

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

## Inhoud

[Inleiding](#)

[Probleem](#)

[Problemen oplossen](#)

[Oplossing](#)

[Monsterconfiguratie](#)

[Gerelateerde Cisco Support Community-discussies](#)

## 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.**

No.	Time	Source	SrcPort	Destination	DestPort	Protocol	Length	Tcp Stream	Info
5413	3621.067000	10.162.21.22	39780	82.129.130.230	443	TCP	74	259 39780-443	[SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 T
5414	3621.070000	82.129.130.230	443	10.162.21.22	39780	TCP	74	259 443-39780	[SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SA
5415	3621.369000	82.129.130.230	443	10.162.21.22	39780	TCP	74	259	[TCP Retransmission] 443-39780 [SYN, ACK] Seq=0 Ack=1 Win=28
5416	3621.819000	10.162.21.22	39780	82.129.130.230	443	TCP	66	259 39780-443	[ACK] Seq=1 Ack=1 Win=14608 Len=0 Tsval=6739606 TS
5417	3622.089000	10.162.21.22	39780	82.129.130.230	443	TCP	78	259	[TCP Dup ACK 5416#1] 39780-443 [ACK] Seq=1 Ack=1 WIn=14608 L
5418	3622.809000	10.162.21.22	39780	82.129.130.230	443	SSL	282	259	Client Hello
5426	3627.317000	10.162.21.22	39780	82.129.130.230	443	SSL	282	259	[TCP Retransmission] Client Hello
5428	3627.696000	82.129.130.230	443	10.162.21.22	39780	TCP	66	259 443-39780	[FIN, ACK] Seq=1 Ack=1 Win=29056 Len=0 Tsval=29202
5435	3629.202000	82.129.130.230	443	10.162.21.22	39780	TCP	66	259	[TCP Retransmission] 443-39780 [FIN, ACK] Seq=1 Ack=1 Win=29
5442	3631.457000	82.129.130.230	443	10.162.21.22	39780	TCP	66	259	[TCP Retransmission] 443-39780 [FIN, ACK] Seq=1 Ack=1 Win=29
5444	3635.969000	82.129.130.230	443	10.162.21.22	39780	TCP	66	259	[TCP Retransmission] 443-39780 [FIN, ACK] Seq=1 Ack=1 Win=29
5449	3638.975000	10.162.21.22	39780	82.129.130.230	443	SSL	282	259	[TCP Retransmission] Client Hello
5453	3680.373000	10.162.21.22	39780	82.129.130.230	443	SSL	282	259	[TCP Retransmission] Client Hello
5465	3800.847000	10.162.21.22	39780	82.129.130.230	443	TCP	66	259 39780-443	[FIN, ACK] Seq=217 Ack=1 Win=14608 Len=0 Tsval=675
5469	3805.165000	10.162.21.22	39780	82.129.130.230	443	SSL	282	259	[TCP Retransmission] Client Hello
5470	3805.170000	82.129.130.230	443	10.162.21.22	39780	TCP	54	259 443-39780	[RST] Seq=1 Win=0 Len=0
6057	4104.907000	82.129.130.230	443	10.162.21.22	39780	TCP	54	259 443-39780	[RST, ACK] Seq=2 Ack=218 Win=0 Len=0

```

0000 0b 0b 0b 0b 0b 0a 0a 0a 0a 08 00 45 00 .....E.
0010 01 0c ea ed 00 40 06 59 df 0a a2 15 16 52 81 ...@.@.Y....R.
0020 82 e6 9b 64 01 bb a6 47 3f d3 b0 ad 61 01 80 18 ...d..G?.a..
0030 03 91 42 ea e0 00 01 01 08 0a 00 66 d6 a0 11 67 ..B.....f..g
0040 cd 90 16 03 01 00 d3 01 00 00 cf 03 01 55 bb 45 .....U.E
0050 8a 0e 68 93 17 13 a9 f8 3c 1a 9c a1 22 a8 1f 7f ..h.....<".
0060 59 c3 e8 7d 04 95 0e 2a 6c e3 23 42 82 20 8e 9f Y..}.*l.#B...
0070 b5 5c b9 ad 4c 92 d1 49 d3 0a 40 6b 6f 47 13 0b \.L.I'.@kog..
0080 d9 57 ff e6 1a 4c 20 a4 49 27 d0 57 5a 06 00 46 .w.L.I'.wz..F
0090 00 04 00 05 00 2f 00 35 c0 02 c0 04 c0 05 c0 0c ...../5.....
00a0 c0 0e c0 0f c0 07 c0 09 c0 0a c0 11 c0 13 c0 14 .....
00b0 00 33 00 39 00 32 00 38 00 0a c0 03 c0 0d c0 08 .3.9.2.8.....
00c0 c0 12 00 16 00 13 00 09 00 15 00 12 00 03 00 08 .....
00d0 00 14 00 11 00 ff 01 00 00 40 00 0b 00 04 03 00 .....@.....
00e0 01 02 00 0a 00 34 00 02 00 0e 00 0d 00 19 00 0b .....4.2.....
00f0 00 0c 00 18 00 09 00 0a 00 16 00 17 00 08 00 06 .....
0100 00 07 00 14 00 15 00 04 00 05 00 12 00 13 00 01 .....
0110 00 02 00 03 00 0f 00 10 00 11 .....#

```

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.

The screenshot shows a Wireshark capture of a TLS client hello packet. The packet list pane shows frame 865 (Time: 191.430000) as a TLSv1 Client Hello from 173.193.239.9 to 173.193.239.9. The packet details pane shows the following structure:

- Session ID Length: 0
- Cipher Suites Length: 70
- Compression Methods Length: 1
- Extensions Length: 96
- Extension: server\_name
  - Type: server\_name (0x0000)
  - Length: 24
  - Server Name Indication extension
    - Server Name list length: 22
    - Server Name Type: host\_name (0)
    - Server Name length: 19
    - Server Name: mmv287.whatsapp.net
- Extension: ec\_point\_formats
- Extension: elliptic\_curves
- Extension: session\_ticket\_TLS

The packet bytes pane shows the hex data for the client hello, with the SNI field highlighted in blue:

```

0070 00 04 00 05 00 2f 00 35 c0 02 c0 04 c0 05 c0 0c ...../5.....
0080 c0 0e c0 0f c0 07 c0 09 c0 0a c0 11 c0 13 c0 14 .....
0090 00 33 00 39 00 32 00 38 00 0a c0 03 c0 0d c0 08 .3.9.2.8.....
00a0 c0 12 00 16 00 13 00 09 00 15 00 12 00 03 00 08 .....
00b0 00 14 00 11 00 ff 01 00 00 40 00 0b 00 04 03 00 .....@.....
00c0 00 00 15 00 00 00 00 00 00 00 00 00 00 00 00 .....mmv287.whatsapp
00d0 00 01 02 00 0a 00 34 00 02 00 0e 00 0d 00 19 00 0b .....4.2.....
00e0 00 09 00 0a 00 16 00 17 00 08 00 06 00 07 00 14 .....
00f0 00 0c 00 18 00 09 00 0a 00 16 00 17 00 08 00 06 .....
0100 00 07 00 14 00 15 00 04 00 05 00 12 00 13 00 01 .....
0110 00 0f 00 10 00 11 00 23 00 00 .....#

```

## 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
```