Dépanner les paquets HTTP mal formés qui sont filtrés et abandonnés par ECS dans Cisco PGW

Contenu

Introduction

Ce document décrit comment dépanner les paquets HTTP mal formés qui sont filtrés et abandonnés par le service de facturation améliorée (ECS) dans Cisco Packet Data Network Gateway (PGW).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- StarOS
- ECS

Components Used

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

Les informations de ce document sont similaires à la configuration présente dans le noeud client, mais seules les informations pertinentes sont affichées ici. Pour démontrer les traces problématiques sans révéler de véritables informations, j'ai modifié ou biffé certaines informations, par exemple les adresses IP.

Problème

Le fournisseur de services a signalé que certains utilisateurs de son réseau ne pouvaient pas

accéder à des sites de jeux spécifiques.

Lorsque les traces de ces utilisateurs ont été vérifiées, il a été découvert que le trafic problématique était catégorisé sous la définition de règle (rouledef) définie afin de filtrer les paquets d'erreur HTTP dans PGW.

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

Dépannage

Qu'est-ce que la règle ?

La détection du trafic HTTP des abonnés est réalisée par des analyseurs de protocole présents dans ECS.

ECS dispose d'analyseurs de protocole qui examinent le trafic de liaison ascendante et descendante. Le trafic entrant entre dans un analyseur de protocole pour l'inspection des paquets. Les règles de routage sont appliquées afin de déterminer les paquets à inspecter. Ce trafic est ensuite envoyé au moteur de charge où les règles de charge sont appliquées afin d'effectuer des actions telles que le blocage, la redirection ou la transmission. Ces analyseurs génèrent également des enregistrements d'utilisation pour le système de facturation.

Les règles sont des expressions définies par l'utilisateur en fonction des champs de protocole et des états de protocole, qui définissent les actions à entreprendre sur les paquets lorsque les valeurs de champ spécifiées correspondent.

Les règles qui sont principalement utilisées dans un document de dépannage sont les suivantes :

Routing Ruledefs : les règles de routage sont utilisées pour acheminer les paquets vers les analyseurs de contenu. Les règles de routage déterminent l'analyseur de contenu vers lequel acheminer le paquet lorsque les champs de protocole et/ou les états de protocole dans l'expression de routage sont vrais. Jusqu'à 256 règles peuvent être configurées pour le routage.

Règles de facturation - Les règles de facturation sont utilisées pour spécifier les actions à entreprendre en fonction de l'analyse effectuée par les analyseurs de contenu. Les actions peuvent inclure la redirection, la valeur de charge et l'émission des enregistrements de facturation.

Configuration des travaux pratiques

Exemple de configuration afin de tester ce scénario dans 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
```

Journaux d'erreur

La trace problématique de l'abonné a été utilisée pour regénérer le réplica exact du trafic HTTP. Lorsque le suivi a été exécuté avec la configuration précédente, ces règles ont été détectées sous le moteur 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
```

Cela dit, il y a des paquets envoyés par l'UE qui ne sont pas des paquets HTTP appropriés et ceux-ci sont classés sous la règle « http-error » qui est présente dans la configuration.

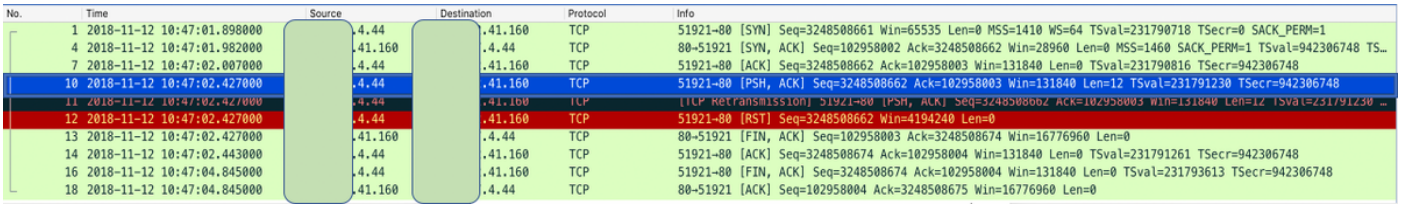
Après avoir vérifié les journaux dans le système, vous pouvez voir que les journaux sont imprimés en tant que message « paquet HTTP non valide » qui s'affiche ici. Vérifiez le message dans ces journaux :

```
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
```

Conformément à la définition présente dans le noeud, l'action de charge de la règle « http-error » est mappée en « block » qui correspondait à ces journaux. En raison de cela, l'abonné final n'a pas pu accéder au site Web car les paquets ont été terminés (flux action de fin de flux) dans le moteur ECS de PGW.

Solution

Après avoir converti le fichier de suivi d'abonné en fichier pcap, vous voyez que ces messages sont échangés 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

En fonction du flux d'appels HTTP, le client doit envoyer la requête HTTP-GET/POST au serveur et demander l'accès une fois que le SYN TCP (vous voyez que dans le paquet no 1, 4 et 7) a été échangé.

Cependant, dans le fichier pcap, aucun trafic HTTP ne s'y trouve. Ainsi, le paquet TCP qui transporte la signalisation HTTP ou la charge utile cause ce problème.

Si vous cochez cette case, la taille de fenêtre TCP autorisée conformément à RFC (rfc-1323) doit être de 6 536 octets (2*16=6 536).

L'en-tête TCP utilise un champ de 16 bits afin de signaler la taille de fenêtre de réception à l'expéditeur. Par conséquent, la plus grande fenêtre pouvant être utilisée est 2**16 = 65 000 octets.

Si vous voyez le paquet 7 WS, il est trop grand pour être d'un paquet ACK (accusé de réception). Normalement, avec l'analyse HTTP activée, le GGSN essaie d'analyser les messages HTTP GET/POST. Lorsque les flux HTTP ne sont pas compatibles RFC, ils peuvent entraîner des erreurs d'analyse (et des échecs afin de classer correctement le flux HTTP comme par URL, etc.).

Comme suspecté, après le paquet ACK (paquet 7), le client n'a pas envoyé de requête HTTP-GET/POST au serveur afin de demander l'accès. Au lieu de cela, « PSH, ACK » est envoyé à partir de l'UE. Ce n'était pas prévu par le moteur ECS de PGW. UE envoyait une charge utile de http (avec le port dest 80) dans les paquets TCP, en raison de quelle passerelle a mis fin à ce flux de paquets lorsqu'il a été filtré et mis en correspondance sous la règle « http-error » qui a une action comme « fin-flow ». Pour PGW, le message attendu de l'UE aurait été HTTP-GET/POST qui n'a pas été vu. Par conséquent, il considérait le paquet 10 comme un paquet incorrect.

Afin de vérifier le doute plus loin, le fichier de trace pcap est modifié lorsque le paquet problématique numéro 10 est supprimé qui a PSH-ACK, et le même appel est réexécuté, où la règle problématique « http-error » ne frappe pas à nouveau sous charge active. Tous les paquets ont été classés sous la règle « ip_any ». Cela indique que le paquet mal formé était le paquet 10.

Reportez-vous à l'exemple de résultat :

```
[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
```

Pour résumer ceci :

Au lieu du paquet HTTP avec la requête **GET/POST**, UE a envoyé un paquet TCP PSH-ACK qui a été considéré comme un paquet mal formé et a été abandonné car il n'était pas le paquet attendu. Le prestataire de services a été informé de ce comportement inapproprié des UE spécifiques. Cisco PGW fonctionne conformément aux normes 3GPP.