FQDN ACL을 사용한 통합 액세스 무선 컨트롤러 (5760/3850/3650) BYOD 클라이언트 온보딩

목차

[소개](#)
[사전 요구 사항](#)
[요구 사항](#)
[사용되는 구성 요소](#)
[DNS 기반 ACL 프로세스 흐름](#)
[구성](#)
[WLC 컨피그레이션](#)
[ISE 컨피그레이션](#)
[다음을 확인합니다.](#)
[참조](#)

소개

이 문서에서는 통합 액세스 컨트롤러에서 웹 인증/BYOD(Client Bring Your Own Device) 프로비저닝 상태 중에 특정 도메인 목록에 대한 액세스를 허용하는 DNS 기반 액세스 목록(ACL), FQDN(Fully Qualified Domain Name) 도메인 목록을 사용하기 위한 컨피그레이션 예를 설명합니다 .

사전 요구 사항

요구 사항

이 문서에서는 기본 CWA(Central Web Authentication)를 구성하는 방법을 이미 알고 있다고 가정합니다. 이는 BYOD를 지원하기 위해 FQDN 도메인 목록을 사용하는 것을 보여주는 데 추가된 것입니다.CWA 및 ISE BYOD 컨피그레이션 예는 이 문서의 끝부분에서 참조됩니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.
Cisco Identity Services Engine 소프트웨어 릴리스 1.4

Cisco WLC 5760 소프트웨어 릴리스 3.7.4

DNS 기반 ACL 프로세스 흐름

ISE(Identity Services Engine)에서 리디렉션 ACL 이름(ISE로 리디렉션될 트래픽을 결정하는 데 사용되는 ACL의 이름) 및 FQDN 도메인 목록 이름(인증 전에 액세스를 허용하기 위해 컨트롤러의 FQDN URL 목록에 매핑된 ACL의 이름)을 반환하면 다음과 같이 플로우가 진행됩니다.

1. WLC(Wireless LAN Controller)는 URL에 대한 DNS 스누핑을 활성화하기 위해 AP(Access Point)에 capwap 페이로드를 전송합니다.
2. 클라이언트에서 DNS 쿼리에 대한 AP 스누프입니다. 도메인 이름이 허용된 URL과 일치하는 경우 AP는 요청을 DNS 서버로 전달하고, DNS 서버의 응답을 대기하며, DNS 응답을 구문 분석하고 확인된 첫 번째 IP 주소만 사용하여 전달합니다.도메인 이름이 일치하지 않으면 DNS 응답은 현재(수정 없이) 클라이언트로 다시 전달됩니다.
3. 도메인 이름이 일치하는 경우, 첫 번째 확인된 IP 주소가 capwap 페이로드의 WLC로 전송됩니다.WLC는 다음 방법을 사용하여 AP에서 얻은 확인된 IP 주소로 FQDN 도메인 목록에 매핑된 ACL을 암시적으로 업데이트합니다. 확인된 IP 주소는 FQDN 도메인 목록에 매핑된 ACL의 각 규칙에서 대상 주소로 추가됩니다.ACL의 각 규칙은 허용에서 거부로 전환되고 그 반대의 경우 ACL이 클라이언트에 적용됩니다. **참고:**이 메커니즘에서는 도메인 목록을 CWA 리디렉션 ACL에 매핑할 수 없습니다. 리디렉션 ACL 규칙을 취소하면 트래픽이 ISE로 리디렉션되는 것을 허용하도록 변경되기 때문입니다.따라서 FQDN 도메인 목록은 컨피그레이션 부품의 다른 "permit ip any" ACL에 매핑됩니다.이 점을 명확히 하기 위해 네트워크 관리자가 목록에 cisco.com url을 사용하여 FQDN 도메인 목록을 구성하고 해당 도메인 목록을 다음 ACL에 매핑했다고 가정합니다.

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

   cisco.com을 요청하는 클라이언트에서 AP는 도메인 이름 cisco.com을 IP 주소 72.163.4.161으로 확인하고 컨트롤러에게 전송합니다. ACL은 아래와 같이 수정되어 클라이언트에 적용됩니다.

