# 融合接入無線控制器(5760/3850/3650)BYOD客戶端自註冊，帶FQDN ACL

## 目錄



## 簡介

本檔案介紹使用基於DNS的存取清單(ACL)、完全限定網域名稱(FQDN)網域清單的組態範例，以在融合存取控制器上的Web驗證/使用者端自帶裝置(BYOD)布建狀態期間允許存取特定網域清單。

## 必要條件

### 需求

本文檔假定您已經知道如何配置基本中央Web身份驗證(CWA)，這只是演示使用FQDN域清單來支援BYOD的一個補充。本文檔末尾引用了CWA和ISE BYOD配置示例。

### 採用元件

本文中的資訊係根據以下軟體和硬體版本：
思科身分識別服務引擎軟體版本1.4

Cisco WLC 5760軟體版本3.7.4

## DNS型ACL流程

身份服務引擎(ISE)返回重定向ACL名稱（用於確定哪些流量將重定向到ISE以及哪些流量不會重定向的ACL名稱）和FQDN域清單名稱（對映到控制器上的FQDN URL清單的ACL名稱，在身份驗證前允許訪問）時，流將如下所示：

1. 無線LAN控制器(WLC)會將capwap負載傳送到存取點(AP)，以啟用URL的DNS窺探。
2. 從客戶端進行DNS查詢的AP監聽。 如果域名與允許的URL匹配，則AP會將請求轉發到DNS伺服器，等待來自DNS伺服器的響應，並分析DNS響應並轉發該響應，僅解析第一個IP地址。如

果域名不匹配，則DNS響應按原樣轉發回客戶端（無需修改）。
3. 如果域名匹配，第一個解析的IP地址將傳送到capwap負載中的WLC。WLC使用以下方法從AP獲取的已解析IP地址隱式更新對映到FQDN域清單的ACL: 解析的IP地址將作為目標地址新增到對映到FQDN域清單的每個ACL規則上。ACL的每個規則從permit到deny顛倒，反之亦然，ACL將應用到客戶端。 **附註**：使用此機制，無法將域清單對映到CWA重定向ACL，因為反向重定向ACL規則將導致將其更改為permit，這意味著流量應重定向到ISE。因此，FQDN域清單將對映到配置部分中單獨的「permit ip any any」ACL。要澄清這一點，假設網路管理員已使用cisco.com url配置了FQDN域清單，並將該域清單對映到以下ACL:

```
ip access-list extended FQDN_ACL
permit ip any any
```

在客戶端請求cisco.com時，AP將域名cisco.com解析為IP地址72.163.4.161並將其傳送到控制器，ACL將被修改為如下所示，並應用於客戶端：

```
ip access-list extended FQDN_ACL
deny ip any host 72.163.4.161
```

4. 當客戶端傳送HTTP「GET」請求時： 如果ACL允許流量，使用者端將重新導向。使用拒絕的IP地址時，將允許http流量。
5. 在客戶端上下載應用並完成調配後，ISE伺服器會將CoA會話終止傳送到WLC。
6. 一旦使用者端從WLC取消驗證，AP將會移除每個使用者端的窺探標誌並停用窺探。

# 設定

### WLC組態

1. 建立重新導向ACL:
此ACL用於定義哪些流量不應重定向到ISE（在ACL中遭到拒絕）以及哪些流量應重定向（在ACL中允許）。

```
ip access-list extended REDIRECT_ACL
deny udp any eq bootps any
deny udp any any eq bootpc
deny udp any eq bootpc any
deny udp any any eq domain
deny udp any eq domain any
deny ip any host 10.48.39.228
deny ip host 10.48.39.228 any
permit tcp any any eq www
permit tcp any any eq 443
```

在此訪問清單中，10.48.39.228是ISE伺服器IP地址。

2. 配置FQDN域清單：此清單包含客戶端在調配或CWA身份驗證之前可以訪問的域名。
```
passthru-domain-list URLS_LIST
match play.google.*.*
match cisco.com
```
3. 使用permit ip any any配置要與URLS_LIST組合的訪問清單：
需要將此ACL對映到FQDN域清單，因為我們必須將實際IP訪問清單應用於客戶端（無法應用獨立FQDN域清單）。

```
ip access-list extended FQDN_ACL
permit ip any any
```

