Dimostrazione della profilatura del client sul controller LAN wireless 9800

Sommario

Introduzione

In questo documento viene descritto il funzionamento della classificazione e della profilatura dei dispositivi sui Cisco Catalyst 9800 Wireless LAN Controller.

Componenti usati

- 9800 CL WLC con immagine 17.2.1
- Access point 1815i
- Client wireless Windows 10 Pro
- Cisco ISE 2.7

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Processo di profilatura

In questo documento viene descritto in modo approfondito il funzionamento della classificazione e della profilatura dei dispositivi sui Cisco Catalyst 9800 Wireless LAN Controller, vengono descritti i potenziali casi di utilizzo, gli esempi di configurazione e i passaggi necessari per risolvere il problema.

La profilatura dei dispositivi è una funzionalità che consente di ottenere ulteriori informazioni su un client wireless che si è unito all'infrastruttura wireless.

Una volta eseguita, la profilatura dei dispositivi può essere utilizzata per applicare criteri locali diversi o per soddisfare specifiche regole del server RADIUS.

Cisco 9800 WLC sono in grado di eseguire tre (3) tipi di profiling dei dispositivi:

1. OUI indirizzo MAC
2. DHCP
3. HTTP

Profiling OUI indirizzo MAC

L'indirizzo MAC è un identificatore univoco di ciascuna interfaccia di rete wireless (e cablata). Si tratta di un numero a 48 bit in genere scritto in formato esadecimale MM:MM:MM:SS:SS:SS.

I primi 24 bit (o 3 ottetti) sono noti come OUI (Organizationally Unique Identifier, identificatore univoco organizzativo) e identificano in modo univoco un fornitore o un produttore.

Vengono acquistate e assegnate dalla IEEE. Un fornitore o un produttore può acquistare più OUI.

Esempio:

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

Una volta che un client wireless si associa al punto di accesso, il WLC esegue la ricerca OUI per determinare il produttore.

Nelle distribuzioni di switching locale Flexconnect, l'access point inoltra ancora le informazioni rilevanti del client al WLC (come i pacchetti DHCP e l'indirizzo MAC del client).

La profilatura basata solo su OUI è estremamente limitata ed è possibile classificare il dispositivo come un marchio specifico, ma non è in grado di distinguere tra un laptop e uno smartphone.

Problemi relativi agli indirizzi MAC amministrati localmente

A causa di problemi di privacy, molti produttori hanno iniziato ad implementare funzionalità di randomizzazione mac nei loro dispositivi.

Gli indirizzi MAC amministrati localmente sono generati in modo casuale e il secondo bit meno significativo del primo ottetto dell'indirizzo è impostato su 1.

Questo bit funge da contrassegno che annuncia che l'indirizzo MAC è in realtà un indirizzo generato in modo casuale.

Esistono quattro possibili formati di indirizzi MAC amministrati localmente (x può essere qualsiasi valore esadecimale):

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

Per impostazione predefinita, i dispositivi Android 10 utilizzano un indirizzo MAC amministrato localmente generato in modo casuale ogni volta che si connettono a una nuova rete SSID.

Questa funzione annulla completamente la classificazione dei dispositivi basata su OUI, in quanto il controller riconosce che l'indirizzo è stato casuale e non esegue alcuna ricerca.

Profilatura DHCP

La profilatura DHCP viene eseguita dal WLC analizzando i pacchetti DHCP inviati dal client wireless.

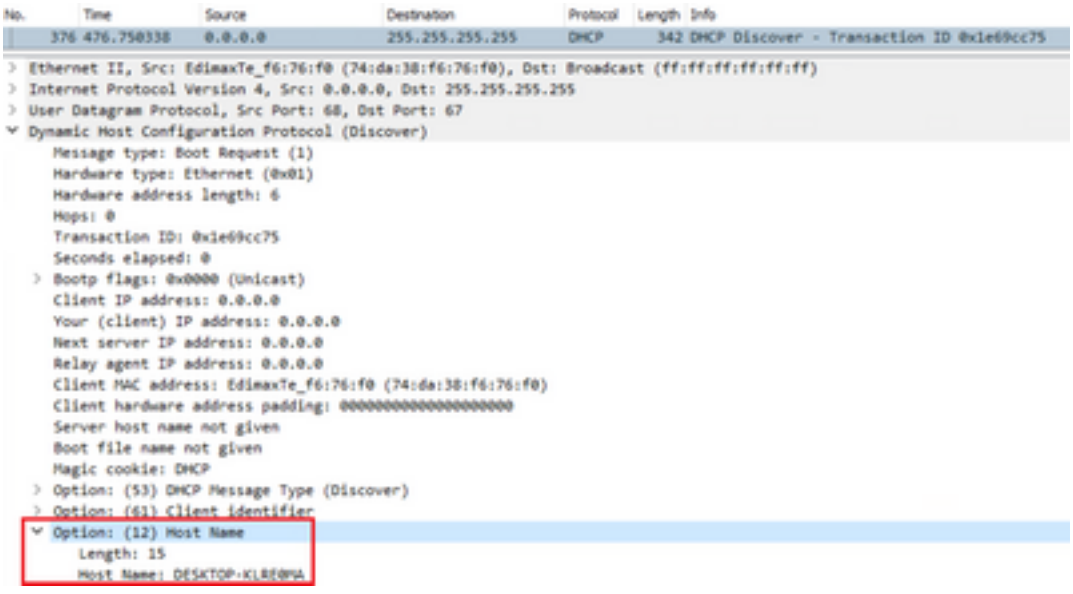
Se per classificare il dispositivo è stata utilizzata la profilatura DHCP, l'output del comando **show wireless client mac-address [MAC_ADDR] detailed** contiene:

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

WLC controlla diversi campi dell'opzione DHCP nei pacchetti inviati dai client wireless:

1. Opzione 12 - Hostname

Questa opzione rappresenta il nome host del client ed è disponibile nei pacchetti DHCP Discover e DHCP Request:



2. Opzione 60 - Identificatore della classe del fornitore

Questa opzione è disponibile anche nei pacchetti DHCP Discover e Request.

Con questa opzione, i client possono identificarsi sul server DHCP e i server possono quindi essere configurati in modo da rispondere solo ai client con un identificatore di classe fornitore specifico.

Questa opzione viene in genere utilizzata per identificare i punti di accesso nella rete e rispondere solo con l'opzione 43.

Esempi di identificatori di classe del fornitore

- "MSFT 5.0" per tutti i client Windows 2000 (e versioni successive)
- "MSFT 98" per tutti i client Windows 98 e Me
- "MSFT" per tutti i client Windows 98, Me e 2000

I dispositivi MacBook Apple non inviano l'opzione 60 per impostazione predefinita.

Esempio di acquisizione di pacchetti dal client Windows 10:

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

3. Opzione 55 - Elenco richieste parametri

L'opzione DHCP Parameter Request List contiene i parametri di configurazione (codici di opzione) richiesti dal client DHCP al server DHCP. È una stringa scritta in notazione separata da virgole (ad esempio 1,15,43).

Non è una soluzione perfetta perché i dati prodotti dipendono dal fornitore e possono essere duplicati da più tipi di dispositivi.

Ad esempio, i dispositivi Windows 10 richiedono sempre per impostazione predefinita un determinato elenco di parametri. Apple iPhone e iPad utilizzano diversi set di parametri su cui è possibile classificarli.

