Converged Access Wireless Controller (5760/3850/3650) BYOD-Client-Integration mit FQDN-ACLs

Inhalt

Einführung

In diesem Dokument wird ein Konfigurationsbeispiel für die Verwendung von DNS-basierten Zugriffslisten (ACLs) und einer Fully Qualified Domain Name (FQDN)-Domänenliste beschrieben, die den Zugriff auf bestimmte Domänenlisten während der Webauthentifizierung/BYOD-Bereitstellung (Client Bring Your Own Device) auf konvergenten Access Controllern ermöglicht.

Voraussetzungen

Anforderungen

In diesem Dokument wird davon ausgegangen, dass Sie bereits wissen, wie Sie eine grundlegende zentrale Webauthentifizierung (CWA) konfigurieren. Dies ist nur eine Ergänzung, um die Verwendung von FQDN-Domänenlisten zur Unterstützung von BYOD zu veranschaulichen. Auf CWA- und ISE BYOD-Konfigurationsbeispiele wird am Ende dieses Dokuments verwiesen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:
Cisco Identity Services Engine Softwareversion 1.4

Cisco WLC 5760 Softwareversion 3.7.4

DNS-basierter ACL-Prozessablauf

Wenn Identity Services Engine (ISE) den Namen der umgeleiteten ACL (den Namen der ACLs zurückgibt, mit dem bestimmt wird, welcher Datenverkehr an die ISE umgeleitet werden soll und welcher nicht) und der Name der FQDN-Domänenliste (den Namen der ACL, der der FQDN-URL-Liste auf dem Controller zugeordnet ist, um vor der Authentifizierung Zugriff zu gewähren) zurückgibt, wird der Fluss wie folgt angezeigt:

1. Der Wireless LAN Controller (WLC) sendet eine Capwap-Payload an den Access Point (AP), um DNS-Snooping für die URLs zu aktivieren.
2. AP-Snoops für die DNS-Abfrage vom Client. Wenn der Domänenname mit der zulässigen URL übereinstimmt, leitet der Access Point die Anforderung an den DNS-Server weiter, wartet auf die Antwort vom DNS-Server und analysiert die DNS-Antwort und leitet sie weiter, wobei nur die erste aufgelöste IP-Adresse aufgelöst wird.Wenn der Domänenname nicht übereinstimmt, wird die DNS-Antwort wie folgt (ohne Änderung) an den Client zurückgeleitet.
3. Wenn der Domänenname übereinstimmt, wird die erste aufgelöste IP-Adresse in der Capwap-Payload an den WLC gesendet. WLC aktualisiert implizit die der FQDN-Domänenliste zugeordnete ACL mit der aufgelösten IP-Adresse, die sie vom Access Point erhalten hat, und verfolgt dabei den folgenden Ansatz: Die aufgelöste IP-Adresse wird jeder ACL-Regel, die der FQDN-Domänenliste zugeordnet ist, als Zieladresse hinzugefügt.Jede ACL-Regel wird von "Zulassen" in "Ablehnen" umkehrt, und umgekehrt wird die ACL auf den Client angewendet. **Hinweis**: Mit diesem Mechanismus können wir die Domänenliste nicht der CWA-Umleitungszugriffskontrollliste zuordnen, da die Umleitung der ACL-Regeln dazu führt, dass sie geändert werden, um sie zuzulassen, was bedeutet, dass der Datenverkehr an die ISE umgeleitet werden sollte. Daher wird die FQDN-Domänenliste einer separaten "permit ip any any"-ACL im Konfigurationsteil zugeordnet.Um diesen Punkt zu klären, gehen Sie davon aus, dass der Netzwerkadministrator die FQDN-Domänenliste mit cisco.com url in der Liste konfiguriert und diese der folgenden ACL zugeordnet hat:

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

   Wenn der Client cisco.com anfordert, löst AP den Domänennamen cisco.com in die IP-Adresse 72.163.4.161 auf und sendet ihn an den Controller. Die ACL wird wie folgt geändert und auf den Client angewendet:

   ```
   ip access-list extended FQDN_ACL
   deny ip any host 72.163.4.161
   ```
4. Wenn der Client eine HTTP-GET-Anforderung sendet: Der Client wird umgeleitet, falls die ACL den Datenverkehr zulässt.Bei einer verweigerten IP-Adresse ist der HTTP-Datenverkehr zulässig.
5. Sobald die App auf den Client heruntergeladen und die Bereitstellung abgeschlossen ist, sendet der ISE-Server die CoA-Sitzung als beendet an den WLC.
6. Sobald der Client vom WLC deauthentifiziert wurde, entfernt der Access Point das Flag für Snooping pro Client und deaktiviert Snooping.

