Cisco PGW에서 ECS에 의해 필터링 및 삭제된 HTTP 형식이 잘못된 패킷 문제 해결

목차

소개

이 문서에서는 Cisco PGW(Packet Data Network Gateway)에서 ECS(Enhanced Charging Service)에 의해 필터링 및 삭제된 HTTP 형식이 잘못된 패킷을 해결하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 스타오스
- ECS

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

이 문서의 정보는 고객 노드에 있는 컨피그레이션과 유사하지만, 여기에 관련 정보만 표시됩니다 .실제 정보를 노출하지 않고 문제가 있는 추적을 시연하기 위해 IP 주소와 같은 일부 정보를 변경하거나 검사했습니다.

문제

서비스 제공업체로부터 네트워크의 일부 사용자가 특정 게임 사이트에 액세스할 수 없다는 불만이 있었습니다.

이러한 사용자의 추적을 확인했을 때 문제가 있는 트래픽이 PGW에서 HTTP 오류 패킷을 필터링하기 위해 정의된 규칙 정의(ruledef)로 분류되었다는 사실이 발견되었습니다.

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

문제 해결

ruledef란?

가입자의 HTTP 트래픽 감지는 ECS에 있는 프로토콜 분석기를 통해 이루어집니다.

ECS에는 업링크 및 다운링크 트래픽을 검사하는 프로토콜 분석기가 있습니다.수신 트래픽은 패킷 검사를 위해 프로토콜 분석기로 들어갑니다.검사할 패킷을 결정하기 위해 라우팅 규칙이 적용됩니다.그런 다음 이 트래픽은 차단, 리디렉션 또는 전송과 같은 작업을 수행하기 위해 충전 규칙이 적용되는 충전 엔진으로 전송됩니다.이러한 분석기는 청구 시스템에 대한 사용 레코드도 생성합니다.

RuleDefs는 지정된 필드 값이 일치할 때 패킷에 수행할 작업을 정의하는 프로토콜 필드 및 프로토콜 상태를 기반으로 하는 사용자 정의 표현식입니다.

문제 해결 문서에서 주로 사용되는 규칙은 다음과 같습니다.

Routing Rule(라우팅 규칙) - 라우팅 규칙은 패킷을 콘텐츠 분석기로 라우팅하는 데 사용됩니다.라우팅 규칙은 규칙 정의 표현식의 프로토콜 필드 및/또는 프로토콜 상태가 true일 때 패킷을 라우팅할 콘텐츠 분석기를 결정합니다.라우팅을 위해 최대 256개의 루프를 구성할 수 있습니다.

규칙 충전 - 규칙 이하는 콘텐츠 분석기에 의해 수행된 분석에 따라 수행할 조치를 지정하는 데 사용됩니다.조치에는 리디렉션, 요금 값, 청구 기록 방출이 포함될 수 있습니다.

랩 설정

PGW에서 이 시나리오를 테스트하기 위한 샘플 컨피그레이션:

```
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
```

오류 로그

가입자의 문제가 있는 추적은 HTTP 트래픽의 정확한 복제본을 재생성하는 데 사용되었습니다.이전 컨피그레이션으로 추적을 실행하면 ECS 엔진에서 이러한 규칙이 탐지됩니다.

```
[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
```

즉, UE에서 전송하는 일부 패킷은 적절한 HTTP 패킷이 아니며 이러한 패킷은 컨피그레이션에 있는 "http-error" 규칙 정의로 분류됩니다.

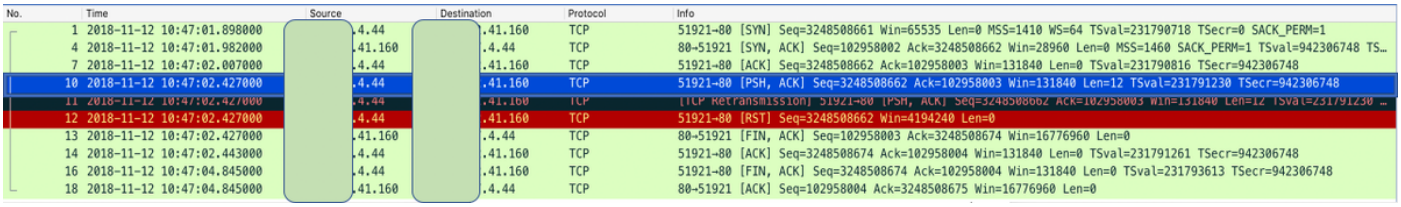
시스템의 로그를 확인한 후 로그가 "HTTP 패킷이 유효하지 않음" 메시지로 인쇄되는 것을 확인할 수 있습니다.다음 로그에서 메시지를 확인합니다.

```
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
```

