Solucionar problemas de pacotes HTTP malformados que são filtrados e descartados pelo ECS no Cisco PGW

Contents

Introduction

Este documento descreve como solucionar problemas de pacotes HTTP malformados que são filtrados e descartados pelo Serviço de Carregamento Avançado (ECS - Enhanced Charging Service) no Cisco Packet Data Network Gateway (PGW).

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- StarOS
- ECS

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

As informações neste documento são semelhantes à configuração presente no nó do cliente, mas somente as informações relevantes são mostradas aqui. Para demonstrar os traços problemáticos sem expor informações reais, mudei ou marcei algumas informações, ou seja, endereços IP.

Problema

Houve reclamações do provedor de serviços de que alguns dos usuários em suas redes não poderiam acessar sites de jogos específicos.

Quando os rastreamentos de tais usuários foram verificados, descobriu-se que o tráfego problemático era categorizado na definição de regra (ruledef) que foi definida para filtrar pacotes de erro HTTP no PGW.

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

Troubleshoot

O que é ruledef?

A detecção do tráfego HTTP dos assinantes é obtida por analisadores de protocolo presentes no ECS.

O ECS tem analisadores de protocolo que examinam o tráfego de uplink e downlink. O tráfego de entrada entra em um analisador de protocolo para inspeção de pacotes. As regras de roteamento são aplicadas para determinar quais pacotes inspecionar. Esse tráfego é então enviado para o mecanismo de cobrança onde as regras de cobrança são aplicadas para executar ações como bloquear, redirecionar ou transmitir. Esses analisadores também geram registros de uso para o sistema de cobrança.

Ruledefs são expressões definidas pelo usuário com base em campos de protocolo e estados de protocolo, que definem quais ações tomar em pacotes quando os valores de campo especificados correspondem.

As regras mais usadas em um documento de solução de problemas são:

Regras de roteamento - As regras de roteamento são usadas para rotear pacotes para os analisadores de conteúdo. As regras de roteamento determinam para qual analisador de conteúdo rotear o pacote quando os campos de protocolo e/ou estados de protocolo na expressão ruledef são verdadeiros. Até 256 regras podem ser configuradas para roteamento.

Regras de cobrança - Regras de cobrança são usadas para especificar que ação tomar com base na análise feita pelos analisadores de conteúdo. As ações podem incluir redirecionamento, valor de cobrança e emissão de registro de cobrança.

Configuração do laboratório

O exemplo de configuração para testar este cenário no 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
```

Logs de erro

O rastreamento problemático do assinante foi usado para gerar novamente a réplica exata do tráfego HTTP. Quando o rastreamento foi executado com a configuração anterior, essas regras foram detectadas no mecanismo 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
```

Isso diz que há alguns pacotes enviados pela UE que não são pacotes HTTP adequados e que são categorizados em "http-error" ruledef que está presente na configuração.

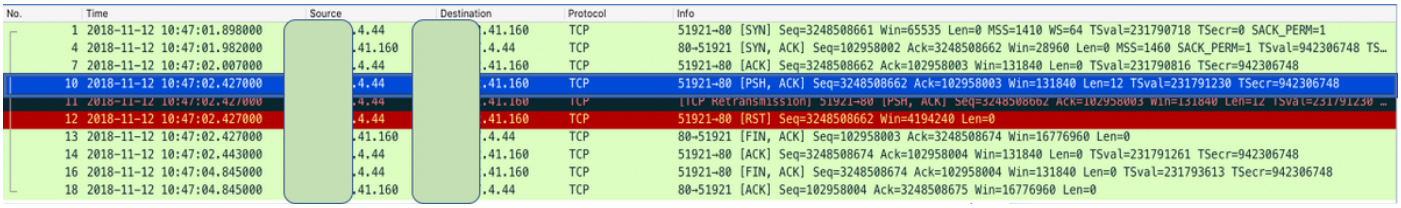
Depois de verificar os registros no sistema, você pode ver que os registros são impressos como uma mensagem "pacote HTTP inválido" exibida ali. Verifique a mensagem nestes registros:

```
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 acordo com a definição presente no nó, o "http-error" da régua tem a ação de cobrança mapeada como "bloco" que corresponde a esses logs. Devido a isso, o assinante final não pôde acessar o site, pois os pacotes foram terminados (fluxo de ação de fluxo - terminal) no mecanismo ECS da PGW.

Solução

Depois de converter o arquivo de rastreamento do assinante no arquivo pcap, você verá que essas mensagens são trocadas entre o cliente (assinante final) e o 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

De acordo com o fluxo de chamada HTTP, o cliente deve enviar a solicitação HTTP-GET/POST ao servidor e pedir acesso quando o TCP SYN (você vê que no pacote 1, 4 e 7) tiver sido trocado.

No entanto, no arquivo pcap, você não vê nenhum tráfego HTTP dentro dele. Portanto, o pacote TCP que transporta a sinalização ou payload HTTP causa esse problema.

Se você verificar, o tamanho da janela TCP permitido de acordo com RFC (rfc-1323) deve ter 65536 (2*16=65536) bytes de comprimento.

O cabeçalho TCP usa um campo de 16 bits para relatar o tamanho da janela de recebimento ao remetente. Portanto, a maior janela que pode ser usada é 2**16 = 65K bytes.

Se você vir o pacote 7 WS, ele é muito grande para ser um pacote de confirmação (ACK). Normalmente, com a análise HTTP ativada, o GGSN tenta analisar as mensagens HTTP GET/POST. Quando os fluxos HTTP não são compatíveis com RFC, isso pode resultar em erros de análise (e falhas para classificar corretamente o fluxo HTTP como por URL etc.).

Como suspeito, após o pacote ACK (pacote 7), o cliente não enviou a solicitação HTTP-GET/POST ao servidor para solicitar acesso. Em vez disso, "PSH,ACK" é enviado da UE. Isso não era esperado pelo mecanismo ECS da PGW. O UE estava enviando payload de http (com a porta 80 mais alta) dentro de pacotes TCP, por causa de qual gateway terminou esse fluxo de pacote quando ele foi filtrado e correspondeu em "http-error" ruledef que tem ação como "terminal-fluxo". Para PGW, a mensagem esperada de UE teria sido HTTP-GET/POST que não foi vista. Portanto, ele considerava o pacote 10 como um pacote malformado.

Para verificar mais a dúvida, o arquivo de rastreamento pcap é modificado quando o pacote problemático número 10 é removido com PSH-ACK, e a mesma chamada é executada novamente, onde a regra "http-error" problemática não é atingida novamente em carga ativa. Todos os pacotes foram classificados em "ip_any" ruledef. Que diz que o pacote malformado era o pacote 10.

Consulte o exemplo de saída:

```
[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:

Em vez do pacote HTTP com solicitação **GET/POST**, a UE enviou o pacote TCP PSH-ACK que era considerado um pacote malformado e foi descartado porque não era o esperado. O prestador de serviços foi informado sobre este comportamento incorreto dos Estados-Membros específicos. O Cisco PGW funciona de acordo com os padrões 3GPP.