Konfigurieren

WLC-Konfiguration

1. Umleitungszugriffskontrollliste erstellen:
   Mit dieser ACL wird festgelegt, welcher Datenverkehr nicht an die ISE umgeleitet werden soll (in der ACL abgelehnt) und welcher Datenverkehr umgeleitet werden soll (Zulassen in der 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 dieser Zugriffsliste ist 10.48.39.228 die IP-Adresse des ISE-Servers.

2. Konfigurieren Sie die FQDN-Domänenliste:Diese Liste enthält die Domänennamen, auf die der Client vor Bereitstellung oder CWA-Authentifizierung zugreifen kann.
   ```
   passthru-domain-list URLS_LIST
   match play.google.*.*
   match cisco.com
   ```
3. Konfigurieren Sie eine Zugriffsliste mit permit ip any any to be kombinieren mit URLS_LIST:
   Diese ACL muss der FQDN-Domänenliste zugeordnet werden, da eine tatsächliche IP-Zugriffsliste auf den Client angewendet werden muss (eine eigenständige FQDN-Domänenliste kann nicht angewendet werden).

   ```
   ip access-list extended FQDN_ACL
   permit ip any any
   ```
4. Ordnen Sie der FQDN_ACL die Domänenliste URLS_LIST zu:

   ```
   access-session passthru-access-group FQDN_ACL passthru-domain-list URLS_LIST
   ```
5. Konfigurieren Sie die Onboarding CWA SSID:
   Diese SSID wird für die zentrale Client-Webauthentifizierung und Client-Bereitstellung verwendet. Die FQDN_ACL und die REDIRECT_ACL werden von der ISE auf diese SSID angewendet.

   ```
   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 dieser SSID-Konfiguration ist die Methodenliste **MACFILTER** die Methodenliste, die auf die ISE-Radius-Gruppe verweist, und **rad-acct** die Accounting-Methodenliste, die auf dieselbe ISE-Radius-Gruppe verweist.

   Zusammenfassung der in diesem Beispiel verwendeten Methodenlistenkonfiguration:

   ```
   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-Konfiguration

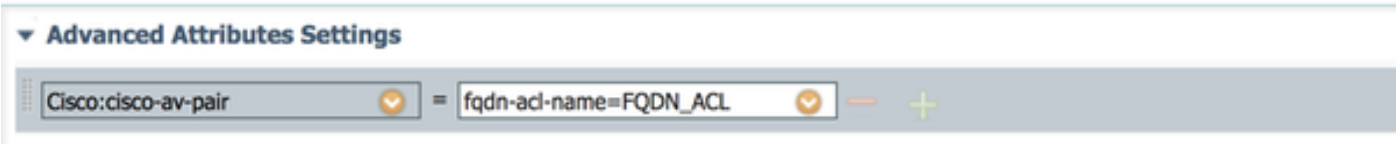
In diesem Abschnitt wird davon ausgegangen, dass Sie mit dem CWA ISE-Konfigurationsteil vertraut sind. Die ISE-Konfiguration ist mit den folgenden Änderungen nahezu identisch.

Das Authentifizierungs-Ergebnis der MAB-Authentifizierung (Wireless CWA Address Authentication Bypass) sollte die folgenden Attribute zusammen mit der URL für die CWA-Umleitung zurückgeben:

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

Dabei steht FQDN_ACL für den Namen der IP-Zugriffsliste, die der Domänenliste zugeordnet ist, und REDIRECT_ACL für die normale CWA-Zugriffsliste für Umleitungen.

Daher sollte das Ergebnis der CWA-MAB-Authentifizierung wie folgt konfiguriert werden:



Überprüfen

So überprüfen Sie, ob die FQDN-Domänenliste auf den Client mit dem folgenden Befehl angewendet wird:

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

Beispiel für Befehlsausgaben mit zulässigen Domänennamen:

```
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
```

Referenzen

[Zentrale Webauthentifizierung im Konfigurationsbeispiel für WLC und ISE]

[BYOD Wireless-Infrastrukturdesign]

[ISE 2.1 für Chromebook-Onboarding konfigurieren]