Configuration des captures de paquets sur le WLC AireOS

Table des matières

Introduction

- Exigences
- Composants utilisés
- Limites

Informations générales

Configurer

- Activer la journalisation des paquets dans WLC

Vérifier

Convertir la sortie de journalisation des paquets en fichier .pcap

Dépannage

Informations connexes

Introduction

Ce document décrit comment exécuter un vidage de paquets sur un contrôleur LAN sans fil (WLC) AireOS.

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Accès au WLC via l'interface de ligne de commande (CLI).
- PC sur lequel Wireshark est 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 version ultérieure

Remarque : cette fonctionnalité est disponible depuis la version 4 d'AireOS.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Limites

La journalisation des paquets capture uniquement les paquets bidirectionnels du plan de contrôle (CP) vers le plan de données (DP) dans le WLC. Les paquets qui ne sont pas envoyés du plan de données WLC vers/depuis le plan de contrôle (c'est-à-dire, le trafic étranger pour ancrer le trafic tunnelisé, les abandons DP-CP, etc.) ne peuvent pas être capturés.

Voici des exemples de types de trafic en provenance/à destination du WLC traité au niveau du PC :

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

Le trafic en provenance/à destination du client est traité dans le plan de données (DP), à l'exception des éléments suivants : Gestion 802.11, 802.1X/EAPOL, ARP, DHCP et authentification Web.

Informations générales

Cette méthode affiche les paquets envoyés et/ou reçus au niveau du processeur du WLC au format hexadécimal, qui seront ensuite traduits en un fichier .pcap avec Wireshark. Elle est utile dans les cas où la communication entre un WLC et un serveur RADIUS (Remote Authentication Dial-In User Service), un point d'accès ou d'autres contrôleurs doit être vérifiée rapidement avec une capture de paquets au niveau du WLC, mais une étendue de port est difficile à effectuer.

Configurer

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Activer la journalisation des paquets dans WLC

Étape 1 : connexion à l’interface de ligne de commande du WLC

En raison de la quantité et de la vitesse des journaux que cette fonctionnalité affiche, il est recommandé de se connecter au WLC par SSH et non par console (SSH est préférable car le résultat est plus rapide que la console).

Étape 2 : application d’une liste de contrôle d’accès pour limiter le trafic capturé

Dans l'exemple donné, la capture montre le trafic vers/depuis l'interface de gestion WLC (adresse IP 172.16.0.34) et le serveur RADIUS (172.16.56.153).

```
<#root>

>

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 vers/depuis le WLC, il est recommandé d'appliquer une ACL qui rejette le trafic SSH vers/depuis l'hôte qui a initié la session SSH. Voici les commandes que vous pouvez utiliser pour créer la liste de contrôle d’accès :

> 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

Étape 3 : configuration du format lisible par Wireshark

```
<#root>

>

debug packet logging format text2pcap
```

Étape 4 : activation de la fonctionnalité de journalisation des paquets

Cet exemple montre comment capturer 100 paquets reçus/transmis (il prend en charge de 1 à 65535 paquets) :

```
<#root>

>
```

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

Étape 5. Consigner le résultat dans un fichier texte

Remarque : Par défaut, il ne consigne que 25 paquets reçus avec la commande debug packet logging enable.

Remarque : Au lieu de tout vous pouvez utiliser rx ou tx pour capturer uniquement le trafic reçu ou transmis.

Pour plus d'informations sur la configuration de la fonction de journalisation des paquets, consultez ce lien :

Guide de configuration du contrôleur sans fil Cisco, version 8.3, utilisation de la fonction de débogage

Vérifier

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

Utilisez la commande donnée pour vérifier la configuration actuelle de la journalisation des paquets.

<#root>

>

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 similaire à celui-ci apparaît :

