Converged Access Wireless Controller(5760/3850/3650) BYODクライアントオンボーディング（FQDN ACLを使用）

内容

概要

このドキュメントでは、コンバージドアクセスコントローラでのWeb認証/クライアントの個人所有デバイス持ち込み(BYOD)プロビジョニング状態で特定のドメインリストへのアクセスを可能にする、DNSベースのアクセスリスト(ACL)、完全修飾ドメイン名(FQDN)ドメインリストの設定例を説明します。

前提条件

要件

このドキュメントでは、基本的な中央Web認証(CWA)の設定方法をすでに理解していることを前提としています。これは、BYODを実現するためのFQDNドメインリストの使用を示すための追加にすぎません。CWAおよびISE BYODの設定例は、このドキュメントの最後で参照されています。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。
Cisco Identity Services Engine ソフトウェアリリース 1.4

Cisco WLC 5760ソフトウェアリリース3.7.4

DNSベースのACLプロセスフロー

Identity Services Engine(ISE)がリダイレクトACL名（ISEにリダイレクトされるトラフィックの判別に使用されるACLの名前）とFQDNドメインリスト名（認証の前にアクセスを許可するコント

ローラのFQDN URLリストにマッピングされるACLののの名前）をで返戻時)、フローはは次です。

1. ワイヤレスLANコントローラ(WLC)は、アクセスポイント(AP)にcapwapペイロードを送信して、URLのDNSスヌーピングを有効にします。
2. APはクライアントからのDNSクエリーをスヌーピングします。 ドメイン名が許可されたURLと一致する場合、APは要求をDNSサーバに転送し、DNSサーバからの応答を待ち、DNS応答を解析して、最初のIPアドレスだけが解決された状態で転送します。ドメイン名が一致しない場合、DNS応答は変更されずにそのままクライアントに転送されます。
3. ドメイン名が一致する場合、最初に解決されたIPアドレスがcapwapペイロード内のWLCに送信されます。WLCは、次の方法を使用して、FQDNドメインリストにマッピングされたACLを、APから取得した解決済みのIPアドレスで暗黙的に更新します。 解決されたIPアドレスは、FQDNドメインリストにマッピングされたACLの各ルールの宛先アドレスとして追加されます。ACLの各ルールがpermitからdenyに逆になり、その逆も逆になると、ACLがクライアントに適用されます。 **注：**このメカニズムでは、ドメインリストをCWAリダイレクトACLにマッピングできません。リダイレクトACLルールを反転すると、許可するように変更され、トラフィックはISEにリダイレクトされます。そのため、FQDNドメインリストは、設定部分で別の「permit ip any any」ACLにマッピングされます。この点を明確にするには、ネットワーク管理者がリスト内のcisco.com urlを使用してFQDNドメインリストを設定し、そのドメインリストを次のACLにマッピングしたとします。

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

   cisco.comを要求するクライアントでは、APがドメイン名cisco.comをIPアドレス72.163.4.161に解決し、それをコントローラに送信すると、ACLは次のように変更され、クライアントに適用されます。

   ```
   ip access-list extended FQDN_ACL
   deny ip any host 72.163.4.161
   ```
4. クライアントがHTTP「GET」要求を送信したとき： ACLがトラフィックを許可した場合、クライアントはリダイレクトされます。拒否されたIPアドレスでは、httpトラフィックが許可されます。
5. クライアントでアプリケーションがダウンロードされ、プロビジョニングが完了すると、ISEサーバはWLCにCoAセッション終了を送信します。
6. クライアントがWLCから認証解除されると、APはクライアントごとのスヌーピングのフラグを削除し、スヌーピングを無効にします。

設定

WLC の設定

1. リダイレクト ACL を作成します。
   このACLは、どのトラフィックをISEにリダイレクトする（ACLで拒否される）べきか、どのトラフィックをリダイレクトする（ACLで許可される）のかを定義するために使用されます。

```
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
```

