Configurez les captures de paquet sur AireOS WLC

Contenu

[Introduction](#)
[Conditions requises](#)
[Composants utilisés](#)
[Limites](#)
[Configurez](#)
[Paquet d'enable ouvrant une session WLC](#)
[Vérifiez](#)
[Sortie de journalisation de paquet de conversion à un fichier .pcap](#)
[Dépannez](#)

Introduction

Ce document décrit comment exécuter un vidage mémoire de paquet sur un RÉSEAU LOCAL Sans fil Controller(WLC) d'AireOS. Cette méthode affiche les paquets envoyés et/ou reçus au niveau CPU du WLC dans le format hexadécimal, qui alors soit traduit à un fichier .pcap avec Wireshark.

Il est utile dans les cas où transmission entre un WLC et un serveur de Service RADIUS (Remote Authentication Dial-In User Service), un Point d'accès (AP) ou d'autres contrôleurs doit être vérifiés d'un moyen rapide avec une capture de paquet au niveau WLC mais il est difficile d'exécuter une port-envergure.

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Accès de l'interface de ligne de commande (CLI) au WLC, de préférence SSH puisque la sortie est plus rapide que la console.
- Le PC avec Wireshark a installé

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- WLC v8.3
- Wireshark v2 ou plus tard

Remarque: Cette caractéristique est disponible depuis la version 4 d'AireOS.

Limites

Se connecter de paquet capturera seulement l'avion bidirectionnel de contrôle (CP) aux paquets du plan de données (DP) dans WLC. Ces paquets qui ne sont pas envoyés du plan de données WLC à/de l'avion de contrôle (c.-à-d. étranger pour ancrer le trafic percé un tunnel, des baisses DP-CP et ainsi de suite) ne seront pas capturés.

Les exemples des types de trafic à/de le WLC traités au CP sont :

- Telnet
- SSH
- HTTP
- HTTPS
- SNMP
- NTP
- RAYON
- TACACS+
- Messages de mobilité
- Contrôle CAPWAP
- NMSP
- TFTP/FTP/SFTP
- Syslog
- IAPP

Le trafic à/de le client est traité dans le plan de données (DP) excepté : Gestion de 802.11, 802.1X/EAPOL, ARP, DHCP et authentification Web.

Configurez

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est vivant, assurez-vous que vous comprenez l'impact potentiel de n'importe quelle commande.

Paquet d'enable ouvrant une session WLC

Étape 1. Procédure de connexion au CLI de WLC.

En raison de la quantité et de la vitesse des logs que cette caractéristique affiche il est recommandé pour ouvrir une session au WLC par SSH et pas par la console.

Étape 2. Appliquez une liste de contrôle d'accès (ACL) pour limiter que le trafic est capturé.

Dans l'exemple donné la capture affiche le trafic à/de l'interface de gestion du WLC (adresse IP 172.16.0.34) et le serveur de RAYON (172.16.56.153).

```
> 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
```

> **Conseil** : Pour capturer tout le trafic à/de le WLC il est recommandé pour appliquer un ACL qui jette le trafic de SSH à/de l'hôte qui a initié la session de SSH. Ce sont les commandes

que vous pouvez employer pour construire l'ACL :

>le debug packet se connectant l'IP 1 d'acl refusent le TCP 22 de <host-IP> <WLC-IP>
>le debug packet se connectant l'IP 2 d'acl refusent à TCP du <host-IP> <WLC-IP> n'importe quels 22
>debug packet se connectant l'autorisation de l'IP 3 d'acl toute

Étape 3. Configurez le format accessible en lecture par Wireshark.

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

Étape 4. Fonctionnalité de journalisation de paquet d'enable.

Cet exemple affiche comment capturer 100 reçus/paquets transmis (il prend en charge 1 - 65535 paquets) :

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

Remarque: Par défaut, il se connecte seulement 25 paquets reçus avec le **logging enable de debug packet de** commande.

Remarque: Au lieu de **tous** vous pouvez employer le **rx** ou le **tx** pour capturer le trafic seulement reçu ou transmis.

Pour d'autres détails au sujet de configurer la fonctionnalité de journalisation de paquet consultez ce lien :

Guide de configuration Sans fil de contrôleur de Cisco, version 8.3, utilisant l'installation de debug

Vérifiez

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

Utilisez l'instruction donnée de vérifier la configuration en cours de se connecter de paquet.

```
> 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
```

Reproduisez le comportement nécessaire pour générer le trafic.