Esempio di acquisizione da 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
```

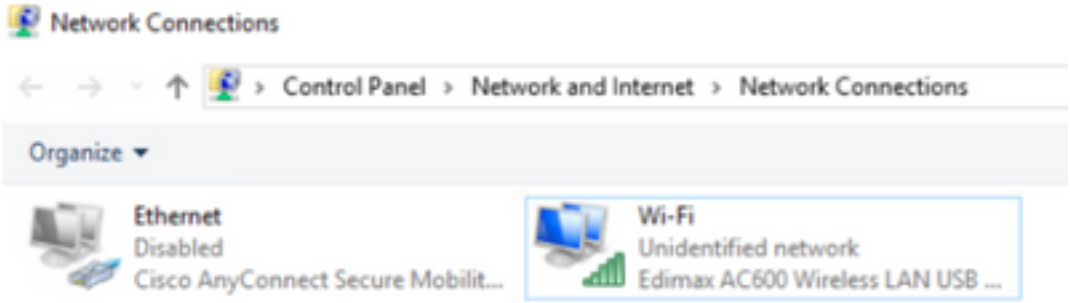
4. Opzione 77 - Classe utente

La classe utente è un'opzione che nella maggior parte dei casi non viene utilizzata per

impostazione predefinita e richiede la configurazione manuale del client. Ad esempio, questa opzione può essere configurata su un computer Windows utilizzando il comando:

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

Il nome della scheda è disponibile in Centro connessioni di rete e condivisione nel Pannello di controllo:



Configurare l'opzione DHCP 66 per il client Windows 10 in CMD (sono necessari i diritti di amministratore):

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

Windows IP Configuration

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

A causa dell'implementazione dell'opzione 66 da parte di Windows, wireshark non è in grado di decodificare questa opzione e una parte del pacchetto proveniente dall'opzione 66 risulta in formato non corretto:

```
  ▾ 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]
```

Profiling HTTP

Il profiling HTTP è il modo più avanzato di profilare 9800 WLC supporta e offre la classificazione dei dispositivi più dettagliata.

Affinché un client possa essere sottoposto a profiling HTTP, deve trovarsi nello stato "Esegui" ed eseguire una richiesta HTTP GET.

WLC intercetta la richiesta e cerca nel campo "User-Agent" nell'intestazione HTTP del pacchetto.

Questo campo contiene informazioni aggiuntive sul client wireless che possono essere utilizzate per classificarlo.

Per impostazione predefinita, quasi tutti i produttori hanno implementato una funzione in cui un client wireless tenta di eseguire il controllo della connettività Internet.

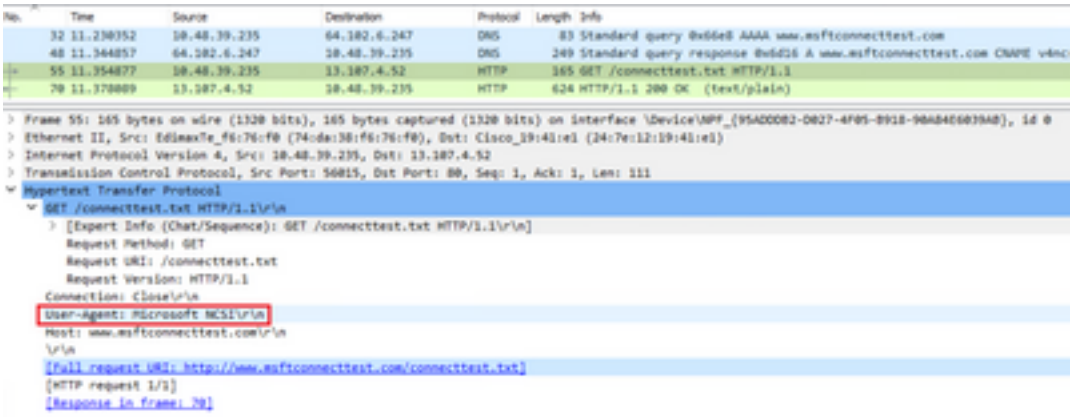
Questo controllo viene utilizzato anche per il rilevamento automatico del portale guest. Se un dispositivo riceve una risposta HTTP con codice di stato 200 (OK), la WLAN non è protetta con webauth.

In caso affermativo, il WLC esegue quindi l'intercettazione necessaria per eseguire il resto dell'autenticazione. Questo HTTP GET iniziale non è l'unico WLC utilizzabile per profilare il dispositivo.

Ogni richiesta HTTP successiva viene ispezionata dal WLC e può risultare con una classificazione ancora più dettagliata.

Per eseguire questo test, i dispositivi Windows 10 utilizzano il dominio **msftconnecttest.com**. I dispositivi Apple utilizzano **captive.apple.com**, mentre i dispositivi Android utilizzano in genere **connectivitycheck.gstatic.com**.

Le acquisizioni dei pacchetti del client Windows 10 che esegue questo controllo sono disponibili di seguito. Il campo Agente utente è popolato con **Microsoft NCSI**, il che fa sì che il client venga profilato sul WLC come **Microsoft-Workstation**:



Output di esempio di **show wireless client mac-address [MAC_ADDR] dettagliato** per un client con profilo tramite 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
```

Profilatura RADIUS

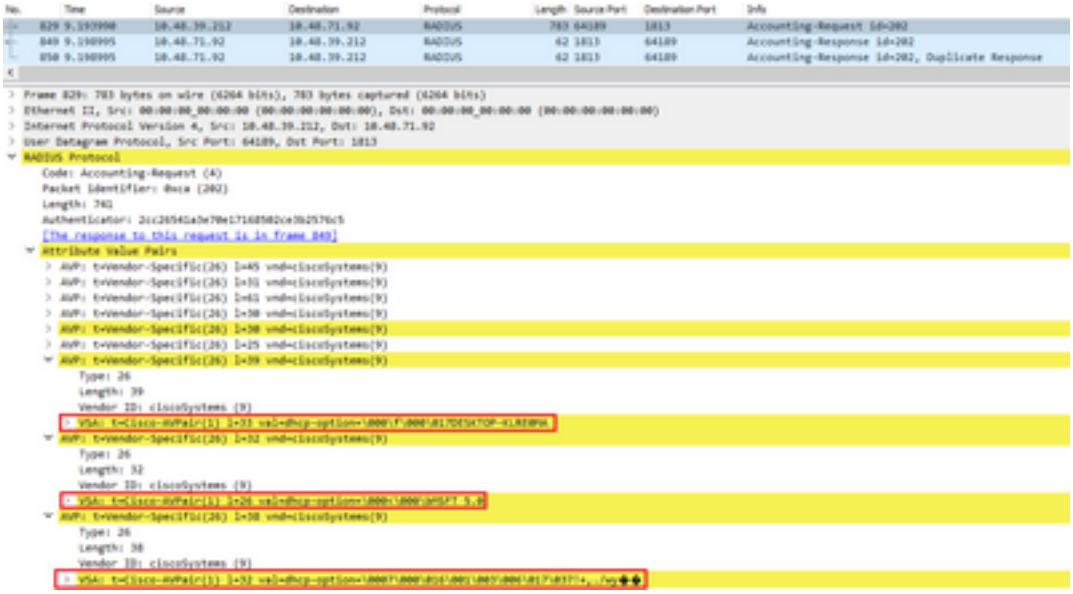
Quando si tratta di metodi utilizzati per classificare il dispositivo, non vi è alcuna differenza tra la profilatura locale e quella RADIUS.

Se la profilatura Radius è abilitata, il WLC inoltra al server RADIUS le informazioni apprese sul dispositivo tramite un insieme specifico di attributi RADIUS specifici del fornitore.

