ASR5x00中SSL流应用的P2P插件分类和检测故障

目录

简介

本文档介绍一种特定场景，在这种场景中，用户在阻止其他用户流量的同时，使用Whatsapp、Snapchat等具有安全套接字层(SSL)流的免费速率应用。此特定应用在思科聚合服务路由器(ASR)5x00系列上运行。SSL是一种计算机网络协议，用于管理服务器身份验证、客户端身份验证以及服务器与客户端之间的加密通信。

问题

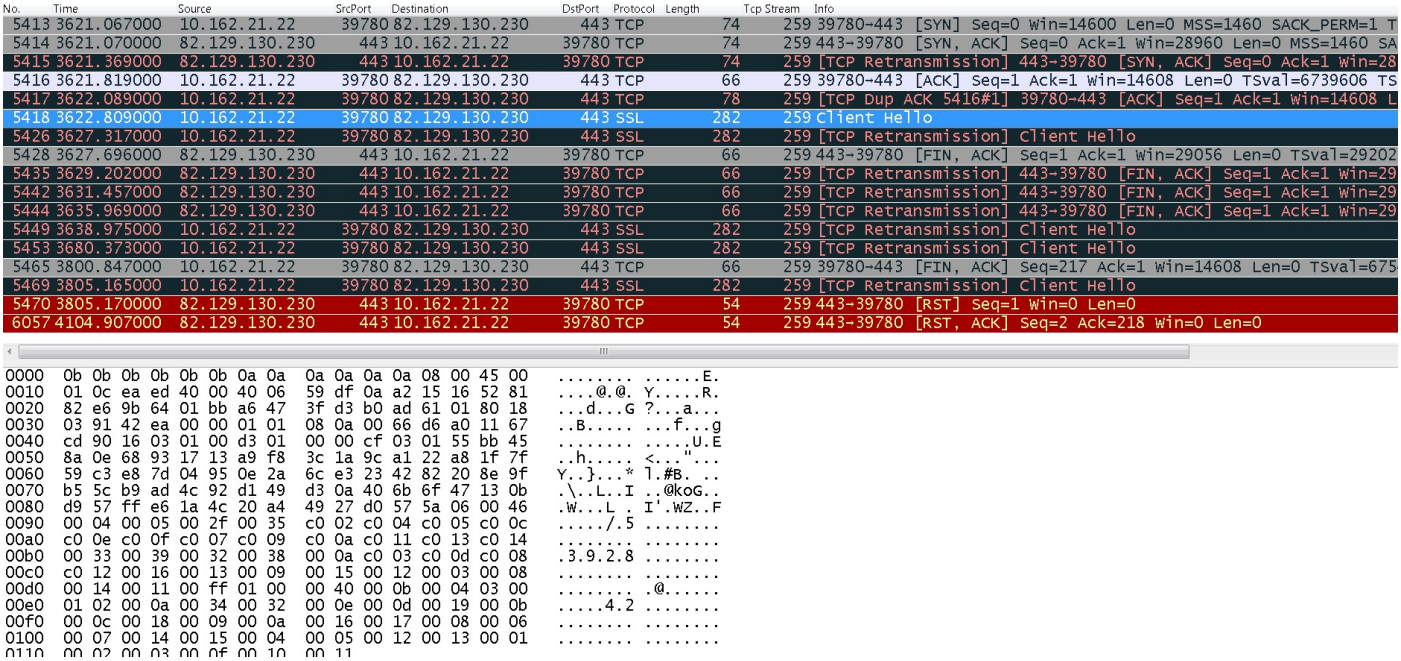
要检测任何应用，您需要一些初始数据包进行分析。这两个矛盾的要求尽可能的得到满足。

