Converged Access Wireless Controller (5760/3850/3650) BYOD client Onboarding with FQDN ACLs

Contents

Introduction

This document describes a configuration example for the use of DNS Based access lists (ACLs), Fully Qualified Domain Name (FQDN) domain list to allow access to specific domain lists during Web-authentication/Client Bring Your Own Device (BYOD) provisioning state on Converged Access Controllers.

Prerequisites

Requirements

This document assumes that you already know how to configure basic Central Web Authentication (CWA), this is just an addition to demonstrate the use of FQDN domain lists to faciltate BYOD. CWA and ISE BYOD configuration examples are referenced at the end of this document.

Components Used

The information in this document is based on these software and hardware versions:
Cisco Identity Services Engine Software Release 1.4

Cisco WLC 5760 Software Release 3.7.4

DNS Based ACL Process Flow

Upon Identity Services Engine (ISE) returning the redirect ACL name (name of ACL used to determine which traffic is to be redirected to ISE and which will not) and FQDN domain list name (name of ACL that is mapped to FQDN URL list on the controller to be allowed for access before

authentication), the flow will be as such:

1. Wireless LAN Controller (WLC) will send capwap payload to access point (AP) to enable DNS snooping for the URLs.
2. AP snoops for the DNS query from the client. If the domain name matches the allowed URL, AP will forward the request to the DNS server, will wait for the response from the DNS server and will parse the DNS response and forward it with only the first IP address resolved.If the domain name does not match, then the DNS response is forwarded as is (without modification) back to the client.
3. In case the domain name matches, the first resolved IP address will be sent to the WLC in the capwap payload. WLC implicitly updates the ACL mapped to the FQDN domain list with the resolved IP address it got from the AP using the following approach: The resolved IP address will be added as a destination address on each rule of ACL mapped to the FQDN domain list.Each rule of ACL gets reversed from permit to deny and vice versa then the ACL will gets applied to the client. **Note**: With this mechanism we can't map the domain list to CWA redirect ACL, because reversing the redirect ACL rules will result into changing them to permit which means that traffic should be redirected to ISE. Therfore FQDN domain list will be mapped to a seperate "permit ip any any" ACL in the configuration part.To clarify that point, assume the network admin has configured FQDN domain list with cisco.com url in the list, and mapped that domain list to the following ACL:
   ```
   ip access-list extended FQDN_ACL
   permit ip any any
   ```
   Upon client requesting cisco.com, AP resolves domain name cisco.com to IP address 72.163.4.161 and send it to the contoller, the ACL will be modified to be as below and gets applied to the client:
   ```
   ip access-list extended FQDN_ACL
   deny ip any host 72.163.4.161
   ```
4. When client sends HTTP "GET" request: The client will get redirected in case the ACL permits the traffic.With denied IP address the http traffic will be allowed.
5. Once the App is downloaded on the client and provisioning is complete, the ISE server sends CoA session terminate to the WLC.
6. Once the client is de-authenticated from the WLC, the AP will remove the flag for snooping per client and disable snooping.

Configure

WLC Configuration

1. Create redirect ACL:
   This ACL is used to define which traffic shouldn't be redirected to ISE (denied in the ACL) and which traffic should be redirected (Permitted in the 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
```
In this access list 10.48.39.228 is the ISE server IP address.

2. Configure the FQDN domain list:This list contains the domain names that client can access before provisioning or CWA authentication.
```
passthru-domain-list URLS_LIST
match play.google.*.*
match cisco.com
```
3. Configure an access list with permit ip any any to be combined with the URLS_LIST:
   This ACL is needed to be mapped to the FQDN domain list because we must apply an actual IP access-list to the client (we can't apply standalone FQDN domain list).
```
ip access-list extended FQDN_ACL
permit ip any any
```
4. Map the URLS_LIST domain list to the FQDN_ACL:
```
access-session passthru-access-group FQDN_ACL passthru-domain-list URLS_LIST
```
5. Configure the Onboarding CWA SSID:
   This SSID will be used for client central web authentication and client provisioning , the FQDN_ACL and REDIRECT_ACL will be applied to this SSID by 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
```
In this SSID configuration **MACFILTER** method list is the method list pointing to ISE radius group and **rad-acct** is the accounting method list that points to the same ISE radius group.

