ASR5x00中具有SSL流的應用程式的P2P外掛分類和檢測故障

目錄

簡介

本文描述一個特定的場景，在該場景中，使用者使用自由速率應用程式（如Whatsapp、Snapchat等）和安全套接字層(SSL)流，同時阻止其他使用者流量。此特定應用運行在思科聚合服務路由器(ASR)5x00系列上。SSL是一種電腦網路協定，用於管理伺服器身份驗證、客戶端身份驗證以及伺服器和客戶端之間的加密通訊。

問題

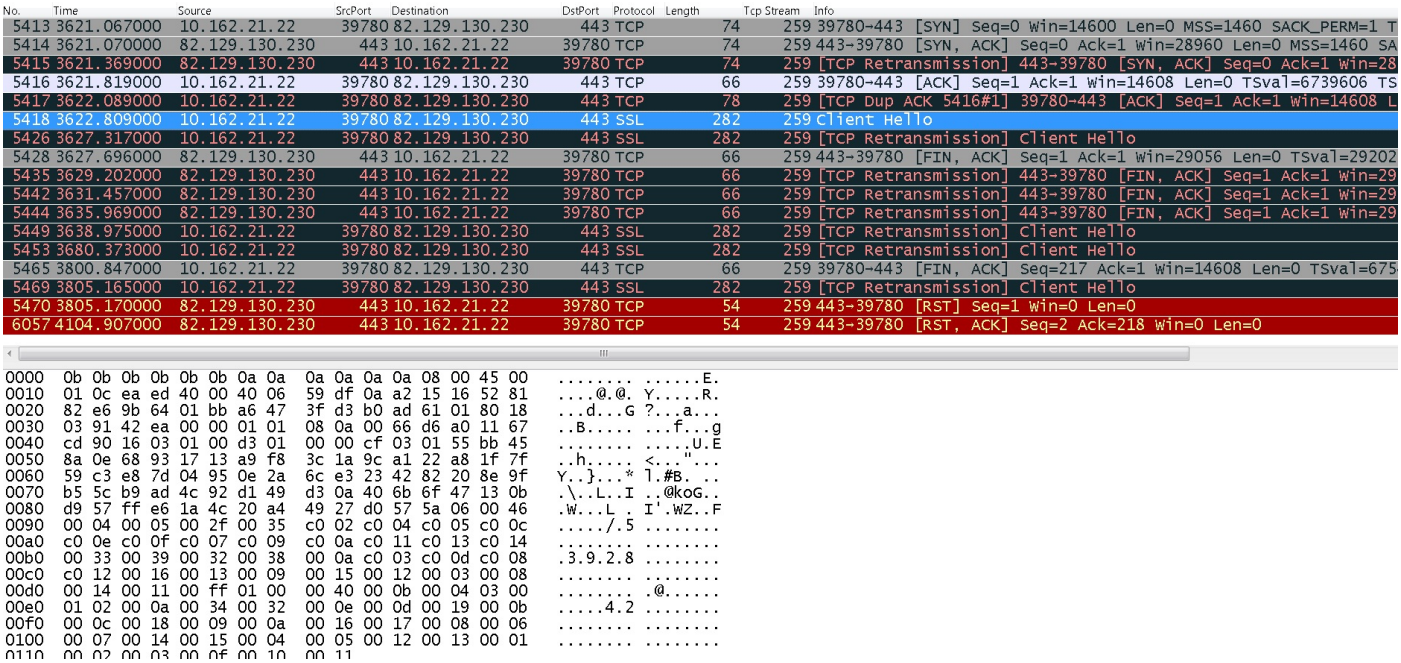
要檢測任何應用，您需要一些用於分析的初始資料包。這兩個相互矛盾的要求得到最大程度的滿足。

