有FQDN ACL的聚合的访问无线控制器(5760/3850/3650) BYOD客户端Onboarding

目录

简介

本文描述配置示例为使用DNS基于访问列表(ACL)，完全合格的域名(FQDN)域列表对允许对特定域列表在Web验证/客户端期间带来您Converged访问控制器的自己的设备(BYOD)设置的状态。

先决条件

要求

本文假设，您已经会配置基本中央Web验证(CWA)，这是新增内容展示使用FQDN域列表给faciltate BYOD。CWA和ISE BYOD配置示例被参考在本文结束时。

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

Cisco WLC 5760软件版本3.7.4

DNS根据ACL进程流

在返回重定向ACL名称的身份服务引擎(ISE) (ACL名称曾经确定哪个流量将重定向到ISE，并且哪些不)，并且FQDN域列表名称(被映射对在为访问将允许的控制器的FQDN URL列表在验证前) ACL的名称，流将是象这样：

1. 无线局域网控制器(WLC)将发送capwap有效负载对接入点(AP)启用监听为URL的DNS。
2. AP为从客户端的DNS查询监听。 如果域名匹配允许URL， AP将寄请求给DNS服务器，将等待从DNS服务器的答复，并且请解析DNS答复并且转发它用被解决的仅第一个IP地址。如果域

名不配比，则DNS答复转发和(没有修改)回到客户端。

3. 万一域名配比，第一个解决的IP地址将发送对在capwap有效负载的WLC。WLC隐含地更新ACL被映射对使用以下方法，从AP获得的FQDN域列表用解决的IP地址： 解决的IP地址将被添加作为在被映射的ACL每个规则的一目的地址对FQDN域列表。ACL获得每个规则被倒转的从permit拒绝反之亦然ACL然后得到应用给客户端。 **Note**:使用此机制我们不能映射域列表到CWA重定向ACL，因为倒转重定向ACL规则将结果到意味着的更改他们允许应该重定向流量到ISE。Therfore FQDN域列表在配置零件中将被映射对单独的“permit ip any any” ACL。要澄清该点，假设网络admin配置与cisco.com URL的FQDN域列表在列表，并且映射该域列表对以下ACL ：

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

在请求cisco.com的客户端， AP解决域名cisco.com对IP地址72.163.4.161并且发送它到控制器，将修改ACL是作为下面并且得到应用给客户端：

```
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： 万一ACL允许流量，客户端将重新定向。用已拒绝IP地址HTTP数据流将允许。
5. 一旦App在客户端下载，并且供应完成， ISE服务器发送CoA会话终止对WLC。
6. 一旦客户端是从WLC的已取消验证， AP将删除监听的标志每个客户端并且禁用监听。

配置

WLC 配置

1. 创建重定向ACL ：
   此ACL用于定义不应该重定向应该重定向哪个流量到ISE (拒绝在ACL)，并且哪个流量(允许在ACL)。

```
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
```

   在此访问列表中10.48.39.228是ISE服务器IP地址。

2. 配置FQDN域列表：此列表包含客户端能在设置或CWA验证前访问的域名。

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

3. 配置与与URLS_LIST将一起的permit ip any any的一访问列表：
   此ACL是需要的被映射到FQDN域列表，因为我们必须应用一实际IP访问控制列表对客户端(我

们不能运用独立FQDN域列表)。

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

4. 映射URLS_LIST域列表对FQDN_ACL ：

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

5. 配置Onboarding CWA SSID ：
   此SSID将使用客户端中央Web验证，并且客户端供应、FQDN_ACL和REDIRECT_ACL将应用对此SSID由ISE

```
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**MACFILTER**方法列表中是指向ISE radius组的方法列表，并且rad**账户**是指向同一ISE radius组的会计方法列表。

   用于此示例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

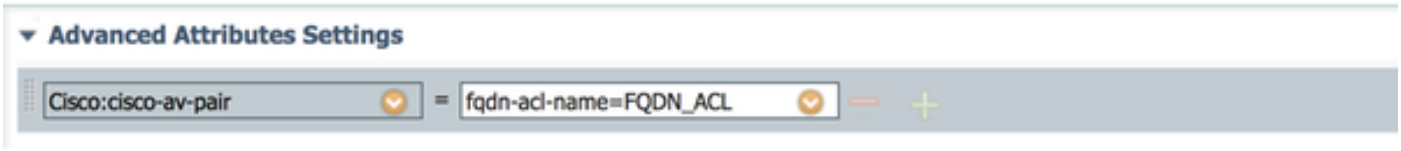
此部分假设，您是与CWA ISE配置零件的熟悉的， ISE配置接近是相同的与以下修改。

无线CWA MAC地址验证旁路(MAB)验证结果应该与CWA重定向URL一起返回以下属性：

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

那里FQDN_ACL被映射对域列表和REDIRECT_ACL IP访问控制列表的名称是正常CWA重定向访问列表。

Thefore CWA MAB应该配置验证结果作为如下：



验证

验证FQDN域列表应用对客户端使用在命令之下：

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

显示允许的域名的命令输出的示例：

```
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

在WLC和ISE配置示例的中央Web验证

BYOD无线结构设计

配置Chromebook的Onboarding ISE 2.1