Probleemoplossing voor HTTP-misvormde pakketten die worden gefilterd en laten vallen door ECS in Cisco PGW

Inhoud

Inleiding

Dit document beschrijft hoe u problemen kunt oplossen bij HTTP-misvormde pakketten die worden gefilterd en gedropt door Enhanced Charging Service (ECS) in Cisco Packet Data Network Gateway (PGW).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- StarOS
- ECS

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is vergelijkbaar met de configuratie die aanwezig is in het klantknooppunt, maar hier wordt alleen relevante informatie weergegeven. Om de problematische sporen aan te tonen zonder echte informatie bloot te stellen, heb ik bepaalde informatie, d.w.z. IP-adressen, gewijzigd of doorgehaald.

Probleem

Er waren klachten van de dienstverlener dat sommige gebruikers in hun netwerk geen toegang hadden tot specifieke speelplaatsen.

Toen de sporen van dergelijke gebruikers werden gecontroleerd, werd ontdekt dat het problematische verkeer was gecategoriseerd onder regel definition (ruledef) die werd gedefinieerd om HTTP-foutpakketten in PGW te filteren.

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

Problemen oplossen

Wat is ruledef?

De detectie van het HTTP-verkeer van abonnees wordt bereikt door protocolanalysatoren die in ECS aanwezig zijn.

ECS heeft protocol analysatoren die uplinks- en downlink-verkeer onderzoeken. Het inkomende verkeer gaat in een protocol analyzer voor pakketinspectie. Routing regels worden toegepast om te bepalen welke pakketten worden geïnspecteerd. Dit verkeer wordt vervolgens naar de oplaadmotor gestuurd, waar oplaadregels worden toegepast voor het uitvoeren van acties zoals blokkeren, omleiden of verzenden. Deze analysatoren genereren ook gebruiksgegevens voor het facturatiesysteem.

Ruledefs zijn door de gebruiker gedefinieerde expressies op basis van protocolvelden en protocolstaten, die definiëren welke handelingen op pakketten moeten worden uitgevoerd wanneer de opgegeven waarden overeenkomen.

Ruledefs die meestal in een document voor probleemoplossing worden gebruikt, zijn:

Routing Ruledefs - routingregels worden gebruikt om pakketten te verzenden naar inhoud-analysatoren. Routing regels bepalen welke contentanalyzer het pakket moet leiden naar wanneer de protocolvelden en/of protocol-staten in ruledef-expressie waar zijn. Tot 256 ruledefs kunnen worden geconfigureerd voor het routing.

De heffingsregels worden gebruikt om aan de hand van de door de inhoudanalysatoren uitgevoerde analyse te bepalen welke maatregelen moeten worden genomen. Handelingen kunnen omleiding, heffingswaarde en factureringsregistratie-emissie omvatten.

Lab instellen

De monsterconfiguratie om dit scenario in PGW te testen:

```
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
```

Foutenlogboek

Het problematische spoor van de Subscriber werd gebruikt om de exacte replica van HTTP-verkeer opnieuw te genereren. Toen het spoor met de vorige configuratie werd uitgevoerd, werden deze regeltjes gedetecteerd onder de ECS-motor.

```
[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
```

Dit zegt, er zijn een paar pakketten verzonden door UE die niet goed HTTP-pakketten zijn en die zijn gecategoriseerd onder "http-error" regel die in de configuratie aanwezig is.

