Démonstration du profilage client sur le contrôleur LAN sans fil 9800

Table des matières

Introduction

Ce document décrit le fonctionnement de la classification et du profilage des périphériques sur les contrôleurs LAN sans fil Cisco Catalyst 9800.

Composants utilisés

- 9800 CL WLC exécutant l'image 17.2.1
- Point d'accès 1815i
- Client sans fil Windows 10 Pro
- Cisco ISE 2.7

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.

Processus de profilage

Cet article présente en détail le fonctionnement de la classification et du profilage des périphériques sur les contrôleurs LAN sans fil Cisco Catalyst 9800, décrit des cas d'utilisation potentiels, des exemples de configuration et les étapes nécessaires pour le dépanner.

Le profilage de périphérique est une fonctionnalité qui permet de trouver des informations supplémentaires sur un client sans fil qui a rejoint l'infrastructure sans fil.

Une fois le profilage de périphérique effectué, il peut être utilisé pour appliquer différentes stratégies locales ou pour correspondre à des règles de serveur RADIUS spécifiques.

Les WLC Cisco 9800 peuvent effectuer trois (3) types de profilage de périphérique :

1. Adresse MAC OUI
2. DHCP
3. HTTP

Profilage OUI d'adresse MAC

L'adresse MAC est un identificateur unique de chaque interface réseau sans fil (et filaire). Il s'agit d'un nombre de 48 bits généralement écrit au format hexadécimal MM:MM:SS:SS:SS.

Les 24 premiers bits (ou 3 octets) sont appelés OUI (Organizationally Unique Identifier) et ils identifient de manière unique un fournisseur ou un fabricant.

Ils sont achetés auprès de l'IEEE et attribués par celui-ci. Un fournisseur ou un fabricant peut acheter plusieurs OUI.

Exemple :

```
00:0D:4B - owned by Roku, LLC
90:78:B2 - owned by Xiaomi Communications Co Ltd
```

Une fois qu'un client sans fil s'associe au point d'accès, le WLC effectue la recherche OUI pour déterminer le fabricant.

Dans les déploiements de commutation locale Flexconnect, le point d'accès relaie toujours les informations pertinentes du client au WLC (comme les paquets DHCP et l'adresse MAC du client).

Le profilage basé uniquement sur l'OUI est extrêmement limité et il est possible de classer l'appareil comme une marque spécifique, mais il ne permet pas de faire la différence entre un ordinateur portable et un smartphone.

Problèmes liés aux adresses MAC administrées localement

Pour des raisons de confidentialité, de nombreux fabricants ont commencé à implémenter des fonctionnalités de randomisation mac dans leurs appareils.

Les adresses MAC administrées localement sont générées aléatoirement et ont un second bit de poids faible du premier octet de l'adresse défini sur 1.

Ce bit agit comme un indicateur qui annonce que l'adresse MAC est en fait une adresse générée

aléatoirement.

Il existe quatre formats possibles d'adresses MAC gérées localement (x peut être n'importe quelle valeur hexadécimale) :

```
x2-xx-xx-xx-xx-xx
x6-xx-xx-xx-xx-xx
xA-xx-xx-xx-xx-xx
xE-xx-xx-xx-xx-xx
```

Par défaut, les périphériques Android 10 utilisent une adresse MAC gérée localement et générée de manière aléatoire chaque fois qu'ils se connectent à un nouveau réseau SSID.

Cette fonctionnalité annule complètement la classification de périphérique basée sur l'OUI car le contrôleur reconnaît que l'adresse a été randomisée et n'effectue aucune recherche.

Profilage DHCP

Le profilage DHCP est effectué par le WLC par l'examen des paquets DHCP que le client sans fil envoie.

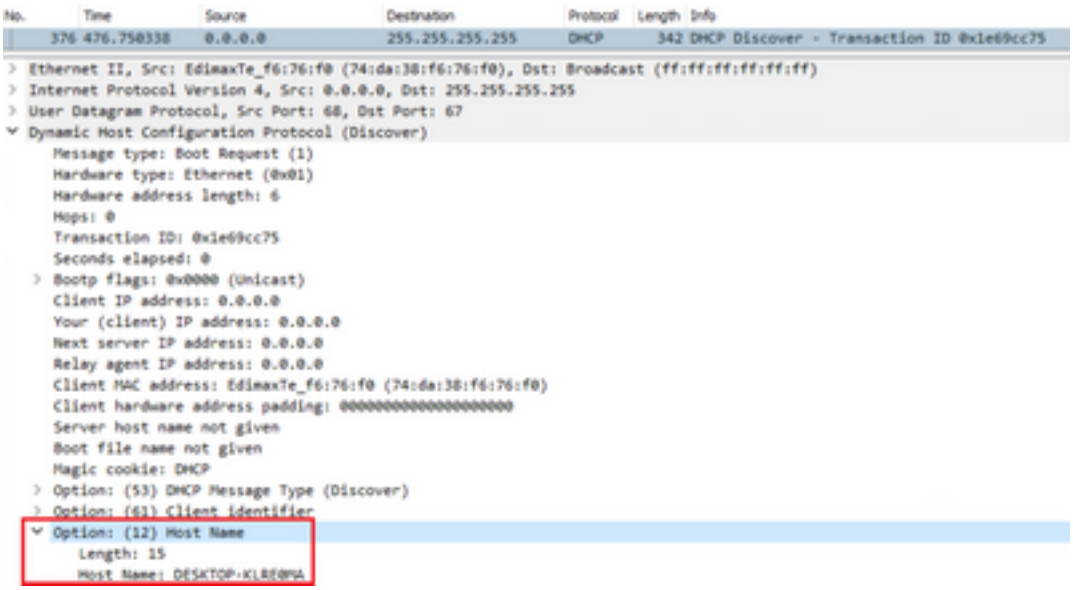
Si le profilage DHCP a été utilisé pour classer le périphérique, le résultat de la commande **show wireless client mac-address [MAC_ADDR] detailed** contient :

```
Device Type          : Microsoft-Workstation
Device Name          : MSFT 5.0
Protocol Map         : 0x000009  (OUI, DHCP)
Protocol             : DHCP
```

Le WLC inspecte plusieurs champs d'option DHCP dans les paquets envoyés par les clients sans fil :

1. Option 12 - Nom d'hôte

Cette option représente le nom d'hôte des clients et se trouve dans les paquets DHCP Discover et DHCP Request :



2. Option 60 - Identifiant de la classe du fournisseur

Cette option se trouve également dans les paquets DHCP Discover et Request.

Avec cette option, les clients peuvent s'identifier auprès du serveur DHCP et les serveurs peuvent alors être configurés pour répondre uniquement aux clients avec un identifiant de classe de fournisseur spécifique.

Cette option est le plus souvent utilisée pour identifier les points d'accès dans le réseau et y répondre uniquement avec l'option 43.

Exemples d'identificateurs de classe fournisseur

- « **MSFT 5.0** » pour tous les clients Windows 2000 (et versions ultérieures)
- « **MSFT 98** » pour tous les clients Windows 98 et Me
- «**MSFT**» pour tous les clients Windows 98, Me et 2000

Les périphériques Apple MacBook n'envoient pas l'option 60 par défaut.

Exemple de capture de paquets à partir du client Windows 10 :

```
Option: (60) Vendor class identifier
    Length: 8
    Vendor class identifier: MSFT 5.0
```

3. Option 55 - Liste des demandes de paramètres

L'option DHCP Parameter Request List contient les paramètres de configuration (codes d'option) que le client DHCP demande au serveur DHCP. Il s'agit d'une chaîne écrite en notation séparée par des virgules (par exemple 1,15,43).

Ce n'est pas une solution parfaite, car les données qu'elle génère dépendent du fournisseur et peuvent être dupliquées par plusieurs types de périphériques.

Par exemple, les périphériques Windows 10 demandent toujours par défaut une liste de paramètres spécifique. Les iPhones et iPads d'Apple utilisent différents ensembles de paramètres sur lesquels il est possible de les classer.

