Fehlerbehebung bei HTTP-fehlerhaften Paketen, die vom ECS gefiltert und im Cisco PGW verworfen werden

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie HTTP-fehlerhafte Pakete behoben werden, die vom Enhanced Charging Service (ECS) im Cisco Packet Data Network Gateway (PGW) gefiltert und verworfen werden.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- StarOS
- ECS

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

Die Informationen in diesem Dokument ähneln der Konfiguration im Kundenknoten, aber hier werden nur relevante Informationen angezeigt. Um die problematischen Spuren zu demonstrieren, ohne reale Informationen preiszugeben, habe ich einige Informationen, z. B. IP-Adressen, geändert oder abgeschnitten.

Problem

Es gab Beschwerden vom Service Provider, dass einige Benutzer in ihrem Netzwerk nicht auf bestimmte Spiele-Sites zugreifen konnten.

Bei der Überprüfung der Spuren dieser Benutzer wurde festgestellt, dass der problematische Datenverkehr unter Regeldefinition (regeledef) kategorisiert wurde, die definiert wurde, um HTTP-Fehlerpakete im PGW zu filtern.

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

Fehlerbehebung

Was ist regeln?

Die Erkennung des HTTP-Datenverkehrs von Abonnenten wird durch Protokollanalysatoren erreicht, die in ECS vorhanden sind.

ECS verfügt über Protokollanalysatoren, die Uplink- und Downlink-Datenverkehr untersuchen. Eingehender Datenverkehr wird zur Paketprüfung in einen Protokollanalyzer geleitet. Routingregeln werden angewendet, um zu bestimmen, welche Pakete überprüft werden sollen. Dieser Datenverkehr wird dann an die Ladestation gesendet, wo die Laderegeln angewendet werden, um Aktionen wie Sperren, Umleiten oder Übertragen auszuführen. Diese Analysatoren generieren außerdem Nutzungsdatensätze für das Abrechnungssystem.

Regeln sind benutzerdefinierte Ausdrücke, die auf Protokollfeldern und Protokollzuständen basieren und festlegen, welche Aktionen bei Übereinstimmung der angegebenen Feldwerte für Pakete ausgeführt werden sollen.

Die wichtigsten Prinzipien bei der Fehlerbehebung sind:

Routingregeln - Routingregeln werden zum Weiterleiten von Paketen an Inhaltsanalysatoren verwendet. Routingregeln bestimmen, an welchen Content-Analyzer das Paket weitergeleitet werden soll, wenn die Protokollfelder und/oder Protokollzustände in der Regelausgabe true sind. Für das Routing können bis zu 256 Regeln konfiguriert werden.

Charging Ruledefs (Aufladungsregeln) - Anhand von Abrechnungsregeln wird festgelegt, welche Aktion auf der Grundlage der von den Inhaltsanalysatoren durchgeführten Analyse durchgeführt werden soll. Mögliche Aktionen sind Umleitung, Ladewert und Emission von Rechnungsdatensätzen.

Übungseinrichtung

Die Beispielkonfiguration zum Testen dieses Szenarios im 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
```

Fehlerprotokolle

Die problematische Ablaufverfolgung des Teilnehmers wurde verwendet, um das genaue Replikat des HTTP-Datenverkehrs neu zu generieren. Wenn die Ablaufverfolgung mit der vorherigen Konfiguration ausgeführt wurde, wurden diese Regelsätze unter der ECS-Engine erkannt.

```
[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
```

Dies bedeutet, dass einige Pakete von UE gesendet werden, die nicht die richtigen HTTP-Pakete sind und die unter "http-error"-Regeldef kategorisiert sind, der in der Konfiguration vorhanden ist.

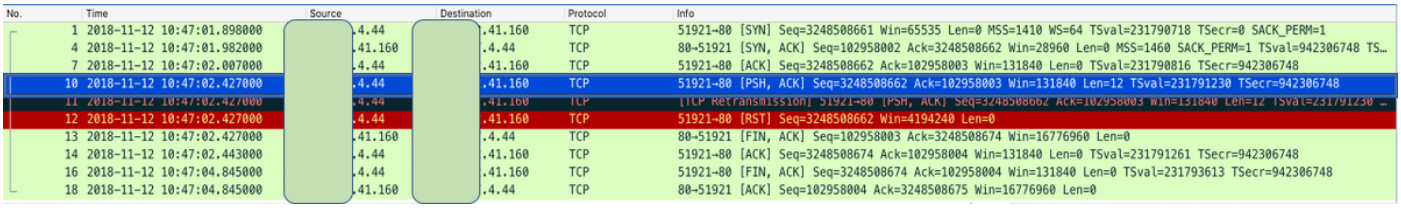
Nachdem Sie die Protokolle im System überprüft haben, sehen Sie, dass die Protokolle als Meldung ausgegeben werden, dass das HTTP-Paket ungültig ist. Überprüfen Sie die Meldung in diesen Protokollen:

```
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
```

Gemäß der im Knoten enthaltenen Definition wird der Regeldef "http-error" als "block" zugeordnet, der diesen Protokollen entspricht. Aus diesem Grund konnte der Endabonnent nicht auf die Website zugreifen, da die Pakete in der ECS-Engine des PGW beendet wurden (Flow Action terminate-flow).

Lösung

Nachdem Sie die Subscriber-Ablaufverfolgungsdatei in die pcap-Datei konvertiert haben, sehen Sie, dass diese Nachrichten zwischen dem Client (Endteilnehmer) und dem Server ausgetauscht werden.



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

Entsprechend dem HTTP-Anruffluss sollte der Client HTTP-GET-/POST-Anfragen an den Server senden und nach dem Austausch der TCP-SYN (wie Sie sehen, dass im Paket Nr. 1, 4 und 7) um Zugriff bitten.

In der pcap-Datei wird jedoch kein HTTP-Datenverkehr darin angezeigt. Das TCP-Paket, das die HTTP-Signalisierung oder Payload überträgt, verursacht dieses Problem.

Wenn Sie diese Option aktivieren, sollte die gemäß RFC (RFC-1323) zulässige TCP-Fenstergröße 65536 (2*16=65536) Byte lang sein.

Der TCP-Header verwendet ein 16-Bit-Feld, um die Größe des Empfangsfensters dem Absender mitzuteilen. Daher ist das größte Fenster, das verwendet werden kann, 2**16 = 65 KB Byte.

Wenn Sie Paket 7 WS sehen, ist es zu groß, um ein Bestätigungs-Paket (ACK) zu sein. Normalerweise versucht das GGSN bei einer HTTP-Analyse, die HTTP-Meldungen GET/POST zu analysieren. Wenn die HTTP-Datenflüsse nicht RFC-konform sind, kann dies zu Parse-Fehlern (und Fehlern bei der korrekten Klassifizierung des HTTP-Datenflusses als URL usw.) führen.

Wie vermutet, hat der Client nach dem ACK-Paket (Paket 7) keine HTTP-GET-/POST-Anforderung an den Server gesendet, um den Zugriff anzufordern. Stattdessen wird "PSH,ACK" von der UE gesendet. Dies wurde von der PGW ECS-Engine nicht erwartet. UE sendete die Nutzlast von http (mit dem Ziel-Port 80) in TCP-Paketen, da das Gateway diesen Paketfluss beendet hatte, da er gefiltert und unter "http-error"-Regelsatz abgeglichen wurde, der als "terminate-flow" agiert. Für das PGW wäre die erwartete Nachricht von UE HTTP-GET/POST gewesen, die nicht angezeigt wurde. Daher wurde Paket 10 als falsch formatiertes Paket angesehen.

Um den Zweifel weiter zu überprüfen, wird die pcap-Ablaufverfolgungsdatei geändert, wenn die problematische Paketnummer 10 entfernt wird, die PSH-ACK enthält, und der gleiche Anruf wird erneut ausgeführt, wobei die problematische "http-error"-Regel bei aktivem Aufladen nicht erneut trifft. Alle Pakete wurden gemäß der Regel "ip_any" klassifiziert. Das besagt, dass das fehlerhafte

Paket Paket Paket 10 war.

Siehe Beispielausgabe:

```
[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
```

Fassen Sie Folgendes zusammen:

Anstelle des HTTP-Pakets mit **GET/POST-**Anforderung sendete UE ein TCP-PSH-ACK-Paket, das als falsch formatiertes Paket angesehen wurde und verworfen wurde, da es nicht das erwartete Paket war. Der Dienstanbieter wurde über dieses unsachgemäße Verhalten der spezifischen UEs informiert. Das Cisco PGW funktioniert gemäß 3GPP-Standards.