ワイヤレス LAN コントローラを使用した外部 Web 認証の設定例

目次

はじめに

このドキュメントでは、外部 Web サーバを使用して、Web 認証用に Wireless LAN Controller（WLC; ワイヤレス LAN コントローラ）を設定する方法について説明しています。

前提条件

要件

この設定を行う前に、次の要件が満たされていることを確認します。

- Lightweight アクセス ポイント（LAP）および Cisco WLC の設定に関する基礎知識
- Lightweight Access Point Protocol（LWAPP）/Control And Provisioning of Wireless Access Points（CAPWAP）の基礎知識
- 外部 Web サーバのセットアップ方法および設定方法に関する知識
- DHCP サーバと DNS サーバのセットアップ方法および設定方法に関する知識

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。

- ファームウェア リリース 7.0.116.0 が稼働している Cisco 4400 WLC
- Cisco 1131AG シリーズ LAP
- ファームウェア リリース 3.6 が稼働している Cisco 802.11a/b/g ワイヤレス クライアント アダプタ
- Web 認証ログイン ページをホストする外部 Web サーバ
- ワイヤレス クライアントに対するアドレス解決と IP アドレス割り当てに使用する DNS サーバおよび DHCP サーバ

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

背景説明

Web 認証は、レイヤ 3 セキュリティ機能です。これにより、コントローラが、有効なユーザ名とパスワードを提示しないクライアントからの IP トラフィック（DHCP パケットと DNS 関連パケットを除く）を許可することを防ぎます。 Web 認証は、サプリカントやクライアント ユーティリティを必要としない簡単な認証方式です。

Web 認証は以下を使用して実現できます。

- WLC のデフォルト ログイン ウィンドウ
- WLC のデフォルト ログイン ウィンドウの修正バージョン。
- 外部 Web サーバ（外部 Web 認証）で設定する、カスタマイズされたログイン ウィンドウ
- コントローラにダウンロードする、カスタマイズされたログイン ウィンドウ

このドキュメントでは、外部 Web サーバからログイン スクリプトを使用するように WLC を設定する方法の説明のために設定例を提供します。

外部 Web 認証プロセス

外部 Web 認証では、Web 認証に使用するログイン ページは外部 Web サーバに保存されます。これは、外部 Web 認証がイネーブルに設定された WLAN ネットワークにワイヤレス クライアントがアクセスを試行するときの一連のイベントのことです。

1. クライアント（エンド ユーザ）は WLAN に接続し、Web ブラウザを開いて www.cisco.com などの URL を入力します。
2. クライアントは DNS サーバに DNS リクエストを送信し、これにより www.cisco.com が IP アドレスに解決されます。
3. WLC は DNS サーバにリクエストを転送し、これにより、www.cisco.com が IP アドレスに解決され、DNS 応答を送信します。 コントローラは応答をクライアントに転送します。