Exemple de capture à partir du client Windows 10 :

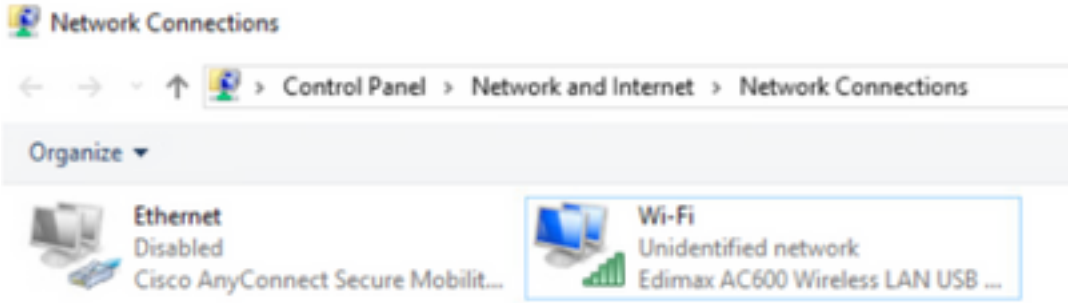
```
Option: (55) Parameter Request List
   Length: 14
   Parameter Request List Item: (1) Subnet Mask
   Parameter Request List Item: (3) Router
   Parameter Request List Item: (6) Domain Name Server
   Parameter Request List Item: (15) Domain Name
   Parameter Request List Item: (31) Perform Router Discover
   Parameter Request List Item: (33) Static Route
   Parameter Request List Item: (43) Vendor-Specific Information
   Parameter Request List Item: (44) NetBIOS over TCP/IP Name Server
   Parameter Request List Item: (46) NetBIOS over TCP/IP Node Type
   Parameter Request List Item: (47) NetBIOS over TCP/IP Scope
   Parameter Request List Item: (119) Domain Search
   Parameter Request List Item: (121) Classless Static Route
   Parameter Request List Item: (249) Private/Classless Static Route (Microsoft)
   Parameter Request List Item: (252) Private/Proxy autodiscovery
```

4. Option 7 - Classe d'utilisateur

La classe d'utilisateur est une option qui n'est généralement pas utilisée par défaut et qui nécessite une configuration manuelle du client. Par exemple, cette option peut être configurée sur un ordinateur Windows à l'aide de la commande suivante :

```
ipconfig /setclassid “ADAPTER_NAME” “USER_CLASS_STRING”
```

Le nom de l'adaptateur se trouve dans le Centre Réseau et partage du Panneau de configuration :



Configurez l'option DHCP 66 pour le client Windows 10 dans CMD (nécessite des droits d'administrateur) :

```
C:\Windows\system32>ipconfig /setclassid "Wi-Fi" "test_user_class"

Windows IP Configuration

Successfully set the DHCPv4 class id for adapter Wi-Fi.
```

En raison de l'implémentation de l'option 66 par Windows, Wireshark n'est pas en mesure de décoder cette option et une partie du paquet suivant l'option 66 apparaît comme malformée :

```
Option: (77) User Class Information
    Length: 15
  Instance of User Class: [0]
      User Class Length: 116
[Malformed Packet: DHCP/BOOTP]
[Expert Info (Error/Malformed): Malformed Packet (Exception occurred)]
    [Malformed Packet (Exception occurred)]
    [Severity level: Error]
    [Group: Malformed]
```

Profilage HTTP

Le profilage HTTP est la méthode la plus avancée de profilage prise en charge par le WLC 9800 et offre la classification de périphérique la plus détaillée.

Pour qu'un client soit profilé HTTP, il doit être à l'état « Exécuter » et exécuter une requête HTTP GET.

WLC intercepte la requête et examine le champ « User-Agent » dans l'en-tête HTTP du paquet.

Ce champ contient des informations supplémentaires sur le client sans fil qui peuvent être utilisées pour le classer.

Par défaut, presque tous les fabricants ont mis en oeuvre une fonctionnalité permettant à un client sans fil de vérifier la connectivité Internet.

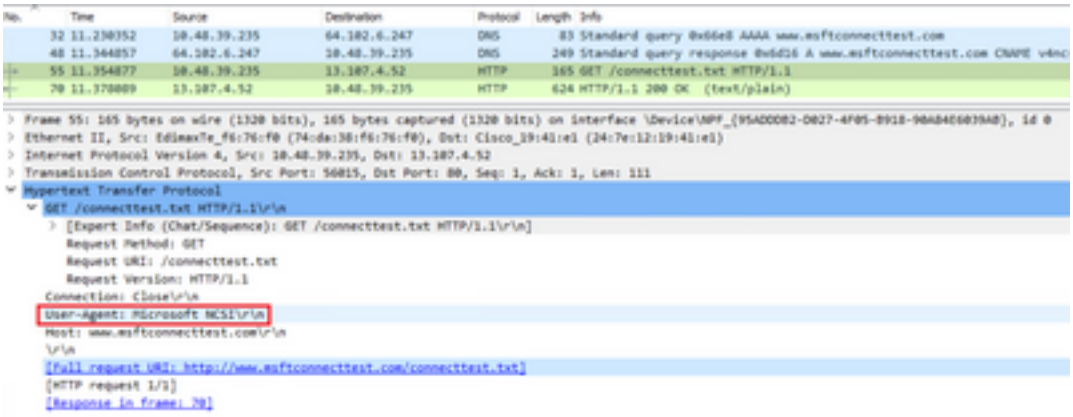
Cette vérification est également utilisée pour la détection automatique du portail invité. Si un périphérique reçoit une réponse HTTP avec le code d'état 200 (OK), cela signifie que le WLAN n'est pas sécurisé avec webauth.

Si c'est le cas, le WLC effectue alors l'interception nécessaire pour effectuer le reste de l'authentification. Ce HTTP GET initial n'est pas le seul que le WLC peut utiliser pour profiler le périphérique.

Chaque requête HTTP suivante est inspectée par le WLC et il en résulte peut-être une classification encore plus détaillée.

Les périphériques Windows 10 utilisent le domaine **msftconnecttest.com** pour effectuer ce test. Les appareils Apple utilisent **captive.apple.com**, tandis que les appareils Android utilisent généralement **connectivitycheck.gstatic.com**.

Les captures de paquets du client Windows 10 effectuant cette vérification sont disponibles ci-dessous. Le champ User Agent est renseigné avec **Microsoft NCSI**, ce qui a pour résultat que le client est profilé sur le WLC comme **Microsoft-Workstation** :



Exemple de sortie de **show wireless client mac-address [MAC_ADDR] détaillé** pour un client qui est profilé via HTTP :

```
Device Type      : Microsoft-Workstation
Device Name      : MSFT 5.0
Protocol Map     : 0x000029  (OUI, DHCP, HTTP)
Device OS        : Windows NT 10.0; Win64; x64; rv:76.0
Protocol         : HTTP
```

Profilage RADIUS

En ce qui concerne les méthodes utilisées pour classer le périphérique, il n'y a aucune différence entre le profilage local et le profilage RADIUS.

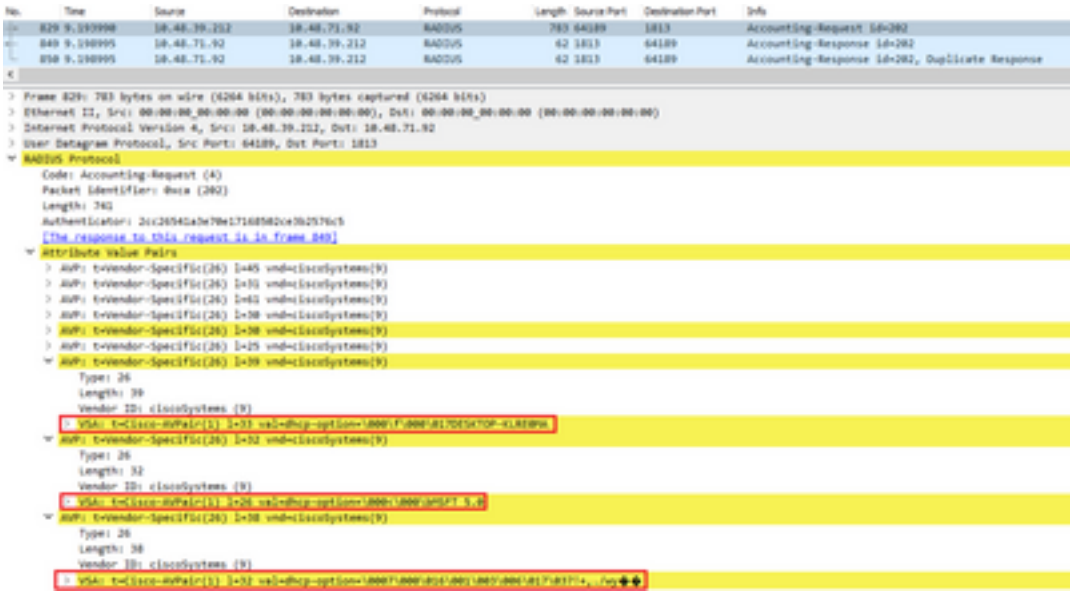
Si le profilage RADIUS est activé, le WLC transfère les informations qu'il a apprises sur le périphérique via un ensemble spécifique d'attributs RADIUS spécifiques au fournisseur au serveur RADIUS.