a)检测必须发生在第一个数据包本身

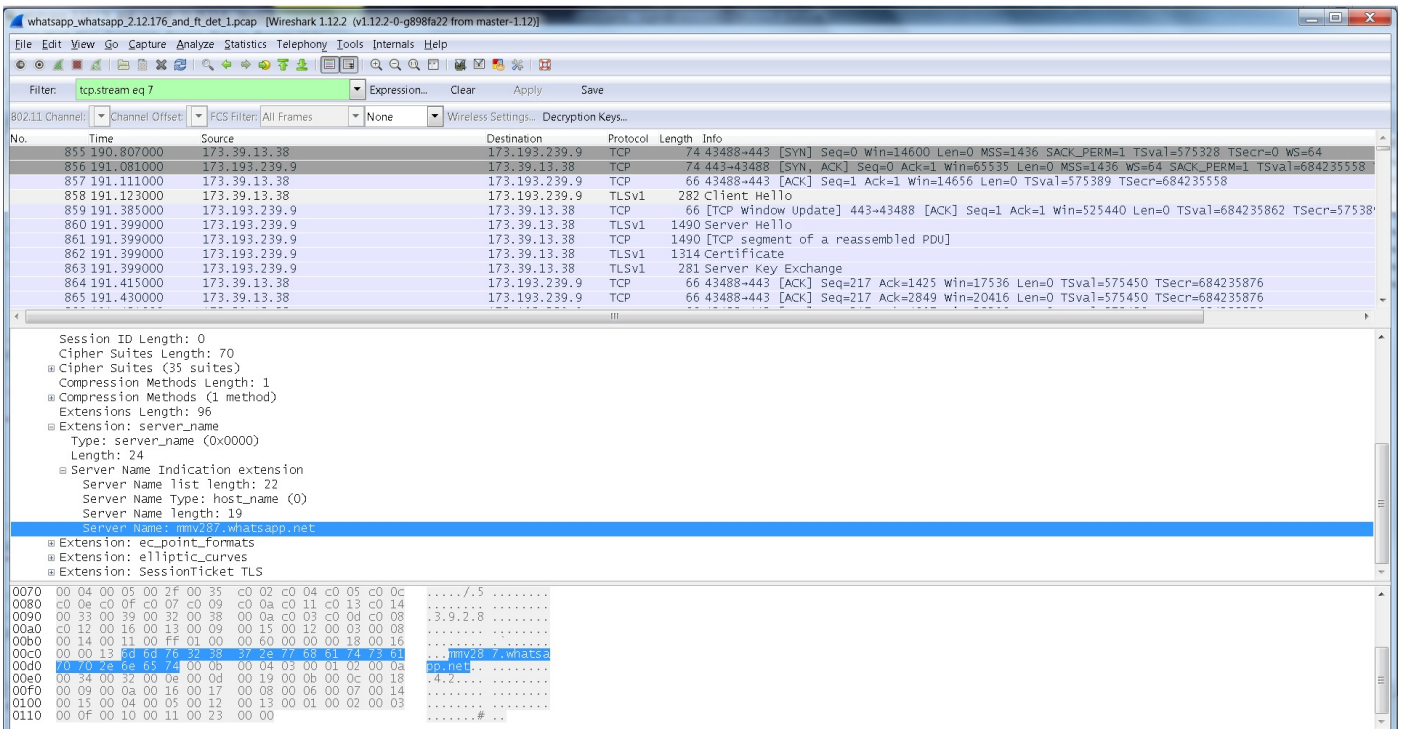
b)检测准确率必须为100%

如果您尝试满足要求(a)并标记第一个数据包中的所有应用（这实际上不可能），则对检测准确性的要求(b)会受到影响。为了使检测准确性良好，您需要更多数据包来分析许多应用（在第一个数据包中检测到应用的应用和流）。 对于同一应用，您可能能够在第一个数据包中标记某些流量，而同一应用的其他流量需要更多数据包进行分析。

因此，如果任何应用在阻止任何其他流量时被免费评级，则可能会发生应用的初始数据包未被检测到，因为它没有传输足够的信息。在基于SSL流的应用的特定情况下，协议使用客户端 — hello数据包中存在的server-name-indication字段或SSL证书中存在的公用名进行标记。由于server-name是可选字段，因此并非始终存在。 如此图所示，在Whatsapp SSL流中，在三次握手(TWH)后，客户端hello数据包由应用发送。**显示无服务器名称指示(SNI)字段的PCAP跟踪。此外，还可以看到最终被丢弃的客户端hello数据包的多次重新传输。**



此外，如此图所示，它们是客户端呼叫数据包的十六进制字节，其中不存在用于标记Whatsapp的SNI字段。因此，客户端问候数据包不能标记为Whatsapp且不被检测。由于此数据包属于不同的额定组，因此会被丢弃，因此会看到客户端呼叫数据包的多次重新传输（请参阅帧号5449、5453、5469）。 最后，连接终止。在pcap中可以看到多种此类流。这是无法执行任何有用活动（例如Whatsapp的映像上传）的原因。



故障排除

1. capture monitor subscriber imsi XXXX with following options
19 - User L3
X - PDU Hexdump
Verbosity level 5
这些命令提供分析器的应用统计信息。

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

要检查插件版本，请执行以下操作：

```
#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
```

解决方案

为避免这种情况，您需要确保应用（例如whatsapp）之前的数据包被标记并必须通过。

使用此规则def:

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

不能丢弃与上述规则定义匹配的任何数据包。此规则def的优先级必须刚好高于匹配此数据包并导致其被丢弃的默认规则def(ip-any ruledef)。

使用此配置时，只有与上述三条规则行匹配的数据包是空闲额定的。这些仅包括使用此规则def允许的SSL流中的初始握手数据包（如client-hello、server-hello），而SSL流中的所有其他数据包与此规则def不匹配。因此，如果有属于某个其他应用（您想要自由速率的什么应用除外）的SSLflow，则不能有任何有用的事务，因为仅允许SSL流的初始两到三个数据包使用此规则定义。

配置示例

建议的ruledef的优先级需要高于all-ip_004_012_00016 ruledef(ip any-match = TRUE),

允许与whatsapp ruledef类似的流量的计费操作。(sid_040_rg_400_rate_99999/sid_040_rg_400_rate_00032/sid_040_rg_400_rate_00064，带rating-group 400和any rate)。

使用此配置时，客户端hello数据包将符合建议的规则定义，并且允许该数据包，而不是被重定向。以下是查看哪些应用规则的两个规则库：

```
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
```