Un résultat semblable à ceci apparaît :

```
> 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
```

Retirez ACLs de se connecter de paquet

Afin de désactiver les filtres appliqués par l'ACLs utilisez ces commandes :

```
> 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
```

Se connecter de paquet de débronchement

Afin de désactiver le paquet se connectant sans retirer l'ACLs utilisez simplement cette commande :

```
> 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:
```

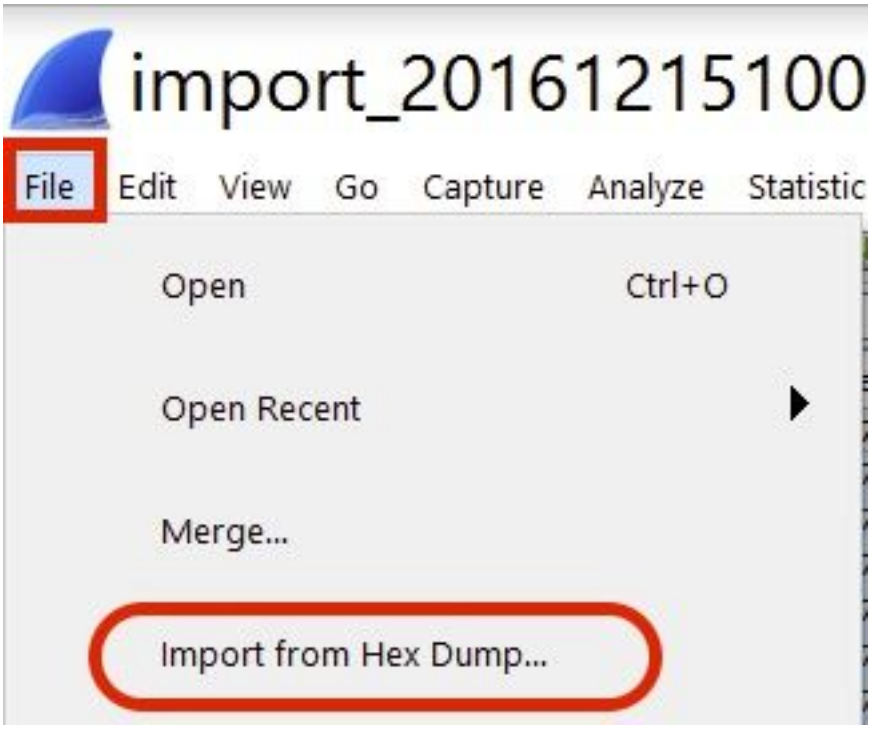
```
   [1]: permit s=172.16.0.34 d=172.16.56.153 any
   [2]: permit s=172.16.56.153 d=172.16.0.34 any
   [3]: disabled
   [4]: disabled
   [5]: disabled
   [6]: disabled
EoIP-Ethernet ACL:
   [1]: disabled
   [2]: disabled
   [3]: disabled
   [4]: disabled
   [5]: disabled
   [6]: disabled
EoIP-IP ACL: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

Sortie de journalisation de paquet de conversion à un fichier .pcap

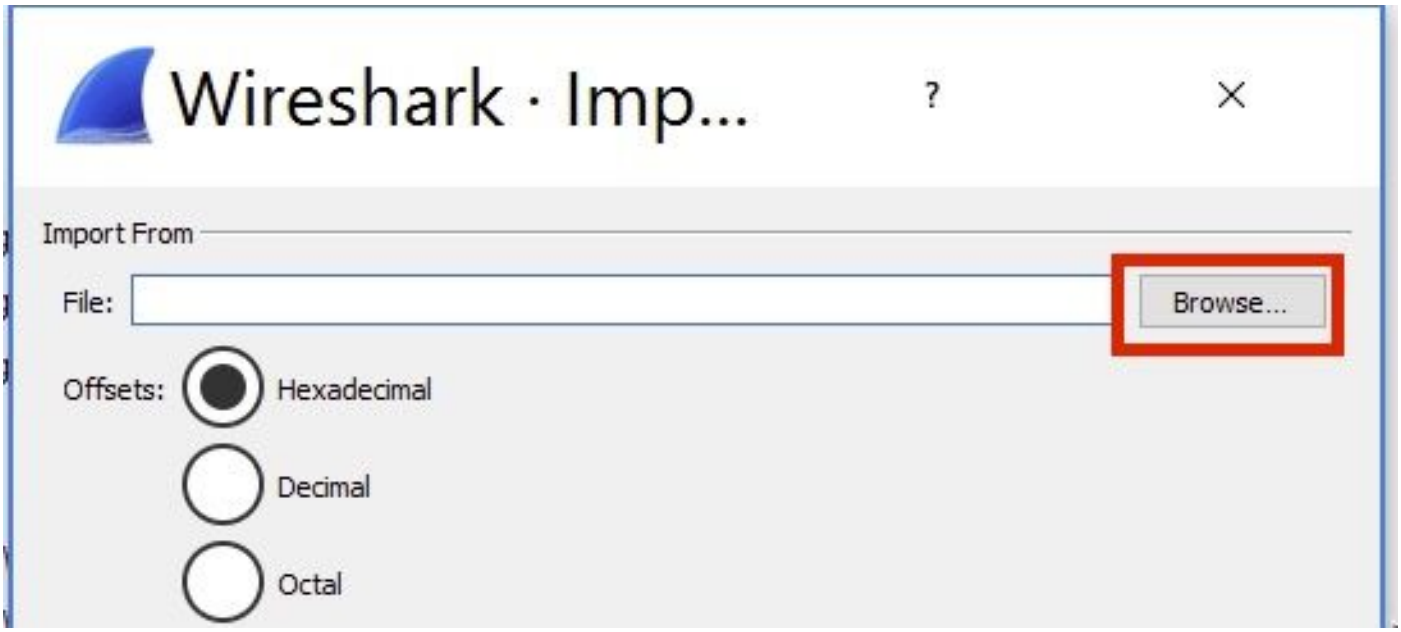
