Solución de problemas de paquetes malformados HTTP que se filtran y descartan por ECS en Cisco PGW

Contenido

Introducción

Este documento describe cómo resolver problemas de paquetes HTTP mal formados que son filtrados y descartados por el servicio de carga mejorada (ECS) en Cisco Packet Data Network Gateway (PGW).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- StarOS
- ECS

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

La información de este documento es similar a la configuración presente en el nodo del cliente, pero aquí sólo se muestra la información relevante. Con el fin de demostrar los rastros problemáticos sin exponer información real, he cambiado o marcado alguna información, es decir, direcciones IP.

Problema

El proveedor de servicios se quejó de que algunos de los usuarios de su red no podían acceder a sitios específicos de juegos.

Cuando se verificaron los rastros de dichos usuarios, se descubrió que el tráfico problemático se categorizó bajo definición de regla (regla) definida para filtrar los paquetes de error HTTP en PGW.

```
active-charging service <name>
ruledef <name>
http error = TRUE
#exit
#exit
```

Troubleshoot

¿Qué es la regla?

La detección del tráfico HTTP de los suscriptores se logra mediante los analizadores de protocolo que están presentes en ECS.

ECS tiene analizadores de protocolo que examinan el tráfico de link ascendente y descendente. El tráfico entrante entra en un analizador de protocolo para la inspección de paquetes. Las reglas de ruteo se aplican para determinar qué paquetes inspeccionar. Este tráfico se envía luego al motor de carga donde se aplican los parámetros de reglas de carga para realizar acciones como bloquear, redirigir o transmitir. Estos analizadores también generan registros de uso para el sistema de facturación.

Las reglas son expresiones definidas por el usuario basadas en campos de protocolo y estados de protocolo, que definen qué acciones tomar en los paquetes cuando los valores de campo especificados coinciden.

Las reglas que se utilizan principalmente en un documento de solución de problemas son:

Rutas de ruteo: las reglas de ruteo se utilizan para rutear paquetes a analizadores de contenido. Las reglas de ruteo determinan a qué analizador de contenido rutear el paquete cuando los campos de protocolo y/o los estados de protocolo en la expresión ruledef son verdaderos. Se pueden configurar hasta 256 valores de reglas para el ruteo.

Normas de carga: las reglas de carga se utilizan para especificar qué acción se debe realizar en función del análisis realizado por los analizadores de contenido. Las acciones pueden incluir redirección, valor de cargo y emisión de registro de facturación.

Configuración de laboratorio

La configuración de ejemplo para probar este escenario en PGW:

```
config
 active-charging service

ruledef http-error
 http error = TRUE
 #exit
```

```
 ruledef ip_any
 ip any-match = TRUE
 #exit

 charging-action block
 content-id 501
 billing-action egcdr
 flow action terminate-flow
 #exit

 charging-action ip-any-ca
 content-id 1
 billing-action egcdr
 #exit

 rulebase rulebase_all
 billing-records egcdr
 action priority 10 ruledef http-error charging-action block desc http-error_ruledef
 action priority 100 ruledef ip_any charging-action ip-any-ca desc ca_ruledef
 flow control-handshaking charge-to-application all-packets
 < some lines removed >
 #exit
 #exit
end
```

Registros de errores

El seguimiento problemático del suscriptor se utilizó para volver a generar la réplica exacta del tráfico HTTP. Cuando se ejecutó el seguimiento con la configuración anterior, estos valores predeterminados de regla se detectaron bajo el motor ECS.

```
[local]spgw# show active-charging ruledef statistics all charging

Ruledef Name Packets-Down Bytes-Down Packets-Up Bytes-Up Hits Match-Bypassed
------------ ------------ ---------- ---------- -------- ---- --------------
ip_any 170 81917 207 34362 332 304
http-error 3 180 7 412 1 0

Total Ruledef(s) : 2
```

Esto dice que hay algunos paquetes enviados por UE que no son paquetes HTTP adecuados y que están categorizados bajo la regla "http-error" que está presente en la configuración.

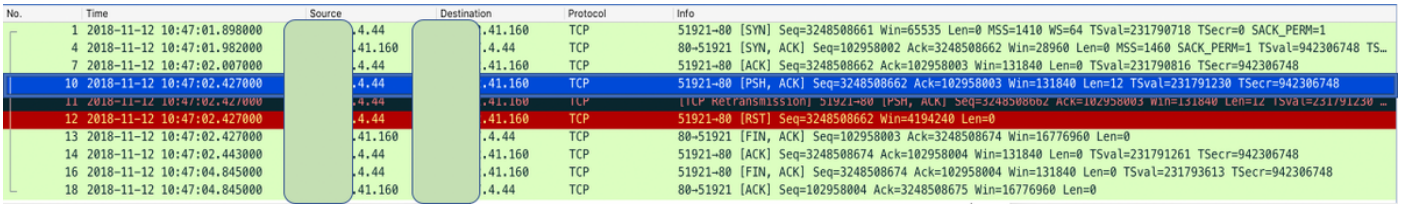
Después de verificar los registros en el sistema, puede ver que los registros se imprimen como un mensaje de "paquete HTTP no válido" visto allí. Verifique el mensaje en estos registros:

```
2018-Nov-14+05:46:50.474 [acsmgr 91654 unusual]
[1/0/17758


2018-Nov-14+05:46:50.474 [acsmgr 91025 trace]
[1/0/17758


2018-Nov-14+05:46:50.474 [acsmgr 91209 debug]
[1/0/17758
```

De acuerdo con la definición presente en el nodo, la regla "http-error" tiene la acción de carga asignada como "bloque" que coincide con estos registros. Debido a esto, el suscriptor final no pudo acceder al sitio web ya que los paquetes fueron terminados (flujo de finalización de la acción de flujo) en el motor ECS de PGW.

