在AireOS WLC上配置資料包捕獲

目錄

簡介

本檔案介紹如何在AireOS無線LAN控制器(WLC)上執行封包轉儲。 此方法以十六進位制格式顯示WLC的CPU級別傳送和/或接收的資料包，然後使用Wireshark將其轉換為.pcap檔案。

在需要透過WLC層級上的封包擷取（但連線埠span難以執行）來快速驗證WLC與遠端驗證撥入使用者服務(RADIUS)伺服器、存取點(AP)或其他控制器之間的通訊時，這很有用。

需求

思科建議您瞭解以下主題：

- 對WLC（特別是SSH）的命令列介面(CLI)訪問，因為輸出速度比控制檯快。
- 安裝了Wireshark的PC

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- WLC v8.3
- Wireshark v2或更高版本

註:此功能自AireOS版本4起可用。

限制

封包記錄只會擷取WLC中的雙向控制平面(CP)到資料平面(DP)封包。不會擷取沒有從WLC資料平面傳送到/從控制平面傳送的封包（例如從外部傳送到錨點通道流量、DP-CP捨棄等）。

在CP處處理的WLC來往流量的型別示例包括：

- Telnet

- SSH
- HTTP
- HTTPS
- SNMP
- NTP
- RADIUS
- TACACS+
- 行動化訊息
- CAPWAP控制
- NMSP
- TFTP/FTP/SFTP
- 系統日誌
- IAPP

傳入/傳出使用者端的流量會在資料平面(DP)中處理，以下情況除外：802.11管理、802.1X/EAPOL、ARP、DHCP和Web身份驗證。

設定

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

在WLC中啟用封包記錄

步驟1.登入WLC的CLI。

由於此功能所顯示的日誌數量和速度，因此建議通過SSH而不是通過控制檯登入到WLC。

步驟2.應用訪問控制清單(ACL)以限制捕獲的流量。

在指定的範例中，擷取顯示來往WLC管理介面（IP位址172.16.0.34）和RADIUS伺服器(172.16.56.153)的流量。

```
> debug packet logging acl ip 1 permit 172.16.0.34 172.16.56.153
> debug packet logging acl ip 2 permit 172.16.56.153 172.16.0.34
```

> **提示：**要捕獲所有來往WLC的流量，建議應用一個ACL，該ACL會丟棄來往/來自啟動SSH會話的主機的SSH流量。以下是可用於構建ACL的命令：
>
> >debug packet logging acl ip 1 deny <WLC-IP> <host-IP> tcp 22 any
> >debug packet logging acl ip 2 deny <host-IP> <WLC-IP> tcp any 22
> >debug packet logging acl ip 3 permit any any

步驟3.配置Wireshark可讀的格式。

```
> debug packet logging format text2pcap
```

步驟4.啟用資料包記錄功能。

此範例顯示如何擷取100個接收/傳輸封包(支援1 - 65535個封包):

```
> debug packet logging enable all 100
```

步驟5.將輸出記錄到文本檔案中。

附註：預設情況下，它僅使用debug packet logging enable命令記錄接收的25個資料包。

附註：您可以將**rx** 或**tx** 而不是**all**用於僅捕獲已接收或傳輸的流量。

有關配置資料包日誌記錄功能的詳細資訊，請參閱以下連結：

思科無線控制器組態設定指南8.3版，使用偵錯工具

驗證

使用本節內容，確認您的組態是否正常運作。

使用給定的命令驗證資料包日誌記錄的當前配置。

```
> show debug packet

Status..................................... rx/tx            !!! This means the capture is
active
Number of packets to display..................... 100
Bytes/packet to display.......................... 0
Packet display format............................ text2pcap

   Driver ACL:
      [1]: disabled
      [2]: disabled
      [3]: disabled
      [4]: disabled
      [5]: disabled
      [6]: disabled
   Ethernet ACL:
      [1]: disabled
      [2]: disabled
      [3]: disabled
      [4]: disabled
      [5]: disabled
      [6]: disabled
   IP ACL:
      [1]: permit s=172.16.0.34 d=172.16.56.153 any
      [2]: permit s=172.16.56.153 d=172.16.0.34 any
      [3]: disabled
      [4]: disabled
      [5]: disabled
      [6]: disabled
   EoIP-Ethernet ACL:
      [1]: disabled
      [2]: disabled
```

```
      [3]: disabled
      [4]: disabled
      [5]: disabled
      [6]: disabled
   EoIP-IP ACL:
      [1]: disabled
      [2]: disabled
      [3]: disabled
      [4]: disabled
      [5]: disabled
      [6]: disabled
   LWAPP-Dot11 ACL:
      [1]: disabled
      [2]: disabled
      [3]: disabled
      [4]: disabled
      [5]: disabled
      [6]: disabled
   LWAPP-IP ACL:
      [1]: disabled
      [2]: disabled
      [3]: disabled
      [4]: disabled
      [5]: disabled
      [6]: disabled
```