Étape 1. Une fois que la sortie termine, collectez-la et sauvegardez-la à un fichier texte.

Assurez-vous que vous recueillez un log propre, autrement Wireshark pourrait afficher les paquets corrompus.

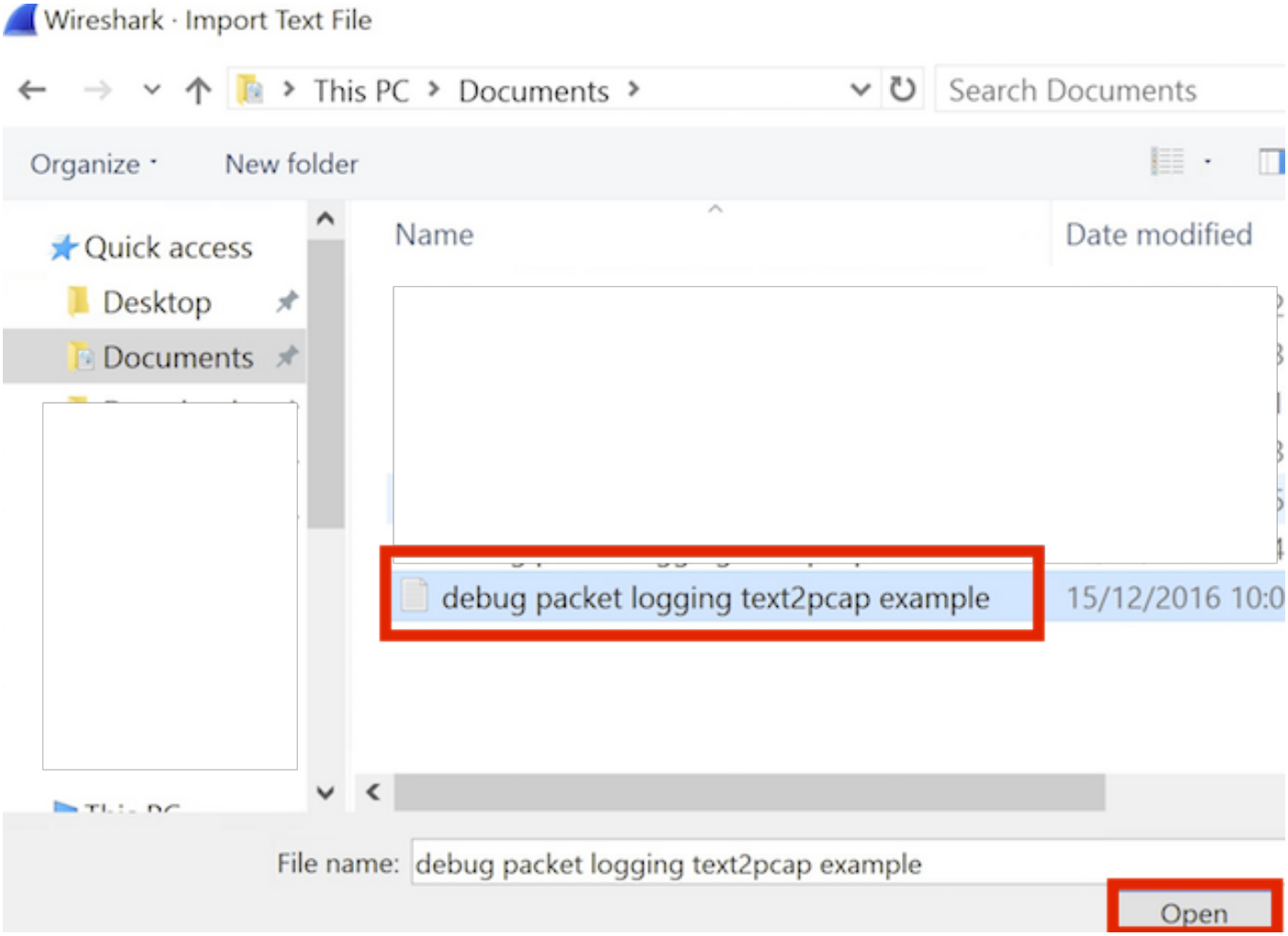
Étape 2. Ouvrez Wireshark et naviguez **pour classer le >Import du vidage hexadécimal…**



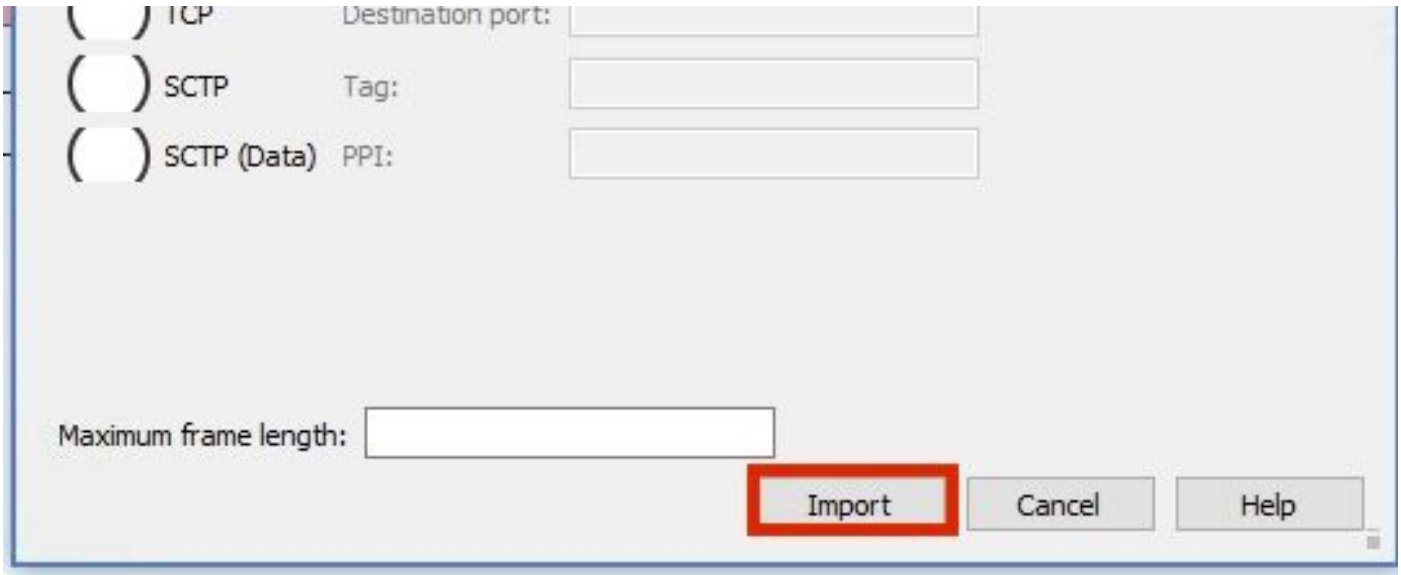
Étape 3. Le clic **parcourent.**



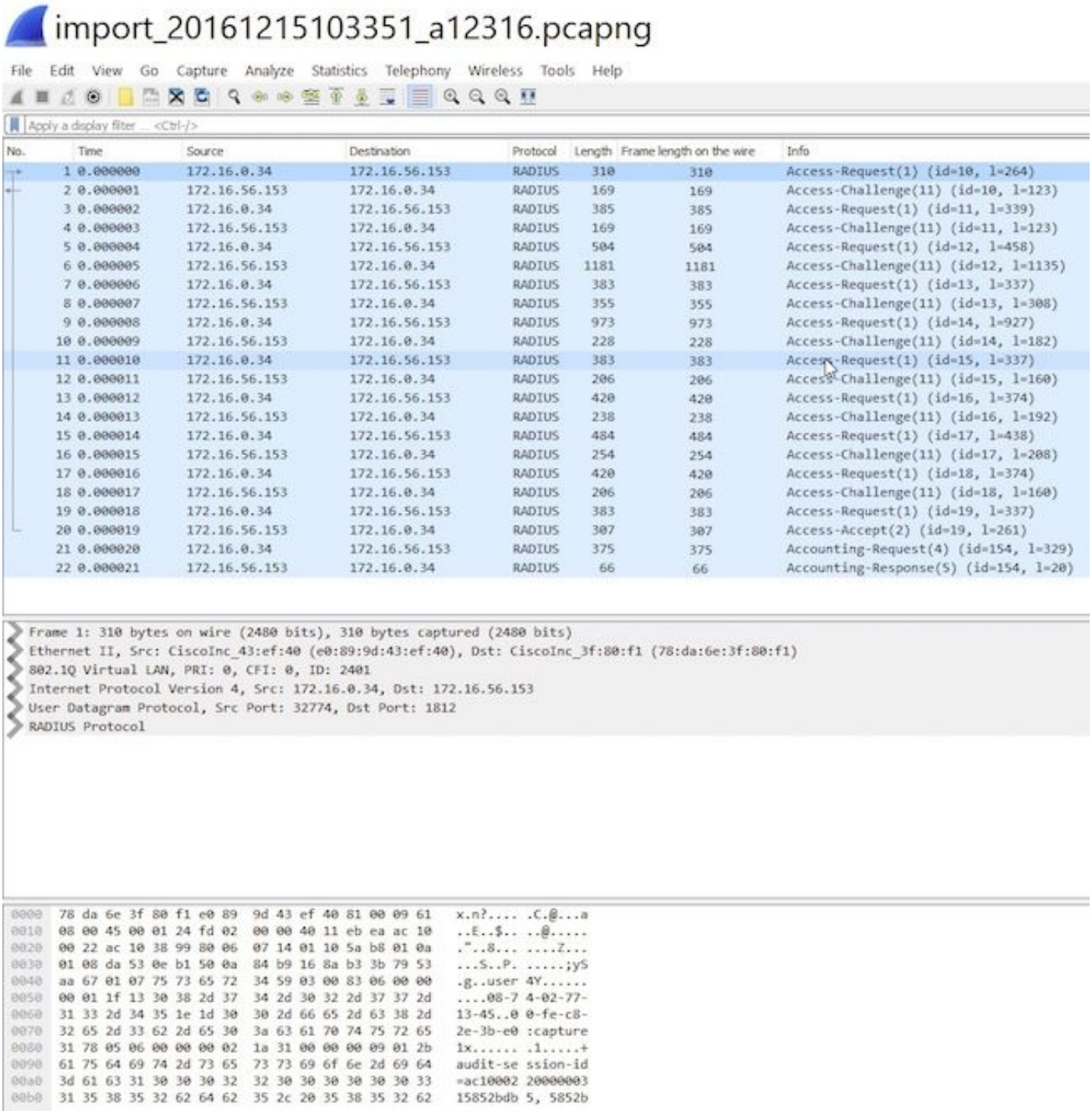
Étape 4. Sélectionnez le fichier texte où vous avez enregistré la sortie de journalisation de paquet.



Étape 5. **Importation de** clic.



Wireshark affiche le fichier comme .pcap.



Remarque: Rendez-vous compte que les groupes date/heure ne sont pas précis ni le temps delta entre les trames.

Dépannez

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Informations connexes

- Vidage mémoire de paquet AP
- Principes fondamentaux du reniflement Sans fil de 802.11
- Support et documentation techniques - Cisco Systems