Mensaje de error Syslog "%CRYPTO-4-RECVD_PKT_MAC_ERR:" con Ping Loss Over IPsec Tunnel Troubleshooting

Contenido

Introducción

Este documento describe cómo resolver la pérdida de ping sobre un túnel IPsec asociado con los mensajes "%CRYPTO-4-RECVD_PKT_MAC_ERR" en el syslog como se muestra en el cuadro:

```
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
```

Un pequeño porcentaje de estas caídas se considera normal. Sin embargo, una alta tasa de caída debido a este problema puede afectar al servicio y puede requerir la atención del operador de red. Tenga en cuenta que estos mensajes notificados en los syslogs se limitan a la velocidad a intervalos de 30 segundos, por lo que un solo mensaje de registro no siempre indica que sólo se descartó un paquete. Para obtener un conteo preciso de estas caídas, ejecute el comando **show crypto ipsec sa detail**, y observe la SA junto al ID de conexión visto en los registros. Entre los contadores SA, el contador de errores **pkts verify failed** explica la pérdida total de paquetes debido a la falla de verificación del código de autenticación de mensajes (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
```

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información en este documento se basa en las pruebas realizadas con Cisco IOS ® versión 15.1(4)M4. Aunque aún no se ha probado, los scripts y la configuración deben funcionar con versiones anteriores del software del IOS de Cisco, ya que ambos applets utilizan la versión 3.0 de EEM (que se admite en la versión 12.4(22)T o posterior del IOS).

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Información sobre la Función

El "%CRYPTO-4-RECVD_PKT_MAC_ERR: descifrar:" implica que se recibió un paquete cifrado que falló la verificación MAC. Esta verificación es el resultado del conjunto de transformación de autenticación configurado:

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

En el ejemplo anterior, *"esp-aes 256"* define el algoritmo de cifrado como AES de 256 bits, y *"esp-md5"* define el MD5 (variante HMAC) como el algoritmo hash utilizado para la autenticación. Los algoritmos hash como MD5 se utilizan normalmente para proporcionar una huella digital del contenido de un archivo. La huella digital se utiliza a menudo para garantizar que el archivo no ha sido alterado por un intruso o virus. Por lo tanto, la aparición de este mensaje de error generalmente implica:

- La clave incorrecta se utilizó para cifrar o descifrar el paquete. Este error es muy raro y podría ser causado por un error de software.

-O-

- El paquete fue manipulado durante el tránsito. Este error puede deberse a un circuito sucio o a un evento hostil.

Metodología de solución de problemas

Dado que este mensaje de error suele estar causado por la corrupción de paquetes, la única manera de hacer un análisis de la causa raíz es utilizar EPC para obtener capturas de paquetes completas del lado de la WAN en ambos puntos finales del túnel y compararlas. Antes de obtener las capturas, es mejor identificar qué tipo de tráfico desencadena estos registros. En algunos casos, puede ser un tipo específico de tráfico; en otros casos, puede ser aleatorio pero fácilmente reproducido (como 5-7 caídas cada 100 pings). En esas situaciones, la cuestión resulta ligeramente más fácil de identificar. La mejor manera de identificar el disparador es marcar el tráfico de prueba con las marcas DSCP y capturar los paquetes. El valor DSCP se copia en el encabezado ESP y luego se puede filtrar con Wireshark. Esta configuración, que asume una prueba con 100 pings, se puede utilizar para marcar los paquetes 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
```

Esta política debe aplicarse ahora a la interfaz de ingreso donde se recibe el tráfico despejado en el router de cifrado:

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

Alternativamente, puede que desee ejecutar esta prueba con tráfico generado por el router. Para ello, no puede utilizar la calidad del servicio (QoS) para marcar los paquetes, pero puede utilizar el routing basado en políticas (PBR).

Nota: Para localizar las marcas DSCP críticas (5), utilice el 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
```

Una vez que se haya configurado la marcación de QoS para el tráfico ICMP, puede configurar la captura de paquetes integrada:

```
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: esta función se introdujo en Cisco IOS Release 12.4(20)T. Refiérase a Captura de Paquetes Incrustados para obtener más información con respecto a los EPC.