Profilage RADIUS DHCP

Les informations obtenues via le profilage DHCP sont envoyées au serveur RADIUS dans la demande de comptabilisation en tant que RADIUS AVPair spécifique au fournisseur **cisco-av-pair**

: dhcp-option=<option DHCP>

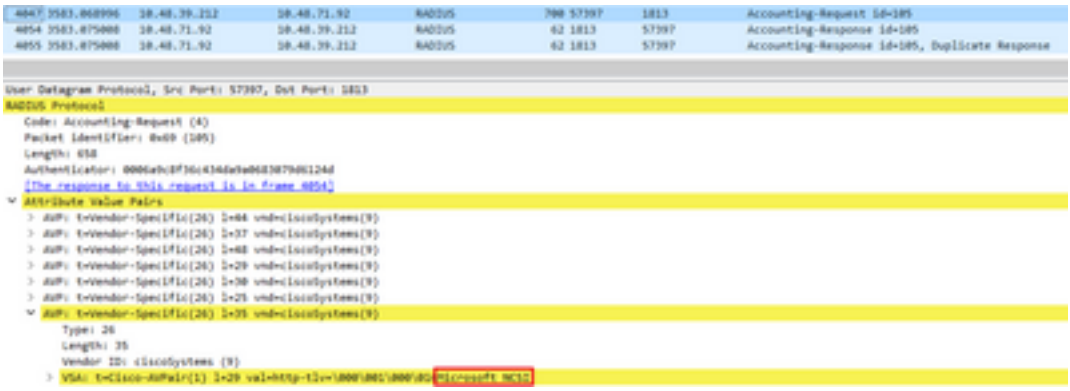
Exemple d'un paquet de demande de comptabilisation montrant des paires AVP pour les options DHCP 12, 60 et 55, respectivement envoyées du WLC au serveur RADIUS (la valeur de l'option 55 peut apparaître comme corrompue en raison du décodage Wireshark) :



Profilage RADIUS HTTP

Les informations obtenues via le profilage HTTP (champ User-Agent de l'en-tête de la requête HTTP GET) sont envoyées au serveur RADIUS à l'intérieur de la requête de comptabilisation en tant que RADIUS AVPair spécifique au fournisseur **cisco-av-pair : http-tlv=User-Agent=<user-agent>**

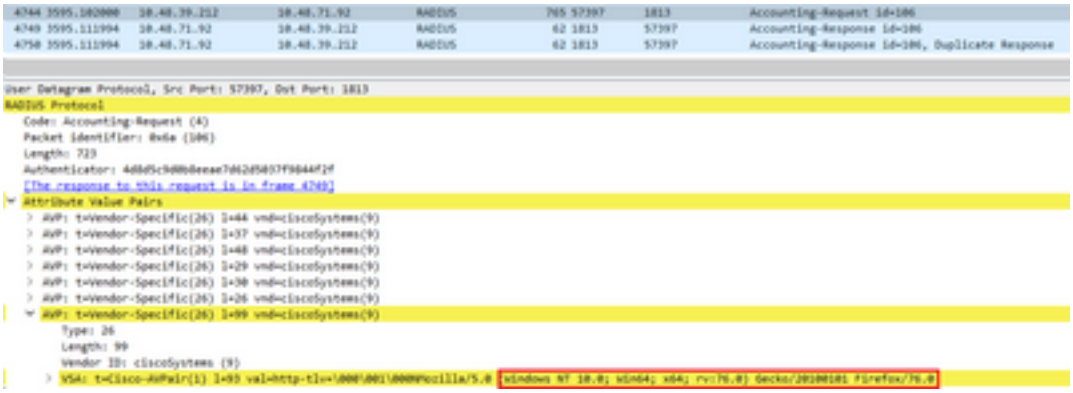
La vérification de connectivité initiale du paquet HTTP GET ne contient pas beaucoup d'informations dans le champ User-Agent, seulement « Microsoft NCSI ». Exemple d'un paquet de gestion des comptes transférant cette valeur simple au serveur RADIUS :



Une fois que l'utilisateur a commencé à naviguer sur Internet et qu'il a créé des requêtes HTTP GET supplémentaires, il est possible d'obtenir plus d'informations à ce sujet.

WLC envoie un paquet de comptabilisation supplémentaire à l'ISE s'il détecte de nouvelles valeurs User-Agent pour ce client.

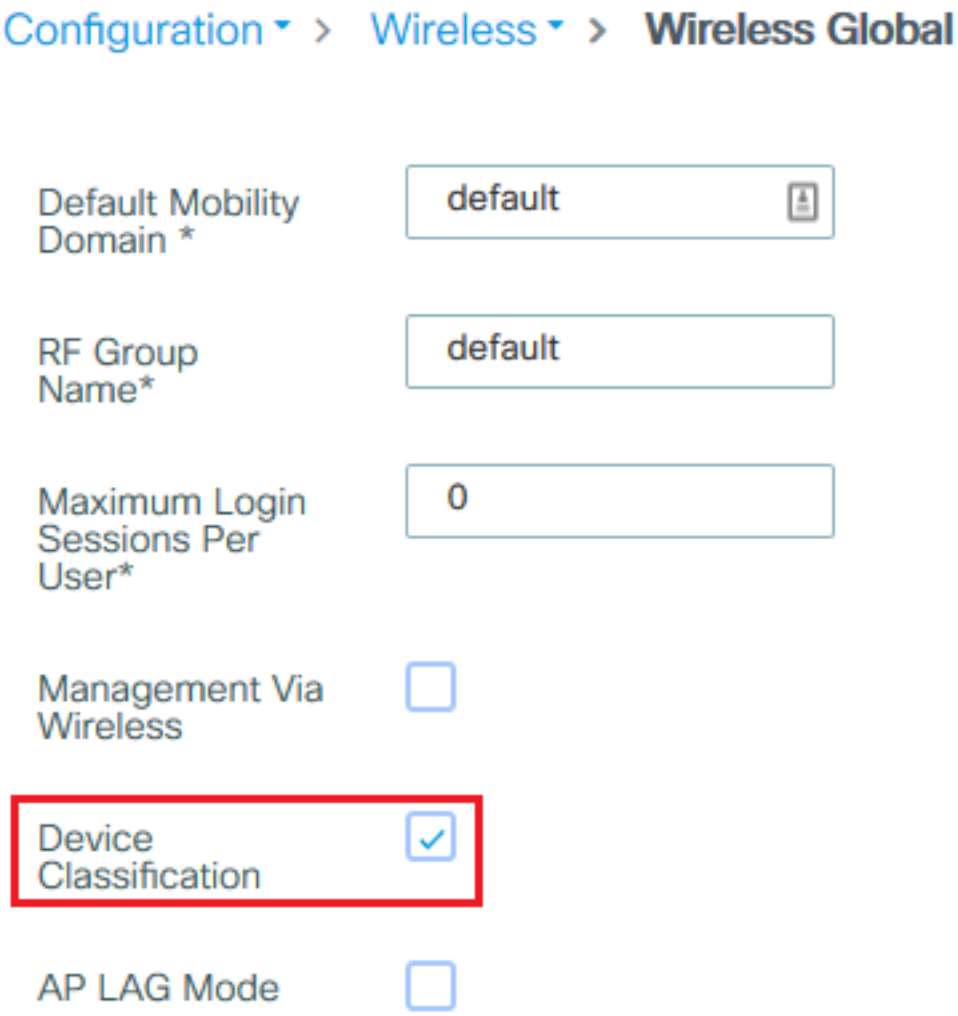
Dans cet exemple, il est possible de voir que le client utilise Windows 10 64 bits et Firefox 76 :



