レイヤ 3 セキュリティの設定

- VPN パススルーを使用したレイヤ 3 セキュリティの設定，1 ページ
- Web 認証を使用したレイヤ 3 セキュリティの設定，2 ページ

VPN パススルーを使用したレイヤ 3 セキュリティの設定

VPN パススルーを使用したレイヤ 3 セキュリティの制約事項

- レイヤ 2 トンネリング プロトコル（L2TP）と IPSec は、コントローラでサポートされていません。
- レイヤ 3 セキュリティ設定は、WLAN でクライアント IP アドレスを無効にしているときはサポートされません。
- VPN パススルー オプションは、Cisco 5500 シリーズのコントローラでは使用できません。しかし、ACL を使用してオープン WLAN を作成すると、その機能をこのコントローラで再現できます。

VPN パススルーについて

コントローラは、VPN パススルー、つまり VPN クライアントから送信されるパケットの「通過」をサポートします。 VPN パススルーの例として、ラップトップから本社オフィスの VPN サーバへの接続が挙げられます。

VPN パススルーの設定

VPN パススルーの設定（GUI）

ステップ 1 [WLANs] を選択して、[WLANs] ページを開きます。

ステップ 2 VPN パススルーを設定する WLAN の ID 番号をクリックします。 [WLANs > Edit] ページが表示されます。

ステップ 3 [Security] タブおよび [Layer 3] タブを選択して、[WLANs > Edit]（[Security] > [Layer 3]）ページを開きます。

ステップ 4 [Layer 3 Security] ドロップダウン リストから、[VPN Pass-Through] を選択します。

ステップ 5 [VPN Gateway Address] テキスト ボックスに、クライアントにより開始され、コントローラを通過した VPN トンネルを終端しているゲートウェイ ルータの IP アドレスを入力します。

ステップ 6 [Apply] をクリックして、変更を確定します。

ステップ 7 [Save Configuration] をクリックして設定を保存します。

VPN パススルーの設定（CLI）

VPN パススルーを設定するには、次のコマンドを使用します。

- **config wlan security passthru** {**enable** | **disable**} *wlan_id gateway*

  gateway には、VPN トンネルを終端している IP アドレスを入力します。

- パススルーが有効であることを確認するには、次のコマンドを入力します。

  show wlan

Web 認証を使用したレイヤ 3 セキュリティの設定

WLAN の Web 認証を設定するための前提条件

- HTTP/HTTPS Web 認証リダイレクションを開始するには、HTTP URL または HTTPS URL を使用します。
- CPU ACL が HTTP / HTTPS トラフィックをブロックするように設定されている場合、正常な Web ログイン認証の後に、リダイレクション ページでエラーが発生する可能性があります。
- Web 認証を有効にする前に、すべてのプロキシ サーバがポート 53 以外のポートに対して設定されていることを確認してください。

- WLAN の Web 認証を有効にする場合、コントローラがワイヤレス クライアントで送受信されるトラフィックを転送することを示すメッセージが認証前に表示されます。 DNS トラフィックを規制し、DNS トンネリング攻撃を検出および予防するために、ゲスト VLAN の背後にファイアウォールまたは侵入検知システム（IDS）を設置することをお勧めします。
- Web 認証が WLAN で有効になっており、さらに、CPU ACL のルールもある場合、クライアント ベースの Web 認証ルールは、クライアントが非認証である限り優先されます（webAuth_Reqd ステート）。 クライアントが RUN 状態になると、CPU ACL ルールが適用されます。 したがって、コントローラで CPU ACL ルールが有効である場合、次の状況で、仮想インターフェイス IP に対する allow ルール（任意の方向）が必要なります。
  - CPU ACL で、両方向とも allow ACL ルールが設定されていない。
  - allow ALL ルールが設定されているが、優先順位が高いポート 443 または 80 に対する DENY ルールも設定されている。
- 仮想 IP に対する allow ルールは、TCP プロトコルおよびポート 80（secureweb が無効な場合）またはポート 443（secureweb が有効な場合）に設定します。 このプロセスは、仮想インターフェイス IP アドレスへのクライアントのアクセスを許可し、CPU ACL ルールが設定されている場合に正常認証をポストするために必要です。

WLAN の Web 認証の設定に関する制約事項

- Web 認証はレイヤ 2 セキュリティ ポリシー（オープン認証、オープン認証+WEP、WPA-PSK）でのみサポートされています。 7.4 リリースでは、Web 認証での 802.1X の使用がサポートされています。
- Web 認証のユーザ名フィールドでの特殊文字はサポートされていません。
- クライアントが WebAuth SSID に接続したときに、事前認証 ACL が VPN ユーザを許可するように設定されていると、クライアントは数分ごとに SSID との接続を解除されます。 Webauth SSID の接続には、Web ページでの認証が必要です。