El uso de una captura de paquetes para resolver este tipo de problema requiere que se capture todo el paquete, no sólo una parte de él. La función EPC en las versiones de Cisco IOS anteriores a 15.0(1)M tiene un límite de búfer de 512K y un límite máximo de tamaño de paquete de 1024 bytes. Para evitar esta limitación, actualice a 15.0(1)M o código más nuevo, que ahora admite un tamaño de búfer de captura de 100M con un tamaño máximo de paquete de 9500 bytes.

Si el problema se puede reproducir de forma fiable con cada ping de conteo 100, el peor de los escenarios es programar una ventana de mantenimiento para permitir solamente el tráfico ping como prueba controlada y tomar las capturas. Este proceso debe tardar unos minutos, pero sí interrumpe el tráfico de producción durante ese tiempo. Si utiliza la marcación de QoS, puede eliminar el requisito de restringir paquetes solamente a pings. Para capturar todos los paquetes ping en un buffer, debe asegurarse de que la prueba no se realice durante las horas pico.

Si el problema no se reproduce fácilmente, puede utilizar un script EEM para automatizar la captura de paquetes. La teoría es que se inician las capturas en ambos lados en un búfer circular y se utiliza EEM para detener la captura en un lado. Al mismo tiempo que el EEM detiene la captura, haga que envíe una trampa snmp al par, que detiene su captura. Este proceso podría funcionar. Pero si la carga es pesada, es posible que el segundo router no reaccione lo

suficientemente rápido como para detener su captura. Se prefiere una prueba controlada. Estos son los scripts EEM que implementarán el proceso:

```
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!"
```

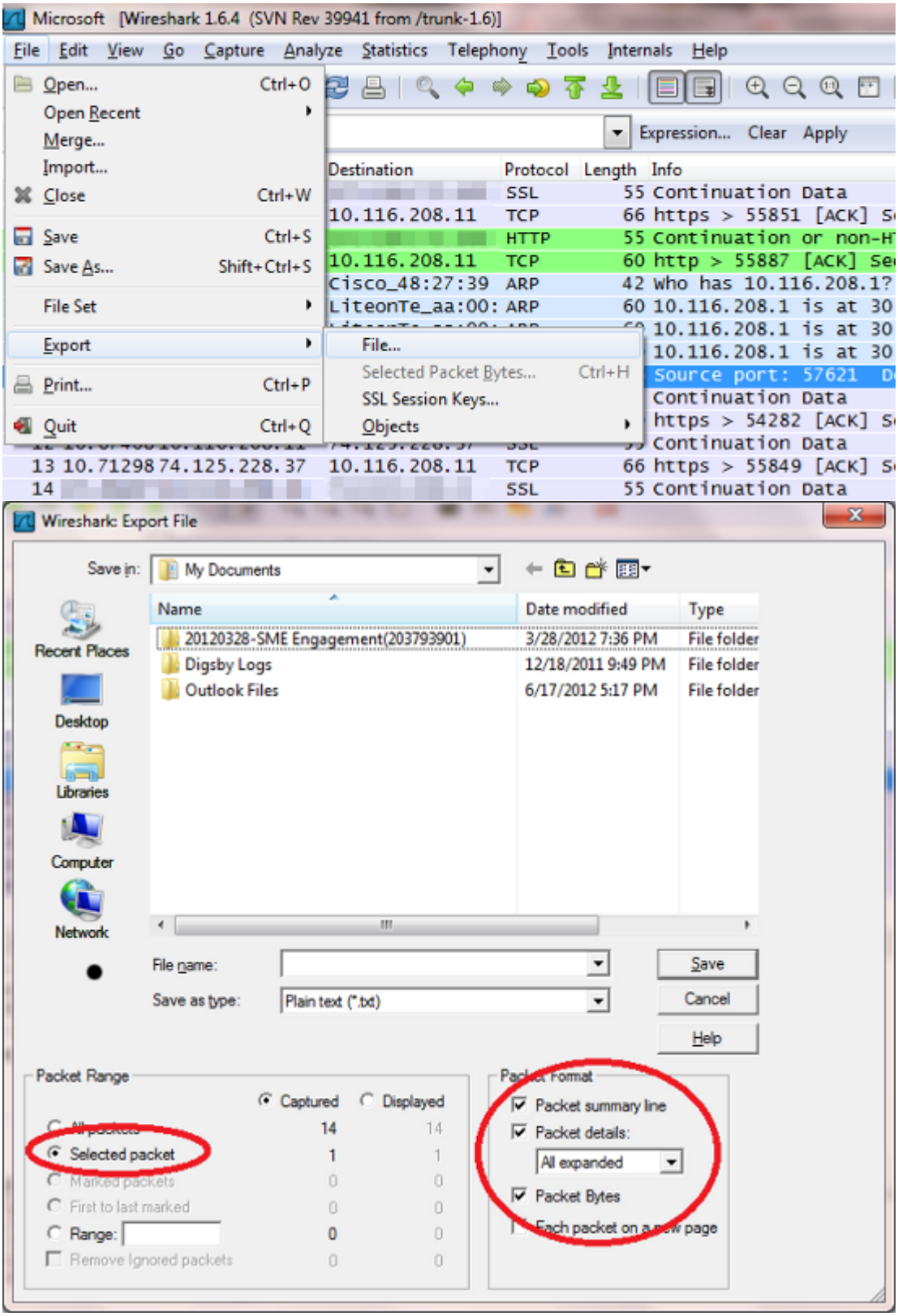
Tenga en cuenta que el código del cuadro anterior es una configuración probada con 15.0(1)M. Es posible que desee probarlo con la versión específica de Cisco IOS que utiliza su cliente antes de implementarlo en el entorno del cliente.