a)檢測必須在第一個資料包本身進行

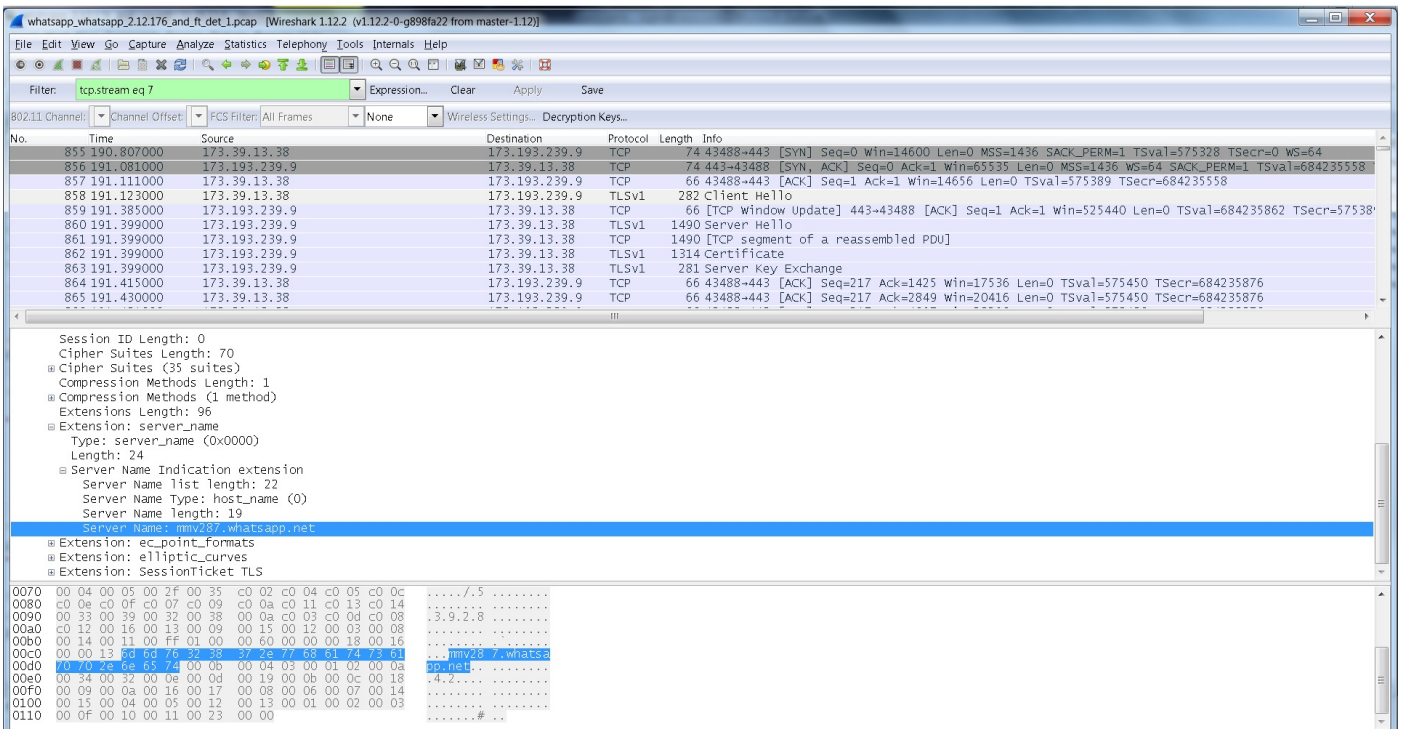
b)檢測準確度必須為100%

如果您嘗試滿足要求(a)並在第一個資料包中標籤所有應用（這在實際上是不可能的），則對檢測準確性的要求(b)會受到影響。為了保證檢測準確度，您需要更多的資料包來分析大量應用（在第一個資料包本身中檢測到應用存在應用和流）。 對於同一應用，可能會發生以下情況：您可以標籤第一個資料包本身中的某些流，而同一應用的其他流需要更多資料包進行分析。

因此，如果在阻止任何其它流量的同時為任何應用提供免費評級，則可能會發生應用的初始資料包由於未攜帶足夠資訊而無法被檢測的情況。在基於SSL流的應用的特定情況下，協定使用在client-hello資料包中存在的server-name-indication欄位或SSL證書中存在的common-name進行標籤。由於server-name是可選欄位，因此它並非始終存在。 如下圖所示，在Whatsapp SSL流中，在三次握手(TWH)之後，應用將傳送客戶端hello資料包。**一個PCAP跟蹤，其中未顯示伺服器名稱指示(SNI)欄位。另外還可以看到客戶端hello資料包多次重傳，最終被丟棄。**



此外，如本圖所示，它們是不存在SNI欄位（用於標籤Whatsapp）的client-hello資料包的十六進位制位元組。因此，無法將client-hello資料包標籤為Whatsapp，並且無法檢測到該資料包。當此資料包落入不同的評級組時，它會被丟棄，因此會看到多個客戶端hello資料包的重傳（參見5449、5453、5469幀）。 最後，連線終止。在pcap中可以看到一些這樣的流動。這就是沒有有用的活動（例如Whatsapp的映像上傳）可以完成的原因。



疑難排解

```
1. capture  monitor subscriber imsi XXXX with following options
19 - User L3
X - PDU Hexdump
Verbosity level 5
```

這些命令提供應用程式的分析器統計資訊。

```
# show act analyzer statistics name p2p application snapchat
# show act analyzer statistics name p2p application whatsapp
```
檢查外掛版本：

```
#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
```

解決方案

為了避免這種情況的發生，您需要確保在應用（比如whatsapp）被標籤之前的資料包必須通過。

使用以下規則：

```
ruledef ssl_clienthello
      tcp either-port = 443
      tcp payload-length >= 44
      tcp payload  starts-with hex-signature 16-03
#exit
```
任何與以上規則def匹配的資料包都不得丟棄。此ruledef的優先順序必須剛好高於與此資料包匹配並導致其丟棄的預設ruledef(ip-any ruledef)。

使用此組態時，只有符合上述三條規則線的封包會免費評分。這些資料包僅包含允許使用此ruledef的SSL流中的初始握手資料包（例如client-hello和server-hello），而SSL流中的所有其他資料包均與此ruledef不匹配。因此，如果存在屬於某個其他應用（您希望自由速率的whatsapp除外）的SSLflow，則不會存在任何有用的事務，因為只允許一個SSL流的前兩個到三個資料包使用此規則def。

示例配置

建議的ruledef的優先順序需要高於all-ip_004_012_00016 ruledef(ip any-match = TRUE)和

計費操作，允許類似於whatsapp ruledef.(sid_040_rg_400_rate_99999/sid_040_rg_400_rate_00032/ sid_040_rg_400_rate_00064 with rating-group 400 and any rate)的流量。

使用此配置，客戶端hello資料包將到達提議的ruledef並被允許而不是被重定向。以下是whatsapp規則可見的兩個規則庫：

```
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
```