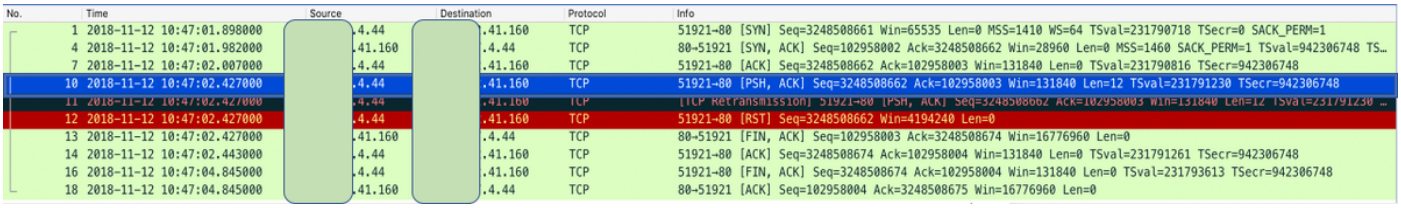
Nadat u de logbestanden in het systeem hebt gecontroleerd, kunt u zien dat de logbestanden worden afgedrukt als een "HTTP-pakket niet geldig"-bericht dat daar wordt gezien. Controleer het bericht in deze logs:

```
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
```

Overeenkomstig de definitie in knooppunt heeft de regel "http-error" de heffingsactie als "blok" in kaart gebracht dat deze stammen heeft. Hierdoor had de eindabonnee geen toegang tot de website omdat de pakketten waren afgesloten (flow action end-flow) in de ECS-motor van PGW.

Oplossing

Nadat u het bestand voor de tracering van de abonnee in het PPP-bestand hebt geconverteerd, ziet u dat deze berichten worden uitgewisseld tussen de client (end subscriber) en de 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

Zoals in de HTTP call flow, zou de client HTTP-GET/POST aanvraag naar de server moeten verzenden en om toegang vragen zodra het TCP SYN (u ziet dat in pakket 1, 4 en 7) is uitgewisseld.

In het pendop-bestand zie je echter geen HTTP-verkeer erin. Het TCP-pakket dat de HTTP-signalering of payload draagt veroorzaakt dit probleem.

Als u controleert, moet de grootte van het TCP-venster die is toegestaan volgens RFC (rFC-1323) 65536 (2*16=65536) bytes lang zijn.

De TCP-header gebruikt een veld met 16 bits om de ontvangstvenstergrootte aan de afzender te melden. Daarom is het grootste venster dat kan worden gebruikt 2**16 = 65K bytes.

Als u pakket 7 WS ziet, is het te groot om een Herkende (ACK) verpakking te hebben. Normaal, met HTTP analyse op, probeert GN de GET/POST HTTP berichten te parseren. Wanneer de HTTP-stromen niet RFC-compatibel zijn, kan dit resulteren in parse-fouten (en fouten om de HTTP-stroom naar behoren in te delen volgens URL e.d.).

Zoals vermoed, na het ACK-pakket (pakket 7) stuurde de client geen HTTP-GET/POST-verzoek naar de server om toegang te vragen. In plaats daarvan wordt "PSH, ACK" vanuit UE gestuurd. Dat werd niet verwacht door de ECS-motor van PGW. UE stuurde payload van http (met testpoort 80) in TCP-pakketten, omdat gateway de pakketstroom beëindigde terwijl deze werd gefilterd en werd gematcht onder "http-error" ruledef dat actie als "expo-flow" heeft. Voor PGW zou de verwachte boodschap van UE HTTP-GET/POST zijn geweest die niet was gezien. Daarom werd pakje 10 beschouwd als een misvormd pakje.

Om de twijfel verder te verifiëren wordt het pcap-spoorbestand aangepast wanneer het problematische paknummer 10 wordt verwijderd dat PSH-ACK heeft en de zelfde oproep wordt opnieuw uitgevoerd, waar de problematische "http-error" regel niet opnieuw wordt geraakt onder actief laden. Alle pakketten zijn geclassificeerd onder "ip_any" ruledef. Dat zegt dat het misvormde pakje pakje 10 was.

Raadpleeg de steekproefuitvoer:

```
[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
```

Zo vat u het volgende samen:

In plaats van het HTTP-pakket met **GET/POST-**aanvraag heeft UE TCP PSH-ACK-pakket verzonden dat als een misvormd pakket werd beschouwd en is gevallen omdat dit niet het verwachte pakket was. De dienstverlener werd op de hoogte gebracht van dit onjuiste gedrag van de specifieke UE's. De Cisco PGW werkt volgens de 3GPP-normen.