重現生成流量所需的行為。

將顯示類似以下的輸出：

```
rx len=108, encap=unknown, port=2
0000 E0 89 9D 43 EF 40 C8 5B 76 1D AB 51 81 00 09 61 `..Co@H[v.+Q...a
0010 08 00 45 00 00 5A 69 81 00 00 80 01 78 A7 AC 10 ..E..Zi.....x',.
0020 00 38 AC 10 00 22 03 03 55 B3 00 00 00 00 45 00 .8,.."..U3....E.
0030 00 3E 0B 71 00 00 FE 11 58 C3 AC 10 00 22 AC 10 .>.q..~.XC,.."",.
0040 00 38 15 B3 13 88 00 2A 8E DF A8 a1 00 0E 00 0E .8.3...*._(!....
0050 01 00 00 00 00 22 F1 FC 8B E0 18 24 07 00 C4 00 ....."q|.`.$..D.
0060 F4 00 50 1C BF B5 F9 DF EF 59 F7 15 t.P.?5y_oYw.
rx len=58, encap=ip, port=2
0000 E0 89 9D 43 EF 40 C8 5B 76 1D AB 51 81 00 09 61 `..Co@H[v.+Q...a
0010 08 00 45 00 00 28 69 82 40 00 80 06 38 D3 AC 10 ..E..(i.@...8S,.
0020 00 38 AC 10 00 22 F6 3A 00 16 AF 52 FE F5 1F 0C .8,.."v:../R~u..
0030 40 29 50 10 01 01 52 8A 00 00 @)P...R...
rx len=58, encap=ip, port=2
0000 E0 89 9D 43 EF 40 C8 5B 76 1D AB 51 81 00 09 61 `..Co@H[v.+Q...a
0010 08 00 45 00 00 28 69 83 40 00 80 06 38 D2 AC 10 ..E..(i.@...8R,.
0020 00 38 AC 10 00 22 F6 3A 00 16 AF 52 FE F5 1F 0C .8,.."v:../R~u..
0030 41 59 50 10 01 00 51 5B 00 00 AYP...Q[..
rx len=58, encap=ip, port=2
0000 E0 89 9D 43 EF 40 C8 5B 76 1D AB 51 81 00 09 61 `..Co@H[v.+Q...a
0010 08 00 45 00 00 28 69 84 40 00 80 06 38 D1 AC 10 ..E..(i.@...8Q,.
0020 00 38 AC 10 00 22 F6 3A 00 16 AF 52 FE F5 1F 0C .8,.."v:../R~u..
0030 43 19 50 10 01 05 4F 96 00 00 C.P...O...
```

從資料包日誌記錄中刪除ACL

若要停用ACL應用的過濾器，請使用以下命令：

```
> debug packet logging acl ip 1 disable
>debug packet logging acl ip 2 disable
```