   ```
   ip access-list extended FQDN_ACL
   deny ip any host 72.163.4.161
   ```
4. 클라이언트가 HTTP "GET" 요청을 보낼 때: ACL에서 트래픽을 허용하는 경우 클라이언트가 리디렉션됩니다.거부된 IP 주소를 사용하면 http 트래픽이 허용됩니다.
5. 클라이언트가 다운로드되고 프로비저닝이 완료되면 ISE 서버는 CoA 세션 종료를 WLC로 보냅니다.
6. 클라이언트가 WLC에서 인증이 해제되면 AP는 클라이언트당 스누핑에 대한 플래그를 제거하고 스누핑을 비활성화합니다.

구성

WLC 컨피그레이션

1. 리디렉션 ACL 생성:
   이 ACL은 어떤 트래픽이 ISE로 리디렉션되지 않아야 하는지(ACL에서 거부됨), 어떤 트래픽을 리디렉션해야 하는지(ACL에서 허용됨)를 정의하는 데 사용됩니다.

   ```
   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
```

이 액세스 목록 10.48.39.228은 ISE 서버 IP 주소입니다.

2. FQDN 도메인 목록을 구성합니다.이 목록에는 프로비저닝 또는 CWA 인증 전에 클라이언트가 액세스할 수 있는 도메인 이름이 포함되어 있습니다.

```
passthru-domain-list URLS_LIST
match play.google.*.*
match cisco.com
```

3. URL_LIST와 결합할 permit ip any any를 사용하여 액세스 목록을 구성합니다.
실제 IP 액세스 목록을 클라이언트에 적용해야 하므로 이 ACL을 FQDN 도메인 목록에 매핑해야 합니다(독립형 FQDN 도메인 목록을 적용할 수 없음).

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

4. URL_LIST 도메인 목록을 FQDN_ACL에 매핑합니다.

```
access-session passthru-access-group FQDN_ACL passthru-domain-list URLS_LIST
```

5. 온보딩 CWA SSID를 구성합니다.
이 SSID는 클라이언트 중앙 웹 인증 및 클라이언트 프로비저닝에 사용되며 FQDN_ACL 및 REDIRECT_ACL은 ISE에 의해 이 SSID에 적용됩니다

```
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
```

이 SSID 컨피그레이션 **MACFILTER** 메서드 목록에서 ISE radius 그룹을 가리키는 방법 목록이며 **rad-acct**는 동일한 ISE RADIUS 그룹을 가리키는 계정 관리 방법 목록입니다.

이 예제에서 사용되는 메서드 목록 구성 요약:

```
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 컨피그레이션

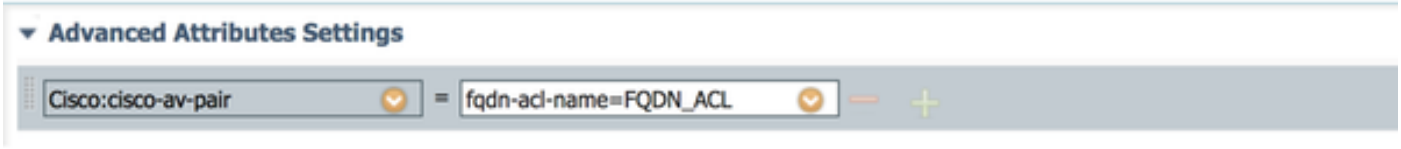
이 섹션에서는 CWA ISE 컨피그레이션 부품을 잘 알고 있으며 ISE 컨피그레이션은 다음 수정 사항과 거의 동일하다고 가정합니다.

무선 CWA MAB(Mac 주소 인증 우회) 인증 결과는 CWA 리디렉션 URL과 함께 다음 특성을 반환해야 합니다.

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

여기서 FQDN_ACL은 도메인 목록에 매핑된 IP 액세스 목록의 이름이고 REDIRECT_ACL은 일반 CWA 리디렉션 액세스 목록입니다.

따라서 다음과 같이 CWA MAB 인증 결과를 구성해야 합니다.



다음을 확인합니다.

FQDN 도메인 목록이 클라이언트에 적용되었는지 확인하려면 아래 명령을 사용하십시오.

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

허용되는 도메인 이름을 표시하는 명령 출력의 예:

```
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
```

참조

WLC 및 ISE 컨피그레이션의 중앙 웹 인증 예

BYOD 무선 인프라 설계

Chromebook 온보딩을 위한 ISE 2.1 구성