4. クライアントは www.cisco.com の IP アドレスに TCP SYN パケットを送信して、www.cisco.com の IP アドレスとの TCP 接続を開こうとします。
5. WLC には、クライアント用に設定されたルールがあるため、www.google.com のプロキシとして動作することができます。 WLC は、www.google.com の IP アドレスを送信元とする TCP SYN-ACK パケットをクライアントに送信します。 クライアントは、3 ウェイ TCP ハンドシェイクを完了するために、TCP ACK パケットを返し、TCP 接続が完全に確立されます。
6. クライアントは、www.google.com 宛ての HTTP GET パケットを送信します。 WLC はこのパケットをインターセプトし、リダイレクト処理のために送信します。 HTTP アプリケーション ゲートウェイは、HTML 本文を準備し、クライアントから要求された HTTP GET への応答として返します。 この HTML によって、クライアントが WLC のデフォルト Web ページ URL（http://<Virtual-Server-IP>/login.html など）に誘導されます。
7. クライアントは、1.1.1.1 に送信するリダイレクト URL への HTTPS 接続を開始します。 これは、コントローラの仮想 IP アドレスです。 SSL トンネルを開始するため、クライアントはサーバ証明書を検証するか、または無視する必要があります。
8. 外部 Web 認証が有効なため、WLC はクライアントを外部 Web サーバにリダイレクトします。
9. 外部 Web 認証ログイン URL には、クライアントがコントローラ Web サーバへの問い合わせに必要な AP_Mac_Address、client_url（www.cisco.com）、action_URL などのパラメータが付加されます。**注:** action_URL は、ユーザ名とパスワードパスワードがコントローラに保存される Web サーバを示します。 認証を受けるには、クレデンシャルをコントローラに戻す必要があります。
10. 外部 Web サーバの URL でユーザをログイン ページに誘導します。
11. ログイン ページはユーザ クレデンシャルの入力を受け取り、WLC Web サーバの action_URL（http://1.1.1.1/login.html など）に要求を送信して戻します。
12. WLC Web サーバは、認証のためにユーザ名とパスワードを送信します。
13. WLC は RADIUS サーバ要求を開始するか、WLC 上のローカル データベースを使用してユーザを認証します。
14. 認証が成功すれば、WLC Web サーバは、設定されたリダイレクト URL またはクライアントが開始された URL（www.cisco.com など）にユーザを転送します。
15. 認証が失敗した場合、WLC Web サーバはカスタマー ログイン URL にユーザをリダイレクトして戻します。

注: HTTP、HTTPS 以外のポートを使用するように外部 Web 認証を設定するには、次のコマンドを発行します。

```
(Cisco Controller) >config network web-auth-port

<port>          Configures an additional port to be redirected for web authentication.
```

ネットワーク構成

設定例では次のような構成を使用します。 LAP が WLC に登録されている。 ゲスト ユーザ用に WLAN **guest** を設定し、そのユーザの Web 認証を有効にする必要があります。 また、コントローラによってユーザを確実に外部 Web サーバの URL（外部 Web 認証）にリダイレクトさせる必要があります。 外部 Web サーバは、認証に使用する Web ログイン ページをホストします。

ユーザ クレデンシャルは、コントローラで保持されるローカル データベースに対して有効である必要があります。 認証が成功した後、WLAN ゲストに対するアクセス権が許可されます。 このセットアップのために、コントローラやその他のデバイスを設定する必要があります。

注: ログイン スクリプトをカスタマイズしたバージョンを使用して Web 認証を行うことができます。 サンプル Web 認証スクリプトは、シスコのソフトウェア ダウンロード ページからダウンロードできます。 たとえば 4400 コントローラの場合、[Products] > [Wireless] > [Wireless LAN Controller] > [Standalone Controllers] > [Cisco 4400 Series Wireless LAN Controllers] > [Cisco 4404 Wireless LAN Controller] > [Software on Chassis] > [Wireless Lan Controller Web Authentication Bundle-1.0.1] に移動し、**webauth_bundle.zip** ファイルをダウンロードします。

注: カスタマイズされた Web 認証バンドルでは、ファイル名が最大 30 文字に制限されます。 バンドル内のすべてのファイル名が 30 文字以内であることを確認する。

注: このドキュメントでは、DHCP、DNS、および外部 Web サーバが設定されているものとします。 DHCP、DNS、および外部 Web サーバの設定方法については、適切なサードパーティのドキュメントを参照してください。

設定

外部 Web 認証用に WLC を設定する前に、基本動作用に WLC を設定し、WLC に LAP を登録する必要があります。 このドキュメントでは、基本動作用に WLC が設定されており、WLC に LAP が登録されていることを前提としています。 LAP を使用した基本動作用に WLC を初めて設定する場合は、「ワイヤレス LAN コントローラ (WLC) への Lightweight AP (LAP) の登録」を参照してください。

