Pesquise defeitos os pacotes malformado HTTP que obtêm filtrados e deixados cair pelo ECS em Cisco PGW

Índice

Introdução

Este documento descreve como pesquisar defeitos os pacotes malformado HTTP que obtêm filtrados e deixados cair pelo serviço de carregamento aumentado (ECS) no gateway da rede dos dados do pacote de Cisco (PGW).

Pré-requisitos

Requisitos

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.

A informação neste documento é similar à configuração atual no nó do cliente, mas somente a informação relevante é mostrada aqui. Para que a finalidade demonstre os traços problemáticos sem expor a informação real, eu mudei ou golpeei alguns endereços IP de Um ou Mais Servidores Cisco ICM NT da informação isto é.

Problema

Havia umas queixas do provedor de serviços que alguns dos usuários em sua rede não poderiam alcançar locais específicos do jogo.

Quando os traços de tais usuários foram verificados, descobriu-se que o tráfego problemático esteve categorizado sob a definição da regra (ruledef) que foi definida a fim filtrar pacotes do erro de HTTP no PGW.

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

Troubleshooting

Que é ruledef?

A detecção do tráfego de HTTP dos assinantes é conseguida pelos analisadores do protocolo que estam presente no ECS.

O ECS tem os analisadores de protocolo que examinam o tráfego do uplink e do downlink. O tráfego de entrada entra em um analisador de protocolo para a inspeção de pacote de informação. Distribuindo ruledefs seja aplicado a fim determinar que pacotes a inspecionar. Este tráfego é enviado então ao motor de carregamento onde os ruledefs de carregamento são aplicados a fim executar ações tais como o bloco, as reorientar, ou as transmitir. Estes analisadores igualmente gerenciem registros do uso para o sistema de faturamento.

Ruledefs é expressões definidas pelo utilizador baseadas em campos do protocolo e em estados do protocolo, que definem que ações a tomar em pacotes quando os valores de campo especificados combinam.

Ruledefs que é usado na maior parte em um documento da pesquisa de defeitos é:

Distribuindo Ruledefs - Distribuindo ruledefs são usados aos pacotes de rota para satisfazer analisadores. Distribuindo ruledefs determine que analisador satisfeito para distribuir o pacote quando o protocolo coloca e/ou os protocolo-estados na expressão do ruledef são verdadeiros. Até o 256 os ruledefs podem ser configurados distribuindo.

Ruledefs de carregamento - Os ruledefs de carregamento são usados para especificar que ação tomar baseou na análise feita pelos analisadores satisfeitos. As ações podem incluir a reorientação, o valor da carga, e a emissão do registro de faturamento.

Instalação de laboratório

A configuração de exemplo a fim testar esta encenação no PGW:

```
config
 active-charging service <name>

 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
```

Log de erros

O traço problemático do subscritor foi usado para regenerar a réplica exata do tráfego de HTTP. Quando o traço foi executado com a configuração precedente, estes ruledefs obtiveram detectados sob o 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
```

Isto diz, há alguns pacotes enviados por UE que não são pacotes de HTTP apropriados e aqueles são categorizados sob o ruledef do “erro de HTTP” que esta presente na configuração.

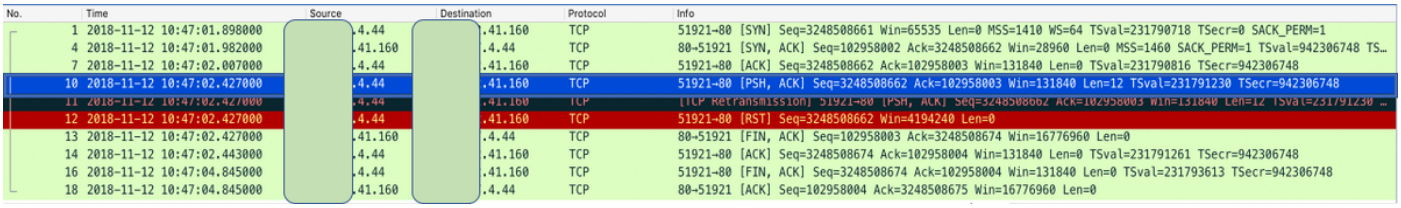
Depois que você verifica entra o sistema, você pode ver que os logs obtêm impressos como do “uma mensagem inválida pacote de HTTP” considerada lá. Verifique a mensagem nestes logs:

```
2018-Nov-14+05:46:50.474 [acsmgr 91654 unusual]
[1/0/17758 <sessmgr:1> http_analyzer.c:3478] [callid 00004e44]
[Call Trace] [context: sgi, contextID: 4] [software internal system syslog]
HTTP packet not valid
2018-Nov-14+05:46:50.474 [acsmgr 91025 trace]
[1/0/17758 <sessmgr:1> acsmgr_rules.c:22912]
[callid 00004e44] [Call Trace] [context: sgi, contextID:
4] [software internal user syslog] ruledef: http-error matches for service ecs
2018-Nov-14+05:46:50.474 [acsmgr 91209 debug]
[1/0/17758 <sessmgr:1> acsmgr_rules.c:22226]
[callid 00004e44] [Call Trace] [context: sgi, contextID: 4]
[software internal user syslog] normal charging-action (block) being applied
```

Do acordo à definição atual no nó, o ruledef “erro de HTTP” tem a ação de carregamento traçada como o “bloco” que combinou estes logs. Devido a isto, o assinante final não podia alcançar o Web site porque os pacotes foram terminados (terminar-fluxo da ação de fluxo) no motor ECS do PGW.

Solução

Depois que você converte o arquivo de rastreamento do subscritor no arquivo do pcap, você vê que estas mensagens obtêm trocadas entre o cliente (assinante final) e o server.



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

Conforme o fluxo de chamadas HTTP, o cliente deve enviar o pedido HTTP-GET/POST ao server e pedi-lo o acesso uma vez que o TCP SYN (você vê que no pacote nenhuns 1, 4 e 7) foi trocado.

Contudo, no arquivo do pcap, você não vê nenhum tráfego de HTTP dentro dele. Assim, o pacote de TCP que leva o HTTP que sinaliza ou o payload causam este problema.

Se você verifica, o tamanho da janela TCP que é permitido conforme RFC (rfc-1323) deve ser 65536 bytes (2*16=65536) por muito tempo.

O cabeçalho de TCP usa um campo de bit 16 a fim relatar o tamanho de janela da recepção ao remetente. Consequentemente, o indicador o maior que pode ser usado é os bytes 2**16 = 65K.

Se você vê o pacote 7 WS, é demasiado grande ser de um pacote do reconhecimento (ACK). Normalmente, com análise HTTP sobre, o GGSN tenta analisar gramaticalmente as mensagens GET/POST HTTP. Quando os fluxos HTTP não são em conformidade com RFC, pôde conduzir aos erros de análise (e às falhas a fim classificar corretamente o fluxo HTTP conforme URL etc.).

Como suspeitado, após o pacote de ACK (pacote 7), o cliente não enviou o pedido HTTP-GET/POST ao server a fim pedir o acesso. Em lugar de, “PSH, ACK” é enviado de UE. Isso não foi esperado pelo motor PGW ECS. UE enviava o payload dos pacotes de TCP do interior HTTP (com porta 80 dest), devido a que o gateway terminou que fluxo de pacote de informação enquanto foi filtrado e combinado sob o ruledef do “erro de HTTP” que tem a ação como o “terminar-fluxo”. Para o PGW, a mensagem prevista de UE seria HTTP-GET/POST que não foi visto. Consequentemente, considerou o pacote 10 como um pacote malformado.

A fim verificar mais a dúvida, o arquivo de rastreamento do pcap é alterado quando o número problemático 10 do pacote é removido que tem PSH-ACK, e a mesma chamada é tornada a colocar em funcionamento outra vez, onde o ruledef problemático do “erro de HTTP” não bate outra vez sob o carregamento ativo. Todos os pacotes foram classificados sob o ruledef “ip_any”. Isso diz que o pacote malformado era o pacote 10.

Refira 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
```

A fim resumir isto:

Em vez do pacote de HTTP com pedido **GET/POST**, UE enviou o pacote TCP PSH-ACK que foi considerado como um pacote malformado e deixado cair porque não era previsto. O provedor de serviços foi informado sobre este comportamento impróprio do UEs específico. Cisco PGW trabalha conforme os padrões 3GPP.