Client convergé Onboarding du contrôleur sans-fil d'Access (5760/3850/3650) BYOD avec FQDN ACLs

Contenu

Introduction

Ce document décrit un exemple de configuration pour l'usage des Listes d'accès basées par DN (ACLs), domain list du nom de domaine complet (FQDN) de permettre l'accès aux domains lists spécifiques pendant l'état d'authentification Web/de ravitaillement Bring Your Own Device de client (BYOD) sur des contrôleurs Converged Access.

Conditions préalables

Conditions requises

Ce document suppose que vous savez déjà configurer l'authentification Web centrale de base (CWA), ceci est juste un ajout pour expliquer l'utilisation des domains lists FQDN au faciltate BYOD. Des exemples de configuration CWA et ISE BYOD sont mis en référence à la fin de ce document.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :
Version 1.4 de Cisco Identity Services Engine Software

Version de logiciel 3.7.4 du Cisco WLC 5760

Les DN ont basé l'écoulement de processus d'ACL

Sur le Cisco Identity Services Engine (ISE) renvoyant le nom du nom d'ACL de réorientation (nom

d'ACL utilisé pour déterminer quel trafic doit être réorienté à ISE et ce qui pas) et du domain list FQDN (le nom de l'ACL qui est tracé à la liste URL FQDN sur le contrôleur à tenir compte de l'accès avant l'authentification), l'écoulement sera en tant que tels :

1. Le contrôleur LAN Sans fil (WLC) enverra la charge utile de capwap au Point d'accès (AP) pour activer des DN pillant pour l'URLs.
2. AP pille pour la requête DNS du client. Si le nom de domaine apparie l'URL permis, AP fera suivre à la demande le serveur DNS, attendra la réponse du serveur DNS et analysera la réponse de DN et l'expédiera avec seulement la première adresse IP résolue.Si le nom de domaine ne s'assortit pas, alors la réponse de DN est expédiée comme est (sans modification) de nouveau au client.
3. Au cas où le nom de domaine s'assortirait, la première adresse IP résolue sera envoyée au WLC dans la charge utile de capwap. WLC met à jour implicitement l'ACL tracé au domain list FQDN avec l'adresse IP résolue qu'il a obtenue d'AP utilisant l'approche suivante : L'adresse IP résolue sera ajoutée comme adresse de destination sur chaque règle d'ACL tracée au domain list FQDN.Chaque règle d'ACL obtient renversé de l'autorisation de refuser et vice versa alors l'ACL veulent obtient appliqué au client. **Note**: Avec ce mécanisme nous ne pouvons pas tracer le domain list à CWA réorientons l'ACL, parce que renverser les règles d'ACL de réorientation résultera dans les changer pour laisser qui signifie que le trafic devrait être réorienté à ISE. Par conséquent le domain list FQDN sera tracé à un « IP distinct d'autorisation tout n'importe quel » ACL dans la cloison de configuration.Pour clarifier ce point, supposez que l'admin de réseau a configuré le domain list FQDN avec l'URL de cisco.com dans la liste, et a tracé ce domain list à l'ACL suivant :

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

   Sur le client demandant cisco.com, le nom de domaine cisco.com de résolutions AP à l'adresse IP 72.163.4.161 et l'envoient au contoller, l'ACL sera modifié pour être en tant que ci-dessous et obtient appliqué au client :

   ```
   ip access-list extended FQDN_ACL
   deny ip any host 72.163.4.161
   ```
4. Quand le client envoie le HTTP « OBTENEZ » la demande : Le client obtiendra réorienté au cas où l'ACL permettrait le trafic.Avec l'adresse IP refusée on permettra le trafic http.
5. Une fois que l'app est téléchargé sur le client et le ravitaillement est complet, le serveur ISE envoie la session CoA se terminent au WLC.
6. Une fois que le client De-est authentifié du WLC, AP retirera l'indicateur pour piller par client et désactivera piller.

Configurez

[Configuration WLC]

1. Create réorientent l'ACL :
   Cet ACL est utilisé pour définir que le trafic ne devrait pas être réorienté à ISE (refusé dans

l'ACL) et que le trafic devrait être réorienté (autorisé dans l'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
```

Dans cette liste d'accès 10.48.39.228 est l'adresse IP du serveur ISE.

2. Configurez le domain list FQDN :Cette liste contient les noms de domaine que le client peut accéder à avant ravitaillement ou authentification CWA.
```
passthru-domain-list URLS_LIST
match play.google.*.*
match cisco.com
```
3. Configurez une liste d'accès avec l'IP d'autorisation tout être combiné avec l'URLS_LIST : Cet ACL est nécessaire pour être tracé au domain list FQDN parce que nous devons nous appliquer un ip access-list réel au client (nous ne pouvons pas appliquer le domain list autonome FQDN).