禁用資料包記錄

若要停用封包記錄而不移除ACL，只需使用以下命令：

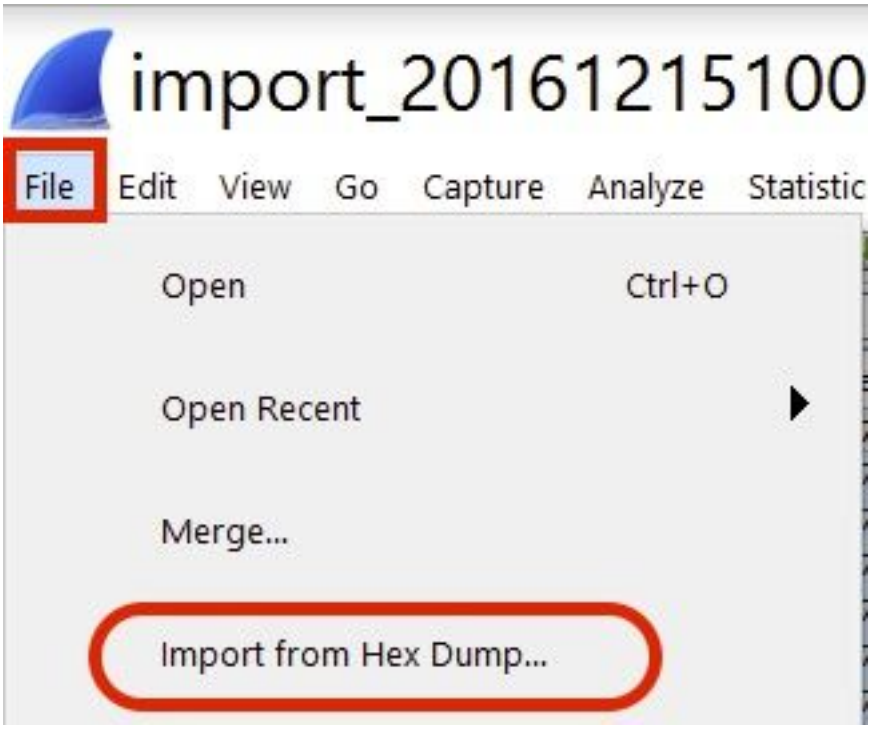
```
> debug packet logging disable
```

將資料包日誌記錄輸出轉換為.pcap檔案

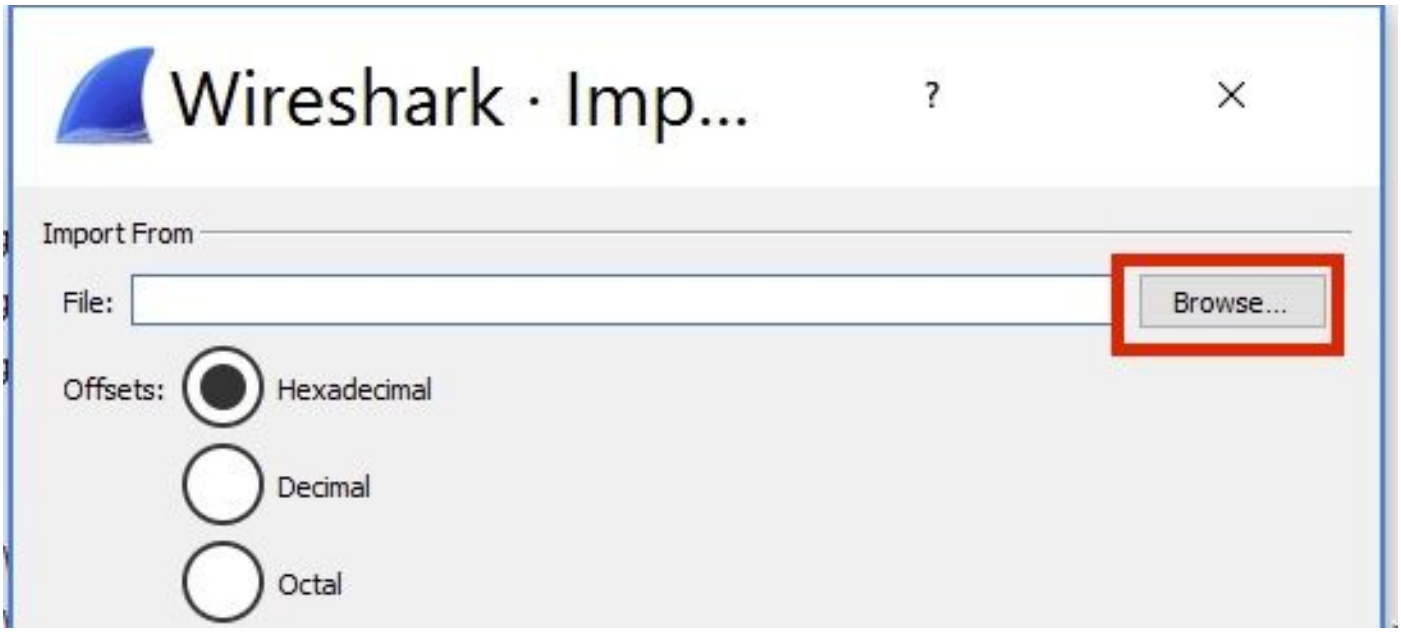
