Risoluzione dei problemi relativi ai pacchetti HTTP in formato non valido che vengono filtrati ed eliminati da ECS in Cisco PGW

Sommario

Introduzione

In questo documento viene descritto come risolvere i problemi relativi ai pacchetti HTTP in formato non valido che vengono filtrati e scartati da Enhanced Charging Service (ECS) in Cisco Packet Data Network Gateway (PGW).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- StarOS
- ECS

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni di questo documento sono simili a quelle della configurazione presente nel nodo del cliente, ma qui vengono mostrate solo le informazioni rilevanti. Allo scopo di dimostrare le tracce problematiche senza esporre informazioni reali, ho modificato o evidenziato alcune informazioni, ad esempio indirizzi IP.

Problema

Il fornitore di servizi si è lamentato del fatto che alcuni utenti della loro rete non potevano accedere a siti di gioco specifici.

Dopo aver controllato le tracce di tali utenti, è stato rilevato che il traffico problematico era stato classificato nella definizione della regola (ruledef) definita per filtrare i pacchetti di errore HTTP in PGW.

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

Risoluzione dei problemi

Informazioni su ruledef

Il rilevamento del traffico HTTP degli abbonati viene eseguito dagli analizzatori di protocollo presenti in ECS.

ECS dispone di analizzatori di protocollo che esaminano il traffico uplink e downlink. Il traffico in entrata viene indirizzato a un analizzatore di protocolli per l'ispezione dei pacchetti. Per determinare i pacchetti da ispezionare, vengono applicati i valori predefiniti delle regole di routing. Questo traffico viene quindi inviato al motore di ricarica in cui vengono applicati i valori di riferimento per la ricarica al fine di eseguire azioni quali il blocco, il reindirizzamento o la trasmissione. Questi analizzatori generano inoltre record di utilizzo per il sistema di fatturazione.

I valori predefiniti sono espressioni definite dall'utente in base ai campi del protocollo e agli stati del protocollo, che definiscono le azioni da eseguire sui pacchetti quando i valori dei campi specificati corrispondono.

Di seguito sono riportati i valori predefiniti utilizzati principalmente in un documento per la risoluzione dei problemi:

Regole di instradamento: le regole di instradamento vengono utilizzate per instradare i pacchetti agli analizzatori di contenuto. Le regole di instradamento determinano a quale analizzatore di contenuti instradare il pacchetto quando i campi del protocollo e/o gli stati del protocollo nell'espressione ruledef sono true. È possibile configurare fino a 256 valori di default delle regole per il routing.

Regole di addebito: le regole di addebito vengono utilizzate per specificare l'azione da intraprendere in base all'analisi eseguita dagli analizzatori di contenuto. Le azioni possono includere il reindirizzamento, il valore di addebito e l'emissione dei record di fatturazione.

Configurazione Lab

La configurazione di esempio per verificare questo scenario in 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
```

Registri errori

La traccia con problemi del Sottoscrittore è stata utilizzata per rigenerare l'esatta replica del traffico HTTP. Quando la traccia è stata eseguita con la configurazione precedente, questi valori di default delle regole sono stati rilevati nel motore 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
```

Questo messaggio segnala la presenza nella configurazione di alcuni pacchetti inviati da UE che non sono pacchetti HTTP corretti e che sono classificati nella definizione delle regole "http-error".

