P2P plug-in classificatie en detectiefout voor toepassing met SSL-stromen in ASR5x00

Inhoud

Inleiding

Dit document beschrijft een specifiek scenario waarin de abonnee gratis toepassingen zoals Whatsapp, Snapchat enzovoort gebruikt met Secure Socket Layer (SSL) en tegelijk ander gebruikersverkeer blokkeert. Deze specifieke toepassing draait op Cisco Aggregated Service Routers (ASR) 5x00 Series. SSL is een computernetwerk protocol dat serververificatie, clientverificatie en versleutelde communicatie tussen servers en klanten beheert.

Probleem

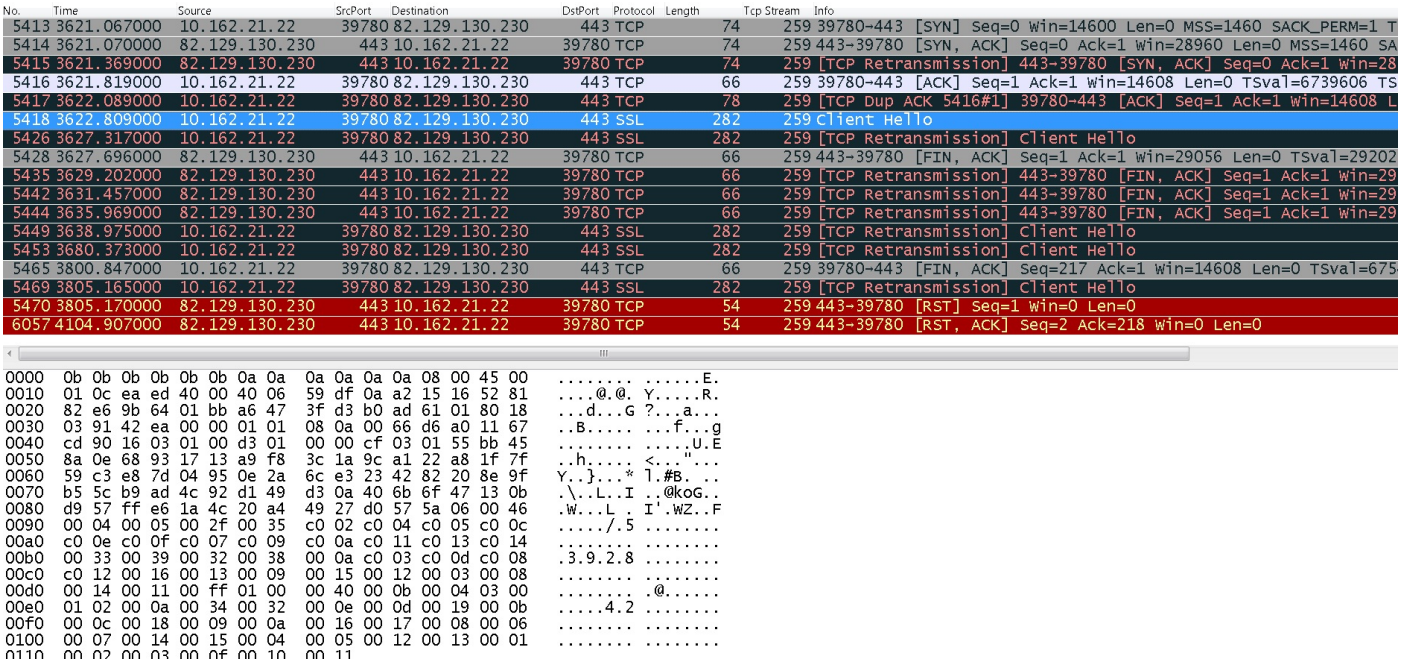
Om een app te detecteren, hebt u een aantal initiële pakketten nodig voor de analyse. Aan deze twee tegenstrijdige eisen wordt zoveel mogelijk voldaan.