この構成用に LAP および WLC を設定するには、次の手順を実行します。

1. ゲスト ユーザ用のダイナミック インターフェイスの作成
2. 事前認証 ACL の作成
3. WLC でのゲスト ユーザ用のローカル データベースの作成
4. 外部 Web 認証用の WLC の設定
5. ゲスト ユーザ用の WLAN の設定

ゲスト ユーザ用のダイナミック インターフェイスの作成

ゲスト ユーザ用のダイナミック インターフェイスを作成するには、次の手順を実行します。

1. WLC GUI で、[Controllers] > [Interfaces] の順に選択します。[Interfaces] ウィンドウが表示されます。 このウィンドウには、コントローラに設定されているインターフェイスの一覧が表示されます。 これには、デフォルトのインターフェイス (管理インターフェイス、AP マネージャ インターフェイス、仮想インターフェイス、サービス ポート インターフェイス) 、およびユーザ定義のダイナミック インターフェイスが含まれます。
2. 新しいダイナミック インターフェイスを作成するには、**[New]** をクリックします。
3. [Interfaces] > [New] ウィンドウで、インターフェイス名と VLAN ID を入力します。 次に、[Apply] をクリックします。この例では、ダイナミック インターフェイスの名前に **guest** を指定し、VLAN ID に **10** を割り当てています。
4. [Interfaces] > [Edit] ウィンドウで、ダイナミック インターフェイスの IP アドレス、サブネット マスク、デフォルト ゲートウェイを入力します。 ダイナミック インターフェイスを WLC の物理ポートに割り当て、DHCP サーバの IP アドレスを入力します。 次に、[Apply] をクリックします。

事前認証 ACL の作成

Web 認証に外部 Web サーバを使用する場合、一部の WLC プラットフォームには外部 Web サーバ用の事前認証 ACL（Cisco 5500 シリーズ コントローラ、Cisco 2100 シリーズ コントローラ、Cisco 2000 シリーズ、およびコントローラ ネットワーク モジュール）が必要になります。 他の WLC プラットフォームには、事前認証 ACL は必須ではありません。

ただし、外部 Web 認証を使用する場合は、外部 Web サーバ用の事前認証 ACL を設定することを推奨します。

WLAN の事前認証 ACL を設定するには、次の手順を実行します。

1. WLC GUI で、[Security] > [Access Control Lists] の順に選択します。このウィンドウでは、標準的なファイアウォール ACL に類似した現在の ACL を確認できます。
2. [New] をクリックして新しい ACL を作成します。
3. ACL の名前を入力し、[Apply] をクリックします。この例では、ACL の名前を **Pre-Auth-for-External-Web-Server** としています。
4. 作成した新しい ACL の [Edit] をクリックします。[Access Control Lists > Edit] ウィンドウが表示されます。 このウィンドウでは、新しい規則を定義したり、既存の ACL の規則を変更したりできます。
5. [Add New Rule] をクリックします。
6. クライアントの外部 Web サーバへのアクセスを許可する ACL 規則を定義します。この例では、172.16.1.92 が外部 Web サーバの IP アドレスです。
7. [Apply] をクリックして、変更を確定します。

WLC でのゲスト ユーザ用のローカル データベースの作成

ゲスト ユーザ用のユーザ データベースは、ワイヤレス LAN コントローラのローカル データベースに保存されるか、コントローラの外部で保存されます。

このドキュメントでは、コントローラ上のローカル データベースがユーザの認証に使用されます。 ローカル ネット ユーザを作成し、Web 認証クライアント ログイン用のパスワードを定義する必要があります。 WLC でユーザ データベースを作成するには、次の手順を実行します。

