Geconvergeerde access draadloze controller (5760/3850/3650) BYOD client-instapend met FQDN ACL's

Inhoud

Inleiding

Dit document beschrijft een configuratievoorbeeld voor het gebruik van DNS-gebaseerde toegangslijsten (ACL's), Full Qualified Domain Name (FQDN)-domeinlijst om toegang tot specifieke domeinlijsten toe te staan tijdens Web-authenticatie/Client Bring Your Ewn Devices (BYOD) in Converged Access Controllers.

Voorwaarden

Vereisten

Dit document gaat ervan uit dat u al weet hoe u basisverificatie van het Centrale Web (CWA) moet configureren, dit is slechts een toevoeging om het gebruik van FQDN-domeinlijsten aan te tonen om BYOD te faciliteren. CWA en ISE BYOD configuratievoorbeelden worden aan het eind van dit document van toepassing verklaard.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:
Cisco Identity Services Engine softwarerelease 12.4

Cisco WLC 5760 softwarerelease 3.7.4

DNS-gebaseerde ACL-processtroom

Op het moment dat Identity Services Engine (ISE) teruggeeft, de naam van ACL-omleiding (naam van ACL die wordt gebruikt om te bepalen welk verkeer naar ISE zal worden omgeleid en welke

niet) en de naam van de FQDN-domeinlijst (naam van ACL die in kaart is gebracht in de lijst van FQDN URL op de controller die voor toegang vóór verificatie is toegestaan), zal de stroom als volgt zijn:

1. Draadloze LAN-controller (WLC) zal capwap payload naar access point (AP) verzenden om DNS-sneeuwen voor de URL's mogelijk te maken.
2. AP snoops voor de DNS query van de client. Als de domeinnaam overeenkomt met de toegestane URL, zal AP het verzoek doorsturen naar de DNS-server, wachten op de reactie van de DNS-server en zullen de DNS-respons worden beëindigd en alleen het eerste IP-adres worden doorgestuurd.Als de domeinnaam niet overeenkomt, wordt de DNS-respons doorgestuurd zoals (zonder wijziging) naar de client.
3. Heeft de domeinnaam gelijk, dan wordt het eerste opgeloste IP-adres naar de WLC verzonden in de opnamelading. WLC werkt impliciet de ACL bij die aan de FQDN-domeinlijst is toegewezen met het opgeloste IP-adres dat het van AP kreeg door gebruik van de volgende benadering: Het opgeloste IP-adres wordt als bestemmingsadres op elke regel van ACL toegevoegd die aan de FQDN-domeinlijst is toegewezen.Elke regel van ACL wordt teruggedraaid van vergunning om te ontkennen en omgekeerd wordt ACL toegepast op de client. Opmerking: Met dit mechanisme kunnen we de domeinlijst niet aan CWA om ACL te richten in kaart brengen, omdat het omkeren van de omleiding ACL regels in het veranderen van hen zal resulteren om toe te staan wat betekent dat het verkeer naar ISE moet worden omgeleid. Daarom zal de FQDN-domeinlijst in kaart worden gebracht aan een afzonderlijke "vergunning ip elk"ACL in het configuratiegedeelte.Om dat punt te verduidelijken, neem aan dat de netwerkbeheerder FQDN-domeinlijst met cisco.com url in de lijst heeft ingesteld en heeft die domeinlijst aan de volgende ACL in kaart gebracht:

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

   Op client met verzoek van cisco.com lost AP domeinnaam cisco.com op naar IP-adres 72.163.4.161 en stuurt het naar de controller, zal ACL worden gewijzigd om zoals hieronder te zijn en wordt toegepast op de client:

   ```
   ip access-list extended FQDN_ACL
   deny ip any host 72.163.4.161
   ```
4. Wanneer client HTTP "Get"-verzoek verstuurt: De client wordt opnieuw gericht voor het geval dat ACL het verkeer toestaat.Met ontkend IP adres is het http verkeer toegestaan.
5. Nadat de App op de client is gedownload en de provisioning is voltooid, verstuurt de ISE-server CoA sessie afgesloten naar de WLC.
6. Zodra de client is gedecodeerd van de WLC, verwijdert AP de vlag voor snooping per client en schakelt u het snooping uit.