Configuration du profilage sur le WLC 9800

Configuration du profilage local

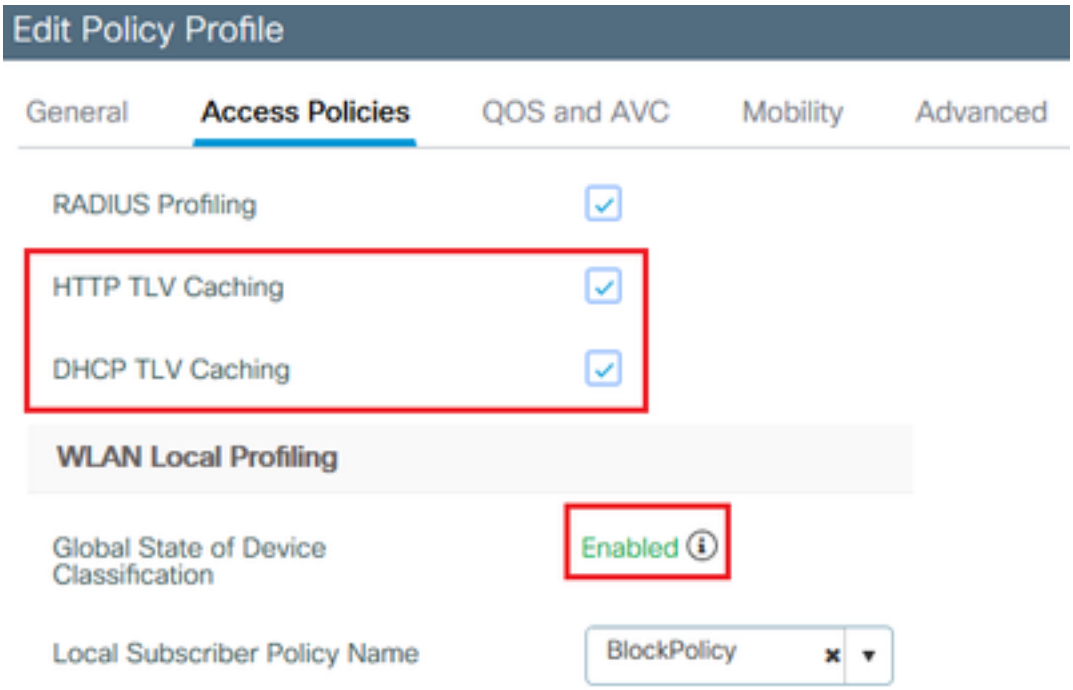
Pour que le profilage local fonctionne, activez simplement Device Classification sous Configuration > Wireless > Wireless Global. Cette option active simultanément les profils MAC OUI, HTTP et DHCP :



En outre, sous Policy configuration, vous pouvez activer HTTP TLV Caching et DHCP TLV Caching. Le WLC effectue le profilage même sans eux.

Lorsque ces options sont activées, le WLC met alors en cache les informations précédemment

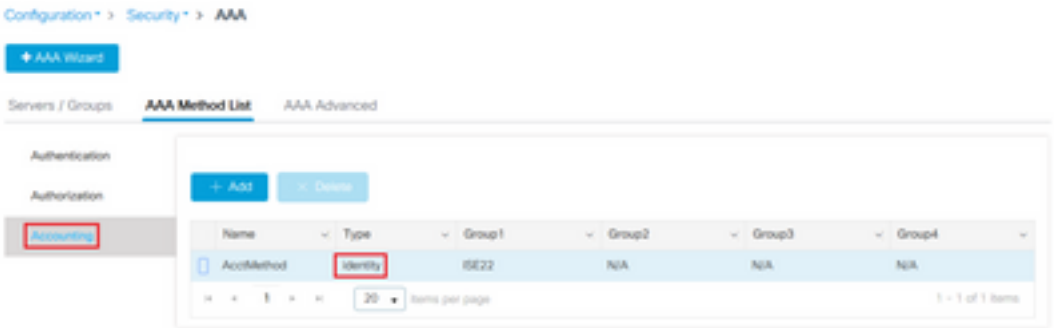
apprises sur ce client et évite d'avoir à inspecter des paquets supplémentaires générés par ce périphérique.



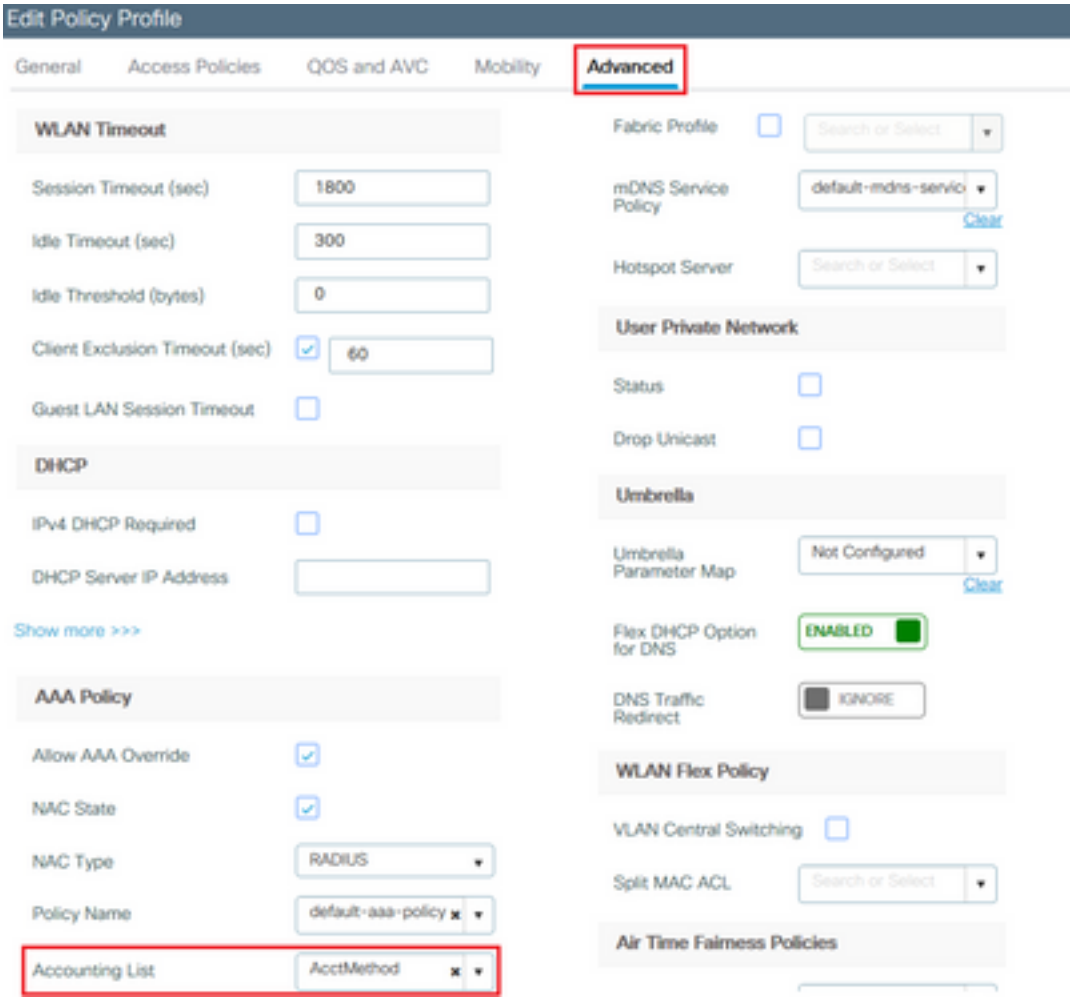
Configuration du profilage RADIUS

Pour que le profilage RADIUS fonctionne, outre l'activation globale de la classification des périphériques (comme mentionné dans la configuration du profilage local), il est nécessaire de :

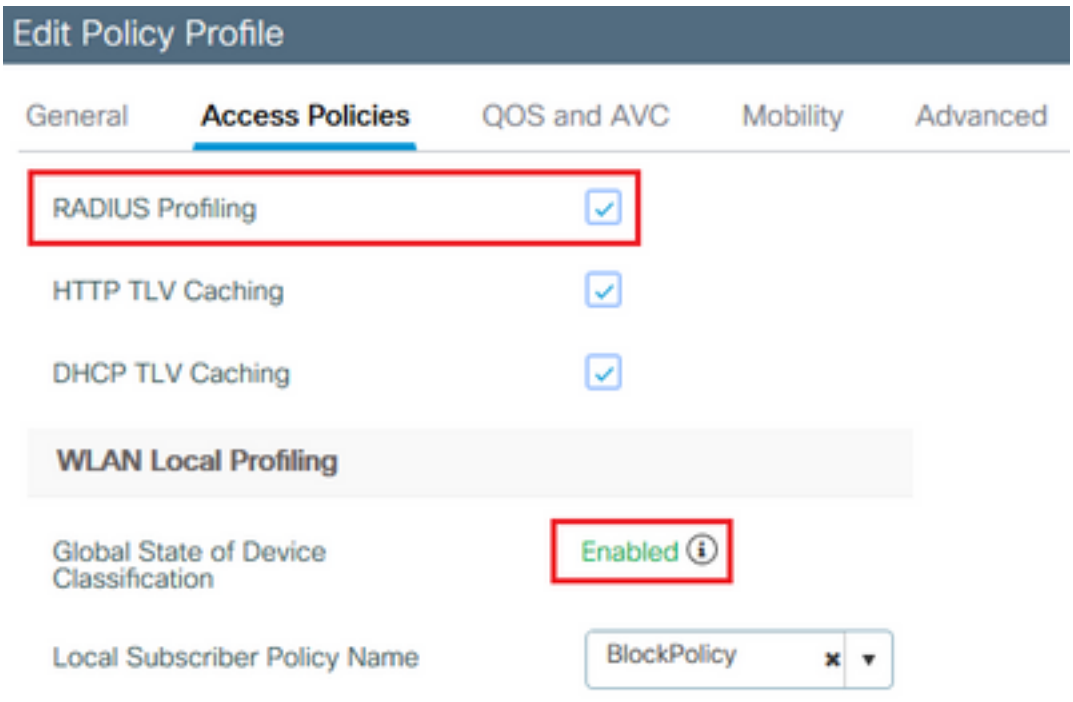
1. Configurez la méthode de comptabilité AAA avec le type «identité» pointant vers le serveur RADIUS :