Profiling RADIUS DHCP

Le informazioni ottenute tramite profiling DHCP vengono inviate al server RADIUS all'interno della richiesta di accounting come AVPair RADIUS specifico del fornitore **cisco-av-pair: dhcp-option=<opzione DHCP>**

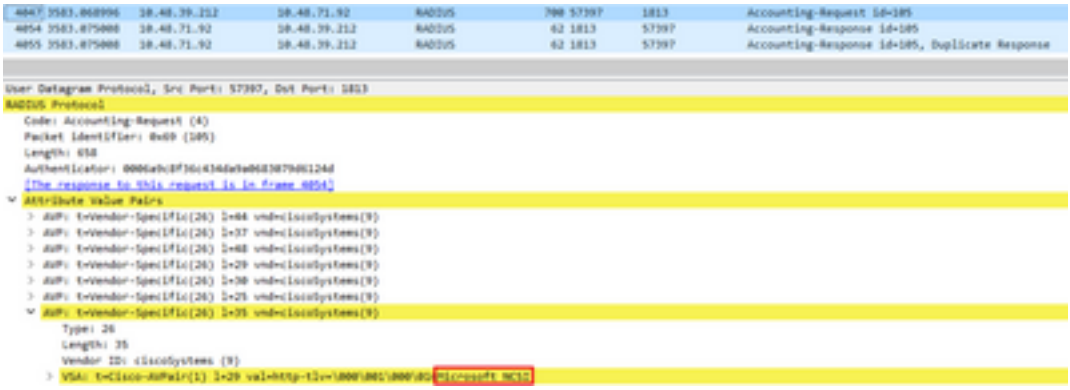
Esempio di pacchetto di richiesta di accounting che mostra gli AVPair per le opzioni DHCP 12, 60 e 55, rispettivamente inviate dal WLC al server RADIUS (il valore dell'opzione 55 potrebbe essere danneggiato a causa della decodifica Wireshark):



Profilatura RADIUS HTTP

Le informazioni ottenute tramite la profilatura HTTP (campo User-Agent dall'intestazione della richiesta HTTP GET) vengono inviate al server RADIUS all'interno della richiesta di accounting come AVPair RADIUS specifico del fornitore **cisco-av-pair: http-tlv=User-Agent=<agente-utente>**

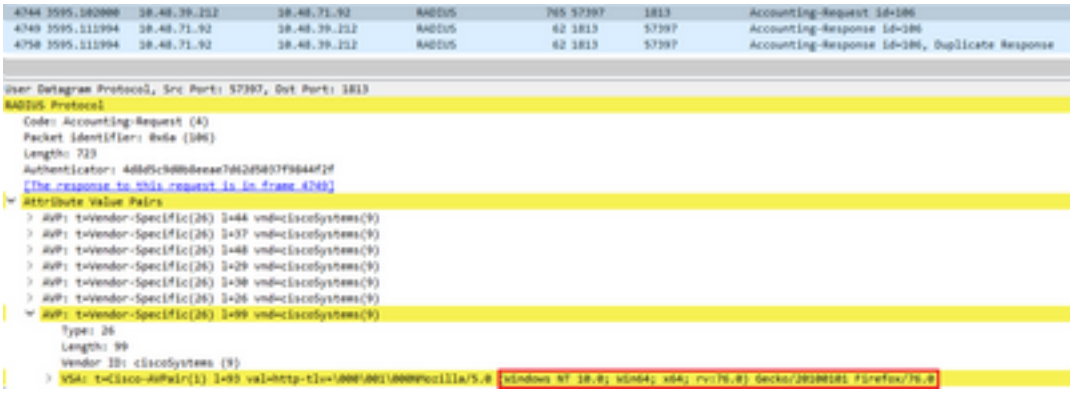
Il pacchetto HTTP GET per il controllo iniziale della connettività non contiene molte informazioni nel campo Agente utente, ma solo "Microsoft NCSI". Esempio di pacchetto di accounting che inoltra questo valore semplice al server RADIUS:



Una volta che l'utente inizia a navigare in Internet e crea alcune richieste HTTP GET aggiuntive, è possibile ottenere ulteriori informazioni su di esso.

WLC invia un pacchetto di accounting aggiuntivo all'ISE se rileva nuovi valori di User-Agent per questo client.

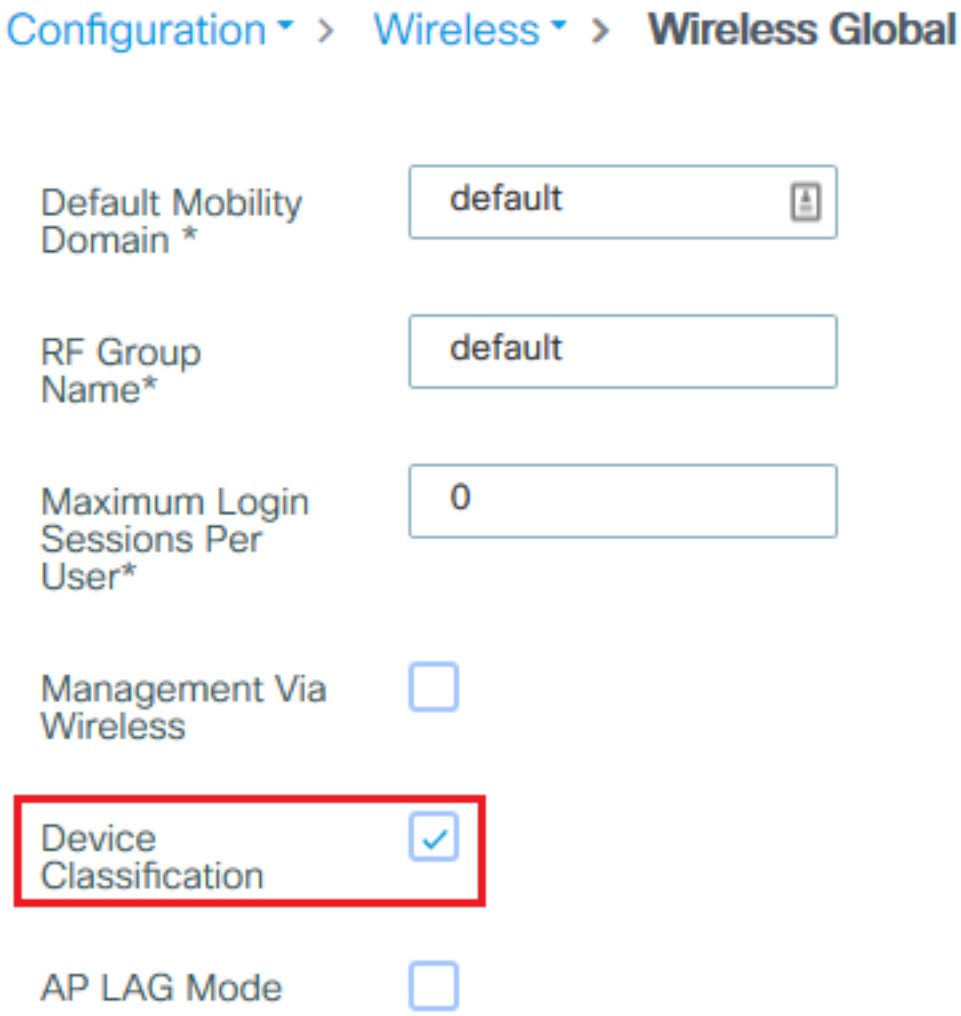
In questo esempio, è possibile vedere che il client utilizza Windows 10 a 64 bit e Firefox 76:



Configurazione della profilatura su 9800 WLC

Configurazione profilatura locale

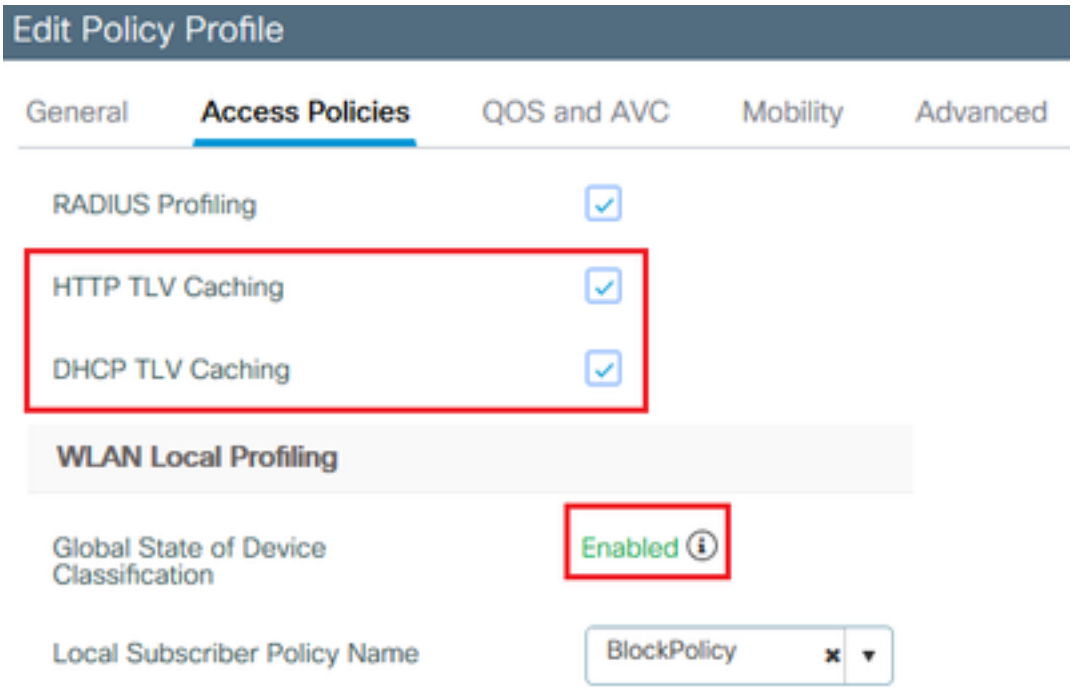
Per il corretto funzionamento della profilatura locale, è sufficiente abilitare la classificazione dei dispositivi in Configurazione > Wireless > Wireless globale. Questa opzione abilita contemporaneamente l'OUI MAC, il profiling HTTP e il profiling DHCP:



Inoltre, in Configurazione criteri è possibile abilitare la memorizzazione nella cache TLV HTTP e la memorizzazione nella cache TLV DHCP. WLC esegue la profilatura anche se senza di essi.

Con queste opzioni abilitate, il WLC memorizza quindi nella cache le informazioni apprese in

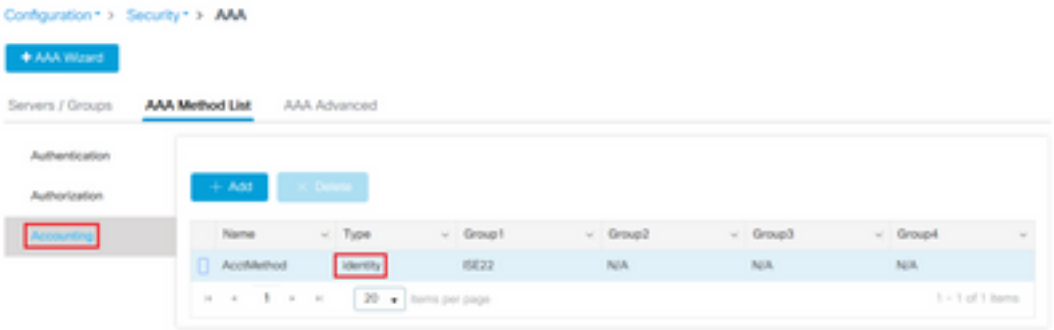
precedenza su questo client ed elimina la necessità di ispezionare pacchetti aggiuntivi generati da questo dispositivo.



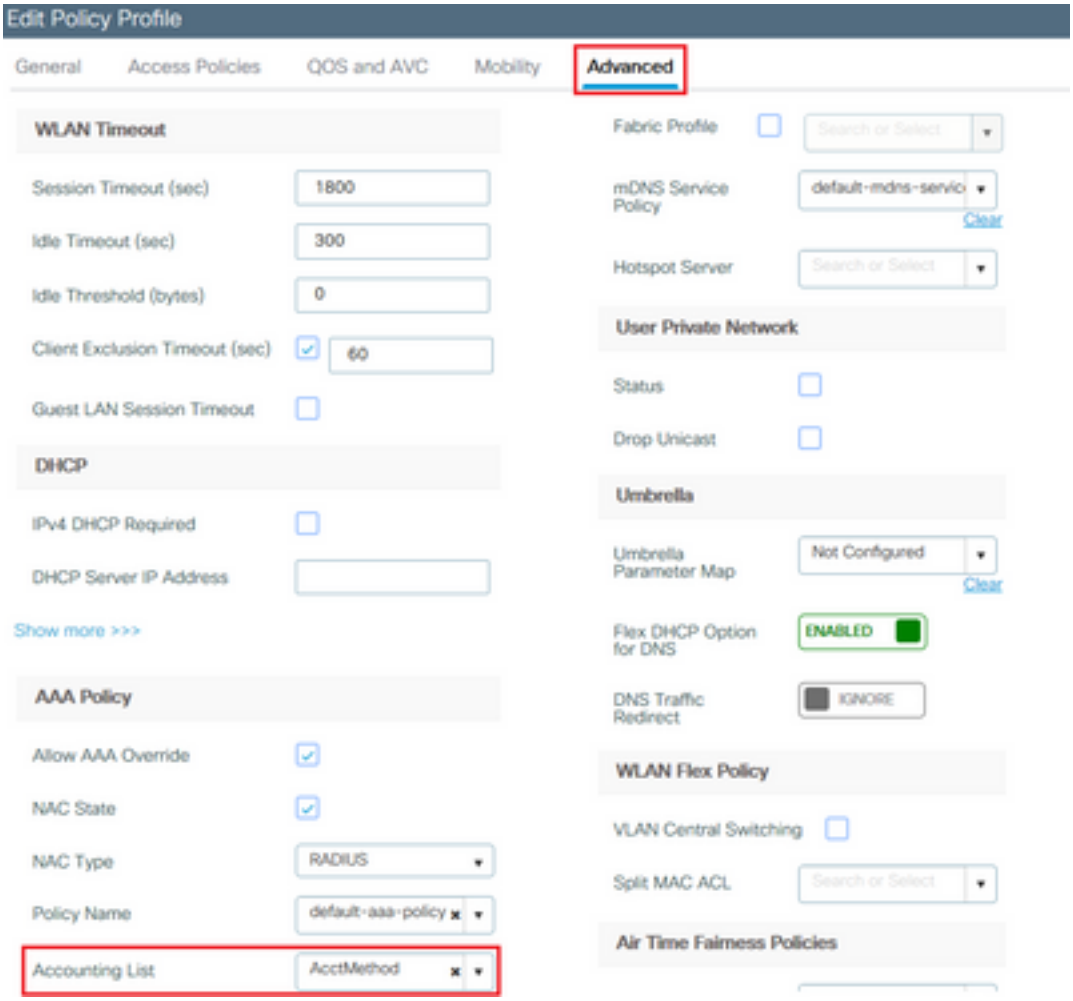
Configurazione profilatura RADIUS

Per il corretto funzionamento della profilatura RADIUS, oltre alla classificazione globale dei dispositivi (come indicato nella configurazione della profilatura locale), è necessario:

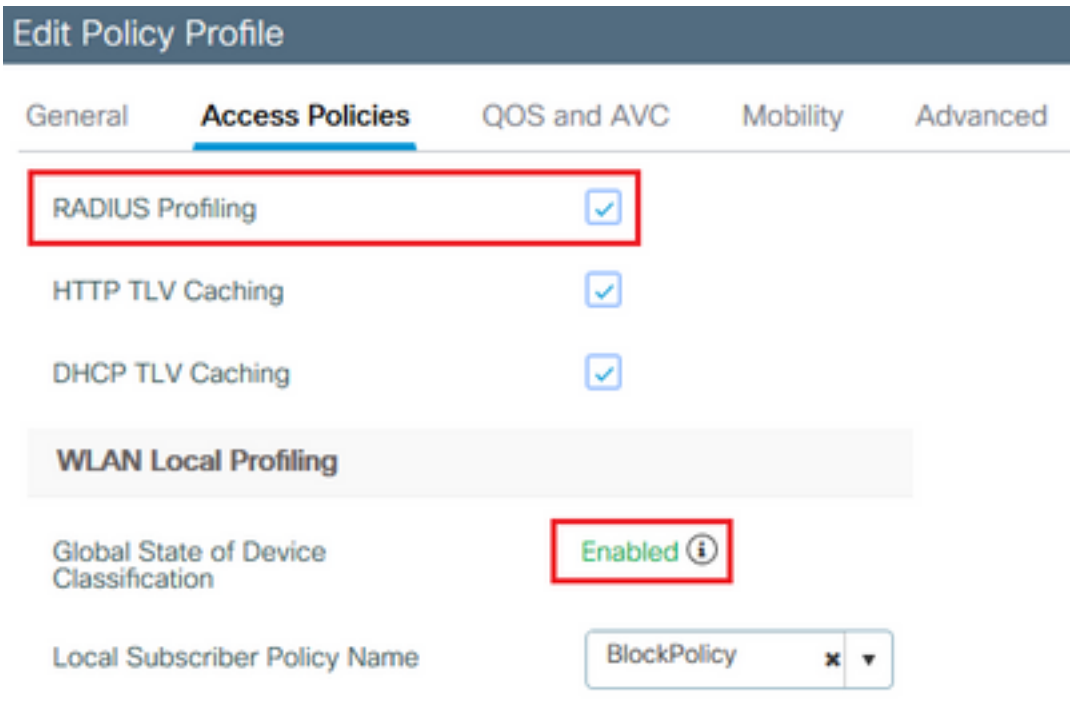
1. Configurare il metodo di accounting AAA con il tipo "identità" che punta al server RADIUS:



2. Il metodo contabile deve essere aggiunto in Configurazione > Tag e profili > Criterio > [Nome_criterio] > Avanzate:



3. Infine, la casella di controllo Profilatura RADIUS deve essere selezionata in Configurazione > Tag e profili > Criterio. Questa casella di controllo abilita la profilatura HTTP e DHCP RADIUS (i vecchi WLC AireOS avevano due caselle di controllo separate):



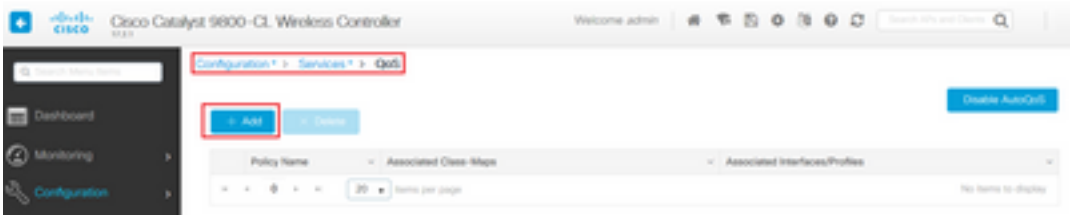
Creazione profilo casi di utilizzo

Applicazione di criteri locali in base alla classificazione della profilatura locale

In questa configurazione di esempio viene illustrata la configurazione di Criteri locali con profilo QoS che blocca l'accesso a YouTube e Facebook applicata solo ai dispositivi con profilo Windows-Workstation.

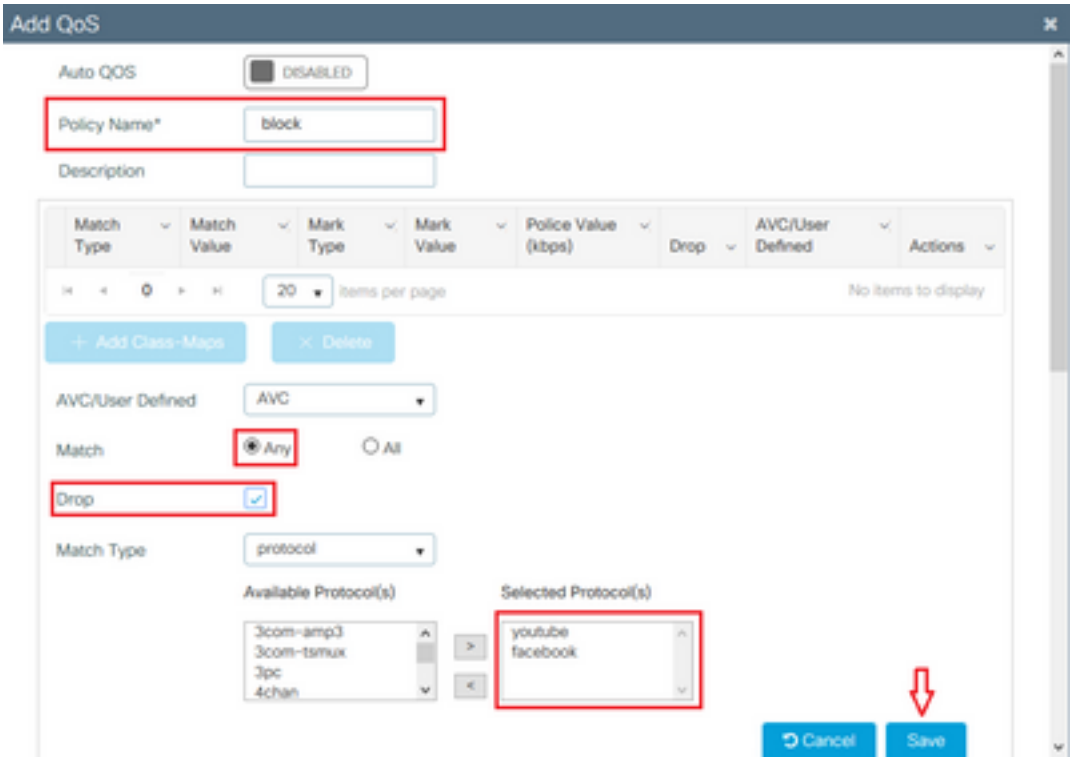
Con alcune piccole modifiche, questa configurazione può essere modificata, ad esempio, impostando un contrassegno DSCP specifico solo per i telefoni wireless.

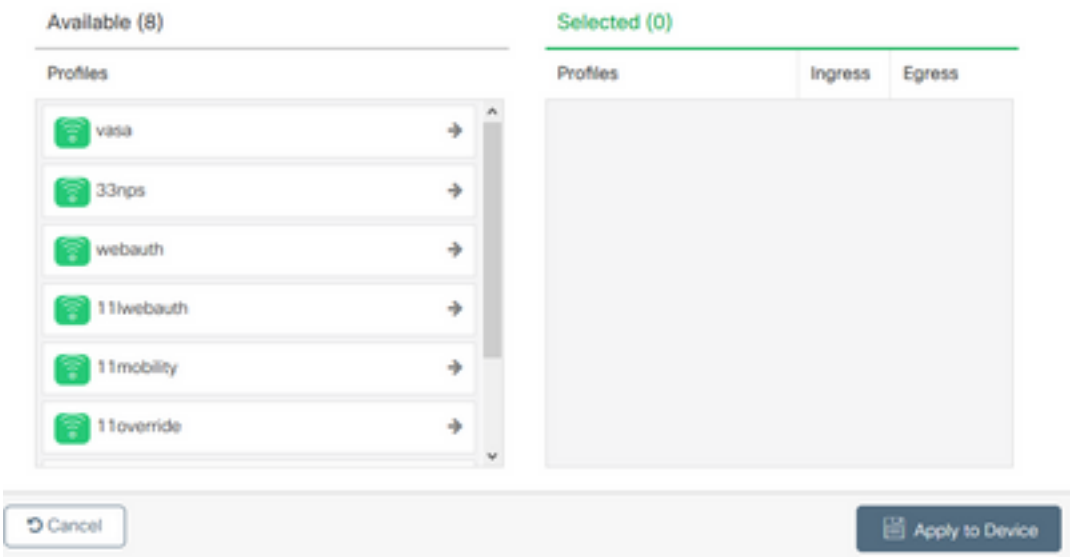
Creare un profilo QoS selezionando **Configurazione > Servizi > QoS**. Fare clic su Aggiungi per creare un nuovo criterio:



Specificare il nome del criterio e aggiungere un nuovo mapping di classi. Dai protocolli disponibili, selezionare quelli che devono essere bloccati, contrassegnati DSCP o con larghezza di banda limitata.