1. WLC GUI で [Security] を選択します。
2. 左側の [AAA] メニューから [Local Net Users] をクリックします。
3. [New] をクリックして新しいユーザを作成します。新しいウィンドウが表示され、ユーザ名とパスワードの情報の入力を求められます。
4. 新しいユーザを作成するため、ユーザ名とパスワードを入力して、使用するパスワードを確認します。この例では、**User1** というユーザを作成します。
5. 必要に応じて説明を追加します。この例では **Guest User1** 使用します。
6. **[Apply]**をクリックして、新しいユーザ設定を保存します。
7. さらにデータベースにユーザを追加するには、手順 3 ~ 6 を繰り返します。

外部 Web 認証用の WLC の設定

次の手順では、外部 Web 認証用の WLC を設定します。 次の手順を実行します。

1. コントローラの GUI で、[Security] > [Web Auth] > [Web Login Page] の順に選択して、[Web Login] ページにアクセスします。
2. [Web Authentication Type] ドロップダウン ボックスから、[External (Redirect to external

server)] を選択します。
3. [External Web server] セクションで、新しい外部 Web サーバを追加します。
4. [Redirect URL after login] フィールドで、エンド ユーザが認証の成功後にリダイレクトされるページの URL を入力します。 [External Web Auth URL] フィールドに、ログイン ページが保存される外部 Web サーバの URL を入力します。**注:** WLC バージョン 5.0 以降では、Web 認証のログアウト ページもカスタマイズできます。 設定方法については、『*ワイヤレス LAN コントローラ コンフィギュレーション ガイド 5.2*』の「WLAN 単位のログイン ページ、ログイン失敗ページ、およびログアウト ページの割り当て」セクションを参照してください。

ゲスト ユーザ用の WLAN の設定

最後に、ゲスト ユーザ用の WLAN を作成します。 次の手順を実行します。

1. WLAN を作成するために、コントローラの GUI で [WLANs] をクリックします。[WLANs] ウィンドウが表示されます。 このウィンドウには、コントローラに設定されている WLAN の一覧が表示されます。
2. 新しい WLAN を設定するために [New] をクリックします。この例では、WLAN の名前に **Guest** を使用し、WLAN ID は **1** です。
3. [Apply] をクリックします。
4. [WLAN] > [Edit] ウィンドウで、WLAN 固有のパラメータを定義します。ゲスト WLAN については、[General] タブの [Interface Name] フィールドで適切なインターフェイスを選択します。この例では、先に作成したダイナミック インターフェイスである **guest** を WLAN ゲストにマップしています。[Security] タブに移動します。 この例では、[Layer 2 Security] で [None] が選択されています。**注:** 802.1x 認証による Web 認証はサポートされません。 これは、Web 認証を使用する場合、レイヤ 2 セキュリティとして、802.1x または 802.1x を使用する WPA/WPA2 を選択できないことを意味します。その他のすべてのレイヤ 2 セキュリティ パラメータを使用した Web 認証がサポートされます。[Layer 3 Security] フィールドで、[Web Policy] チェックボックスにチェック マークを入れて、[Authentication] オプションを選択します。Web 認証を使用してワイヤレス ゲスト クライアントを認証するため、このオプションを選択します。[Preauthentication ACL] ドロップダウン メニューから適切な事前認証 ACL を選択します。この例では、すでに作成済みの事前認証 ACL を使用します。[Apply] をクリックします。

確認

ワイヤレス クライアントが起動したら、Web ブラウザに URL（www.cisco.com など）を入力します。 ユーザが認証されていないため、WLC はそのユーザを外部 Web ログイン URL にリダイレクトします。

ユーザ クレデンシャルの入力が求められます。 ユーザ名とパスワードを入力すると、ログイン ページでユーザ クレデンシャルの入力を受け取り、WLC Web サーバの action_URL（http://1.1.1.1/login.html など）に要求を on submit で送信して戻します。 これが入力パラメータとしてカスタマーのリダイレクト URL に提供されます。ここで、1.1.1.1 は、スイッチの仮想インターフェイス アドレスです。

WLC は、WLC に設定されたローカル データベースと照らし合わせてユーザを認証します。 認証が成功した後、WLC Web サーバは、設定されたリダイレクト URL またはクライアントが開始さ

