排除Cisco PGW中ECS过滤和丢弃的HTTP格式错误的数据包故障

目录

[简介](#)
[先决条件](#)
[要求](#)
[使用的组件](#)
[问题](#)
[故障排除](#)
[规则定义是什么？](#)
[实验设置](#)
[错误日志](#)
[解决方案](#)

简介

本文档介绍如何对思科数据包数据网络网关(PGW)中的增强型计费服务(ECS)过滤和丢弃的HTTP格式错误的数据包进行故障排除。

先决条件

要求

Cisco 建议您了解以下主题：

- StarOS
- ECS

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息类似于客户节点中的配置，但此处仅显示相关信息。为了演示有问题的跟踪而不暴露真实信息，我更改或删除了一些信息，即IP地址。

问题

服务提供商抱怨其网络中的某些用户无法访问特定游戏站点。

当检查此类用户的跟踪时，发现问题流量是根据为过滤PGW中的HTTP错误数据包而定义的规则定义(ruledef)进行分类的。

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

故障排除

规则定义是什么？

用户的HTTP流量检测由ECS中的协议分析器实现。

ECS具有协议分析器，可检查上行链路和下行链路流量。传入流量进入协议分析器进行数据包检测。应用路由规则定义以确定要检查的数据包。然后，该流量被发送到计费引擎，在该计费引擎中应用计费规则定义，以执行诸如块、重定向或传输等操作。这些分析器还生成计费系统的使用记录。

规则默认是基于协议字段和协议状态的用户定义的表达式，定义当指定字段值匹配时对数据包执行的操作。

故障排除文档中最常用的规则定义如下：

路由规则定义 — 路由规则定义用于将数据包路由到内容分析器。当ruledef表达式中的协议字段和/或协议状态为true时，路由规则定义确定将数据包路由到哪个内容分析器。最多可为路由配置256个规则默认。

计费规则定义 — 计费规则定义用于根据内容分析器所做的分析指定要执行的操作。操作可包括重定向、计费值和计费记录发放。

实验设置

在PGW中测试此场景的示例配置：

```
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
```

错误日志

用户有问题的跟踪用于重新生成HTTP流量的精确副本。当使用之前的配置运行跟踪时，在ECS引擎下检测到这些规则默认。

```
[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
```

这表示，UE发送的一些数据包不是正确的HTTP数据包，这些数据包在配置中的“http-error”规则def下分类。

检查系统中的日志后，您可以看到日志被打印为“HTTP数据包无效”消息。检查以下日志中的消息：

```
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
```

根据节点中的定义，规则def“http-error”将计费操作映射为与这些日志匹配的“块”。因此，在PGW的ECS引擎中终止数据包（流操作terminate-flow）时，最终用户无法访问网站。

解决方案

将用户跟踪文件转换为pcap文件后，您会看到客户端（最终用户）和服务器之间交换了这些消息。

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

根据HTTP呼叫流，客户端应向服务器发送HTTP-GET/POST请求，并在TCP SYN交换后请求访问

（在数据包1、4和7中，您看到）。

但是，在pcap文件中，您看不到其内的任何HTTP流量。因此，传输HTTP信令或负载的TCP数据包会导致此问题。

如果您检查，根据RFC(rfc-1323)允许的TCP窗口大小应为65536(2*16=65536)字节长。

TCP报头使用16位字段向发送方报告接收窗口大小。因此，可使用的最大窗口为2**16 = 65K字节。

如果您看到数据包7 WS，它太大，无法发出确认(ACK)数据包。通常，在启用HTTP分析时，GGSN会尝试解析GET/POST HTTP消息。当HTTP流不符合RFC时，可能会导致解析错误（以及失败，以便根据URL对HTTP流进行正确分类等）。

如怀疑的那样，在ACK数据包（数据包7）之后，客户端未向服务器发送HTTP-GET/POST请求以请求访问。相反，“PSH，ACK”从UE发送。PGW ECS引擎并不预期。UE在TCP数据包内发送http（目的端口为80）的负载，因为在“http-error”规则def下过滤和匹配该数据包流时，该网关终止了该数据包流，其操作为“terminate-flow”。 对于PGW，UE的预期消息应该是HTTP-GET/POST，但是未看到。因此，它将数据包10视为格式错误的数据包。

为了进一步验证疑问，当删除有问题的数据包编号10并重新运行具有PSH-ACK的同一呼叫时，会修改pcap跟踪文件，在活动计费下，有问题的“http-error”规则def不会再次命中。所有数据包都在“ip_any”规则def下分类。这表示格式错误的数据包是数据包10。

请参阅示例输出：

```
[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
```

为了总结以下内容：

UE发送的TCP PSH-ACK数据包被视为格式错误的数据包，因为它不是预期数据包，所以被丢弃，而不是带有**GET/POST请求的HTTP数据包。**服务提供商获知了特定UE的这种不当行为。Cisco PGW按照3GPP标准工作。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。