2. La méthode de comptabilisation doit être ajoutée sous Configuration > Tags & Profiles > Policy > [Policy_Name] > Advanced :



3. Enfin, la case à cocher Profilage RADIUS doit être cochée sous Configuration > Tags & Profiles > Policy Cette case à cocher active à la fois le profilage RADIUS HTTP et DHCP (les anciens WLC AireOS avaient 2 cases à cocher distinctes) :



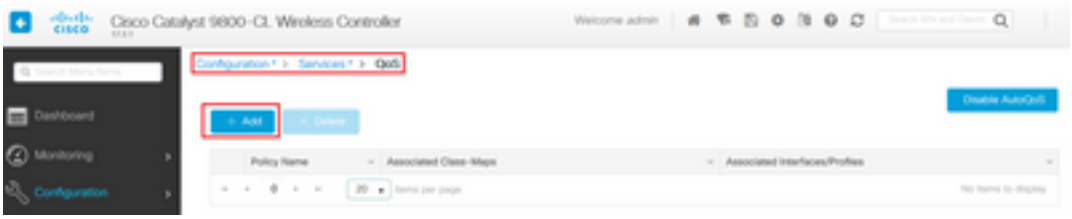
Profilage des cas d'utilisation

Application de stratégies locales basées sur la classification de profil local

Cet exemple de configuration illustre la configuration de la stratégie locale avec un profil QoS bloquant l'accès à YouTube et à Facebook qui est appliqué uniquement aux périphériques profilés comme Windows-Workstation.

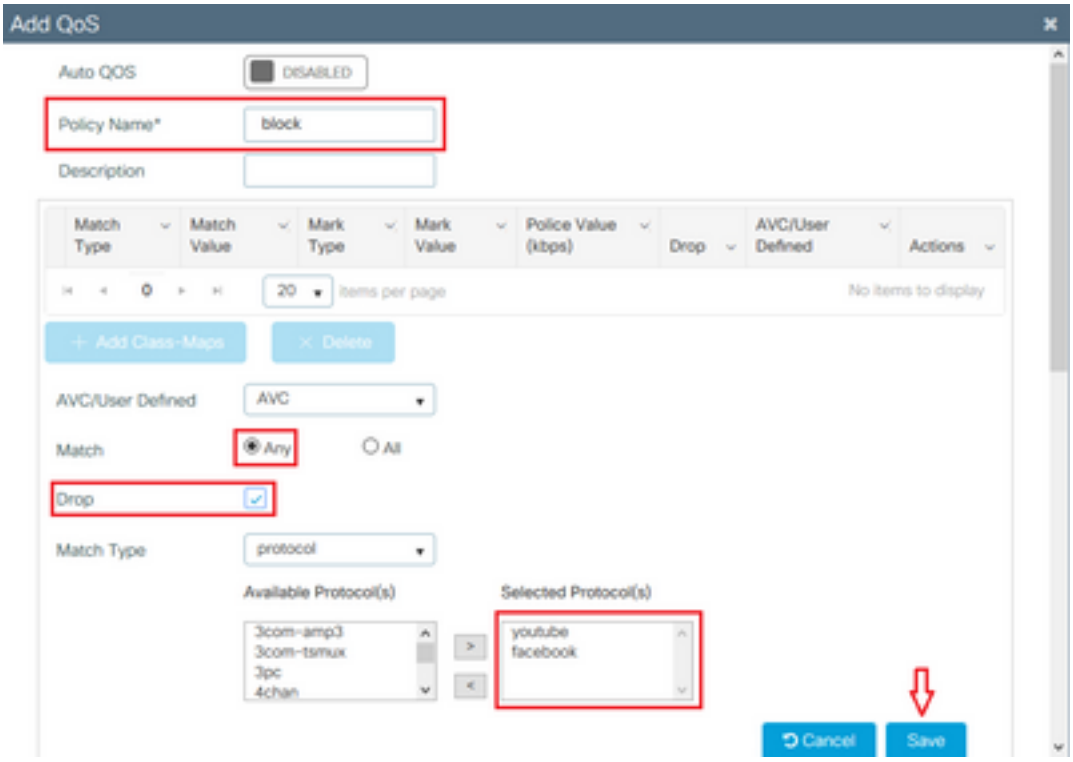
Avec de légères modifications, cette configuration peut être modifiée pour, par exemple, définir un marquage DSCP spécifique pour les téléphones sans fil uniquement.

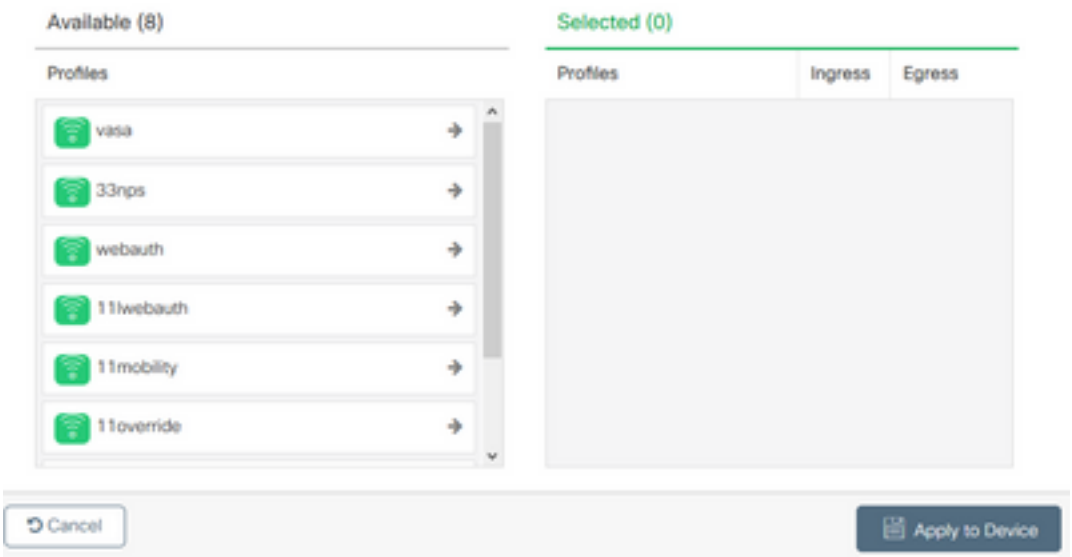
Créez un profil QoS en accédant à **Configuration** > **Services** > **QoS**. Cliquez sur Ajouter pour créer une nouvelle stratégie :



Spécifiez le nom de la stratégie et ajoutez une nouvelle carte de classe. Parmi les protocoles disponibles, sélectionnez ceux qui doivent être bloqués, marqués DSCP ou limités en bande passante.