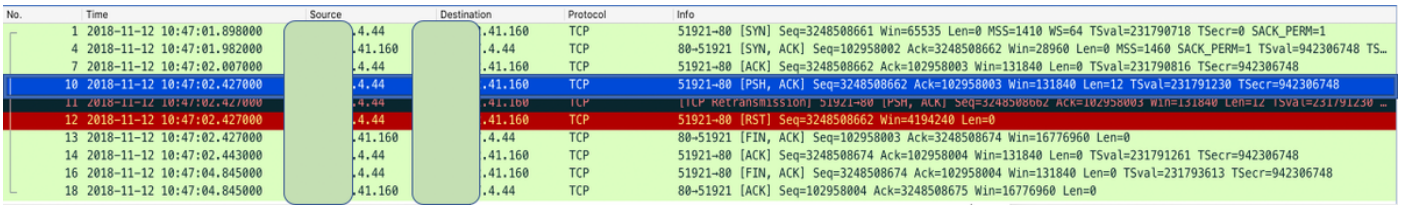
Dopo aver controllato i log nel sistema, si noterà che i log vengono stampati come messaggio "HTTP packet not valid" visualizzato in quel punto. Controllare il messaggio nei seguenti registri:

```
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
```

In base alla definizione presente nel nodo, l'azione di addebito di ruledef "http-error" è mappata come "blocco" corrispondente a questi registri. Per questo motivo, l'utente finale non è stato in grado di accedere al sito Web perché i pacchetti sono stati terminati (azione di flusso termina-flusso) nel motore ECS di PGW.

Soluzione

Dopo aver convertito il file di traccia del sottoscrittore nel file pcap, si noterà che questi messaggi vengono scambiati tra il client (sottoscrittore finale) e il server.



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

In base al flusso di chiamata HTTP, il client deve inviare una richiesta HTTP-GET/POST al server e chiedere l'accesso una volta scambiata la SYN TCP (nel pacchetto n. 1, 4 e 7).

Tuttavia, nel file pcap non viene visualizzato alcun traffico HTTP al suo interno. Il problema è causato quindi dal pacchetto TCP che trasmette il payload o la segnalazione HTTP.

Se si seleziona questa opzione, le dimensioni della finestra TCP consentite in base alla RFC (rfc-1323) dovrebbero essere di 65536 byte (2*16=65536).

L'intestazione TCP utilizza un campo a 16 bit per segnalare le dimensioni della finestra di ricezione al mittente. Pertanto, la finestra più grande che può essere utilizzata è 2**16 = 65K byte.

Se il pacchetto 7 WS è visibile, è troppo grande per essere un pacchetto di conferma (ACK). In genere, se l'analisi HTTP è attivata, il GSN tenta di analizzare i messaggi HTTP GET/POST. Quando i flussi HTTP non sono conformi alla RFC, potrebbero verificarsi errori di analisi (e errori per classificare correttamente il flusso HTTP in base all'URL e così via).

Come sospettato, dopo il pacchetto ACK (pacchetto 7), il client non ha inviato una richiesta HTTP-GET/POST al server per richiedere l'accesso. Invece, "PSH,ACK" viene inviato da UE. Ciò non era previsto dal motore PGW ECS. UE stava inviando il payload di http (con la porta di destinazione 80) all'interno dei pacchetti TCP, a causa del quale il gateway ha terminato il flusso del pacchetto come era stato filtrato e ha trovato una corrispondenza nella regola "http-error" che ha azione come "terminate-flow". Per PGW, il messaggio previsto da UE sarebbe stato HTTP-GET/POST che non è stato visualizzato. Pertanto, ha considerato il pacchetto 10 come non valido.

Per verificare ulteriormente il dubbio, il file di traccia pcap viene modificato quando viene rimosso il pacchetto con problemi numero 10 che ha PSH-ACK e la stessa chiamata viene rieseguita, dove il problema "http-error" ruledef non si ripresenta in modalità di caricamento attivo. Tutti i pacchetti sono stati classificati sotto "ip_any" ruledef. Dice che il pacchetto non valido era il pacchetto 10.

Fare riferimento all'output di esempio:

```
[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
```

In sintesi:

Al posto del pacchetto HTTP con richiesta **GET/POST**, UE ha inviato un pacchetto TCP PSH-ACK considerato in formato non valido e quindi scartato perché diverso da quello previsto. Il provider di servizi è stato informato di questo comportamento improprio degli UE specifici. Il PGW Cisco funziona secondo gli standard 3GPP.