Mensaje de error del Syslog el "%CRYPTO-4-RECVD_PKT_MAC_ERR:" con la pérdida del ping sobre el troubleshooting del túnel IPsec

Contenido

Introducción

Este documento describe cómo resolver la pérdida del ping sobre un túnel IPsec juntado con los mensajes del "%CRYPTO-4-RECVD_PKT_MAC_ERR" en el Syslog tal y como se muestra en del 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 tales descensos se considera normal. Sin embargo, una alta tarifa del descenso debido a este problema puede afectar el servicio y pudo requerir la atención del operador de la red. Observe que estos mensajes señalados en los Syslog son tarifa limitada en 30 segundos intervalos, así que un solo mensaje del registro no indica siempre que solamente un solo paquete conseguido cayó. Para obtener una cuenta exacta de estos descensos, publique el comando show crypto ipsec sa detail, y la mirada en el SA al lado del ID de conexión visto en los registros. Entre los contadores SA, el **pkts verifica al** contador de errores **fallado** explica el descenso del total de paquetes debido a la falla de verificación del código de autenticación de mensaje (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
```

Prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

La información en este documento se basa en las pruebas hechas con la versión 15.1(4)M4 del ® del Cisco IOS. Aunque no todavía estén probados, los scripts y la configuración deban trabajar con versiones del Cisco IOS Software anteriores también puesto que ambos applet utilizan el 3.0 de la versión EEM (que se soporta en la versión de IOS 12.4(22)T o arriba).

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Información sobre la Función

El “%CRYPTO-4-RECVD_PKT_MAC_ERR: decrypt: ” implica que un paquete encriptado fue recibido que falló la verificación MAC. Esta verificación es un resultado de la autenticación transforma el conjunto configurado:

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

En el ejemplo antedicho, el *“ESP-aes el 256"* define el algoritmo de encripción como 256-bit AES, y el *"esp-md5"* define el MD5 (variante HMAC) como el algoritmo de troceo usado para la autenticación. Los algoritmos de troceo como el MD5 se utilizan típicamente para proporcionar una huella dactilar digital del contenido de un archivo. La huella dactilar digitial es de uso frecuente asegurarse de que el archivo no ha sido alterado por un intruso o un virus. Así el acontecimiento de este mensaje de error implica generalmente cualquiera:

- La clave incorrecta fue utilizada para cifrar o para desencriptar el paquete. Este error es muy raro y se podría causar por un bug de software.

- O

- El paquete fue tratado de forzar con durante transita. Este error podía ser debido a un circuito sucio o a un evento hostil.

Metodología de Troubleshooting

Puesto que este mensaje de error es causado típicamente por el daño del paquete, la única forma de hacer una análisis de la causa raíz es utilizar el EPC para obtener a las capturas de paquetes completas del lado de WAN en ambos puntos extremos del túnel y compararlos. Antes de que usted obtenga las capturas, es el mejor identificar qué clase de tráfico acciona estos registros. En algunos casos, puede ser una clase específica de tráfico; en otros casos, puede ser que sea al azar pero se reprodujo fácilmente (por ejemplo 5-7 cae cada 100 ping). En tales situaciones, el problema llega a ser levemente más fácil de identificar. La mejor manera de identificar el activador es marcar el tráfico de prueba con las marcas DSCP y capturar los paquetes. El valor DSCP se copia al encabezado ESP y se puede entonces filtrar con Wireshark. Esta configuración, que asume una prueba con 100 ping, 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 directiva se debe ahora aplicar a la interfaz de ingreso donde el tráfico claro se recibe en el router de encripción:

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

Alternativamente, usted puede ser que quiera funcionar con esta prueba con el tráfico router-generado. Para esto, usted no puede utilizar el Calidad de Servicio (QoS) para marcar los paquetes, sino que usted puede (PBR) del Use Policy-Based Routing.

> Nota: Para localizar (5) las marcas críticas DSCP, utilice el **== 0x28 del** filtro **ip.dsfield.dscp de** Wireshark.

```
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 la marca de QoS se configura para su tráfico ICMP, usted puede configurar a la captura de paquetes integrada:

```
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"
```

Nota: esta característica fue introducida en el Cisco IOS Release 12.4(20)T. Refiera a la captura de paquetes integrada para más información con respecto a EPCs.