```
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...
```

Supprimer les ACL de la journalisation des paquets

Afin de désactiver les filtres appliqués par les ACL, utilisez ces commandes :

<#root>

>

debug packet logging acl ip 1 disable

>

debug packet logging acl ip 2 disable

Désactiver la journalisation des paquets

Afin de désactiver la journalisation des paquets sans supprimer les ACL, utilisez simplement cette commande :

<#root>

>

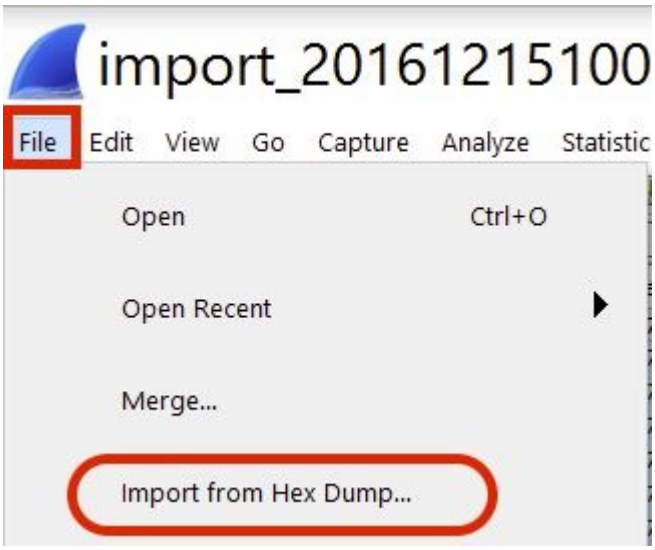
debug packet logging disable