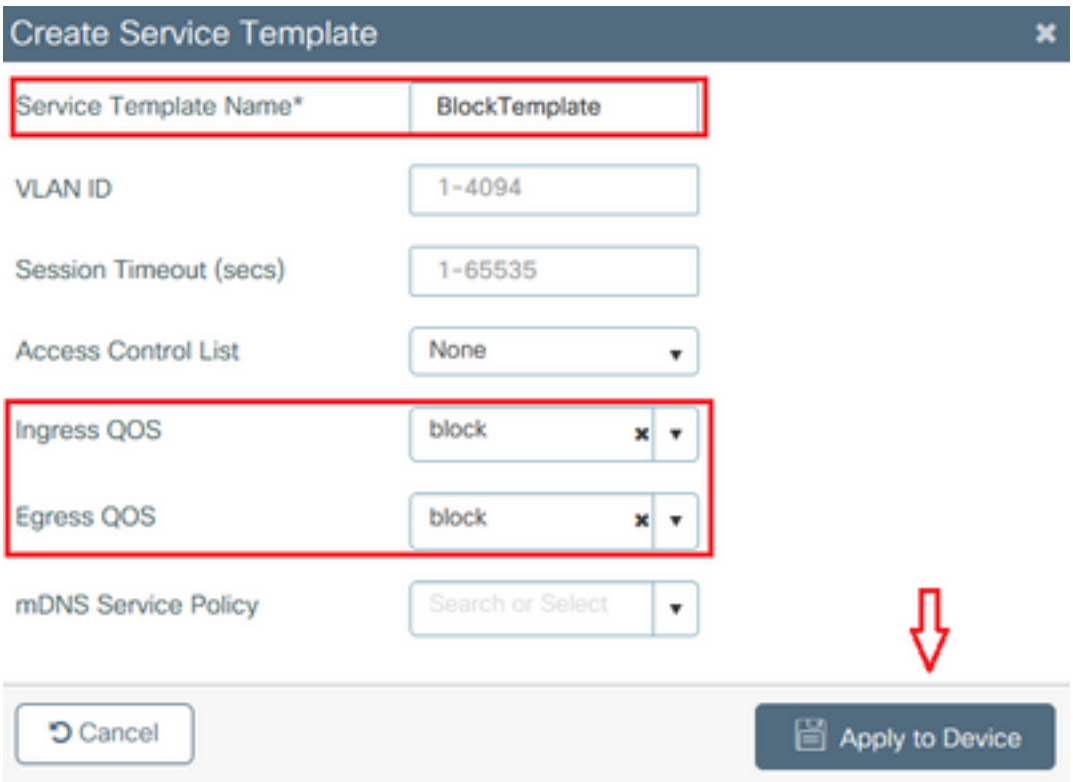
In questo esempio, youtube e facebook sono bloccati. Accertarsi di non applicare questo profilo QoS a nessuno dei profili dei criteri nella parte inferiore della finestra QoS:





Passare a **Configurazione > Protezione > Criterio locale** e creare un nuovo modello di servizio:

Specificare il profilo QoS in ingresso e in uscita creato nel passaggio precedente. In questo passaggio è possibile applicare anche un elenco degli accessi. Se non è necessario modificare la VLAN, lasciare vuoto il campo vlan:



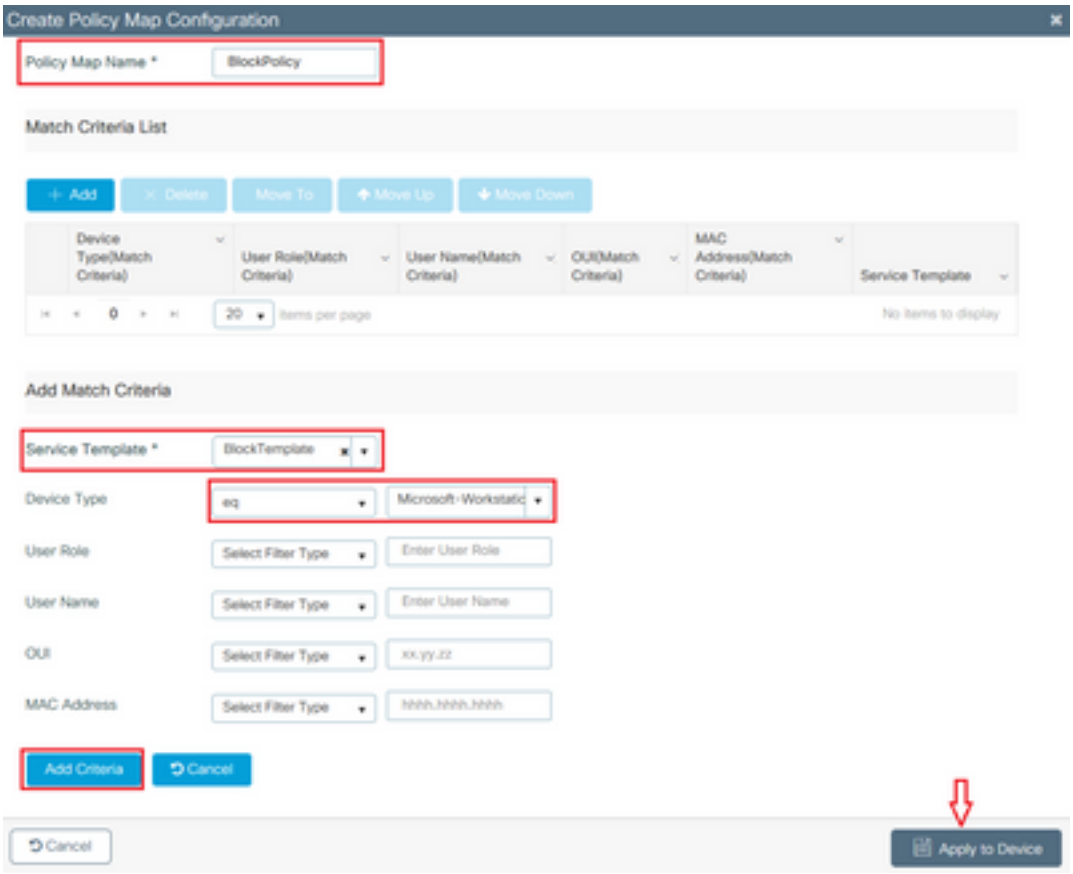
Passare alla scheda Mappa criteri e fare clic su Aggiungi:

Impostare il nome della mappa dei criteri e aggiungere nuovi criteri. Specificare il modello di servizio creato nel passaggio precedente e selezionare il tipo di dispositivo a cui viene applicato il modello.

In questo caso, viene utilizzato Microsoft-Workstation. Se vengono definiti più criteri, viene utilizzata la prima corrispondenza.