4. 將URLS_LIST域清單對映到FQDN_ACL:

```
access-session passthru-access-group FQDN_ACL passthru-domain-list URLS_LIST
```

5. 配置自註冊CWA SSID:
   此SSID將用於客戶端中央Web身份驗證和客戶端調配，ISE將FQDN_ACL和REDIRECT_ACL應用到此SSID

```
wlan byod 2 byod
 aaa-override
 accounting-list rad-acct
 client vlan VLAN0200
 mac-filtering MACFILTER
 nac
 no security wpa
 no security wpa akm dot1x
 no security wpa wpa2
 no security wpa wpa2 ciphers aes
 no shutdown
```

   在此SSID配置中，**MACFILTER**方法清單是指向ISE radius組的方法清單，**rad-acct**是指向同一ISE radius組的記帳方法清單。

   本示例中使用的方法清單配置摘要：

```
aaa group server radius ISEGroup
 server name ISE1

aaa authorization network MACFILTER group ISEGroup

aaa accounting network rad-acct start-stop group ISEGroup

radius server ISE1
 address ipv4 10.48.39.228 auth-port 1812 acct-port 1813
 key 7 112A1016141D5A5E57

aaa server radius dynamic-author
 client 10.48.39.228 server-key 7 123A0C0411045D5679
 auth-type any
```

## ISE 組態

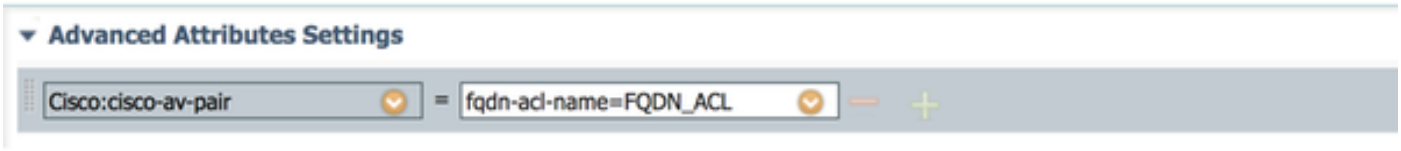
本節假定您熟悉CWA ISE配置部分，ISE配置與以下修改幾乎相同。

無線CWA Mac位址驗證略過(MAB)驗證結果應返回以下屬性以及CWA重新導向URL:

```
cisco-av-pair = fqdn-acl-name=FQDN_ACL
cisco-av-pair = url-redirect-acl=REDIRECT_ACL
```

其中FQDN_ACL是對映到域清單的IP訪問清單的名稱，REDIRECT_ACL是普通CWA重定向訪問清單。

因此，CWA MAB身份驗證結果應配置如下：


# 驗證

要驗證FQDN域清單是否已應用到客戶端，請使用以下命令：

```
show access-session mac <client_mac> details
```

顯示允許的域名的命令輸出示例：

```
5760-2#show access-session mac 60f4.45b2.407d details
            Interface:  Capwap7
               IIF-ID:  0x41BD400000002D
            Wlan SSID:  byod
       AP MAC Address:  f07f.0610.2e10
          MAC Address:  60f4.45b2.407d
         IPv6 Address:  Unknown
         IPv4 Address:  192.168.200.151
               Status:  Authorized
               Domain:  DATA
       Oper host mode:  multi-auth
     Oper control dir:  both
      Session timeout:  N/A
    Common Session ID:  0a30275b58610bdf0000004b
      Acct Session ID:  0x00000005
               Handle:  0x42000013
       Current Policy:  (No Policy)
        Session Flags:  Session Pushed

Server Policies:

             FQDN ACL: FQDN_ACL
         Domain Names: cisco.com play.google.*.*

         URL Redirect:  https://bru-
ise.wlaaan.com:8443/portal/gateway?sessionId=0a30275b58610bdf0000004b&portal=27963fb0-e96e-11e4-
a30a-005056bf01c9&action=cwa&token=fcc0772269e75991be7f1ca238cbb035
     URL Redirect ACL:  REDIRECT_ACL

Method status list: empty
```

# 參考資料

WLC 和 ISE 的中央 Web 驗證的組態範例

BYOD無線基礎設施設計

為Chromebook Onboarding配置ISE 2.1