El uso de una captura de paquetes de resolver problemas este tipo de problema requiere que el paquete entero esté capturado, no apenas una porción de él. La característica del EPC en las versiones del Cisco IOS antes del 15.0(1)M tiene un límite de búfer de 512K y un límite máximo del tamaño de paquetes de 1024 bytes. Para evitar esta limitación, la actualización hasta el 15.0(1)M o un más nuevo código, que ahora soporta un tamaño de almacén intermedio de la captura del 100M con un tamaño de paquetes máximo de 9500 bytes.

Si el problema se puede reproducir confiablemente con cada ping de 100 cuentas, el escenario de caso peor es programar una ventana de mantenimiento para permitir solamente el tráfico de ping como prueba controlada y tomar las capturas. Este proceso debe tardar solamente algunos minutos, pero interrumpe el tráfico de producción por ese tiempo. Si usted utiliza la marca de QoS, usted puede eliminar el requisito de restringir los paquetes solamente a los ping. Para capturar todos los paquetes ping en un buffer, usted debe asegurarse de que la prueba no está conducida durante las horas pico.

Si el problema no se reproduce fácilmente, usted puede utilizar un script EEM para automatizar a la captura de paquetes. La teoría es que usted comienza las capturas en los ambos lados en un buffer circular y utiliza EEM para parar la captura en un lado. Al mismo tiempo el EEM para la captura, hace que envíe un desvío SNMP al par, que para su captura. Este proceso pudo trabajar. Pero si la carga es pesada, el segundo router no pudo reaccionar rápidamente bastante para parar su captura. Se prefiere una prueba controlada. Aquí están 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!"
```

Observe que el código en el cuadro anterior es una configuración probada con el 15.0(1)M. Usted puede ser que quiera probarlo con la versión deL Cisco IOS específica sus aplicaciones del cliente antes de que usted la implemente en el entorno del cliente.

Análisis de datos

1. Las capturas se han completado, utilizan una vez el TFTP para exportarlas a un PC.
2. Abra las capturas con un analizador del Network Protocol (tal como Wireshark).
3. Si la marca de QoS fue utilizada, filtre hacia fuera los paquetes respectivos.
   `ip.dsfield.dscp==0x08`
   el "0x08" es específico para el valor AF21 DSCP. Si se utiliza un diverso valor DSCP, el valor correcto se puede obtener de la captura de paquetes sí mismo o de la lista de gráfico de conversión de los valores DSCP. Refiera al DSCP y a los valores de precedencia para más información.
4. Identifique el ping caído en las capturas del remitente, y localícelo que echa a un lado el paquete en las capturas en el lado de la recepción y el remitente.
5. Exporte ese paquete de ambas capturas tal y como se muestra en de esta imagen:
6. Conduzca una comparación binaria de los dos. Si son idénticos, después no había errores adentro transita y el Cisco IOS lanzó una negativa falsa en el extremo receptor o utilizó la clave incorrecta en el extremo del remitente. En ambos casos, el problema es un bug del Cisco IOS. Si los paquetes son diferentes, después los paquetes fueron tratados de forzar con adentro transmiten.

   Aquí está el paquete como él 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.[!.
```

   Aquí está el mismo paquete que fue recibido 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 momento, es más probable un problema ISP, y ese grupo debe estar implicado en el

troubleshooting.

Problemas Comunes

- El Id. de bug Cisco CSCed87408 describe los problemas del hardware con el motor de criptografía en el 83xs donde los paquetes de salida al azar se corrompen durante el cifrado, que lleva a los errores de autenticación (en caso de que se utiliza la autenticación) y las caídas de paquetes en el extremo receptor. Es importante realizar que usted no verá estos errores en el 83x sí mismo, pero en el dispositivo receptor.

- A veces Routers que ejecuta la vieja demostración del código este error. Usted puede actualizar a las más versiones del código reciente tales como 15.1(4) M4 para resolver el problema.

- Para verificar si el problema es un problema de hardware o de software, inhabilite la encripción por hardware. Si los mensajes del registro continúan, es un problema de software. Si no, entonces un RMA debe resolver el problema.
  Recuerde que si usted inhabilita la encripción por hardware, puede causar la degradación severa de la red para los túneles pesadamente cargados VPN. Por lo tanto, Cisco le recomienda tentativa que los procedimientos describieron en este documento durante una ventana de mantenimiento.

Información Relacionada

- Soporte Técnico y Documentación - Cisco Systems