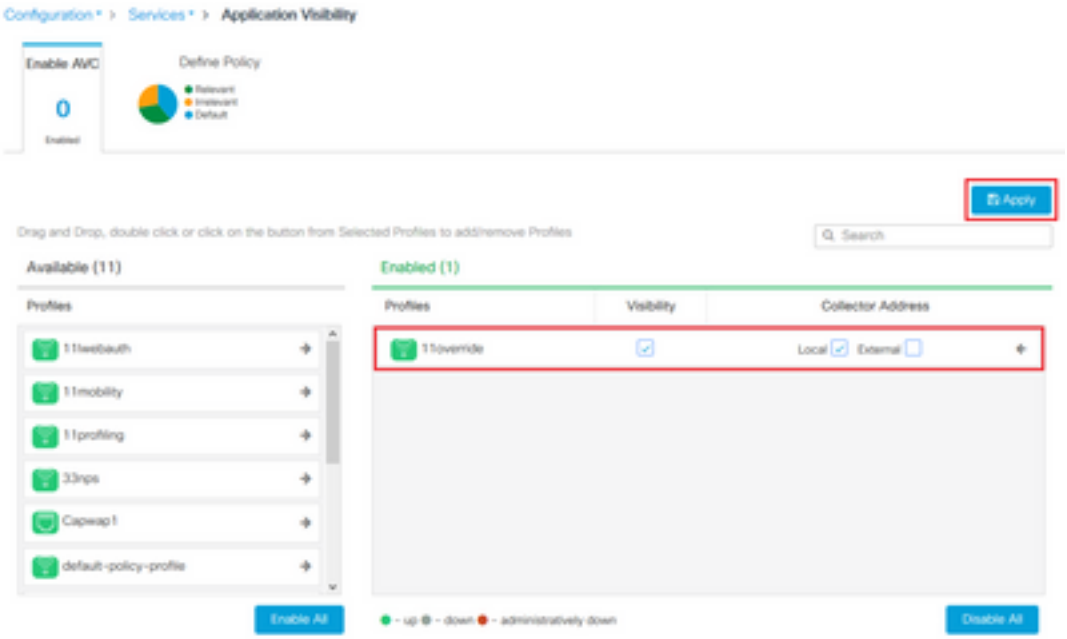
Un altro caso d'uso comune sarebbe quello di specificare i criteri di corrispondenza basati su OUI. Se una distribuzione dispone di un numero elevato di scanner o stampanti dello stesso modello, in genere dispone dello stesso OUI MAC.

Questa opzione può essere utilizzata per applicare un contrassegno DSCP QoS specifico o un ACL:

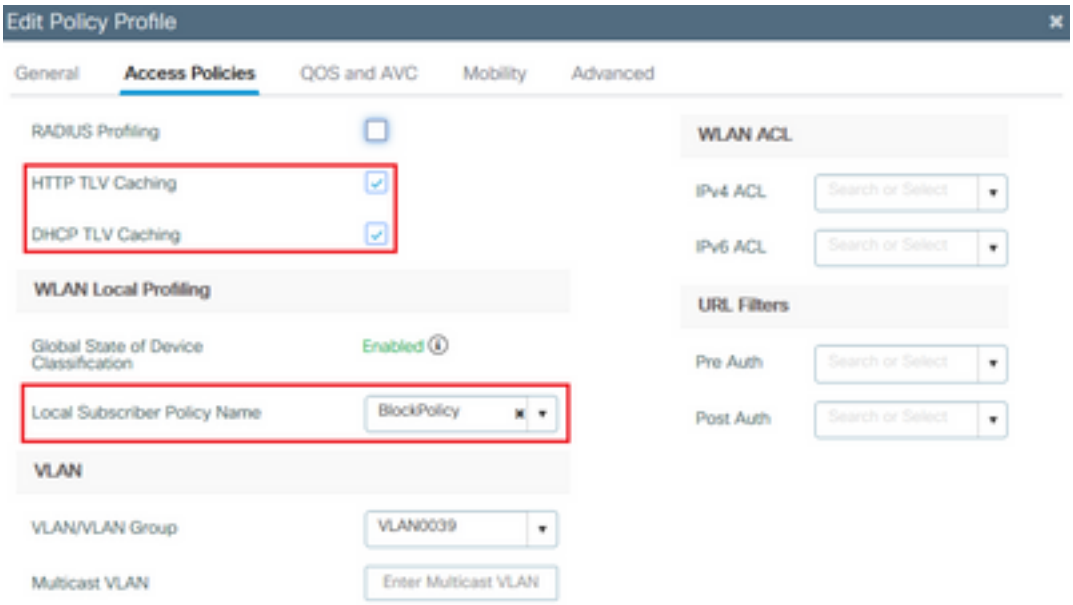


Affinché il WLC sia in grado di riconoscere il traffico su youtube e su facebook, è necessario attivare la visibilità delle applicazioni.

Passare a **Configurazione > Servizi > Visibilità applicazione** eAbilitare la visibilità del profilo delle policy della WLAN:



Verificare che in Profilo criterio la memorizzazione nella cache TLV HTTP, la memorizzazione nella cache TLV DHCP e la classificazione globale dei dispositivi siano abilitate e che Criteri del sottoscrittore locale faccia riferimento alla mappa dei criteri locali creata in uno dei passaggi precedenti:



Dopo la connessione del client, è possibile verificare se la politica locale è stata applicata e verificare se youtube e facebook sono effettivamente bloccati.

L'output del comando show wireless client mac-address [MAC_ADDR] dettagliato contiene:

```
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
```

Profilatura Radius per Advanced Policy Set in Cisco ISE

Se la profilatura RADIUS è abilitata, il WLC inoltra le informazioni di profilatura all'ISE. In base a queste informazioni, è possibile creare regole di autenticazione e autorizzazione avanzate.

In questo documento non viene trattata la configurazione ISE. Per ulteriori informazioni, consultare la Cisco ISE Profiling Design Guide.

Questo flusso di lavoro in genere richiede l'uso di CoA, quindi accertarsi che sia abilitato sul WLC 9800.

Creazione profilo nelle distribuzioni FlexConnect

Autenticazione centrale, switching locale

In questa configurazione, la profilatura locale e RADIUS continua a funzionare esattamente come descritto nei capitoli precedenti. Se il punto di accesso entra in modalità standalone (il punto di accesso perde la connessione al WLC), la profilatura dei dispositivi smette di funzionare e nessun nuovo client è in grado di connettersi.

Autenticazione locale, switching locale

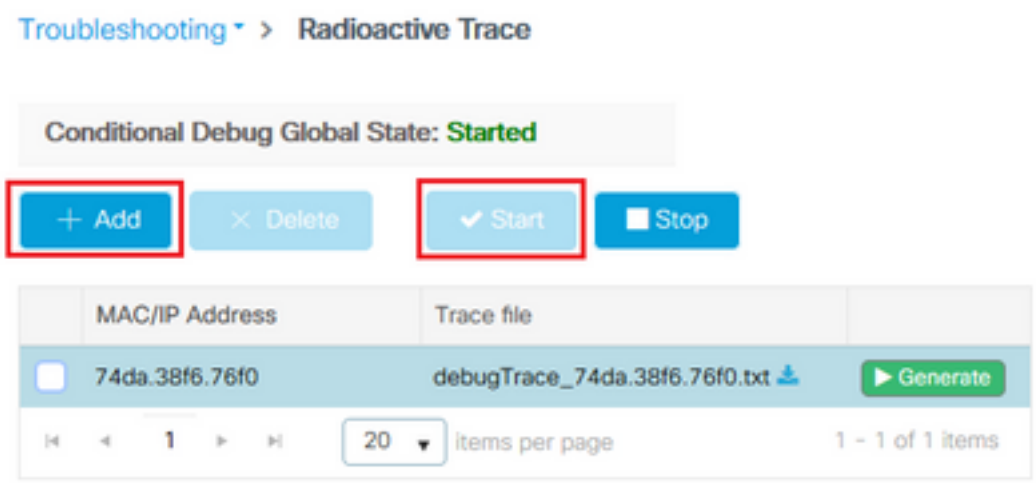
Se l'access point è in modalità connessa (un access point è stato aggiunto al WLC), la profilatura continua a funzionare (l'access point invia una copia dei pacchetti DHCP client al WLC per eseguire il processo di profilatura).