   Summary of method list configuration used in this example:
```
aaa group server radius ISEGroup
 server name ISE1aaa authorization network MACFILTER group ISEGroup aaa accounting network
rad-acct start-stop group ISEGroupradius server ISE1
 address ipv4 10.48.39.228 auth-port 1812 acct-port 1813
 key 7 112A1016141D5A5E57aaa server radius dynamic-author
 client 10.48.39.228 server-key 7 123A0C0411045D5679
 auth-type any
```

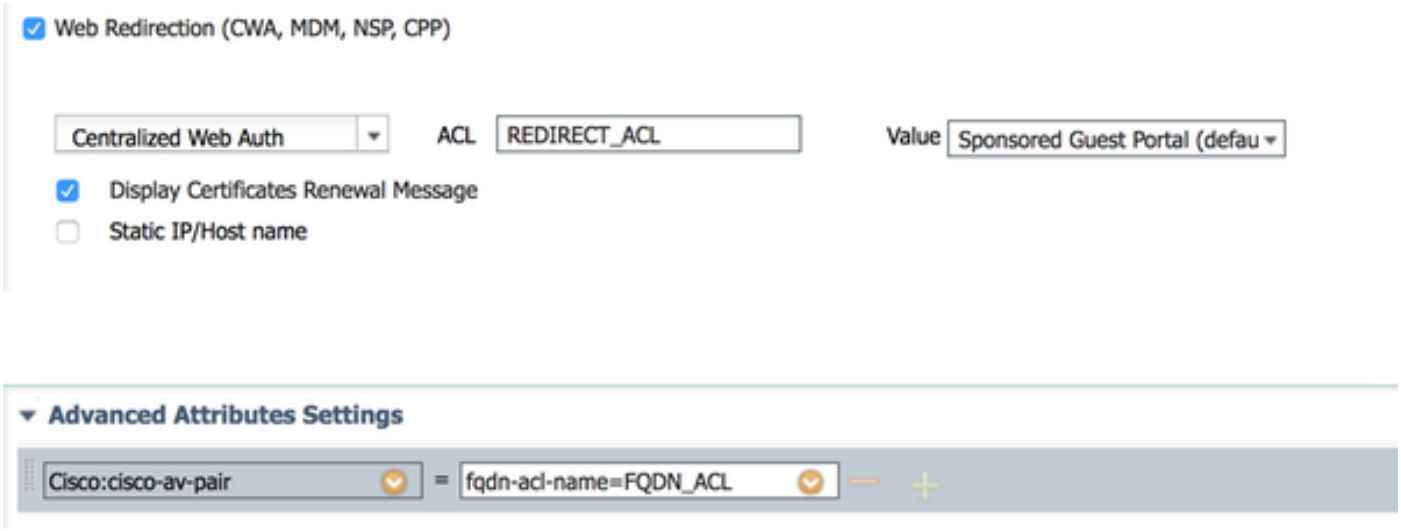
ISE Configuration

This section assumes that you are familar with CWA ISE configuration part, ISE configuration is nearly the same with the following modifications.

Wireless CWA Mac address Authentication Bypass (MAB) authentication result should return the following attributes along with the CWA redirect URL:

```
cisco-av-pair = fqdn-acl-name=FQDN_ACL
cisco-av-pair = url-redirect-acl=REDIRECT_ACL
```
Where FQDN_ACL is the name of the IP access list that is mapped to the domain list and REDIRECT_ACL is the normal CWA redirect access list.

Thefore CWA MAB authentication result should be configured as in below:



Verify

To verify that FQDN domain list is applied to the client use below command:

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

Example of the command outputs showing permitted domain names:

```
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
```

References

[Central Web Authentication on the WLC and ISE Configuration Example]

BYOD Wireless Infrastructure Design

Configure ISE 2.1 for Chromebook Onboarding