Configureren

WLC-configuratie

1. ACL-richting maken

Dit ACL wordt gebruikt om te definiëren welke verkeer niet opnieuw naar ISE (ontkend in ACL) moet worden gericht en welke verkeer opnieuw gericht (toegestaan in ACL) moet zijn.

```
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 deze toegangslijst is 10.48.39.228 het IP-adres van de ISE-server.

2. Configuratie van de FQDN-domeinlijst:Deze lijst bevat de domeinnamen waartoe de client toegang heeft voordat voorzieningen worden getroffen of CWA-verificatie.
```
passthru-domain-list URLS_LIST
match play.google.*.*
match cisco.com
```
3. Configuratie van een toegangslijst met vergunning ip elke om met URLS_LIST te worden gecombineerd:
Dit ACL moet aan de FQDN-domeinlijst worden gekoppeld omdat we een eigenlijke IP-toegangslijst naar de client moeten toepassen (we kunnen geen standalone FQDN-domeinlijst toepassen).

```
ip access-list extended FQDN_ACL
permit ip any any
```
4. Stel de domeinlijst URLS_LIST in op de FQDN_ACL:

```
access-session passthru-access-group FQDN_ACL passthru-domain-list URLS_LIST
```
5. Configuratie van de Onboarding CWA SSID:
Deze SSID zal worden gebruikt voor client-centrale web verificatie en clientprovisioning, FQDN_ACL en REDIRECT_ACL zullen door ISE op deze SSID worden toegepast

```
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 deze lijst van de **MACFILTER**-configuratiemethoden van SSID is de methodelijst die wijst op ISE-Straalgroep en **rad-act** is de boekhoudingsmethodelijst die naar dezelfde ISE-Straalgroep wijst.

Samenvatting van de in dit voorbeeld gebruikte methodelijstconfiguratie:

```
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-configuratie

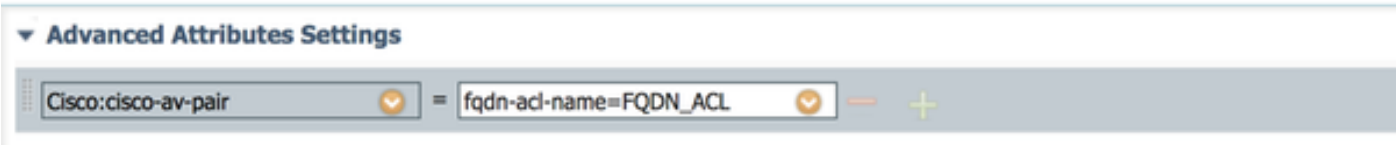
In dit gedeelte wordt ervan uitgegaan dat u bekend bent met het CWA ISE-configuratieonderdeel. De ISE-configuratie is vrijwel gelijk met de volgende wijzigingen.

Draadloos CWA Mac Address Authentication Bypass (MAB)-verificatieresultaat moet samen met de CWA redirect URL de volgende kenmerken teruggeven:

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

Waar FQDN_ACL de naam van de IP toegangslijst is die aan de domeinlijst in kaart wordt gebracht en REDIRECT_ACL is de normale CWA om toegangslijst te richten.

Het resultaat van CWA MAB-verificatie moet zoals hieronder worden geconfigureerd:



Verifiëren

Om te verifiëren dat de FQDN-domeinlijst van toepassing is op het clientgebruik onder opdracht:

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

Voorbeeld van de opdrachtoutput met toegestane domeinnamen:

```
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
```

Referenties

Central-webverificatie in het configuratievoorbeeld van WLC en ISE

BYOD draadloos infrastructuurontwerp

ISE 2.1 configureren voor instappen van Microsoft