Nonostante il funzionamento della profilatura, poiché l'autenticazione viene eseguita localmente nell'access point, le informazioni di profilatura non possono essere utilizzate per alcuna configurazione di Criteri locali o regole di profilatura RADIUS.

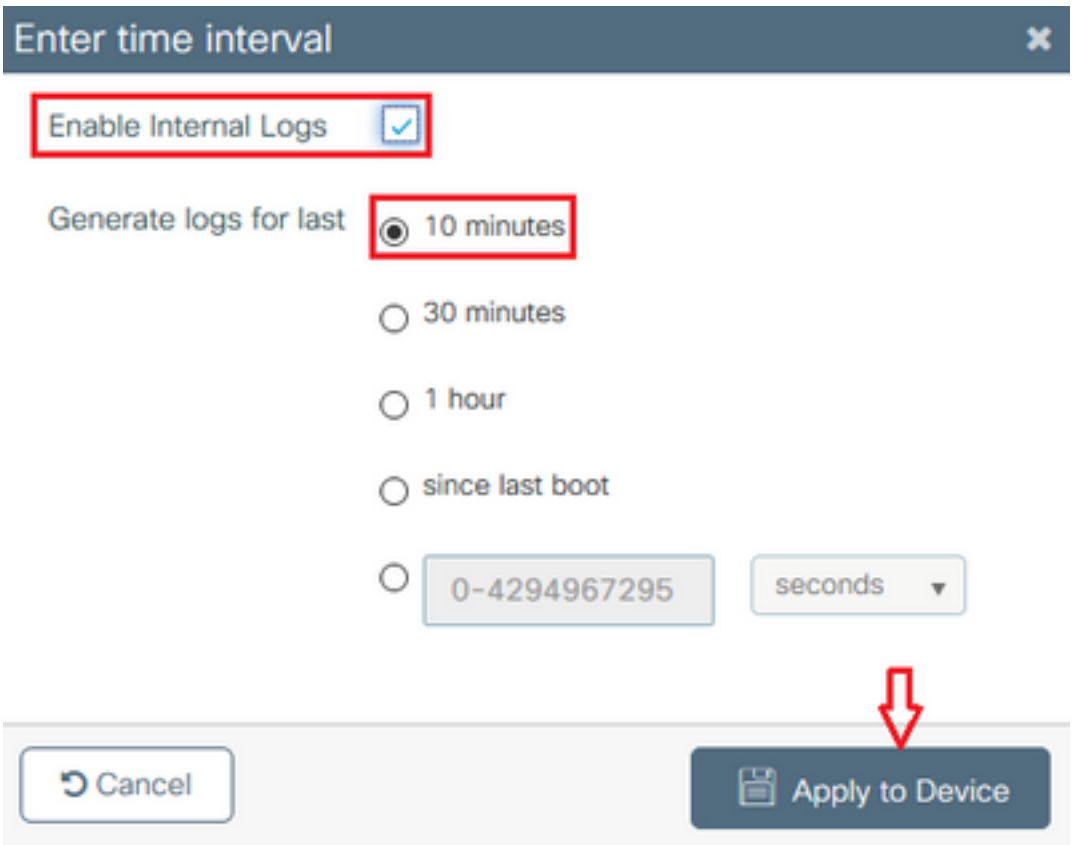
Risoluzione dei problemi

Tracce radioattive

Il modo più semplice per risolvere i problemi relativi ai profili dei client sul WLC è tramite tracce radioattive. Selezionare **Risoluzione dei problemi > Traccia radioattiva**, immettere l'indirizzo MAC della scheda di rete wireless del client e fare clic su Start:



Connettere il client alla rete e attendere che raggiunga lo stato di esecuzione. Arrestare le tracce e fare clic su **Genera**. Accertarsi che i registri interni siano abilitati (questa opzione è disponibile solo nelle versioni 17.1.1 e successive):



Di seguito sono riportati alcuni frammenti della traccia radioattiva:

Il client viene profilato da WLC come 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
```

Memorizzazione nella cache WLC della classificazione del dispositivo:

```
(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: ricerca della classificazione dei dispositivi nella cache in corso:

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

WLC applicazione dei criteri locali in base alla classificazione:

```
(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
```

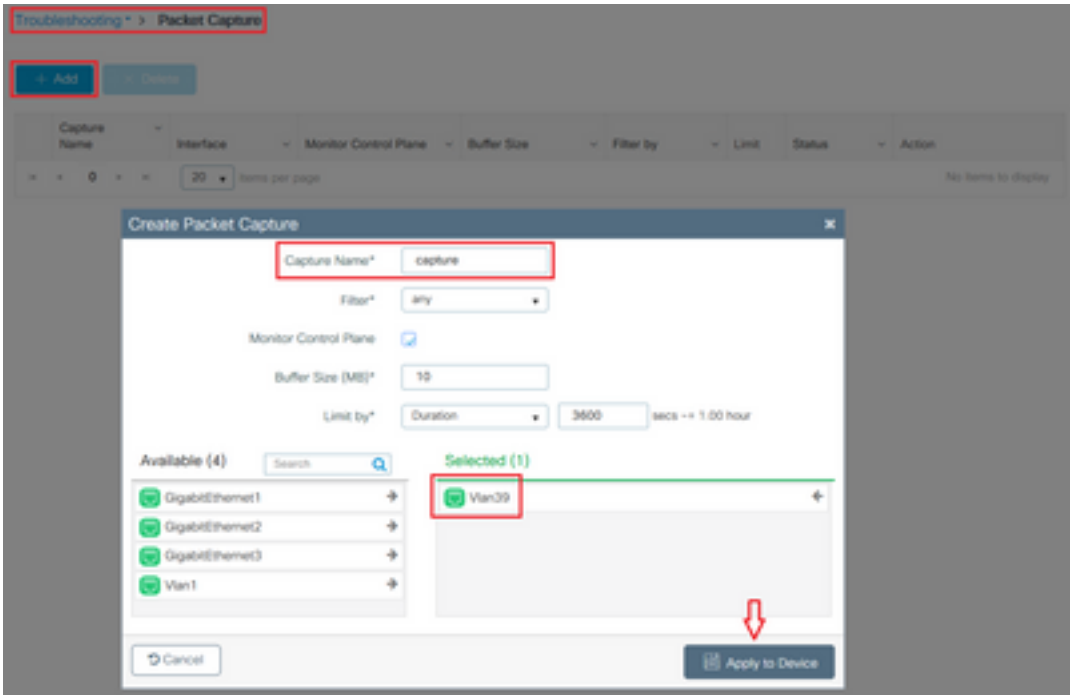
WLC: invio di pacchetti di accounting contenenti gli attributi di profiling DHCP e HTTP:

```
[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
```

Acquisizioni pacchetti

In un'implementazione a commutazione centrale, le acquisizioni dei pacchetti possono essere eseguite sul WLC stesso. Passare a **Risoluzione dei problemi > Acquisizione pacchetto** e creare un nuovo punto di acquisizione su una delle interfacce utilizzate dal client.

Per eseguire l'acquisizione sulla vlan, è necessario disporre di una SVI sulla vlan, altrimenti è possibile acquisirla sulla porta fisica


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

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).