ASR5x00에서 SSL 플로우를 사용하는 애플리케이션에 대한 P2P 플러그인 분류 및 탐지 실패

목차

소개

이 문서에서는 가입자가 SSL(Secure Sockets Layer) 플로우와 함께 Whatsapp, Snapchat 등과 같은 무료 속도 애플리케이션을 사용하면서 다른 사용자 트래픽을 차단하는 특정 시나리오를 설명합니다.이 애플리케이션은 Cisco ASR(Aggregated Service Router) 5x00 시리즈에서 실행됩니다 .SSL은 서버와 클라이언트 간의 서버 인증, 클라이언트 인증 및 암호화된 통신을 관리하는 컴퓨터 네트워킹 프로토콜입니다.

문제

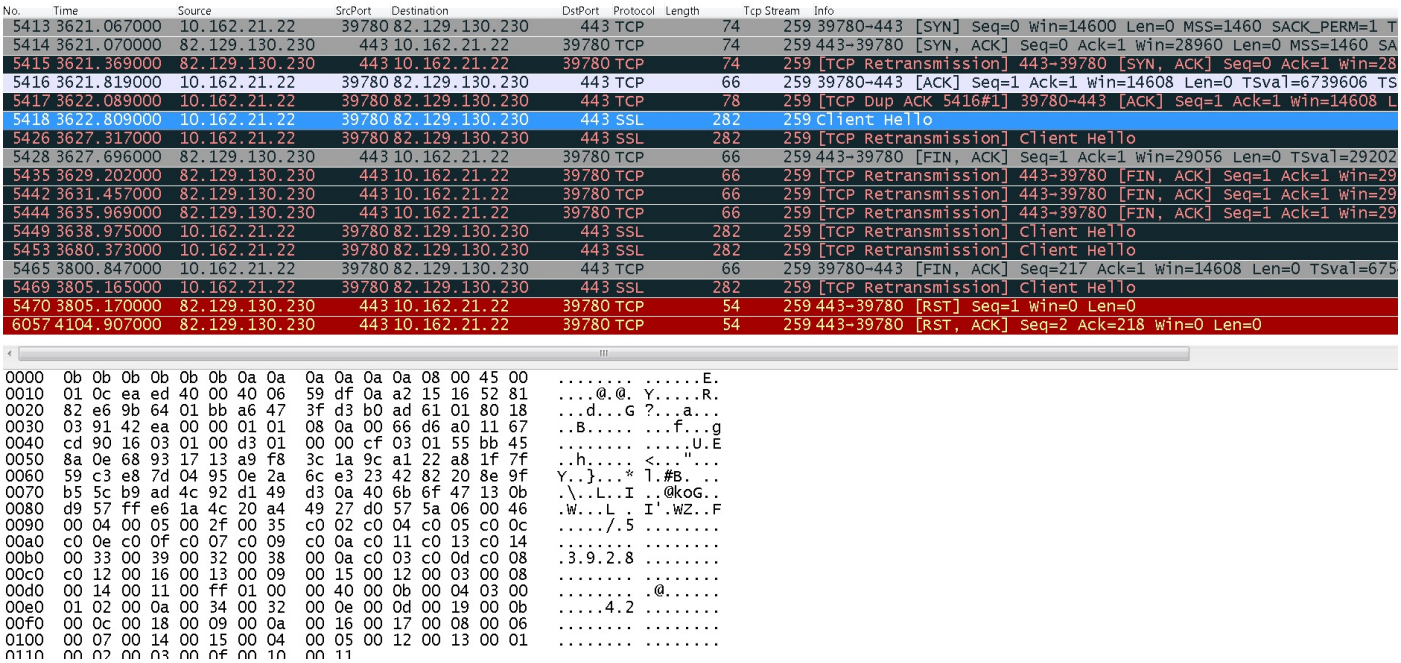
앱을 탐지하려면 분석을 위한 몇 가지 초기 패킷이 필요합니다.이 두 가지 모순된 요구 사항은 가능한 한 최대한 이행됩니다.

a) 첫 번째 패킷 자체에서 탐지가 이루어져야 함

b) 탐지 정확도는 100%여야 합니다.