Convertir la sortie de journalisation des paquets en fichier .pcap

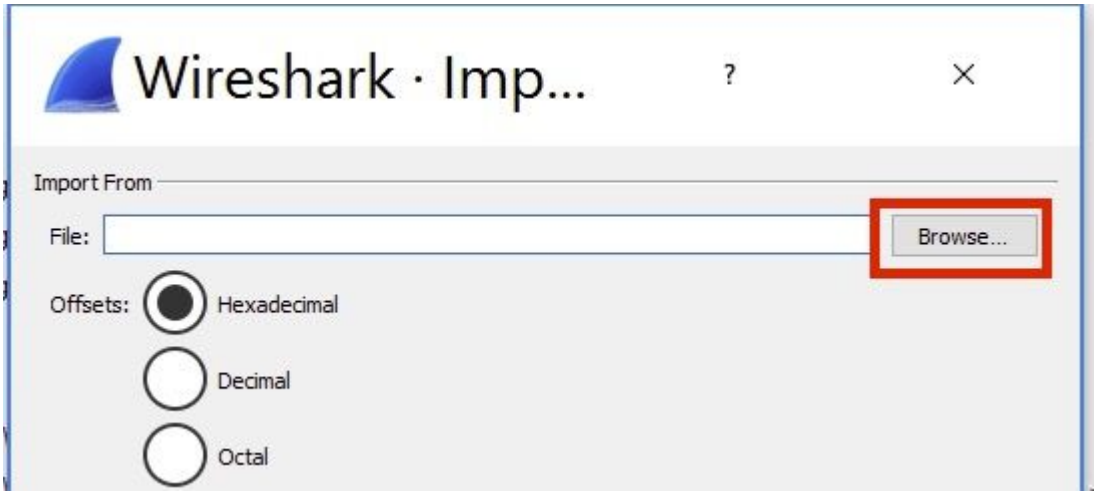
Étape 1. Une fois la sortie terminée, collectez-la et enregistrez-la dans un fichier texte.

Assurez-vous que vous collectez un journal propre, sinon Wireshark peut afficher des paquets corrompus.

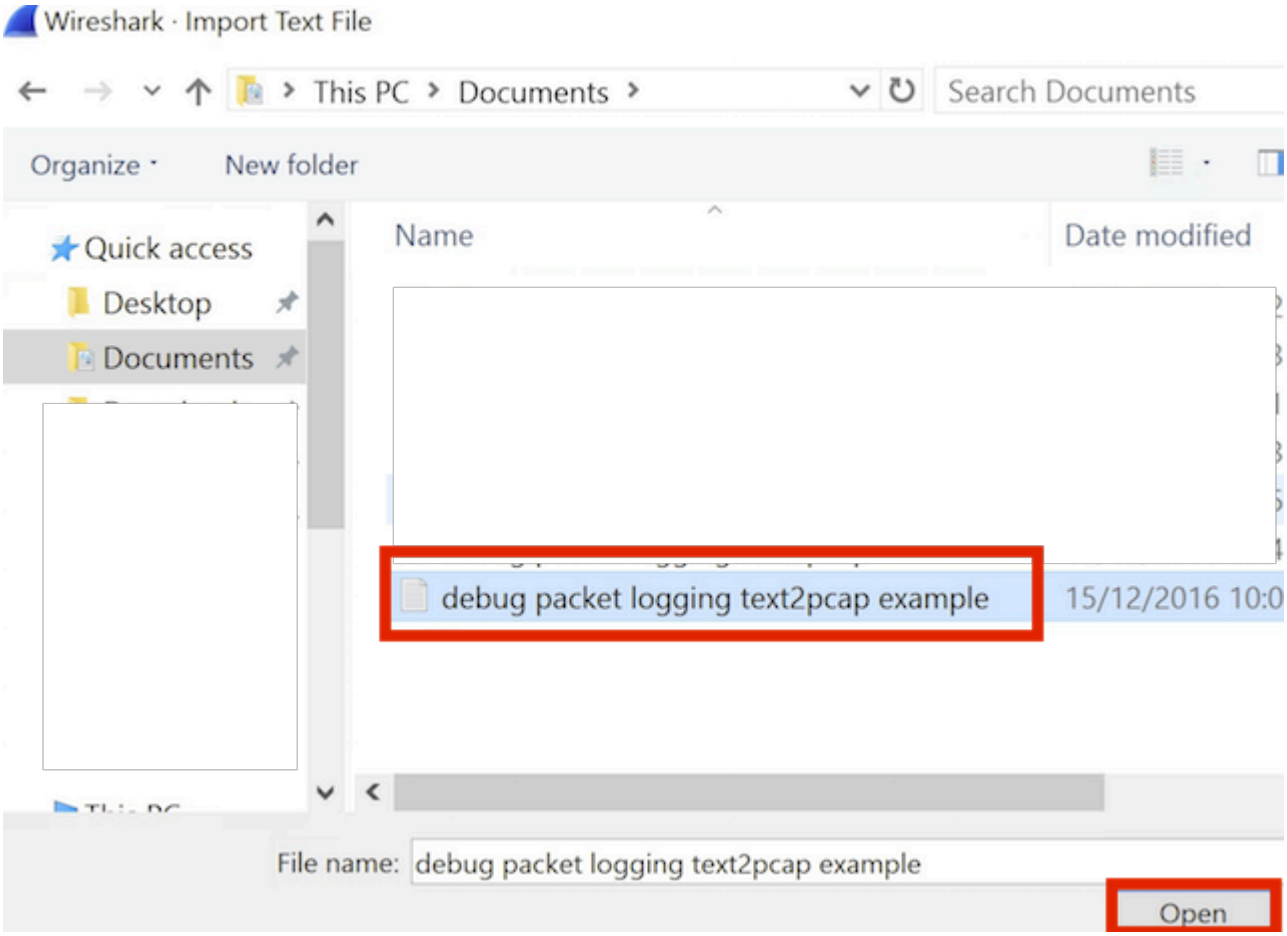
Étape 2. Ouvrez Wireshark et accédez à Fichier>Importer à partir d'un vidage hexadécimal...



Étape 3. Cliquez sur Browse.



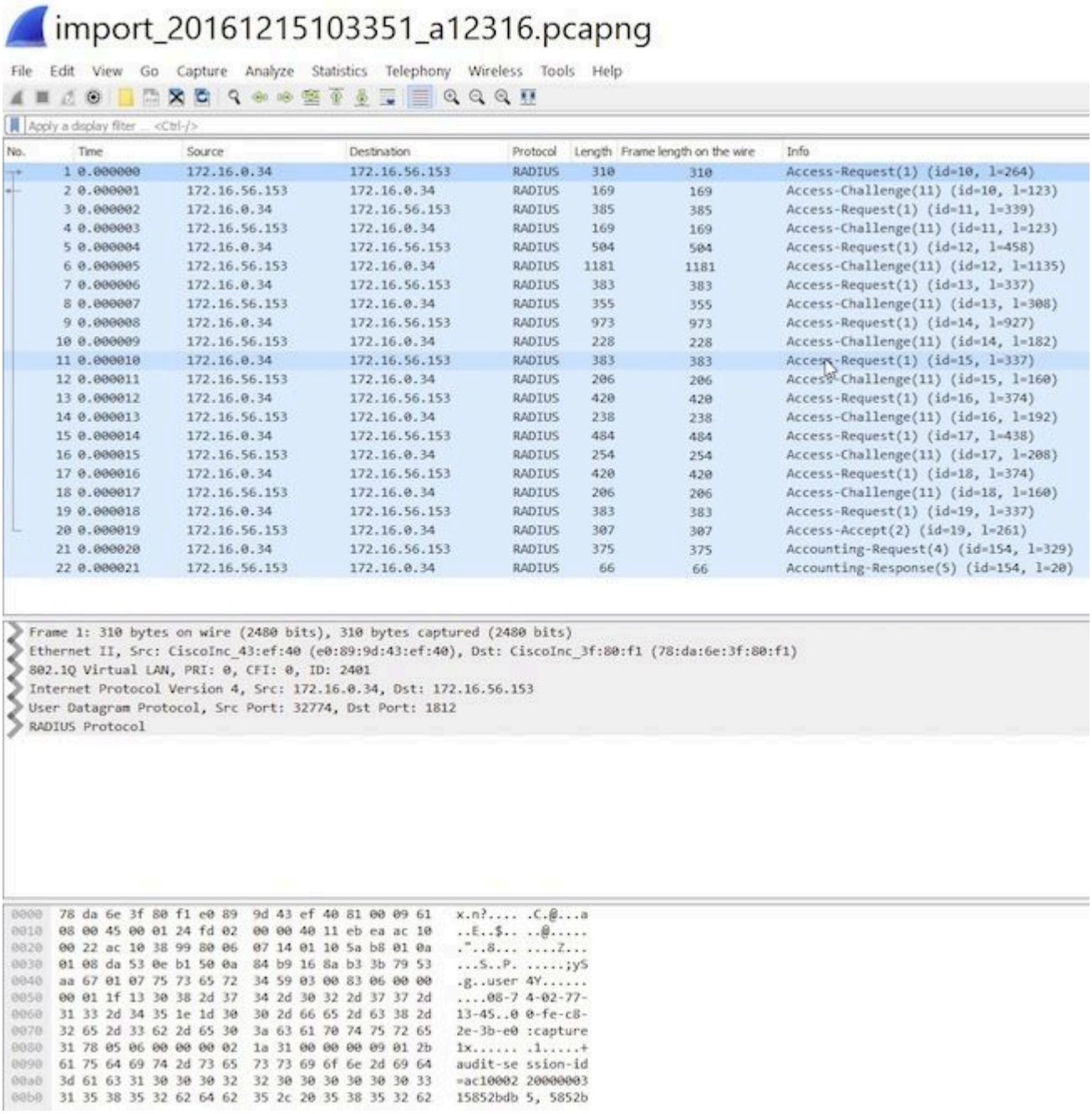
Étape 4. Sélectionnez le fichier texte dans lequel vous avez enregistré la sortie de journalisation des paquets.



Étape 5. Cliquez sur Import.



Wireshark affiche le fichier sous la forme .pcap.



Remarque : N’oubliez pas que les horodatages ne sont pas précis, ni le temps delta entre les trames.

Dépannage

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

Informations connexes

- Principes fondamentaux d’une analyse de réseau sans fil 802.11
- Assistance technique de Cisco et téléchargements

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.