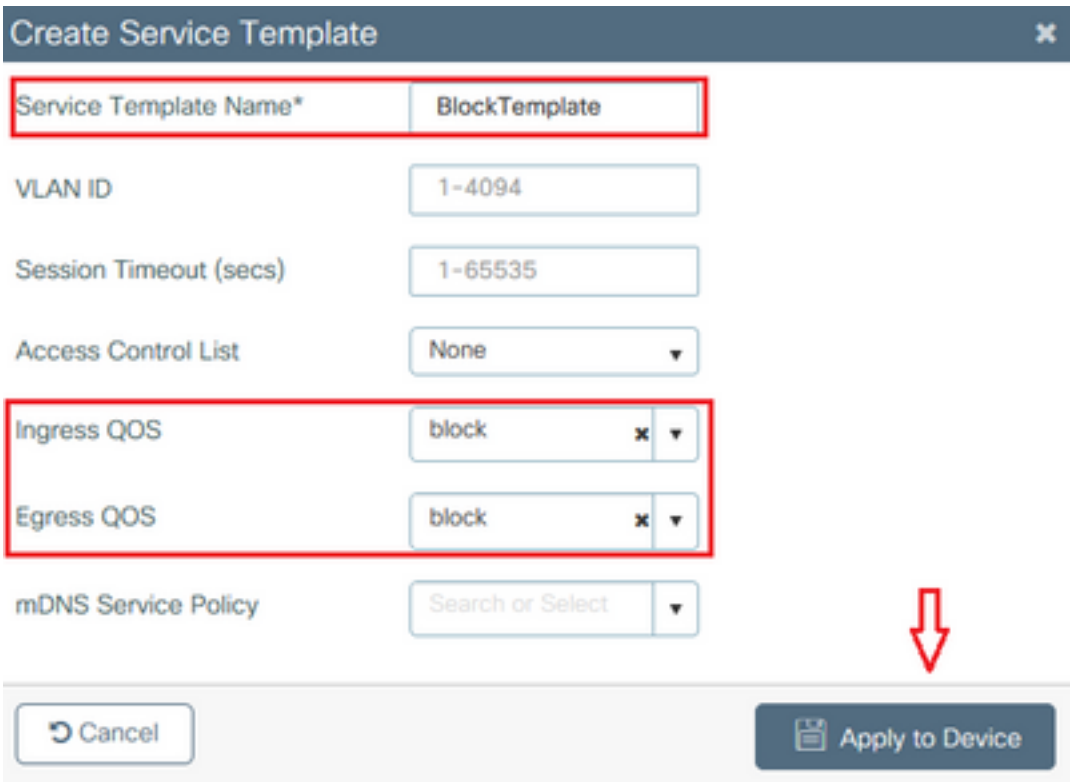
Dans cet exemple, youtube et facebook sont bloqués. Veillez à ne pas appliquer ce profil QoS aux profils de stratégie situés au bas de la fenêtre QoS :





Accédez à **Configuration > Security > Local Policy** et créez un nouveau modèle de service :

Spécifiez le profil QoS d'entrée et de sortie créé à l'étape précédente. Une liste d'accès peut également être appliquée à cette étape. Si aucune modification de VLAN n'est nécessaire, laissez le champ vlan vide :



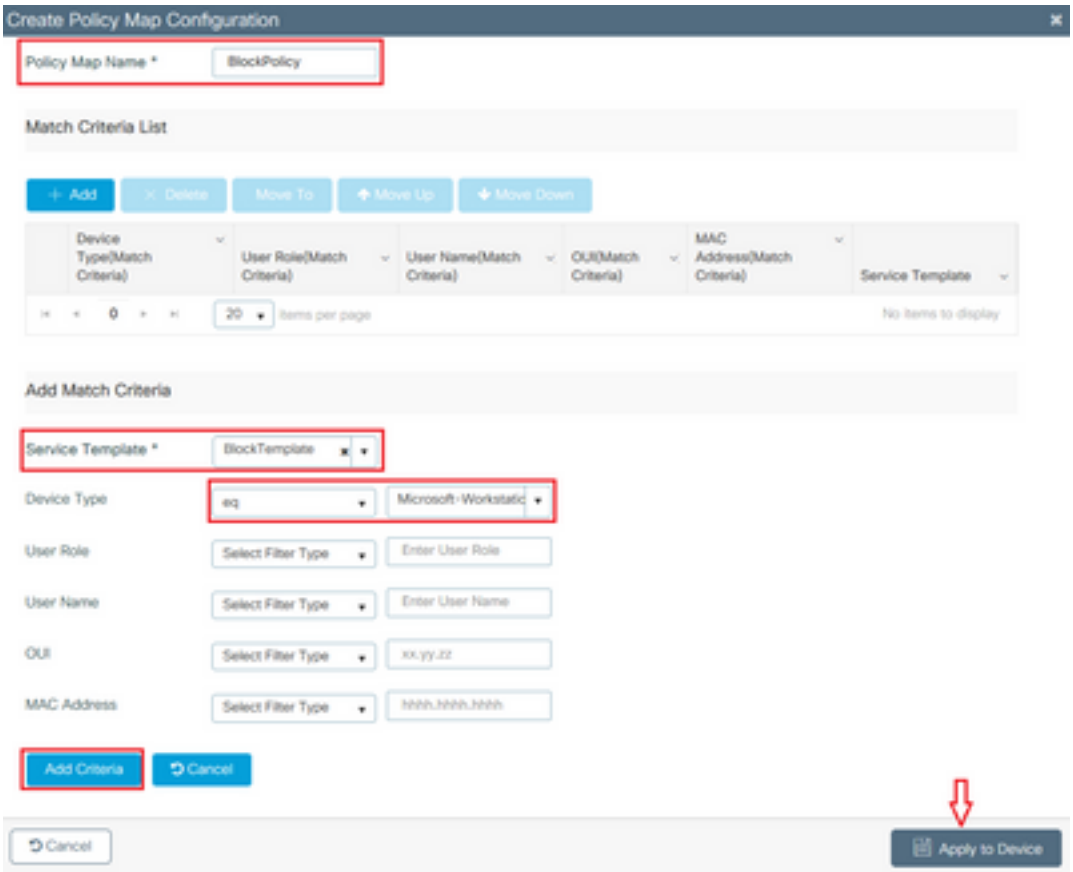
Accédez à l'onglet Carte de stratégie et cliquez sur Ajouter :

Définissez le nom du mappage de stratégie et ajoutez de nouveaux critères. Spécifiez le modèle de service créé à l'étape précédente et sélectionnez le type de périphérique auquel ce modèle est appliqué.

Dans ce cas, Microsoft-Workstation est utilisé. Si plusieurs stratégies sont définies, la première correspondance est utilisée.

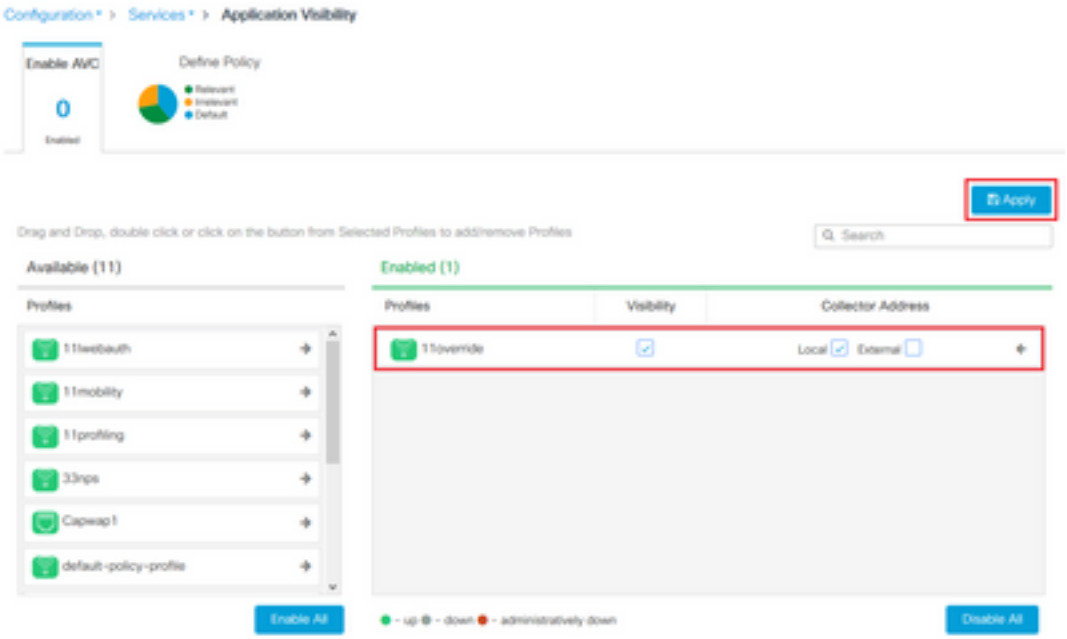
Un autre cas d'utilisation courant serait de spécifier des critères de correspondance basés sur l'OUI. Si un déploiement comporte un grand nombre de scanners ou d'imprimantes du même modèle, ils ont généralement le même OUI MAC.

