Intégration du client BYOD Converged Access Wireless Controller (5760/3850/3650) avec ACL FQDN

Contenu

Introduction

Ce document décrit un exemple de configuration pour l'utilisation de listes de contrôle d'accès DNS (ACL), de listes de domaine FQDN (Fully Qualified Domain Name) pour autoriser l'accès à des listes de domaines spécifiques pendant l'état d'approvisionnement BYOD (Bring Your Own Device) de l'authentification Web/Client sur les contrôleurs d'accès convergents.

Conditions préalables

Conditions requises

Ce document suppose que vous savez déjà configurer l'authentification Web centralisée de base (CWA). Il s'agit d'un ajout qui démontre l'utilisation de listes de domaines FQDN pour faciliter le BYOD. Les exemples de configuration du BYOD CWA et ISE sont référencés à la fin de ce document.

Components Used

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

Logiciel Cisco WLC 5760 version 3.7.4

Flux de processus ACL basé sur DNS

Lorsque ISE (Identity Services Engine) retourne le nom de la liste de contrôle d'accès de

redirection (nom de la liste de contrôle d'accès utilisée pour déterminer le trafic à rediriger vers ISE et ceux qui ne le seront pas) et le nom de la liste de domaine FQDN (nom de la liste de contrôle d'accès mappée à la liste d'URL FQDN sur le contrôleur à autoriser l'accès avant authentification), le flux sera tel que :

1. Le contrôleur de réseau local sans fil (WLC) enverra des données utiles capwap au point d'accès (AP) pour activer la surveillance DNS pour les URL.
2. AP effectue des recherches pour la requête DNS du client. Si le nom de domaine correspond à l'URL autorisée, le point d'accès transfère la requête au serveur DNS, attend la réponse du serveur DNS et analyse la réponse DNS et la transmet uniquement avec la première adresse IP résolue.Si le nom de domaine ne correspond pas, alors la réponse DNS est transférée telle quelle (sans modification) au client.
3. Dans le cas où le nom de domaine correspond, la première adresse IP résolue sera envoyée au WLC dans la charge utile du paquet capwap. WLC met implicitement à jour la liste de contrôle d'accès mappée à la liste de domaines FQDN avec l'adresse IP résolue qu'il a obtenue de l'AP en utilisant l'approche suivante : L'adresse IP résolue sera ajoutée en tant qu'adresse de destination sur chaque règle de liste de contrôle d'accès mappée à la liste de domaines FQDN.Chaque règle de la liste de contrôle d'accès est inversée de permit à deny et vice versa, puis la liste de contrôle d'accès est appliquée au client. **Note**: Avec ce mécanisme, nous ne pouvons pas mapper la liste de domaines à la liste de contrôle d'accès de redirection CWA, car si vous inversez les règles de la liste de contrôle d'accès de redirection, vous les modifierez pour autoriser, ce qui signifie que le trafic doit être redirigé vers ISE. Par conséquent, la liste de domaines FQDN sera mappée à une liste de contrôle d'accès permit ip any any distincte dans la partie de configuration.Pour clarifier ce point, supposons que l'administrateur réseau a configuré la liste de domaines FQDN avec l'url cisco.com dans la liste, et mappé cette liste de domaines à la liste de contrôle d'accès suivante :

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

   Lorsque le client demande cisco.com, le point d'accès résout le nom de domaine cisco.com en adresse IP 72.163.4.161 et l'envoie au contrôleur, la liste de contrôle d'accès sera modifiée pour être la suivante et sera appliquée au client :

   ```
   ip access-list extended FQDN_ACL
   deny ip any host 72.163.4.161
   ```
4. Lorsque le client envoie une requête HTTP « GET » : Le client sera redirigé au cas où la liste de contrôle d'accès autoriserait le trafic.Avec une adresse IP refusée, le trafic http est autorisé.
5. Une fois l'application téléchargée sur le client et le provisionnement terminé, le serveur ISE envoie une session CoA se terminer au WLC.
6. Une fois que le client est déauthentifié du WLC, l'AP supprime l'indicateur pour la surveillance par client et désactive la surveillance.

Configuration

Configuration WLC

1. Créer une liste de contrôle d'accès de redirection :
   Cette liste de contrôle d’accès est utilisée pour définir le trafic qui ne doit pas être redirigé vers ISE (refusé dans la liste de contrôle d’accès) et le trafic qui doit être redirigé (autorisé dans la liste de contrôle d’accès).

   ```
   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 correspond à l’adresse IP du serveur ISE.

2. Configurez la liste de domaines FQDN :Cette liste contient les noms de domaine auxquels le client peut accéder avant le provisionnement ou l'authentification CWA.
   ```
   passthru-domain-list URLS_LIST
   match play.google.*.*
   match cisco.com
   ```
3. Configurez une liste d'accès avec permit ip any any à combiner avec URLS_LIST :
   Cette liste de contrôle d’accès doit être mappée à la liste de domaines FQDN car nous devons appliquer une liste d’accès IP réelle au client (nous ne pouvons pas appliquer la liste de domaines FQDN autonome).

   ```
   ip access-list extended FQDN_ACL
   permit ip any any
   ```
4. Mappez la liste de domaines URLS_LIST à la liste de contrôle d'accès FQDN_ACL :

   ```
   access-session passthru-access-group FQDN_ACL passthru-domain-list URLS_LIST
   ```
5. Configurez le SSID d'intégration CWA :
   Ce SSID sera utilisé pour l'authentification Web centralisée du client et le provisionnement du client , 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 liste de méthodes **MACFILTER de** configuration SSID est la liste de méthodes pointant vers le groupe de rayons ISE et **rad-acct** est la liste de méthodes comptables pointant vers le même groupe de rayons ISE.

   Résumé de la configuration de la liste de méthodes 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

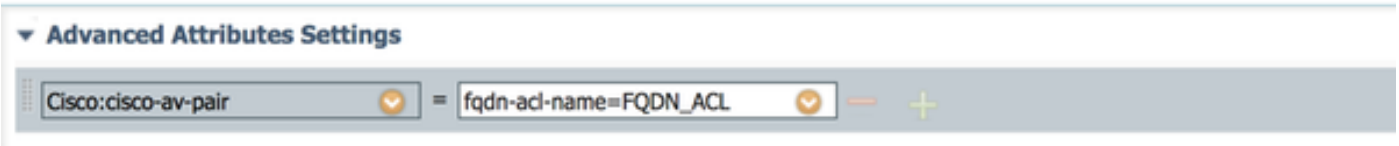
Cette section suppose que vous êtes familier avec la partie de configuration ISE CWA, la configuration ISE est presque identique avec les modifications suivantes.

Le résultat de l'authentification MAB (Authentication Bypass) d'adresse MAC sans fil CWA doit renvoyer les attributs suivants avec l'URL de redirection CWA :

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

Où FQDN_ACL est le nom de la liste d'accès IP mappée à la liste de domaines et REDIRECT_ACL est la liste d'accès de redirection CWA normale.

Par conséquent, le résultat de l'authentification MAB CWA doit être configuré comme suit :



Vérification

Pour vérifier que la liste de domaines FQDN est appliquée au client, utilisez la commande ci-dessous :

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

Exemple de sortie de commande montrant les noms de domaine autorisés :

```
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

[Exemple de configuration de l'authentification Web centralisée sur le WLC et ISE]

[Conception de l'infrastructure sans fil BYOD]

[Configurer ISE 2.1 pour l'intégration de Chromebook]