```
ip access-list extended FQDN_ACL
permit ip any any
```
4. Tracez le domain list URLS_LIST au FQDN_ACL :

```
access-session passthru-access-group FQDN_ACL passthru-domain-list URLS_LIST
```
5. Configurez l'Onboarding CWA SSID :
Ce SSID sera utilisé pour l'authentification Web centrale de client et le ravitaillement de client, le FQDN_ACL et REDIRECT_ACL seront appliqués à ce SSID par 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
```

Dans cette méthode de la configuration **MACFILTER** SSID la liste est la liste de méthode indiquant le groupe de rayon ISE et **rad-acct** est la liste d'accounting method ces points au même groupe de rayon ISE.

Résumé de la configuration de liste de méthode utilisée dans cet exemple :

```
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
```

Configuration ISE

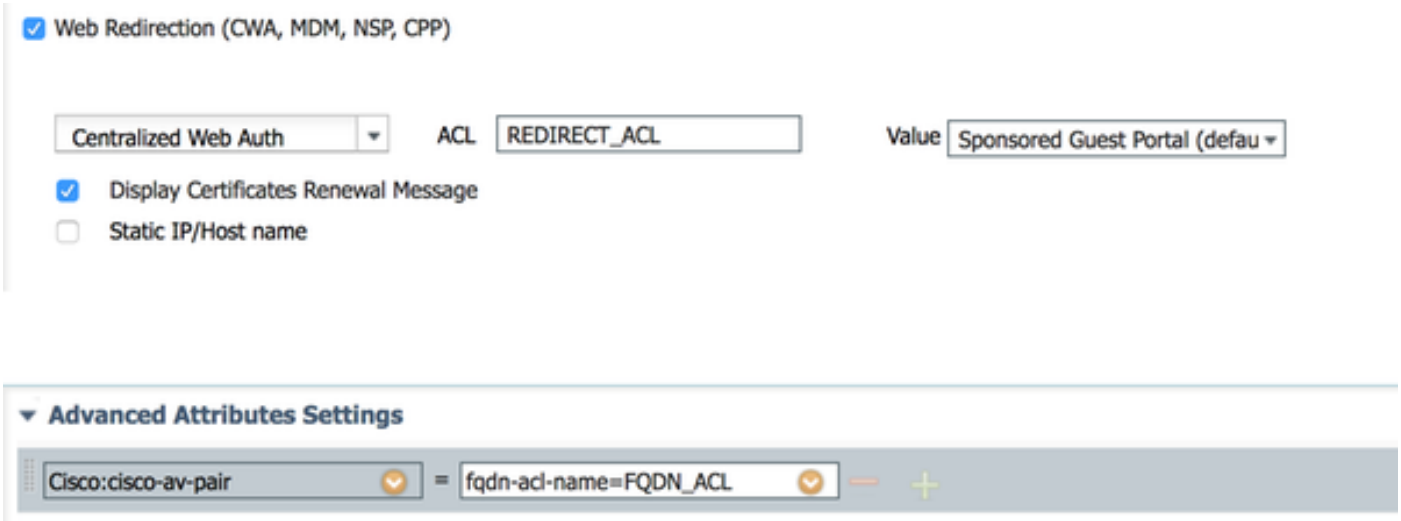
Cette section suppose que vous êtes au courant de la pièce de configuration CWA ISE, configuration ISE est presque identique avec les modifications suivantes.

Le résultat Sans fil d'authentification de contournement d'authentification de MAC address CWA (MAB) devrait renvoyer les attributs suivants avec le CWA réorientent l'URL :

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

Là où FQDN_ACL est le nom de la liste d'accès IP qui est tracé au domain list et au REDIRECT_ACL est le CWA normal réorientent la liste d'accès.

Le résultat d'authentification de MAB de Thefore CWA devrait être configuré en tant que dedans ci-dessous :



Vérifiez

Pour vérifier que le domain list FQDN est appliqué à la commande ci-dessous d'utilisation de client :

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

Exemple des sorties de commande affichant des noms de domaine permis :

```
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
```

Références

[Authentification Web centrale exemple sur WLC et ISE configuration]

[Conception Sans fil d'infrastructure BYOD]

[Configurez ISE 2.1 pour Chromebook Onboarding]