a) De detectie moet plaatsvinden in het eerste pakket zelf

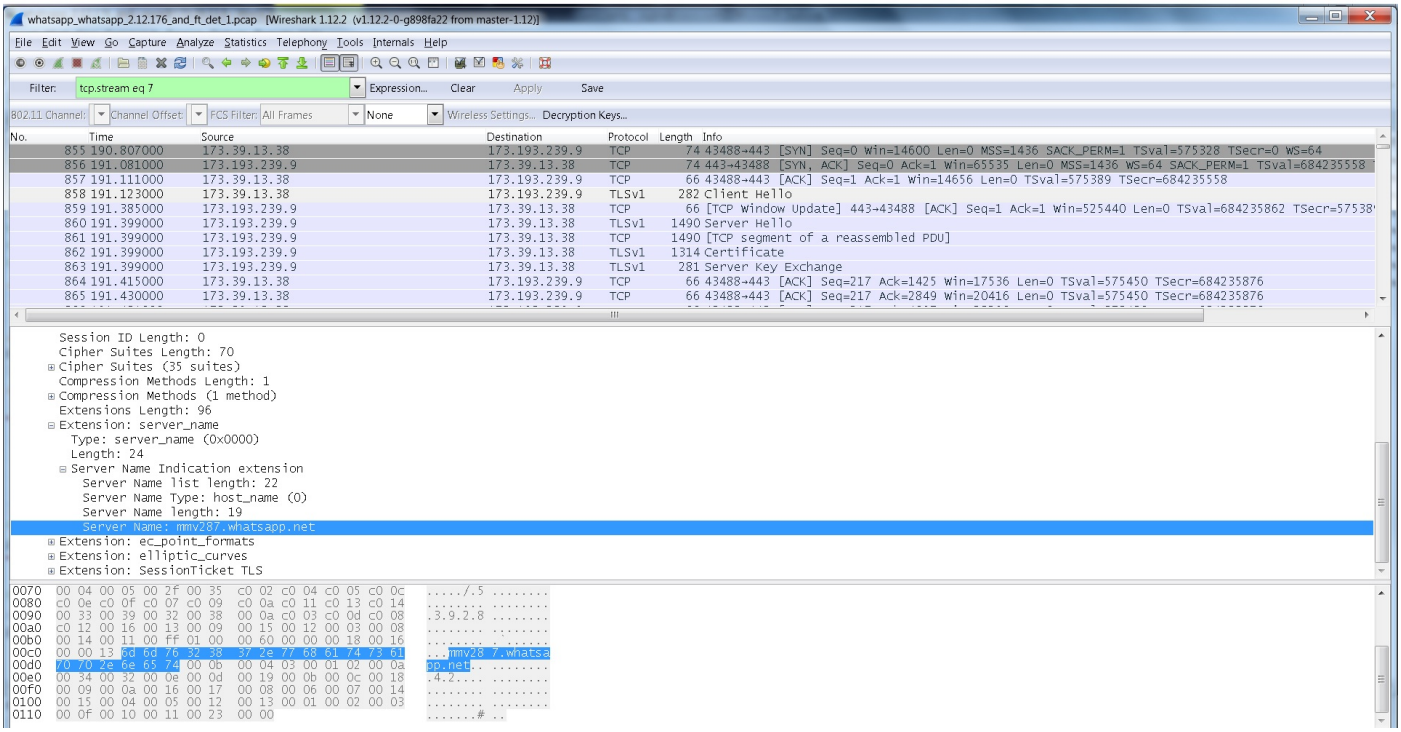
b) Nauwkeurigheid van de detectie moet 100% zijn

Als u probeert te voldoen aan vereiste (a) & alle apps in het eerste pakket te markeren (dat praktisch niet mogelijk is), lijdt de eis (b) op detectie accuratesse aan. Om de detectie accuraat goed te maken, hebt u meer pakketten nodig om veel apps te analyseren (er zijn apps en stromen waar de app wordt gedetecteerd in het eerste pakket zelf). Het geval van dezelfde app is dat u bepaalde stromen in het eerste pakket zelf kunt markeren terwijl andere stromen van dezelfde app meer pakketten nodig hebben ter analyse.

Dus als een app een gratis beoordeling heeft terwijl u een ander verkeer blokkeert, kan er gebeuren dat de eerste verpakking van de app niet wordt gedetecteerd omdat deze niet voldoende informatie bevat. In het bijzonder geval van apps die op SSL stromen worden gebaseerd, wordt het protocol gemarkeerd met behulp van het server-name-Indicatieveld dat in het client-hallo-pakket aanwezig is of het common-name dat in het SSL-certificaat aanwezig is. Aangezien de server-name optioneel veld is, is het niet altijd aanwezig. Zoals in deze afbeelding wordt getoond, in een Whatsapp SSL-stroming, na Driemaands Handshake (TWH), wordt het client-hallo-pakket door de app verzonden. **Een PCAP-sporen die geen veld van de servernaam (SNI) tonen. Ook worden er meerdere terugzendingen van client hallo-pakketten gezien die uiteindelijk worden laten vallen.**



Zoals in deze afbeelding wordt getoond, zijn hun de hex-bytes voor het client-hallo-pakket waarin het SNI-veld, gebruikt voor het markeren van Whatsapp, niet aanwezig is. Daarom kan het client-hallo-pakket niet worden gemarkeerd als Whatsapp en onopgemerkt blijven. Aangezien dit pakje in een andere groep met meerdere beoordelingen valt, wordt het ingetrokken en worden dus meerdere terugzendingen van client-hallo-pakje gezien (zie frame nr. 5449, 5453, 5469). Ten slotte wordt de verbinding beëindigd. In het beschermkapje zijn al dergelijke stromen te zien. Dit is de reden dat geen bruikbare activiteit, bijvoorbeeld het uploaden van afbeeldingen voor Whatsapp, kan worden
uitgevoerd.



