Dépannez les paquets mal formés de HTTP qui obtiennent filtré et chuté par ECS à Cisco PGW

Contenu

Introduction

Ce document décrit comment dépanner les paquets mal formés de HTTP qui obtiennent filtré et chuté par le service de remplissage amélioré (ECS) dans la passerelle de réseau de données de paquets de Cisco (PGW).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- StarOS
- ECS

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

Les informations dans ce document sont semblables à la configuration actuelle dans le noeud de client, mais seulement les informations pertinentes sont affichées ici. Pour que le but explique les suivis problématiques sans exposer les vraies informations, j'ai changé ou ai frappé quelques adresses IP de l'information c.-à-d.

Problème

Il y avait des plaintes du fournisseur de services que certains des utilisateurs dans leur réseau ne

pourraient pas accéder aux sites de jeux spécifiques.

Quand les suivis de tels utilisateurs ont été vérifiés, on l'a découvert que le trafic problématique a été classé par catégorie sous la définition de règle (ruledef) qu'a été défini afin de filtrer des paquets d'erreurs de HTTP dans PGW.

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

Dépanner

Quel est ruledef ?

La détection du trafic http des abonnés est réalisée par les analyseurs de protocole qui sont présents dans l'ECS.

L'ECS a les analyseurs de protocole qui examinent le trafic de liaison ascendante et de liaison descendante. Le trafic entrant entre dans un analyseur de protocole pour l'inspection de paquet. En conduisant des ruledefs soyez appliqué afin de déterminer quels paquets à examiner. Ce trafic est alors envoyé à l'engine de remplissage où les ruledefs de remplissage sont appliqués afin d'exécuter des actions telles que le bloc, les réorienter, ou les transmettre. Ces analyseurs génèrent également des enregistrements d'utilisation pour le système de facturation.

Ruledefs sont des expressions définies par l'utilisateur basées sur des champs de protocole et des états de protocole, qui définissent quelles actions de prendre des paquets quand le champ spécifié évalue la correspondance.

Ruledefs qui sont en grande partie utilisés dans un document de dépannage sont :

Conduisant Ruledefs - Conduisant des ruledefs sont utilisés pour conduire des paquets pour contenter des analyseurs. En conduisant des ruledefs déterminez à quel analyseur satisfait pour conduire le paquet quand le protocole met en place et/ou les Protocol-états dans l'expression de ruledef sont vrais. Jusqu'à 256 ruledefs peuvent être configurés pour l'acheminement.

Ruledefs de remplissage - Des ruledefs de remplissage sont utilisés pour spécifier quelle action de prendre a basée sur l'analyse faite par les analyseurs satisfaits. Les actions peuvent inclure la redirection, la valeur de charge, et l'émission d'enregistrement de facturation.

Installation de laboratoire

La configuration d'échantillon afin de tester ce scénario dans PGW :

```
config
 active-charging service <name>

 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
```

Journaux des erreurs

Le suivi problématique de l'abonné a été utilisé pour régénérer la reproduction précise du trafic http. Quand le suivi a été exécuté avec la configuration précédente, ces ruledefs obtenus les ont détecté sous l'engine 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
```

Ceci indique, il y a quelques paquets envoyés par UE qui ne sont pas les paquets appropriés de HTTP et ceux sont classés par catégorie sous le ruledef de « HTTP-erreur » qui est présent dans la configuration.

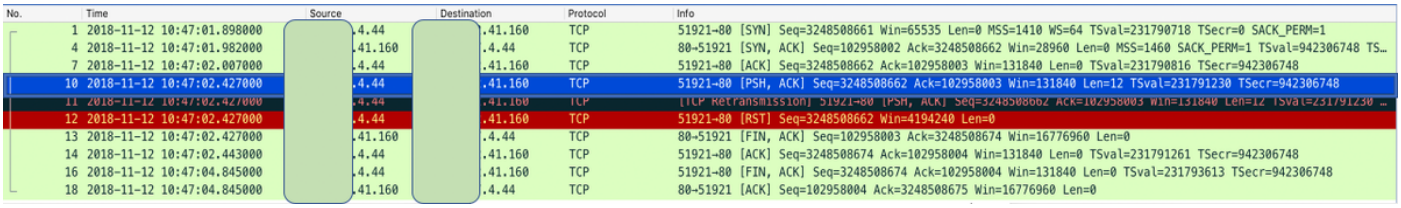
Après que vous vérifiiez les logins le système, vous pouvez voir que les logs obtiennent imprimé comme message « non valide » de paquet de HTTP vu là. Vérifiez le message dans ces logs :