Solución

Después de convertir el archivo de seguimiento del suscriptor en el archivo pcap, verá que estos mensajes se intercambian entre el cliente (suscriptor final) y el servidor.



No.	Time	Source	Destination	Protocol	Info
1	2018-11-12 10:47:01.898000	.4.44	.41.160	TCP	51921→80 [SYN] Seq=3248508661 Win=65535 Len=0 MSS=1410 WS=64 TSval=231790718 TSecr=0 SACK_PERM=1
4	2018-11-12 10:47:01.982000	.41.160	.4.44	TCP	80→51921 [SYN, ACK] Seq=102958002 Ack=3248508662 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=942306748 TS…
7	2018-11-12 10:47:02.007000	.4.44	.41.160	TCP	51921→80 [ACK] Seq=3248508662 Ack=102958003 Win=131840 Len=0 TSval=231790816 TSecr=942306748
10	2018-11-12 10:47:02.427000	.4.44	.41.160	TCP	51921→80 [PSH, ACK] Seq=3248508662 Ack=102958003 Win=131840 Len=12 TSval=231791230 TSecr=942306748
11	2018-11-12 10:47:02.427000	.4.44	.41.160	TCP	[TCP Retransmission] 51921→80 [PSH, ACK] Seq=3248508662 Ack=102958003 Win=131840 Len=12 TSval=231791230 …
12	2018-11-12 10:47:02.427000	.4.44	.41.160	TCP	51921→80 [RST] Seq=3248508662 Win=4194240 Len=0
13	2018-11-12 10:47:02.427000	.41.160	.4.44	TCP	80→51921 [FIN, ACK] Seq=102958003 Ack=3248508674 Win=16776960 Len=0
14	2018-11-12 10:47:02.443000	.4.44	.41.160	TCP	51921→80 [ACK] Seq=3248508674 Ack=102958004 Win=131840 Len=0 TSval=231791261 TSecr=942306748
16	2018-11-12 10:47:04.845000	.4.44	.41.160	TCP	51921→80 [FIN, ACK] Seq=3248508674 Ack=102958004 Win=131840 Len=0 TSval=231793613 TSecr=942306748
18	2018-11-12 10:47:04.845000	.41.160	.4.44	TCP	80→51921 [ACK] Seq=102958004 Ack=3248508675 Win=16776960 Len=0

Según el flujo de llamada HTTP, el cliente debe enviar la solicitud HTTP-GET/POST al servidor y solicitar acceso una vez que se haya intercambiado el SYN TCP (se ve que en el paquete no 1, 4 y 7).

Sin embargo, en el archivo pcap, no se ve ningún tráfico HTTP dentro de él. Por lo tanto, el paquete TCP que transporta la señalización o carga HTTP causa este problema.

Si marca, el tamaño de la ventana TCP permitido según RFC (rfc-1323) debe ser 65536 (2*16=65536) bytes de largo.

El encabezado TCP utiliza un campo de 16 bits para informar el tamaño de la ventana de recepción al remitente. Por lo tanto, la ventana más grande que se puede utilizar es 2**16 = 65K bytes.

Si ve el paquete 7 WS, es demasiado grande para ser de un paquete de reconocimiento (ACK). Normalmente, con el análisis HTTP activado, el GGSN intenta analizar los mensajes HTTP GET/POST. Cuando los flujos HTTP no son conformes con RFC, puede dar lugar a errores de análisis (y fallas para clasificar correctamente el flujo HTTP según la URL, etc.).

Como se sospechaba, después del paquete ACK (paquete 7), el cliente no envió la solicitud HTTP-GET/POST al servidor para solicitar acceso. En su lugar, "PSH,ACK" se envía desde la UE. Esto no se esperaba en el motor PGW ECS. UE estaba enviando la carga útil de http (con el puerto más bajo 80) dentro de los paquetes TCP, debido a qué gateway terminó ese flujo de paquetes ya que se filtró y coincidió en la regla "http-error" que tiene acción como "end-flow". Para PGW, el mensaje esperado de UE habría sido HTTP-GET/POST que no se vio. Por lo tanto, consideró al paquete 10 como un paquete mal formado.

Para verificar más la duda, el archivo de seguimiento pcap se modifica cuando se elimina el número de paquete problemático 10 que tiene PSH-ACK, y la misma llamada se vuelve a ejecutar, donde la regla problemática "http-error" no se vuelve a pegar bajo carga activa. Todos los paquetes se clasificaron en la regla "ip_any". Eso dice que el paquete malformado fue el paquete 10.

Consulte el ejemplo de salida:

```
[local]spgw# show active-charging ruledef statistics all charging

Ruledef Name Packets-Down Bytes-Down Packets-Up Bytes-Up Hits Match-Bypassed
------------ ------------ ---------- ---------- -------- ---- --------------
ip_any 5 260 11 596 7 0
http-error 0 0 0 0 0 0

Total Ruledef(s) : 2
```

Para resumir esto:

En lugar del paquete HTTP con la solicitud **GET/POST**, UE envió el paquete TCP PSH-ACK que se consideró como un paquete mal formado y se descartó porque no era el esperado. Se informó al proveedor de servicios de este comportamiento inadecuado de los UE específicos. Cisco PGW funciona según los estándares 3GPP.