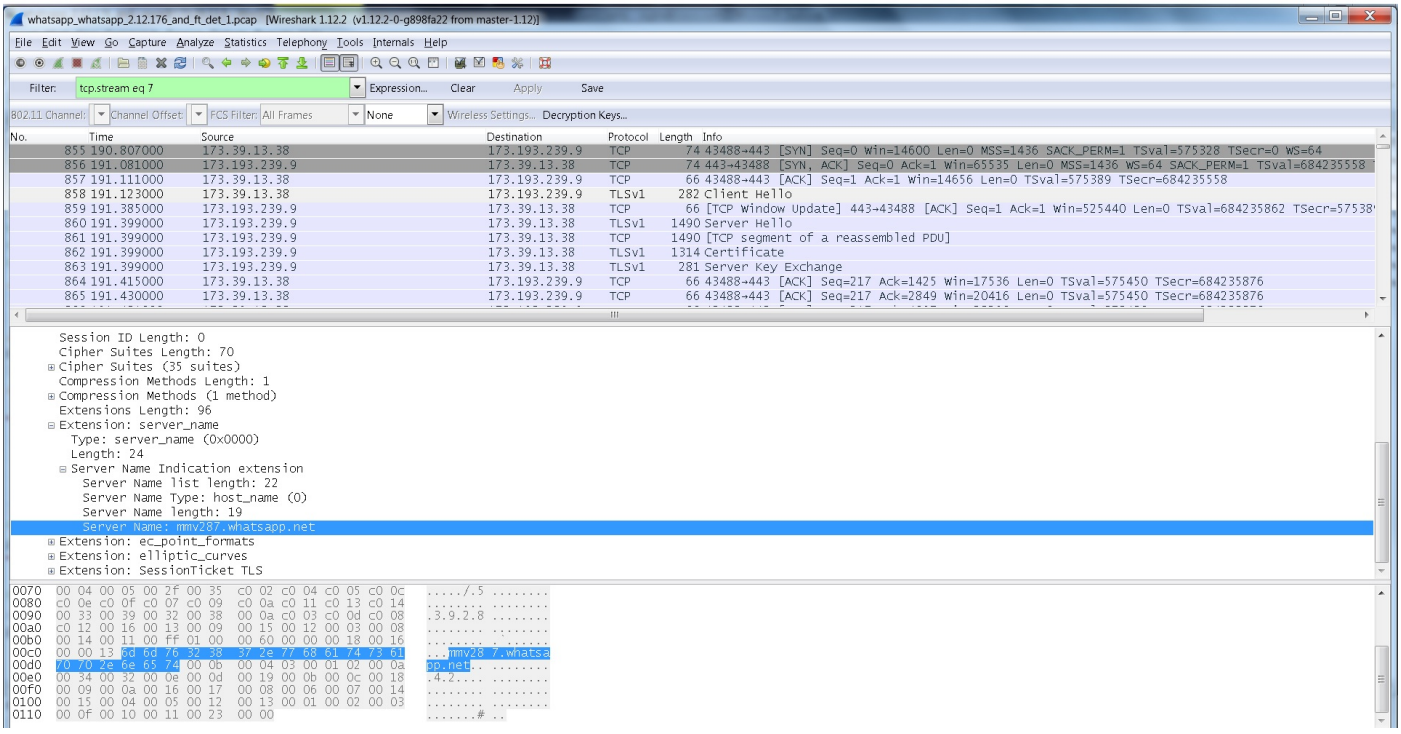
요건(a)을 충족하고 첫 번째 패킷에서 모든 앱을 표시할 경우(실제로 가능하지 않음) 탐지 정확성에 대한 요구 사항(b)이 어려워집니다.탐지 정확성을 제대로 유지하려면 많은 앱을 분석할 수 있는 패킷이 필요합니다(첫 번째 패킷 자체에서 앱이 탐지되는 앱 및 플로우가 있음). 동일한 앱의 경우 첫 번째 패킷 자체에서 일부 흐름을 표시할 수 있는 반면 동일한 앱의 다른 플로우에는 분석을 위해 더 많은 패킷이 필요합니다.