Cela peut être utilisé pour appliquer un marquage QoS DSCP spécifique ou une liste de contrôle d'accès :

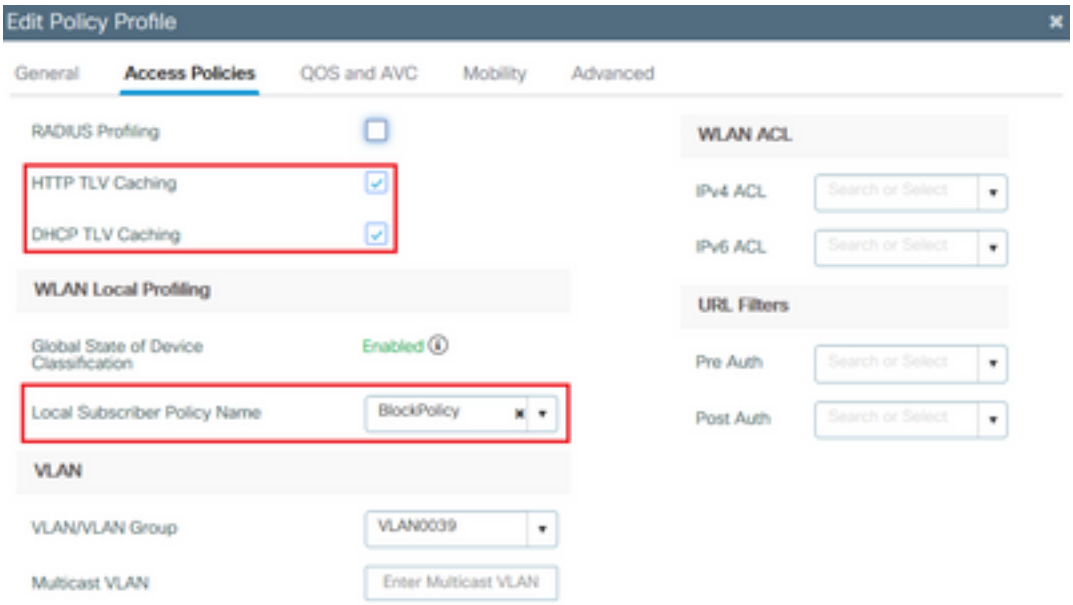


Pour que le WLC puisse reconnaître le trafic de youtube et de facebook, la visibilité de l'application doit être activée.

Naviguez jusqu'à **Configuration > Services > Application Visibility** eActivez la visibilité pour le profil de stratégie de votre WLAN :



Vérifiez que, sous le profil de stratégie, la mise en cache TLV HTTP, la mise en cache TLV DHCP et la classification globale des périphériques sont activées et que la stratégie d'abonné local pointe vers la carte de stratégie locale créée au cours de l'une des étapes précédentes :



Une fois le client connecté, il est possible de vérifier si la stratégie locale a été appliquée et de tester si youtube et facebook sont réellement bloqués.

Le résultat de la commande show wireless client mac-address [MAC_ADDR] detailed contient :

```
Input Policy Name  : block
Input Policy State : Installed
Input Policy Source : Native Profile Policy
Output Policy Name  : block
Output Policy State : Installed
Output Policy Source : Native Profile Policy

Local Policies:
  Service Template : BlockTemplate (priority 150)
  Input QOS        : block
```

```
  Output QOS       : block
  Service Template : wlan_svc_11override_local (priority 254)
  VLAN             : VLAN0039
  Absolute-Timer   : 1800

Device Type      : Microsoft-Workstation
Device Name      : MSFT 5.0
Protocol Map     : 0x000029  (OUI, DHCP, HTTP)
Protocol         : HTTP
```

Profilage Radius pour les ensembles de politiques avancés dans Cisco ISE

Lorsque le profilage RADIUS est activé, le WLC transfère les informations de profilage à l'ISE. Sur la base de ces informations, il est possible de créer des règles d'authentification et d'autorisation avancées.

Cet article ne couvre pas la configuration ISE. Pour plus d'informations, reportez-vous au Guide de conception de profilage Cisco ISE.

Ce flux de travail nécessite généralement l'utilisation de CoA, donc assurez-vous qu'il est activé sur le WLC 9800.

Profilage dans les déploiements FlexConnect

Authentification centrale, Commutation locale

Dans cette configuration, le profilage local et le profilage RADIUS continuent de fonctionner exactement comme décrit dans les chapitres précédents. Si le point d'accès passe en mode autonome (le point d'accès perd la connexion au WLC), le profilage de périphérique cesse de fonctionner et aucun nouveau client ne peut se connecter.

Authentification locale, Commutation locale

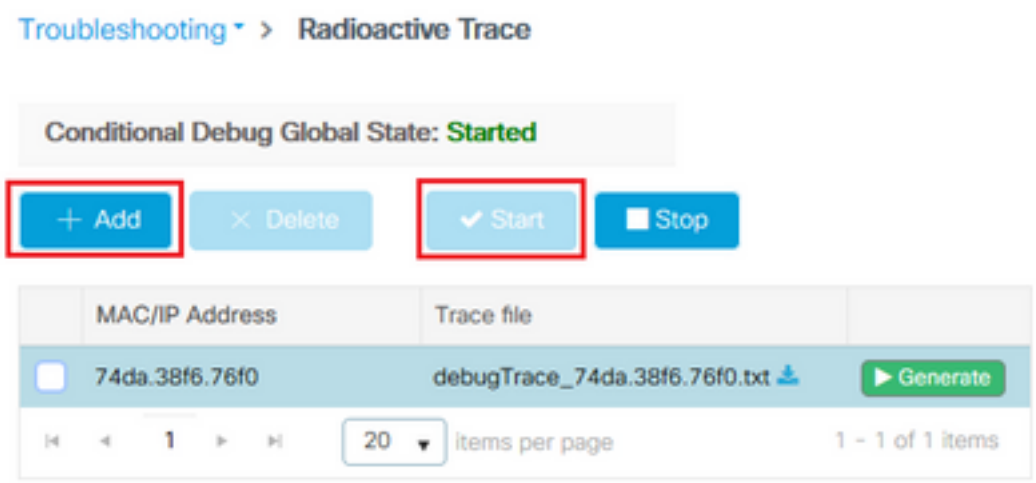
Si AP est en mode connecté (AP joint au WLC), le profilage continue à fonctionner (AP envoie une copie des paquets DHCP client au WLC pour effectuer le processus de profilage).

Bien que le profilage fonctionne, étant donné que l'authentification est effectuée localement sur le point d'accès, les informations de profilage ne peuvent pas être utilisées pour une configuration de stratégie locale ou des règles de profilage RADIUS.

