أستكشاف أخطاء حزم HTTP التي تم تكوينها بشكل غير صحيح وإصالحها والتي يتم تصفيتها وإسقاطها بواسطة ECS في Cisco PGW

المحتويات

المقدمة

يصف هذا المستند كيفية أستكشاف أخطاء حزم HTTP التي تم تكوينها بشكل غير صحيح والتي يتم تصفيتها وإسقاطها بواسطة خدمة الشحن المحسن (ECS) في عبارة شبكة بيانات الحزم (PGW) من Cisco وإصالحها.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- StarOS
- ECS

المكونات المستخدمة

ال يقتصر هذا المستند على إصدارات برامج ومكونات مادية معينة.

المعلومات الواردة في هذا المستند مماثلة للتكوين الموجود في عقدة العميل، ولكن يتم عرض المعلومات ذات الصلة فقط هنا. لغرض توضيح اآلثار اإلشكالية دون الكشف عن معلومات حقيقية، قمت بتغيير أو تحديد بعض المعلومات، مثل عناوين IP.

المشكلة

وكانت هناك شكاوى من موزع الخدمة مفادها أن بعض المستخدمين في الشبكة لا يستطيعون الوصول إلى مواقع ألعاب معينة.

عندما تم التحقق من آثار مثل هؤلاء المستخدمين، تم اكتشاف أن حركة المرور المسببة للمشاكل تم تصنيفها تحت تعريف القاعدة (ruledef) الذي تم تعريفه لتصفية حزم أخطاء HTTP في PGW.

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

استكشاف الأخطاء وإصلاحها

ما هو الروليديف؟

يتم تحقيق اكتشاف حركة مرور HTTP للمشتركين من خلال تحليلات البروتوكول الموجودة في ECS.

يحتوي ECS على محلل بروتوكول يفحص حركة مرور الوصلة والارتباط. تدخل حركة المرور الواردة في محلل بروتوكول لتفتيش الحزمة. يتم تطبيق أنظمة التوجيه لتحديد الحزم التي يجب فحصها. يتم بعد ذلك إرسال حركة المرور هذه إلى محرك الشحن حيث يتم تطبيق أنظمة الشحن لتنفيذ إجراءات مثل الكتلة أو إعادة التوجيه أو الإرسال. كما توقم هذه التحليلات بإنشاء سجلات إستخدام لنظام الفوترة.

Rouledefs هي تعبيرات معرفة من قبل المستخدم استنادا إلى حقول البروتوكول والحالات البروتوكول، والتي تحدد الإجراءات التي يجب إتخاذها على الحزم عند تطابق قيم الحقل المحددة.

Rouledefs أن يكون غالبا استعملت في وثيقة أستكشاف الأخطاء وإصلاحها:

Routing Rouledefs - يتم إستخدام Routing Rouledefs لتوجيه الحزم إلى محلل المحتوى. تحدد قواعد التوجيه للمحلل المحتوى الذي يجوز توجيه الحزمة إليه عندما تكون حقول البروتوكول و/أو حالات البروتوكول في تعبير الموجه صحيحة. يمكن تكوين ما يصل إلى 256 محرك للتوجيه.

Ruledefs الشحن - يتم إستخدام ChargeDefs لتحديد الإجراء الذي يجب إتخاذه استنادا إلى التحليل الذي تم إجراؤه بواسطة أدوات تحليل المحتوى. يمكن أن تتضمن الإجراءات إعادة التوجيه، وقيمة الشحن، وانبعاثات سجل الفوترة.

إعداد المختبر

عينة تشكيل in order to اختبرت هذا سيناريو في 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
```

سجلات الأخطاء

تم إستخدام التتبع الإشكالي للمشترك لإعادة إنشاء النسخة المتماثلة الدقيقة لحركة مرور HTTP. عند تشغيل التتبع بالتكوين السابق، تم اكتشاف هذه الدقائق ضمن محرك 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
```

وهذا يقول، هناك بعض الحزم المرسلة من قبل UE والتي ليست حزم HTTP مناسبة وتلك مصنفة تحت موجه "http-error" الموجودة في التكوين.