따라서 다른 트래픽을 차단하는 동안 무임으로 평가되는 앱이 있으면 충분한 정보를 전달하지 않으므로 앱의 초기 패킷이 탐지되지 않을 수 있습니다.SSL 플로우를 기반으로 하는 앱의 경우, 프로토콜은 client-hello 패킷에 있는 server-name-indication 필드 또는 SSL 인증서에 있는 common-name 필드를 사용하여 표시됩니다.server-name은 선택 필드이므로 항상 있는 것은 아닙니다. 이 이미지에 표시된 것처럼 Whatsapp SSL 흐름에서 TWH(Three-Way-Handshake) 이후 클라이언트 hello 패킷이 앱에서 전송됩니다.**SNI(Server Name Indication) 필드를 표시하지 않는 PCAP 추적또한 클라이언트 hello 패킷의 여러 재전송에서 결국 삭제됩니다.**



또한 이 이미지에 표시된 것처럼, Whatsapp을 표시하는 데 사용되는 SNI 필드가 없는 클라이언트 hello 패킷의 16진수 바이트입니다.따라서 client-hello 패킷은 Whatsapp로 표시할 수 없으며 탐지되지 않습니다.이 패킷은 다른 등급 그룹에 속하므로 삭제되므로 client-hello 패킷의 여러 재전송이 표시됩니다(프레임 번호 5449, 5453, 5469 참조). 마지막으로 연결이 종료됩니다.pcap에는 이러한 플로우가 여러 개 있습니다.따라서 Whatsapp에 대한 이미지 업로드와 같은 유용한 작업이 수행되지 않습니다

.



문제 해결

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

```
Verbosity level 5
```
이러한 명령은 응용 프로그램의 분석 통계를 제공합니다.

```
# show act analyzer statistics name p2p application snapchat
# show act analyzer statistics name p2p application whatsapp
```
플러그인 버전을 확인하려면

```
#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
```

솔루션

이를 방지하려면 앱(예: 앱)이 표시되기 전에 패킷이 표시되고 통과해야 하는지 확인해야 합니다.

이 규칙 정의 사용:

```
ruledef ssl_clienthello
      tcp either-port = 443
      tcp payload-length >= 44
      tcp payload  starts-with hex-signature 16-03
#exit
```
위의 규칙 정의 와 일치하는 패킷은 삭제해서는 안 됩니다.이 규칙 정의의 우선 순위는 이 패킷과 일치하고 삭제되도록 하는 기본 규칙 정의(ip-any ruledef) 바로 위에 있어야 합니다.

이 컨피그레이션을 사용하면 위의 세 규칙 라인과 일치하는 패킷만 무등급이 됩니다.여기에는 이 규칙 정의를 사용하여 허용되는 SSL 흐름의 초기 핸드셰이크 패킷(예: client-hello, server-hello)만 포함되며, SSL 흐름의 다른 모든 패킷은 이 규칙 정의와 일치하지 않습니다.따라서 SSL 흐름의 초기 2~3개의 패킷만 이 규칙 정의를 사용할 수 있으므로, 다른 일부 앱에 속하는 SSLflow가 있는 경우(무료로 사용할 수 있는 앱 제외) 유용한 트랜잭션이 있을 수 없습니다.

샘플 컨피그레이션

권장 ruledef는 all-ip_004_012_00016 ruledef(ip any-match = TRUE)보다 우선 순위가 높아야 합니다.

whsapp ruledef.(sid_040_rg_400_rate_99999/sid_040_rg_400032/
sid_040_rg_400_rate_00064(rat-group 4000_rate_000064 및 임의 비율)와 유사한 트래픽을 허용하는 부과 조치.

이 컨피그레이션을 사용하면 클라이언트 hello 패킷이 제안된 규칙 정의에 도달하고 리디렉션되는 대신 허용됩니다.다음은 애플리케이션 규칙이 표시되는 두 가지 규칙입니다.

```
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