노드에 있는 정의에 따라, 규칙 정의 "http-error"에는 이러한 로그와 일치하는 "block"으로 매핑된 충전 작업이 있습니다.이로 인해 PGW의 ECS 엔진에서 패킷이 종료(흐름 작업 종료-흐름)되어 최종 가입자가 웹 사이트에 액세스할 수 없습니다.

솔루션

가입자 추적 파일을 pcap 파일로 변환하면 이러한 메시지가 클라이언트(최종 가입자)와 서버 간에 교환됩니다.



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

HTTP 통화 흐름에 따라 클라이언트는 HTTP-GET/POST 요청을 서버로 전송하고 TCP SYN(패킷 번호 1, 4 및 7)이 교환되면 액세스를 요청해야 합니다.

그러나 pcap 파일에서 내부 HTTP 트래픽은 표시되지 않습니다.따라서 HTTP 신호 또는 페이로드를 전달하는 TCP 패킷이 이 문제를 유발합니다.

선택하는 경우 RFC(rfc-1323)에 따라 허용되는 TCP 창 크기는 65536(2*16=65536) 바이트여야 합니다.

TCP 헤더는 수신 윈도우 크기를 발신자에게 보고하기 위해 16비트 필드를 사용합니다.따라서 사용할 수 있는 가장 큰 창은 2**16 = 65K 바이트입니다.

패킷 7 WS가 표시되는 경우 패킷 크기가 너무 커서 승인(ACK) 패킷이 될 수 없습니다.일반적으로 HTTP 분석이 에서는 GGSN이 GET/POST HTTP 메시지를 구문 분석하려고 시도합니다.HTTP 흐름이 RFC를 준수하지 않으면 구문 분석 오류(URL에 따라 HTTP 흐름을 올바르게 분류하기 위한 실패)가 발생할 수 있습니다.

의심되는 경우, ACK 패킷(패킷 7) 이후 클라이언트는 액세스를 요청하기 위해 서버에 HTTP-GET/POST 요청을 보내지 않았습니다.대신 "PSH,ACK"가 UE에서 전송됩니다.PGW ECS 엔진에서 예상되지 않았습니다.UE가 TCP 패킷 내에서 http(대상 포트 80)의 페이로드를 전송했습니다. 이 때문에 패킷이 필터링되어 "terminate-flow"라는 작업이 있는 "http-error" 러데프에서 해당 패킷 흐름이 종료되고 일치됩니다. PGW의 경우, UE의 예상 메시지는 표시되지 않은 HTTP-GET/POST였습니다.따라서 패킷 10을 잘못된 패킷으로 간주했습니다.

더 이상 의심을 확인하기 위해 PSH-ACK가 있는 문제가 있는 패킷 번호 10이 제거되고 동일한 통화가 다시 실행될 때 pcap 추적 파일이 수정되며, 문제가 있는 "http-error" ruledef가 활성 충전 중에 다시 적중되지 않습니다.모든 패킷은 "ip_any" 규칙 정의 아래에 분류되었습니다.형식이 잘못된 패킷이 패킷 10이라고 합니다.

샘플 출력을 참조하십시오.

```
[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
```

요약하자면,

GET/POST 요청이 포함된 HTTP 패킷 대신 UE는 잘못된 패킷으로 간주되어 예기치 않은 패킷이 아니므로 삭제된 TCP PSH-ACK 패킷을 전송했습니다.서비스 공급업체는 특정 UE의 부적절한 행동에 대해 알림을 받았습니다. Cisco PGW는 3GPP 표준에 따라 작동합니다.