對Cisco PGW中ECS過濾和丟棄的HTTP格式錯誤資料包進行故障排除

目錄

簡介

本檔案介紹如何對思科封包資料網路閘道(PGW)中增強型計費服務(ECS)過濾和捨棄的HTTP錯誤封包進行疑難排解。

必要條件

需求

思科建議您瞭解以下主題：

- StarOS
- ECS

採用元件

本文件所述內容不限於特定軟體和硬體版本。

本文檔中的資訊與客戶節點中存在的配置類似，但此處只顯示相關資訊。為了在不暴露真實資訊的情況下演示有問題的跟蹤，我更改或刪除了一些資訊，即IP地址。

問題

服務供應商抱怨說，他們網路中的某些使用者無法訪問特定的遊戲站點。

檢查此類使用者的跟蹤後，發現問題流量根據規則定義(ruledef)進行分類，該定義是為了過濾PGW中的HTTP錯誤資料包。

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

疑難排解

什麼是ruledef?

使用者HTTP流量的檢測通過ECS中存在的協定分析器來實現。

ECS具有檢查上行鏈路和下行鏈路流量的協定分析器。傳入流量進入協定分析器以進行資料包檢測。應用路由規則定義以確定要檢查的資料包。然後，此流量將傳送到計費引擎，在該引擎中應用計費規則定義，以便執行阻止、重定向或傳輸等操作。這些分析器還會生成計費系統的使用記錄。

Ruledefs是基於協定欄位和協定狀態的使用者定義表達式，它定義了在指定欄位值匹配時對資料包執行的操作。

故障排除文檔中最常用的規則定義有：

Routing Ruledefs — 路由ruledefs用於將資料包路由到內容分析器。路由ruledef確定當ruledef表達式中的協定欄位和/或協定狀態為真時要將資料包路由到的內容分析器。最多可配置256個ruledefs用於路由。

Charging Ruledefs — 計費ruledefs用於根據內容分析器進行的分析指定要執行的操作。操作可能包括重定向、計費值和計費記錄傳送。

實驗室設定

在PGW中測試此方案的示例配置：

```
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
```

錯誤日誌

使用者有問題的跟蹤用於重新生成HTTP流量的精確副本。使用以前的配置運行跟蹤時，在ECS引擎下檢測到這些ruledefs。

```
[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
```

這表示，UE傳送的一些資料包不是正確的HTTP資料包，這些資料包在配置中存在的「http-error」規則定義下分類。

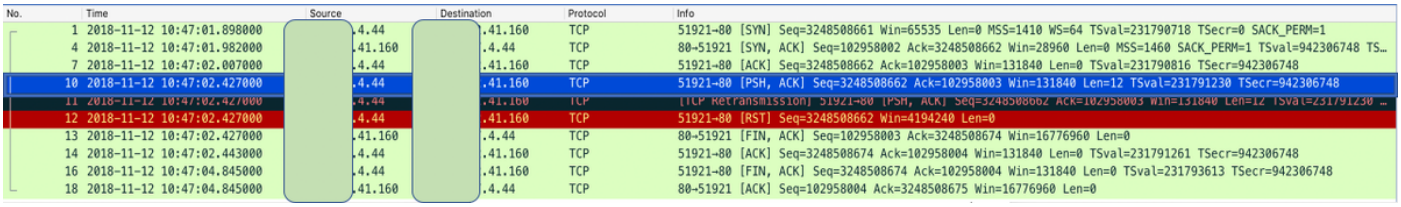
在檢查系統中的日誌之後，可以看到日誌被列印為「HTTP資料包無效」消息。檢查這些日誌中的消息：

```
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
```

根據節點中存在的定義，ruledef "http-error"將計費操作對映為與這些日誌匹配的「block」。因此，終端使用者無法訪問該網站，因為PGW的ECS引擎中的資料包已終止(flow action terminate-flow)。

解決方案

將使用者跟蹤檔案轉換為pcap檔案後，您會看到這些消息在客戶端（終端使用者）和伺服器之間交換。



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

根據HTTP呼叫流，客戶端應傳送HTTP-GET/POST請求到伺服器，並在交換TCP SYN（您在第1、4和7號資料包中看到）後請求訪問。

但是，在pcap檔案中，您看不到其中的任何HTTP流量。因此，承載HTTP訊號或負載的TCP封包會導致此問題。

如果勾選，則根據RFC(rfc-1323)允許的TCP視窗大小應為65536(2*16=65536)位元組。

TCP標頭使用16位元欄位將接收視窗大小報告給傳送者。因此，可以使用的最大視窗為2**16 = 65K位元組。

如果您看到封包7 WS，該封包過大，無法成為確認(ACK)封包。通常，啟用HTTP分析後，GGSN會嘗試分析GET/POST HTTP消息。當HTTP流不符合RFC時，可能會導致解析錯誤（和失敗，以便根據URL正確分類HTTP流等）。

正如所懷疑的那樣，在ACK資料包（資料包7）之後，客戶端未向伺服器傳送HTTP-GET/POST請求以請求訪問。而是從UE傳送「PSH，ACK」。PGW ECS引擎沒有預料到這一點。UE在TCP資料包內傳送http（目標埠80）的負載，因為哪個網關在過濾資料包流並根據「http-error」ruledef（其操作為「terminate-flow」）進行匹配時終止該資料包。 對於PGW，來自UE的預期消息將是HTTP-GET/POST，而未看到。因此，它將資料包10視為格式錯誤的資料包。

為了進一步驗證疑問，當刪除具有PSH-ACK的有問題的資料包編號10，並且再次運行相同的呼叫時，修改了pcap跟蹤檔案，其中有問題的「http-error」 ruledef在活動充電下不再命中。所有資料包都歸類為「ip_any」 ruledef。表示格式錯誤的資料包是資料包10。

請參閱輸出範例：

```
[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
```

為了概括這一點：

UE不是通過**GET/POST**請求傳送HTTP資料包，而是傳送了TCP PSH-ACK資料包，該資料包被視為格式錯誤資料包，由於不是預期資料包，因此被丟棄。服務提供商已被告知特定UE的這種不當行為。Cisco PGW按照3GPP標準工作。