步驟1。輸出完成後，收集並儲存到文本檔案。

確保收集乾淨的日誌，否則Wireshark可能會顯示損壞的資料包。

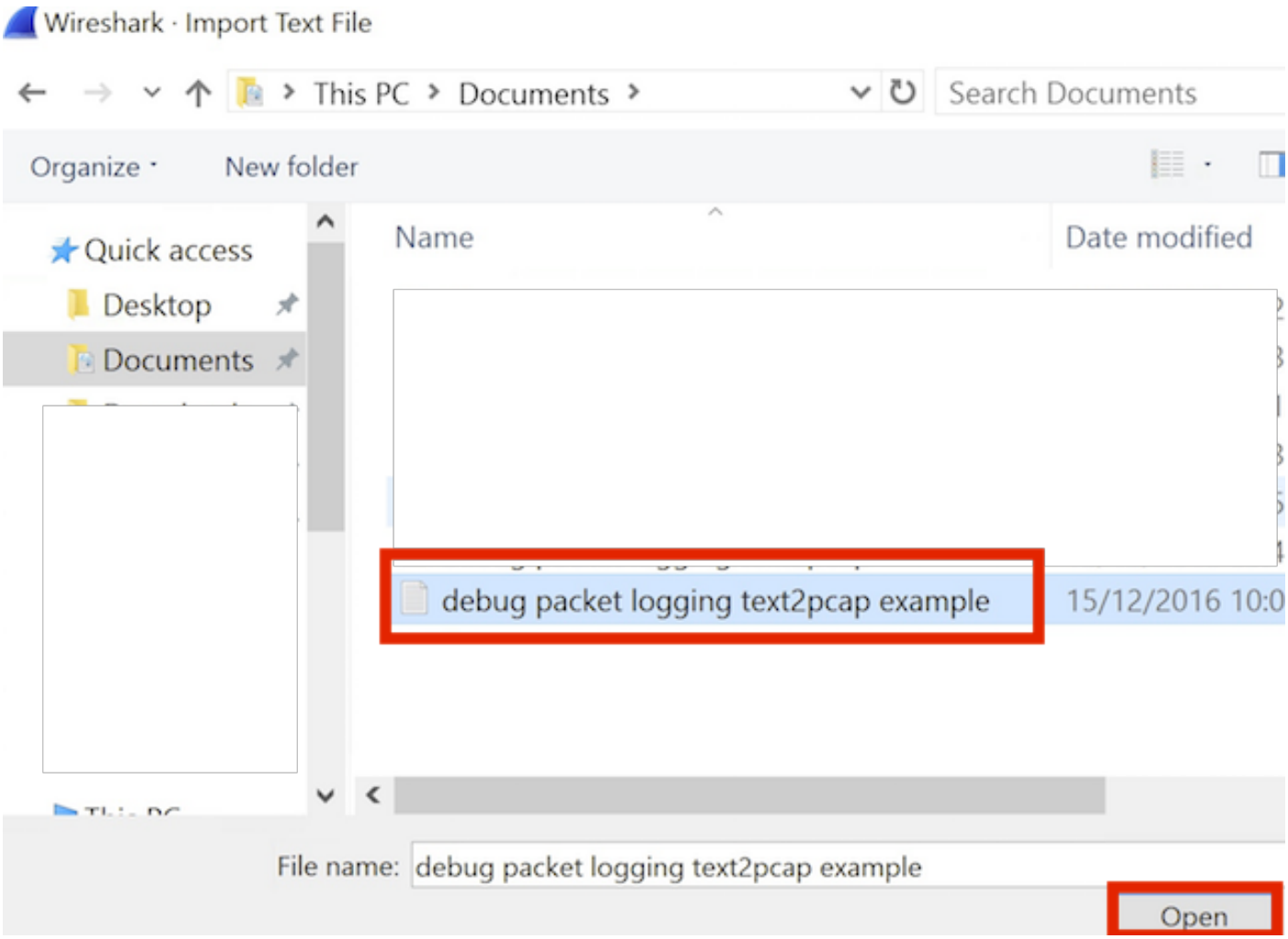
步驟2.開啟Wireshark並導航到**File>Import from Hex Dump...**



