Cisco PGWでECSによってフィルタリングおよびドロップされるHTTP不正パケットのトラブルシューティング

内容

概要

このドキュメントでは、Cisco Packet Data Network Gateway(PGW)のEnhanced Charging Service(ECS)によってフィルタリングおよびドロップされるHTTP不正パケットのトラブルシューティング方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- StarOS
- ECS

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このドキュメントの情報は、お客様のノードに存在する設定に似ていますが、ここでは関連情報のみを示します。実際の情報を公開せずに問題のあるトレースを示すために、IPアドレスなどの情報を変更または取得しました。

問題

サービスプロバイダーから、ネットワーク内の一部のユーザが特定のゲームサイトにアクセスできないという苦情がありました。

このようなユーザのトレースを確認すると、問題のあるトラフィックがPGWでHTTPエラーパケットをフィルタリングするために定義されたルール定義(ruledef)に分類されたことが検出されました。

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

トラブルシュート

ruledefとは何ですか。

加入者のHTTPトラフィックの検出は、ECSに存在するプロトコルアナライザによって実現されます。

ECSには、アップリンクおよびダウンリンクのトラフィックを検査するプロトコルアナライザがあります。着信トラフィックはプロトコルアナライザに送られ、パケット検査が行われます。どのパケットを検査するかを決定するために、ルーティングルールが適用されます。その後、このトラフィックは課金エンジンに送信されます。課金ルールの定義は、ブロック、リダイレクト、送信などのアクションを実行するために適用されます。これらのアナライザは、課金システムの使用状況レコードも生成します。

Ruledefsは、プロトコルフィールドとプロトコル状態に基づくユーザ定義式で、指定されたフィールド値が一致したときにパケットに対してどのようなアクションを実行するかを定義します。

トラブルシューティング文書で主に使用されるルール定義は次のとおりです。

ルーティングルール定義：ルーティングルール定義は、コンテンツアナライザにパケットをルーティングするために使用されます。ルーティングのルール定義は、ruledef式のプロトコルフィールドおよび/またはプロトコル状態がtrueの場合にパケットをルーティングするコンテンツアナライザを決定します。最大256のルール定義をルーティング用に設定できます。

Charging Ruledefs – 課金ルールdefsは、コンテンツアナライザによって行われた分析に基づいて実行するアクションを指定するために使用されます。アクションには、リダイレクション、請求額、請求レコードの排出などがあります。

ラボのセットアップ

PGWでこのシナリオをテストするための設定例：

```
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
```

エラーログ

サブスクライバの問題のあるトレースは、HTTPトラフィックの正確なレプリカを再生成するために使用されました。以前の設定でトレースを実行すると、ECSエンジンでこれらのルール定義が検出されました。

```
[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
```

これは、UEから送信されるパケットの中には、適切なHTTPパケットではなく、設定に含まれる「http-error」のruledefに分類されるものがあります。

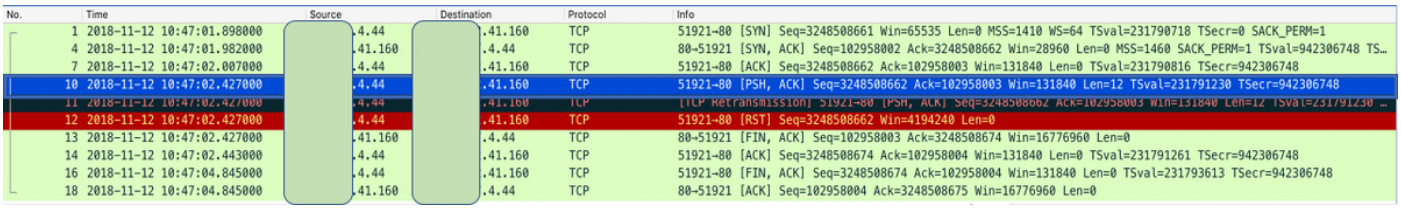
システムのログを確認すると、ログがそこに表示される「HTTP packet not valid」メッセージとして出力されていることがわかります。次のログのメッセージを確認します。

```
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
```

ノードに存在する定義に従って、ruledef "http-error"には、これらのログに一致する「ブロック」としてマッピングされた課金アクションがあります。このため、PGWのECSエンジンでパケットが終了したため（フローアクションterminate-flow）、エンドサブスクライバはWebサイトにアクセスできませんでした。

解決方法

サブスクライバトレースファイルをpcapファイルに変換すると、これらのメッセージがクライアント（エンドサブスクライバ）とサーバの間で交換されることがわかります。



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コールフローに従って、クライアントはHTTP-GET/POST要求をサーバに送信し、TCP SYN（パケット番号1、4、および7で確認）が交換されるとアクセスを要求する必要があります。

ただし、pcapファイルでは、その内部にHTTPトラフィックは表示されません。そのため、HTTPシグナリングまたはペイロードを伝送するTCPパケットがこの問題を引き起こします。

これを確認すると、RFC(rfc-1323)に従って許可されるTCPウィンドウサイズは65536(2*16=65536)バイト長になります。

TCPヘッダーは16ビットフィールドを使用して、受信ウィンドウサイズを送信者に報告します。したがって、使用可能な最大のウィンドウは2**16 = 65Kバイトです。

パケット7 WSが表示される場合、パケットが大きすぎて確認応答(ACK)パケットになりません。通常、HTTP分析がオンの場合、GGSNはGET/POST HTTPメッセージの解析を試行します。HTTPフローがRFCに準拠していない場合は、解析エラー（およびURLなどに従ってHTTPフローを適切に分類するための失敗）が発生する可能性があります。

疑いなく、ACKパケット（パケット7）の後、クライアントはアクセスを要求するためにHTTP-GET/POST要求をサーバに送信しませんでした。代わりに、UEから「PSH,ACK」が送信されます。これはPGW ECSエンジンでは想定されていませんでした。UEはTCPパケット内のhttp（宛先ポート80）のペイロードを送信していました。これは、どのゲートウェイがフィルタリングされてパケットフローを終了し、「terminate-flow」というアクションを持つ「http-error」ruledefで照合されたためです。 PGWの場合、UEからの予期されるメッセージはHTTP-GET/POSTであり、表示されません。したがって、パケット10は不正なパケットと見なされます。

さらに疑いを確認するために、PSH-ACKを含む問題のあるパケット番号10が削除され、同じコールが再実行されると、pcapトレースファイルが変更されます。この場合、問題のある「http-error」のruledefはアクティブ課金中に再度ヒットしません。すべてのパケットは「ip_any」のruledefに分類されました。これは、不正なパケットがパケット10であることを示しています。

出力例を参照してください。

```
[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
```

これを要約すると、次のようになります。

GET/POST要求を含むHTTPパケットの代わりに、UEは不正なパケットと見なされてドロップされたTCP PSH-ACKパケットを送信しました。サービスプロバイダーは、特定のUEの不適切な動作について通知されました。Cisco PGWは3GPP標準に従って動作します。