れた URL（www.cisco.com など）にユーザを転送します。

トラブルシューティング

設定のトラブルシューティングを行うには、次の debug コマンドを使用します。

- debug mac addr <client-MAC-address xx: xx: xx: xx: xx: xx>
- debug aaa all enable
- debug pem state enable
- debug pem events enable
- debug dhcp message enable
- debug dhcp packet enable
- debug pm ssh-appgw enable
- debug pm ssh-tcp enable

ここでは、設定に関するトラブルシューティングについて説明します。

外部 Web 認証サーバにリダイレクトされたクライアントが証明書警告を受信する

問題： クライアントがシスコの外部 Web 認証サーバにリダイレクトされると、クライアントが証明書警告を受信します。 サーバには有効な証明書があり、外部 Web 認証サーバに直接接続する場合は、証明書警告は受信しません。 これは、証明書に関連付けられた外部 Web 認証サーバの実際の IP アドレスではなく、WLC の仮想 IP アドレス（1.1.1.1）がクライアントに示されていることが原因でしょうか。

解決策： はい。 ローカルまたは外部のいずれの Web 認証を実行するかにかかわりなく、コントローラの内部 Web サーバをヒットしています。 外部 Web サーバにリダイレクトする場合でも、コントローラ自体に有効な証明書がない限り、コントローラから証明書警告を受信します。 リダイレクトが https に送信された場合、コントローラおよび外部 Web サーバの両方に有効な証明書がない限り、両方から証明書警告を受信します。

すべてまとめて証明書警告を受信しないようにするには、ルート レベルの証明書を発行して、コントローラにダウンロードする必要があります。 証明書はホスト名に対して発行されるため、そのホスト名をコントローラの仮想インターフェイスの [DNS host name] ボックスに入力します。 また、そのホスト名をローカル DNS サーバに追加し、WLC の仮想 IP アドレス（1.1.1.1）を指すようにする必要があります。

詳細については、「WLAN コントローラ（WLC）上でのサード パーティ証明書用の証明書署名要求（CSR）の生成」を参照してください。

エラー：「ページを表示できません」

問題： コントローラを 4.2.61.0 にアップグレードした後、Web 認証用にダウンロードした Web ページを使用すると、「page cannot be displayed」のエラー メッセージが表示されます。 アップグレードする以前は機能していました。 デフォルトの内部 Web ページでは問題なくロードされます。

ソリューション： WLC バージョン 4.2 以降から、Web 認証用にカスタマイズされたログイン ページを複数使用できる新しい機能が導入されています。

Web ページを適切にロードさせるには、[Security] > [Web Auth] > [Web login] ページで Web 認

証の種類をグローバルに [customized] として設定するだけでは十分ではありません。 特定の WLAN でも設定する必要があります。 このためには、次の手順を実行します。

1. WLC の GUI にログインします。
2. [WLANs] タブをクリックし、Web 認証用に設定された WLAN のプロファイルにアクセスします。
3. [WLANs > Edit] ページで [Security] タブをクリックします。 次に、[Layer 3] を選択します。
4. このページで、レイヤ 3 セキュリティとして [None] を選択します。
5. [Web Policy] ボックスにチェックマークを入れ、[Authentication] オプションを選択します。
6. [Over-ride Global Config] の [Enable] ボックスにチェックマークを入れ、Web 認証タイプとして [Customized (Downloaded)] を選択して、[Login Page] プルダウン メニューから目的のログイン ページを選択します。 [Apply] をクリックします。

関連情報

- ワイヤレス LAN コントローラの Web 認証の設定例
- ビデオ： Cisco ワイヤレス LAN コントローラ (WLC) での Web 認証
- 無線 LAN コントローラでの VLAN の設定例
- Wireless LAN Controller と Lightweight アクセス ポイントの基本設定例
- テクニカル サポートとドキュメント – Cisco Systems