このアクセスリスト10.48.39.228は、ISEサーバのIPアドレスです。

2. FQDNドメインリストを設定します。このリストには、クライアントがプロビジョニングまたはCWA認証の前にアクセスできるドメイン名が含まれています。

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

3. URLS_LISTと組み合わせて、permit ip any anyを使用してアクセスリストを設定します。このACLは、実際のIPアクセスリストをクライアントに適用する必要があるため（スタンドアロンFQDNドメインリストは適用できません）、FQDNドメインリストにマッピングする必要があります。

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

4. URLS_LISTドメインリストをFQDN_ACLにマッピングします。

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

5. オンボーディングCWA SSIDを設定します。このSSIDは、クライアントの中央Web認証とクライアントプロビジョニング（ISEによってFQDN_ACLとREDIRECT_ACL）に使用されます

```
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
```

このSSID設定では、**MACFILTER**方式リストはISE RADIUSグループを指す方式リストで、**rad-acct**は同じISE RADIUSグループを指すアカウンティング方式リストです。

この例で使用する方式リストの設定の要約を次に示します。

```
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 の設定

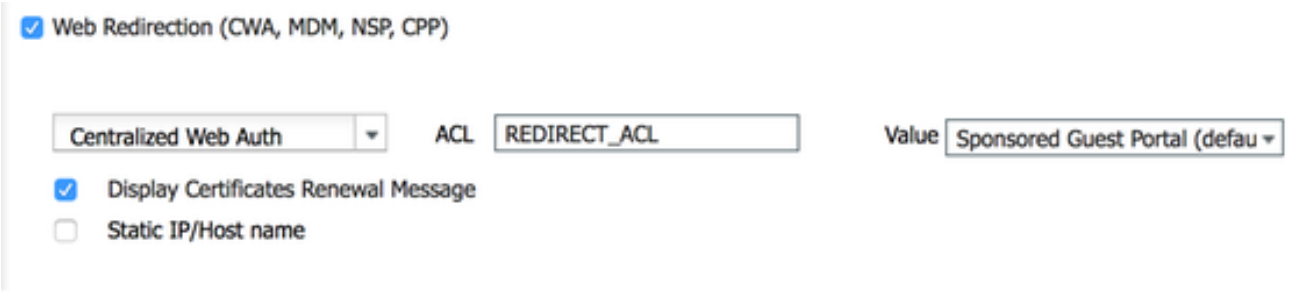
このセクションでは、CWA ISE設定の部分に精通しており、ISE設定は次の変更とほぼ同じであることを前提としています。

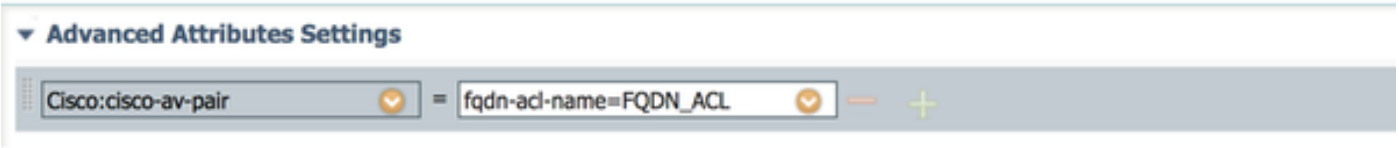
無線CWA Macアドレス認証バイパス(MAB)認証結果は、CWAリダイレクトURLとともに次の属性を返します。

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

ここで、FQDN_ACLはドメインリストにマッピングされたIPアクセスリストの名前で、REDIRECT_ACLは通常のCWAリダイレクトアクセスリストです。

したがって、CWA MAB認証結果は次のように設定する必要があります。





確認

FQDNドメインリストがクライアントに適用されていることを確認するには、次のコマンドを使用します。

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

許可されたドメイン名を示すコマンド出力の例：

```
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
```

参考資料

[WLC と ISE での中央 Web 認証の設定例]

[BYODワイヤレスインフラストラクチャ設計]

[Chromebook オンボーディング用の ISE 2.1 を設定する]