بعد التحقق من السجلات الموجودة في النظام، يمكنك رؤية طباعة السجلات كرسالة "حزمة HTTP غير صحيحة" تتم رؤيتها هناك. تحقق من الرسالة الموجودة في هذه السجلات:

```
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
```

وقف للتعريف الموجود في العقدة، يحتوي الموجه "http-error" على إجراء الشحن المعين ك "block" الذي تطابق هذه السجلات. ولهذا السبب، لم يتمكن المشترك النهائي من الوصول إلى موقع الويب حيث تم إنهاء الحزم (إيقاف تدفق إجراء التدفق) في محرك ECS ل PGW.

الحل

بعد أن تقوم بتحويل ملف تتبع المشترك إلى ملف PCAP، سترى أن تلك الرسائل يتم تبادلها بين العميل (المشترك النهائي) والخادم.

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

وقف لتدفق مكالمات HTTP، يجب على العميل إرسال طلب HTTP-GET/POST إلى الخادم وطلب الوصول بمجرد تبادل نظام TCP (ترى ذلك في الحزمة رقم 1 و 4 و 7).

على أي حال، في ملف PCAP، لا ترى أي حركة مرور HTTP بداخله. لذلك، تتسبب حزمة TCP التي تحمل إشارات HTTP أو الحمولة في هذه المشكلة.

إذا قمت بالتحقق، فيجب أن يكون حجم نافذة TCP المسموح به وفقا ل RFC (RFC-1323) 65536 (2*16=65536) بايت طويلة.

يستخدم رأس TCP حقل 16 بت لإرسال تقرير عن حجم نافذة التلقي إلى المرسل. لذلك، فإن أكبر نافذة يمكن إستخدامها هي 2**16 = 65 كيلو بايت.

إذا كنت ترى الحزمة 7 WS، فإنها أكبر من أن تكون من حزمة إقرار (ACK). عادة، مع تشغيل تحليل HTTP، يحاول GGSN توزيع رسائل GET/POST HTTP. عندما لا تكون تدفقات HTTP متوافقة مع RFC، فقد يؤدي ذلك إلى أخطاء في التحليل (حالات فشل لتصنيف تدفق HTTP بشكل صحيح وفقا ل URL، وما إلى ذلك).

كما هو مشتبه به، بعد حزمة ACK (الحزمة 7)، لم يرسل العميل طلب HTTP-GET/POST إلى الخادم لطلب الوصول. بدلا من ذلك، "PSH، ACK" تم إرسالها من UE. لم يكن هذا متوقعا من قبل محرك PGW ECS. كان UE يرسل حمولة من HTTP (مع المنفذ الأقدم 80) داخل حزم TCP، بسبب أي عبارة ينهي تدفق الحزمة حيث كان تتم تصفيتها ومطابقتها تحت موجه "http-error" الذي يحتوي على إجراء "terminate-flow". بالنسبة ل PGW، كانت الرسالة المتوقعة من UE هي HTTP-GET/POST والتي لم يتم رؤيتها. لذلك، اعتبرت الحزمة 10 كحزمة مشكل بشكل غير صحيح.

للتحقق من الشك أكثر، يتم تعديل ملف تتبع PCAP عندما تتم إزالة الحزمة الإشكالية رقم 10 التي تحتوي على PSH-ACK، وتتم إعادة تشغيل نفس المكالمة مرة أخرى، حيث لا يتم تشغيل الموجه الإشكالي "http-error" مرة أخرى تحت الشحن النشط. تم تصنيف جميع الحزم تحت رقم "ip_any". الذي يقول أن الربط غير شكل كان ربط 10.

ارجع إلى إخراج النموذج:

```
[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
```

ولتلخيص هذا:

بدلا من حزمة HTTP مع طلب **GET/POST**، قام المستخدم بإرسال حزمة TCP PSH-ACK التي تم اعتبارها كحزمة تم تكوينها بشكل غير صحيح وتم إسقاطها لأنها لم تكن الحزمة المتوقعة. تم إعلام موفر الخدمة بهذا السلوك غير الصحيح من قبل UEs المحددة. يعمل PGW من Cisco وفقا لمعايير 3GPP.

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).