Análisis de datos

1. Una vez que se han completado las capturas, utilice TFTP para exportarlas a un PC.
2. Abra las capturas con un analizador de protocolo de red (como Wireshark).
3. Si se usó la marcación de QoS, filtre los paquetes respectivos.

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

   "0x08" es específico para el valor DSCP AF21. Si se utiliza un valor DSCP diferente, se puede obtener el valor correcto de la captura del paquete en sí o de la lista del gráfico de conversión de valores DSCP. Refiérase a Valores de Precedencia y DSCP para obtener más información.
4. Identifique el ping descartado en las capturas del remitente y localice ese paquete en las capturas tanto en el lado del receptor como en el del remitente.
5. Exporte ese paquete de ambas capturas como se muestra en esta imagen:



6. Realice una comparación binaria de los dos. Si son idénticos, entonces no hubo errores en el tránsito y el IOS de Cisco lanzó un falso negativo en el extremo receptor o utilizó la clave incorrecta en el extremo del remitente. En cualquier caso, el problema es un error de funcionamiento de Cisco IOS. Si los paquetes son diferentes, entonces los paquetes fueron manipulados en la transmisión.

   Este es el paquete cuando dejó el motor de criptografía en el 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.[!.
```

Este es el mismo paquete que se recibió en el par:

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

En este punto, es muy probable que se trate de un problema ISP, y ese grupo debería participar en la resolución de problemas.

Problemas Comunes

- El Id. de error de Cisco CSCed87408 describe un problema de hardware con el motor crypto en las 83xs donde los paquetes salientes aleatorios se corrompen durante el cifrado, lo que conduce a errores de autenticación (en los casos en que se utiliza la autenticación) y caídas de paquetes en el extremo receptor. Es importante darse cuenta de que no verá estos errores en el propio 83x, sino en el dispositivo receptor.

- A veces, los routers que ejecutan código antiguo muestran este error. Puede actualizar a las versiones de código más recientes, como 15.1(4) M4, para resolver el problema.

- Para verificar si el problema es un problema de hardware o software, inhabilite el cifrado de hardware. Si los mensajes de registro continúan, se trata de un problema de software. Si no, un RMA debería resolver el problema.
  Recuerde que si desactiva el cifrado de hardware, puede causar una degradación grave de la red para túneles VPN muy cargados. Por lo tanto, Cisco recomienda que intente los procedimientos descritos en este documento durante una ventana de mantenimiento.

Información Relacionada

- Soporte Técnico y Documentación - Cisco Systems