FQDN ACL のコンバージしたアクセス ワイヤレス コントローラ（5760/3850/3650） BYOD クライアント Onboarding

目次

概要

この資料は Web 認証/クライアントの間に特定のドメインリストにアクセスを許可するために DNS によって基づくアクセス リスト（ACL）の使用のための設定例を、完全修飾ドメイン名（FQDN）ドメインリスト持って来ますコンバージしたアクセスコントローラのあなた自身のデバイス（BYOD）提供状態を記述したものです。

前提条件

要件

この資料は基本的な中央 Web 認証（CWA）を設定する方法を既にこれである faciltate BYOD に FQDN ドメインリストの使用を示すちょうど付加知っていると仮定します。 CWA および ISE BYOD 設定例はこの資料の終わりに参照されます。

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くものです。
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 は ACL プロセスフローを基づかせていました

リダイレクト ACL 名前を戻す Identity Services Engine （ISE）に（ACL の名前はどのトラフィックが ISE にリダイレクトされるべきで、どれがか判別するのが常であり、）FQDN ドメインリスト名前（認証の前にアクセスを可能にされるべきコントローラの FQDN URLリストにマッピン

グ される ACL の名前は）、フローそのようにあります:

1. ワイヤレス LAN コントローラ（WLC）は Access Point （AP）に URL のための DNS スヌーピングを有効に するために capwap ペイロードを送信 します。
2. AP はクライアントからの DNS クエリのために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 DNSサーバに要求を、待っています DNSサーバからの応答を転送し、ために DNS 応答を解析し、解決される最初の IP アドレスだけと転送して下さい。ドメイン名が一致する場合、DNS 応答はクライアントに戻って（修正なしで）あるように転送されます。
3. ドメイン名が一致すれば、最初の解決される IP アドレスは capwap ペイロードの WLC に送信 されます。 WLC は次のアプローチを使用して AP から得た解決される IP アドレスの FQDN ドメインリストに暗黙のうちにマッピング される ACL をアップデートします: 解決される IP アドレスは FQDN ドメインリストへのマッピング 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。またその逆にもそれから ACL を否定する割り当てからの反転する ACL gets の各ルールはクライアントに適用されます。 **注:** このメカニズムを使うとリダイレクト ACL ルールを反転させることがトラフィックは ISE にリダイレクトする必要があることを意味する割り当てへそれらを変更することに起因するので CWA リダイレクト ACL にドメインリストをマッピング することができません。 Therfore FQDN ドメインリストは設定部品の別途の「permit ip any any」ACL にマッピング されます。ネットワーク admin がリストの cisco.com URL で FQDN ドメインリストを設定し、次の ACL にそのドメインリストをマッピング したことをそのポイントを明白にするために、仮定して下さい:
   ```
   ip access-list extended FQDN_ACLpermit ip any any
   ```
   cisco.com を要求しているクライアントに AP は IP アドレス 72.163.4.161 にドメイン名 cisco.com を変換し、contoller に送信 します、ACL は下記にとしてあるために修正され、クライアントに適用されます:
   ```
   ip access-list extended FQDN_ACLdeny ip any host 72.163.4.161
   ```
4. クライアントが HTTP「GET」要求を送信 する時: クライアントは ACL 割り当てトラフィック リダイレクトされます。否定された IP アドレスによって HTTPトラフィックは許可されます。
5. アプリケーションがクライアントでダウンロードされ、プロビジョニングが完了した、ISE サーバは WLC に CoA セッション 終端を送信 します。
6. クライアントが WLC から非認証されれば、AP はクライアント 1 人あたりのスヌーピングのためのフラグを取除き、スヌーピングをディセーブルにします。

設定

WLC の設定

1. リダイレクト ACL を作成して下さい:
   およびどのトラフィックがリダイレクトする必要があるかこの ACL がどのトラフィックが ISE にべきではないか定義するのに使用されています（ACL で否定される）リダイレクトする（ACL で許可されて）。
   ```
   ip access-list extended REDIRECT_ACLdeny udp any eq bootps anydeny udp any any eq bootpcdeny udp any eq bootpc anydeny udp any any eq domaindeny udp any eq domain anydeny ip any host 10.48.39.228deny ip host 10.48.39.228 anypermit tcp any any eq wwwpermit tcp any any eq 443
   ```
   このアクセス リストで 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て下さい:このリストはクライアントが提供するか、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_LISTmatch play.google.*.*match cisco.com`
3. permit ip any any でアクセス リストを URLS_LIST と結合されるために設定して下さい:
   この ACL はクライアント（スタンドアロン FQDN ドメインリストを追加できません）に実際の IPアクセスリストを適用する必要があるので必要 FQDN ドメインリストにマッピングされるためにです。
   `ip access-list extended FQDN_ACLpermit ip any any`
4. FQDN_ACL に URLS_LIST ドメインリストをマッピング して下さい:
   `access-session passthru-access-group FQDN_ACL passthru-domain-list URLS_LIST`
5. Onboarding CWA SSID を設定して下さい:
   この SSID はクライアント中央 Web 認証のために使用され、クライアント プロビジョニング、FQDN_ACL および REDIRECT_ACL は ISE によってこの SSID に適用されます
   `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 **MACFILTER** メソッドリストで ISE 半径グループを指すメソッドリストはあり、**ラドacct は**同じ ISE 半径グループを指すアカウンティング方式リストです。

   この例で使用されるメソッドリスト 設定の概略:
   ```
   aaa group server radius ISEGroup server name ISE1aaa authorization network MACFILTER group ISEGroup aaa accounting network rad-acct start-stop group ISEGroupradius server ISE1 address ipv4 10.48.39.228 auth-port 1812 acct-port 1813 key 7 112A1016141D5A5E57aaa server radius dynamic-author client 10.48.39.228 server-key 7 123A0C0411045D5679 auth-type any
   ```

ISE 設定

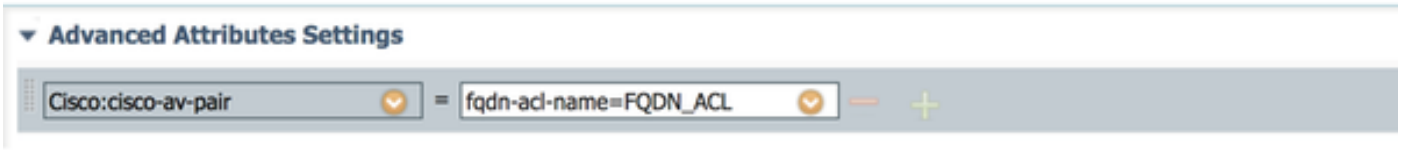
このセクションは CWA ISE 設定部品について詳しく知っていると、ISE 設定ですほぼ同じ仮定します次の修正と。

ワイヤレス 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 と共に次の属性を戻す必要があります:

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

FQDN_ACL がある一方、ドメインリストおよび REDIRECT_ACL にマッピング される IPアクセスリストの名前は標準 CWA リダイレクト アクセス リストです。

Thefore CWA MAB 認証結果は下記のように設定された次であるはずです:



確認

FQDN ドメインリストがコマンドの下のクライアント 使用に追加されることを確認するため:

```
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 PushedServer
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_ACLMethod status list: empty
```

参考資料

[WLC と ISE での中央 Web 認証の設定例]

[BYOD 無線インフラストラクチャー 設計]

[Chromebook Onboarding のための ISE 2.1 を設定して下さい]