Problemen oplossen

1. capture monitor subscriber imsi XXXX with following options

```
19 - User L3
X - PDU Hexdump
Verbosity level 5
```

Deze opdrachten geven de status van de analysator voor de toepassingen.

```
# show act analyzer statistics name p2p application snapchat
# show act analyzer statistics name p2p application whatsapp
```

Zo controleert u de stekker:

```
#show plugin p2p
Wednesday July 29 22:12:07 SAST 2015
plugin p2p
  patch-directory /var/opt/lib
  base-directory /lib
  base-version 1.50.52055
  module priority 1 version 1.139.505
```

Oplossing

Om te voorkomen, moet u ervoor zorgen dat de pakketten voordat een app (bijvoorbeeld whatsapp) wordt gemarkeerd en doorlopen.

Gebruik deze regel :

```
ruledef ssl_clienthello
      tcp either-port = 443
      tcp payload-length >= 44
      tcp payload  starts-with hex-signature 16-03
#exit
```

Alle pakketten die overeenkomen met de bovenstaande regels, mogen niet worden ingetrokken. De prioriteit van deze regel moet net boven de standaardregel staan (ip-any ruledef) die dit pakket pakte en ervoor zorgde dat het werd gedropt.

Door deze configuratie te gebruiken, worden alleen de pakketten die overeenkomen met de bovenstaande drie regels gratis bevonden. Deze omvatten slechts de eerste handdruk pakketten in SSL stroom (zoals client-hallo, server-hallo) die gebruikt deze ruledef worden toegestaan, terwijl alle andere pakketten in SSL stroom niet deze ruledef aanpassen. Als er dus een SSLflow is die van een andere app hoort (anders dan whatsapp die u wilt vrijgeven), kan er geen bruikbare transactie zijn, omdat alleen de eerste twee tot drie pakketten van een SSL-stroom deze regel mogen gebruiken.

Monsterconfiguratie

De voorgestelde ruledef moet een hogere prioriteit hebben dan all-ip_004_012_00016 ruledef (ip any-match = TRUE) en

oplaadactie die het verkeer mogelijk maakt vergelijkbaar met whatsapp ruledef.(sid_040_rg_400_rate_9999/sid_040_rg_400_rate_0032/ sid_040_rg_400_0_0 064 met rating-groep 400 en alle tarieven).

Met deze configuratie, bereikt het client hallo pakket de voorgestelde regel en wordt toegestaan in plaats van opnieuw gericht. Dit zijn de twee achtergronden waarop de volgende regels zijn

vastgesteld:

rulebase mbc-internet-rs action priority 1087 dynamic-only ruledef WhatsApp_P2P_040_400_99999_All_internet charging-action sid_040_rg_400_rate_99999 action priority 1088 dynamic-only ruledef WhatsApp_P2P_040_400_00064_All_internet charging-action sid_040_rg_400_rate_00064 action priority 1089 dynamic-only ruledef WhatsApp_P2P_040_400_00032_All_internet charging-action sid_040_rg_400_rate_00032 **action priority [1090-9909] dynamic-only ruledef ssl_clienthello charging-action sid_040_rg_400_rate99999/00064/00032 --> Higher priority than all-ip ruledef and charging action with rating group 400**
action priority 9910 dynamic-only ruledef all-ip_004_012_00016_MI_internet charging-action sid_004_rg_012_rate_00016
action priority 9920 dynamic-only ruledef all-ip_004_012_00032_MI_internet charging-action sid_004_rg_012_rate_00032
action priority 9930 dynamic-only ruledef all-ip_004_012_00064_MI_internet charging-action sid_004_rg_012_rate_00064

rulebase mbc-iphone-rs
action priority 1206 dynamic-only ruledef WhatsApp_P2P_040_400_99999_All_iphone charging-action sid_040_rg_400_rate_99999
action priority 1207 dynamic-only ruledef WhatsApp_P2P_040_400_00064_All_iphone charging-action sid_040_rg_400_rate_00064
action priority 1208 dynamic-only ruledef WhatsApp_P2P_040_400_00032_All_iphone charging-action sid_040_rg_400_rate_00032
action priority [1209-8999] dynamic-only ruledef ssl_clienthello charging-action sid_040_rg_400_rate99999/00064/00032 --> Higher priority than all-ip ruledef and charging action with rating group 400
action priority 9000 dynamic-only ruledef all-ip_015_150_00016_ALL_iphone charging-action sid_015_rg_150_rate_00016
action priority 9010 dynamic-only ruledef all-ip_015_150_00032_ALL_iphone charging-action sid_015_rg_150_rate_00032
action priority 9020 dynamic-only ruledef all-ip_015_150_00064_ALL_iphone charging-action sid_015_rg_150_rate_00064
action priority 9030 dynamic-only ruledef all-ip_015_150_99999_ALL_iphone charging-action sid_015_rg_150_rate_99999

charging-action sid_040_rg_400_rate_99999
content-id 400
service-identifier 40
billing-action egcdr
cca charging credit
exit

ruledef ssl_clienthello
tcp either-port = 443
tcp payload-length >= 44
tcp payload starts-with hex-signature 16-03
exit