```
2018-Nov-14+05:46:50.474 [acsmgr 91654 unusual]
[1/0/17758 <sessmgr:1> http_analyzer.c:3478] [callid 00004e44]
[Call Trace] [context: sgi, contextID: 4] [software internal system syslog]
HTTP packet not valid
2018-Nov-14+05:46:50.474 [acsmgr 91025 trace]
[1/0/17758 <sessmgr:1> acsmgr_rules.c:22912]
[callid 00004e44] [Call Trace] [context: sgi, contextID:
4] [software internal user syslog] ruledef: http-error matches for service ecs
2018-Nov-14+05:46:50.474 [acsmgr 91209 debug]
[1/0/17758 <sessmgr:1> acsmgr_rules.c:22226]
[callid 00004e44] [Call Trace] [context: sgi, contextID: 4]
[software internal user syslog] normal charging-action (block) being applied
```

Dans l'accord à la définition actuelle dans le noeud, le ruledef « HTTP-erreur » a l'action de remplissage tracée en tant que « bloc » qui a apparié ces logs. En raison de ceci, l'abonné final ne pouvait pas accéder au site Web car les paquets ont été terminés (terminer-écoulement d'action d'écoulement) dans l'engine ECS de PGW.

Solution

Après que vous convertissiez le fichier de suivi d'abonné en fichier de pcap, vous voyez que ces messages obtiennent permuté entre le client (abonné final) et le serveur.



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

Selon l'écoulement d'appel de HTTP, le client devrait envoyer la demande HTTP-GET/POST au serveur et demander l'accès une fois que la synchronisation de TCP (vous voyez cela en le NO1 de paquet, 4 et 7) a été permuté.

Cependant, dans le fichier de pcap, vous ne voyez aucun trafic http à l'intérieur de lui. Ainsi, le paquet TCP qui porte le HTTP signalant ou la charge utile pose ce problème.

Si vous vérifiez, la taille de la fenêtre de TCP qui est permise selon RFC (rfc-1323) devrait être de 65536 octets (2*16=65536) de long.

L'en-tête de TCP emploie un champ de 16 bits afin de signaler la taille de la fenêtre de réception à l'expéditeur. Par conséquent, la plus grande fenêtre qui peut être utilisée est les octets 2**16 = 65K.

Si vous voyez le paquet 7 WS, il est trop grand pour être d'un paquet de la reconnaissance (ACK). Normalement, avec l'analyse de HTTP en fonction, les essais GGSN pour analyser les messages de HTTP GET/POST. Quand les écoulements de HTTP ne sont pas RFC conforme, il pourrait avoir comme conséquence des erreurs d'analyser (et des pannes afin de classifier correctement l'écoulement de HTTP selon URL etc.).

Comme suspecté, après le paquet ACK (le paquet 7), le client n'a pas envoyé la demande HTTP-GET/POST au serveur afin de demander l'accès. Au lieu de cela, « PSH, ACK » est envoyé d'UE. Cela n'a pas été prévu par l'engine PGW ECS. UE envoyait la charge utile des paquets TCP d'intérieur de HTTP (avec port 80 DEST), en raison desquels la passerelle a terminé cet écoulement de paquet pendant qu'elle était filtrée et appariée sous le ruledef de « HTTP-erreur » qui a l'action en tant que « terminer-écoulement ». Pour PGW, le message prévu d'UE aurait été HTTP-GET/POST qui n'a pas été vu. Par conséquent, il a considéré le paquet 10 comme paquet mal formé.

Afin de vérifier le doute plus loin, le fichier de suivi de pcap est modifié quand on retire le paquet problématique le numéro 10 qui a PSH-ACK, et le même appel est réexécuté de nouveau, où le ruledef problématique de « HTTP-erreur » ne frappe pas de nouveau sous le remplissage actif. Tous les paquets ont été classifiés sous le ruledef « ip_any ». Cela indique que le paquet mal formé était le paquet 10.

Référez-vous à la sortie témoin :

```
[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
```

Afin de récapituler ceci :

Au lieu du paquet de HTTP avec la demande **GET/POST**, UE a envoyé le paquet du TCP PSH-ACK qui a été considéré comme paquet mal formé et a été lâché parce qu'il n'était pas prévu. Le fournisseur de services a été informé au sujet de ce comportement inexact de l'UEs spécifique. Les travaux de Cisco PGW selon les normes 3GPP.