融合接入无线控制器(5760/3850/3650)BYOD客户端自注册与FQDN ACL

目录

[简介](#)
[先决条件](#)
[要求](#)
[使用的组件](#)
[基于DNS的ACL流程](#)
[配置](#)
[WLC 配置](#)
[ISE配置](#)
[验证](#)
[参考](#)

简介

本文档介绍使用基于DNS的访问列表(ACL)、完全限定域名(FQDN)域列表的配置示例，以允许在融合接入控制器的Web身份验证/客户端自带设备(BYOD)调配状态期间访问特定域列表。

先决条件

要求

本文档假定您已经了解如何配置基本的中央网络身份验证(CWA)，这只是演示如何使用FQDN域列表来促进BYOD的补充。本文档末尾参考了CWA和ISE BYOD配置示例。

使用的组件

本文档中的信息基于以下软件和硬件版本：
思科身份服务引擎软件版本1.4

思科WLC 5760软件版本3.7.4

基于DNS的ACL流程

当身份服务引擎(ISE)返回重定向ACL名称（用于确定要重定向到ISE的流量以及不会重定向的流量的ACL名称）和FQDN域列表名称（映射到控制器上允许访问的FQDN URL列表的ACL名称）时，流将如下：

1. 无线LAN控制器(WLC)将向接入点(AP)发送capwap负载，以启用URL的DNS监听。
2. AP监听客户端的DNS查询。 如果域名与允许的URL匹配，AP会将请求转发到DNS服务器，等待DNS服务器的响应，并解析DNS响应，然后仅使用解析的第一个IP地址转发该响应。如果域

名不匹配，则DNS响应将按原样（不修改）转发回客户端。

3. 如果域名匹配，第一个解析的IP地址将发送到capwap负载中的WLC。WLC使用从AP获取的解析IP地址通过以下方法隐式更新映射到FQDN域列表的ACL: 解析的IP地址将作为目标地址添加到映射到FQDN域列表的ACL的每条规则。ACL的每条规则从允许变为拒绝，反之亦然，然后ACL将应用到客户端。 **注意：**使用此机制，我们无法将域列表映射到CWA重定向ACL，因为反转重定向ACL规则将导致将其更改为允许，这意味着流量应重定向到ISE。因此，FQDN域列表将映射到配置部分中单独的“permit ip any any” ACL。要阐明此点，假设网络管理员已在列表中使用cisco.com url配置了FQDN域列表，并将该域列表映射到以下ACL:

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

当客户端请求cisco.com时，AP将域名cisco.com解析为IP地址72.163.4.161并将其发送到控制器，ACL将修改为如下所示并应用于客户端：

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

4. 当客户端发送HTTP“GET”请求时： 如果ACL允许流量，客户端将被重定向。使用拒绝的IP地址，将允许http流量。
5. 在客户端上下载应用并完成调配后，ISE服务器将CoA会话终止发送到WLC。
6. 从WLC取消对客户端的身份验证后，AP将删除每个客户端的监听标志并禁用监听。

配置

WLC 配置

1. 创建重定向ACL:
   此ACL用于定义哪些流量不应重定向到ISE（在ACL中被拒绝）以及哪些流量应重定向（在ACL中允许）。

```
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
```

   在此访问列表10.48.39.228中是ISE服务器IP地址。

2. 配置FQDN域列表：此列表包含客户端在调配或CWA身份验证之前可以访问的域名。

```
passthru-domain-list URLS_LIST
match play.google.*.*
match cisco.com
```

3. 配置访问列表，使用permit ip any any any与URLS_LIST组合：
   此ACL需要映射到FQDN域列表，因为我们必须将实际IP访问列表应用到客户端（我们无法应用独立FQDN域列表）。

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

4. 将URLS_LIST域列表映射到FQDN_ACL:

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

5. 配置自注册CWA SSID:
   此SSID将用于客户端中心Web身份验证和客户端调配，FQDN_ACL和REDIRECT_ACL将由ISE应用到此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方法列表是指向ISE radius组的方法列表，**rad-acct**是指向同一ISE radius组的记帐方法列表。

   本示例中使用的方法列表配置摘要：

```
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配置

本节假设您熟悉CWA ISE配置部分，ISE配置与以下修改几乎相同。

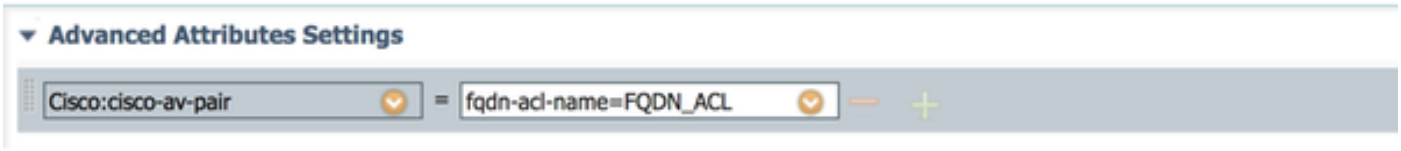
无线CWA Mac地址身份验证绕行(MAB)身份验证结果应返回以下属性以及CWA重定向URL:

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

其中，FQDN_ACL是映射到域列表的IP访问列表的名称，而REDIRECT_ACL是普通CWA重定向访问列表。

因此，CWA MAB身份验证结果应按如下方式配置：





验证

要验证FQDN域列表是否已应用到客户端，请使用以下命令：

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

显示允许域名的命令输出示例：

```
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
```

参考

WLC和ISE上的中央Web身份验证配置示例

BYOD无线基础设施设计

配置ISE 2.1以进行Chromebook登录