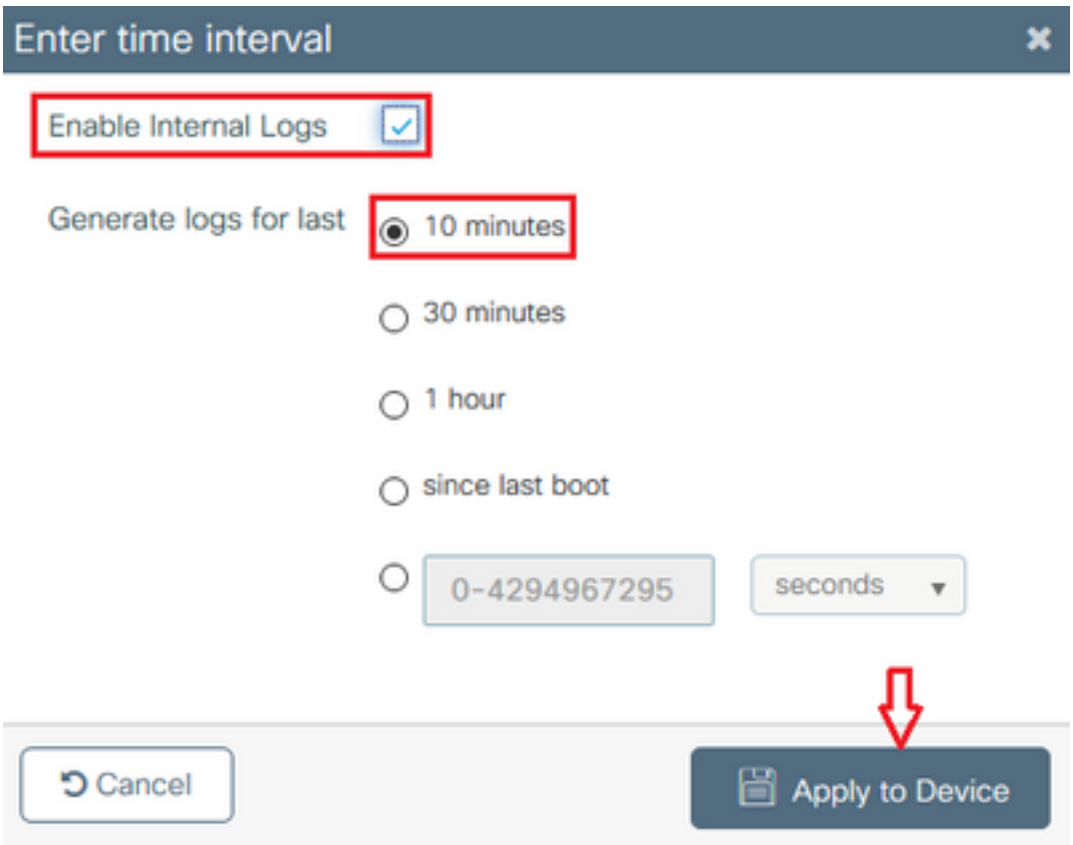
Dépannage

Traces radioactives

La façon la plus simple de dépanner le profilage client sur le WLC est via des traces radioactives. Accédez à **Troubleshooting > Radioactive Trace**, entrez l'adresse MAC de la carte sans fil cliente et cliquez sur Start :



Connectez le client au réseau et attendez qu'il atteigne l'état d'exécution. Arrêtez les traces et cliquez sur **Generate**. Assurez-vous que les journaux internes sont activés (cette option n'existe que dans les versions 17.1.1 et ultérieures) :



Des extraits pertinents de la trace radioactive sont disponibles ci-dessous :

Client profilé par WLC comme Microsoft-Workstation :

```
2020/06/18 10:46:41.052366 {wncd_x_R0-0}{1}: [auth-mgr] [21168]: (info):
[74da.38f6.76f0:capwap_90000004] Device type for the session is detected as Microsoft-
Workstation and old device-type not classified earlier &Device name for the session is detected
as MSFT 5.0 and old device-name not classified earlier & Old protocol map 0 and new is 41
2020/06/18 10:46:41.052367 {wncd_x_R0-0}{1}: [auth-mgr] [21168]: (debug):
[74da.38f6.76f0:capwap_90000004] updating device type Microsoft-Workstation, device name MSFT
5.0
```

Mise en cache WLC de la classification du périphérique :

```
(debug): [74da.38f6.76f0:unknown] Updating cache for mac [74da.38f6.76f0] device_type:
Microsoft-Workstation, device_name: MSFT 5.0 user_role: NULL protocol_map: 41
```

WLC recherchant la classification de périphérique dans le cache :

```
(info): [74da.38f6.76f0:capwap_90000004] Device type found in cache Microsoft-Workstation
```

WLC appliquant une politique locale basée sur la classification :

```
(info): device-type filter: Microsoft-Workstation required, Microsoft-Workstation set - match
for 74da.38f6.76f0 / 0x9700001A
(info): device-type Filter evaluation succeeded
(debug):  match device-type eq "Microsoft-Workstation" :success
```

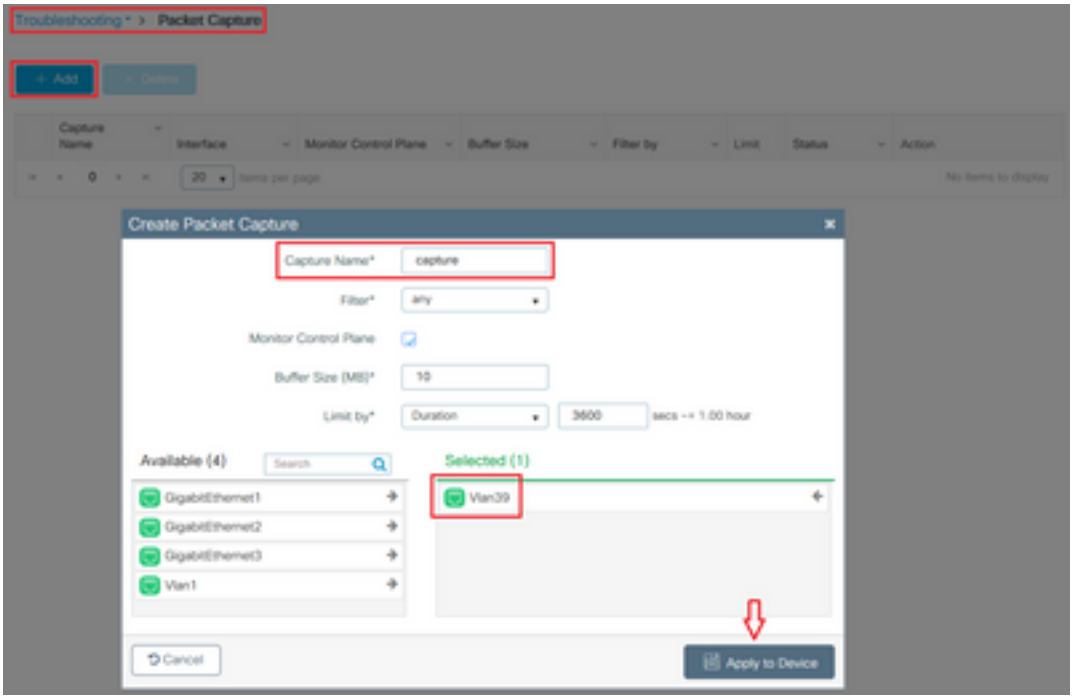
WLC envoyant des paquets de comptabilité contenant l'attribut de profilage DHCP et HTTP :

```
[caaa-acct] [21168]: (debug): [CAAA:ACCT:c9000021] Accounting session created
[auth-mgr] [21168]: (info): [74da.38f6.76f0:capwap_90000004] Getting active filter list
[auth-mgr] [21168]: (info): [74da.38f6.76f0:capwap_90000004] Found http
[auth-mgr] [21168]: (info): [74da.38f6.76f0:capwap_90000004] Found dhcp
[aaa-attr-inf] [21168]: (debug): Filter list http-tlv 0
[aaa-attr-inf] [21168]: (debug): Filter list dhcp-option 0

[aaa-attr-inf] [21168]: (debug): Get acct attrs dc-profile-name 0 "Microsoft-Workstation"
[aaa-attr-inf] [21168]: (debug): Get acct attrs dc-device-name 0 "MSFT 5.0"
[aaa-attr-inf] [21168]: (debug): Get acct attrs dc-device-class-tag 0 "Workstation:Microsoft-
Workstation"
[aaa-attr-inf] [21168]: (debug): Get acct attrs dc-certainty-metric 0 10 (0xa)
[aaa-attr-inf] [21168]: (debug): Get acct attrs dhcp-option 0 00 0c 00 0f 44 45 53 4b 54 4f 50
2d 4b 4c 52 45 30 4d 41
[aaa-attr-inf] [21168]: (debug): Get acct attrs dhcp-option 0 00 3c 00 08 4d 53 46 54 20 35 2e
30
[aaa-attr-inf] [21168]: (debug): Get acct attrs dhcp-option 0 00 37 00 0e 01 03 06 0f 1f 21 2b
2c 2e 2f 77 79 f9 fc

### http profiling sent in a separate accounting packet
[aaa-attr-inf] [21168]: (debug): Get acct attrs http-tlv 0 00 01 00 0e 4d 69 63 72 6f 73 6f 66
74 20 4e 43 53 49
```

Captures de paquets

Dans un déploiement à commutation centrale, les captures de paquets peuvent être effectuées sur le WLC lui-même. Accédez à **Troubleshooting > Packet Capture** et créez un nouveau point de capture sur l'une des interfaces qui sont utilisées par ce client.

Il est nécessaire d'avoir une interface SVI sur le VLAN afin d'effectuer la capture sur celui-ci, sinon prendre la capture sur le port physique lui-même


Troubleshooting
Packet Capture
Add
Delete
Capture Name
Interface
Monitor Control Plane
Buffer Size
Filter by
Limit
Status
Action
No items to display
Create Packet Capture
Capture Name*
capture
Filter*
any
Monitor Control Plane
Buffer Size (MB)*
10
Limit by*
Duration
3600
secs = 1.00 hour
Available (4)
Search
GigabitEthernet1
GigabitEthernet2
GigabitEthernet3
Vlan1
Selected (1)
Vlan39
Cancel
Apply to Device

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.