della crittografia hardware può causare un grave deterioramento della rete per i tunnel VPN con carico elevato. Pertanto, Cisco consiglia di tentare le procedure descritte in questo documento durante un intervento di manutenzione.

Informazioni correlate

- Documentazione e supporto tecnico – Cisco Systems