步驟3.按一下**Browse。**

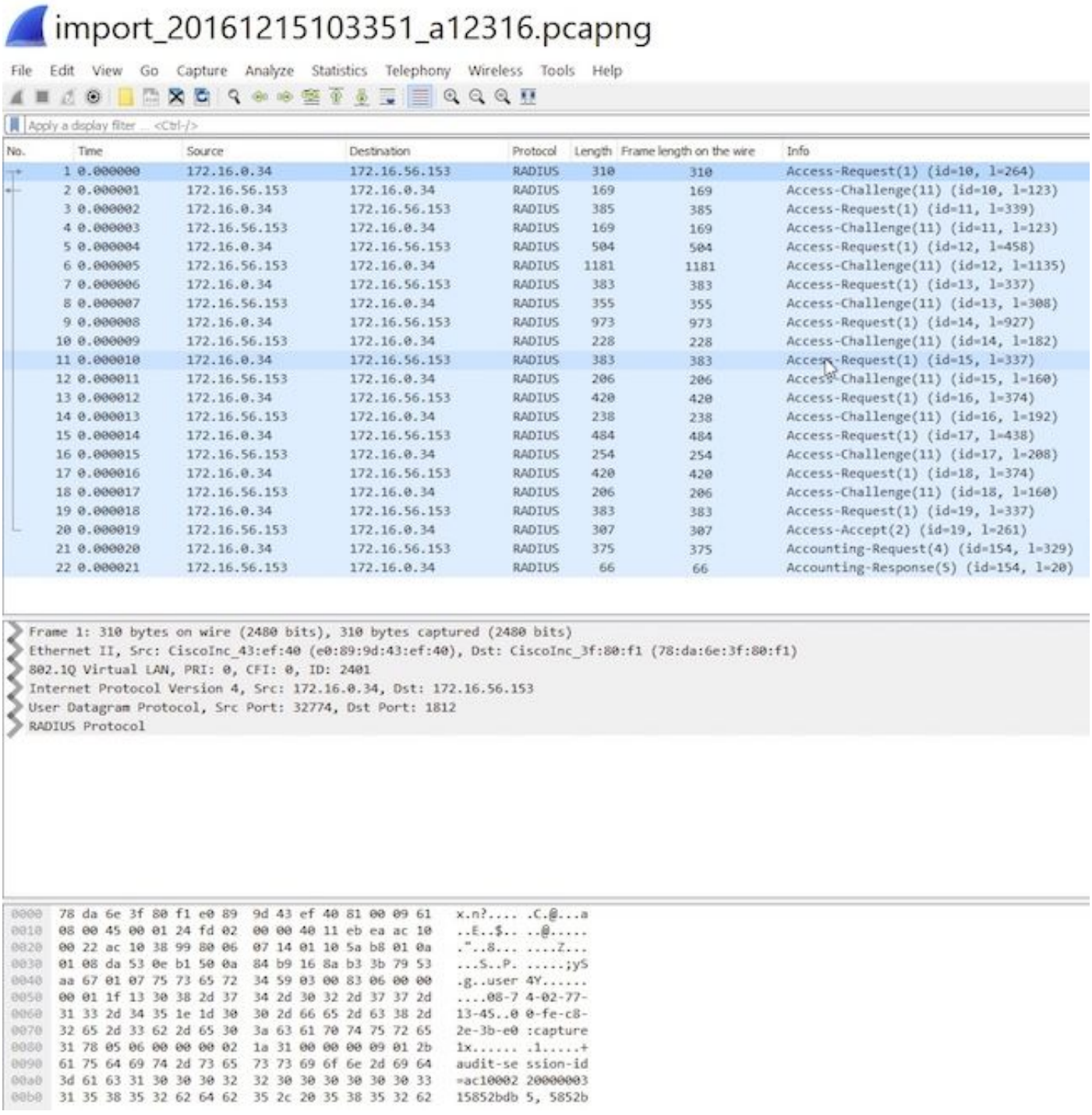


步驟4.選擇儲存資料包日誌記錄輸出的文本檔案。



步驟5.按一下「Import」。

Wireshark將檔案顯示為.pcap。



附註：請注意，時間戳不準確，幀之間的增量時間也不準確。

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。

相關資訊

- [AP資料包轉儲](#)
- [802.11 無線監聽的基礎知識](#)
- [技術支援與文件 - Cisco Systems](#)