  Web 認証ユーザ セクションの [WLANs] > [Security] > [AAA servers] > [Authentication priority] で次の ID ストアを選択して、Web 認証ユーザを認証できます。

  - ローカル
  - RADIUS
  - LDAP

  複数の ID ストアを選択すると、コントローラはユーザの認証が成功するまで、リストの各 ID ストアを指定された順序で上から下までチェックします。 コントローラがリストの最後に達しても ID ストアのいずれかに未認証のユーザが残っている場合、認証は失敗します。

Web 認証について

コントローラで VPN パススルーが有効になっていない場合に限り、WLAN では Web 認証を使用できます。 Web 認証は、セットアップも使用方法も簡単で、SSL とともに使用することで WLAN 全体のセキュリティを向上させることができます。

802.1x と Web 認証の使用

WLAN で 802.1x と一緒に Web 認証を使用する場合は、3 種類のタイマーがアクティブになります。 これらのタイマーは、AAA サーバから受信したタイムアウト値または WLAN セッション タイムアウトに基づきます。

- セッション タイマー：再認証を要求する WLAN 用に設定されたクライアント セッション タイムアウト。 このタイマーは、Web 認証の成功後に起動します。
- 再認証タイマー：WPA1 用のクライアント再認証をトリガーするために使用されるタイマー。
- PMK キャッシュ タイマー：WPA2 用のクライアント再認証をトリガーするために使用されるキャッシュ ライフタイム タイマー。

このセクションでは、WLAN が 802.1x と一緒に Web 認証を使用するように設定されている場合に、クライアントで発生する可能性のある 2 つのシナリオについて説明します。

1 つのコントローラにアソシエートされたクライアント：このシナリオでは、再認証または PMK キャッシュ タイマーの有効期限が切れると、クライアントが再認証を行い、再認証/PMK キャッシュ タイマーを更新し、実行状態を維持します。 クライアント セッション タイマー（ST）の有効期限が切れると、再認証/PMK キャッシュ タイマーがまだ有効であっても、クライアントが認証解除されます。

コントローラ間のクライアント ローミング：このシナリオでは、クライアントがローミングしてから、外部コントローラが L2 認証をトリガーし、アンカー コントローラが L3 認証をトリガーします。 802.1x 再認証/PMK タイマーは外部コントローラ上で動作し、クライアント セッション タイマーはアンカー コントローラ上で動作します。 再認証/PMK タイマーの有効期限が切れると、802.1x クライアント再認証が実施され、クライアントが実行状態になります。 クライアントは、クライアント セッション タイマーの有効期限が切れたときにのみ認証解除されます。

セッションタイムアウトは、認証のタイプ（AAA またはローカル）とユーザの人数によって異なります。

- AAA ユーザの AAA オーバーライドが有効になっている場合は、セッション タイムアウトが RADIUS サーバから受信されます。
- AAA ユーザの AAA オーバーライドが無効になっている場合は、セッション タイムアウトが対応する WLAN から取得されます。
- ローカル認証が使用されている場合は、802.1x 再認証/PMK キャッシュ タイマーが WLAN ST 値になり、Web 認証ローカル ユーザの残りのライフタイムが ST として設定されます。

（注） 802.1x と Web 認証の両方を同じユーザに使用することも、別々のユーザに使用することもできます。

Web 認証の設定

Web 認証の設定（GUI）

ステップ 1 [WLANs] を選択して、[WLANs] ページを開きます。

ステップ 2 Web 認証を設定する WLAN の ID 番号をクリックします。 [WLANs > Edit] ページが表示されます。

ステップ 3 [Security] タブおよび [Layer 3] タブを選択して、[WLANs > Edit]（[Security] > [Layer 3]）ページを開きます。

ステップ 4 [Web Policy] チェックボックスをオンにします。

ステップ 5 [Authentication] オプションが選択されていることを確認します。

ステップ 6 [Apply] をクリックして、変更を確定します。

ステップ 7 [Save Configuration] をクリックして設定を保存します。

Web 認証の設定（CLI）

ステップ 1 特定の WLAN で Web 認証を有効または無効にするには、次のコマンドを入力します。
config wlan security web-auth {**enable** | **disable**} *wlan_id*

ステップ 2 Web 認証ポリシーのタイマーが切れたときにゲスト ユーザの IP アドレスを解放して、ゲスト ユーザが 3 分間 IP アドレスを取得しないようにするには、次のコマンドを入力します。
config wlan webauth-exclude *wlan_id* {**enable** | **disable**}

デフォルト値は [disabled] です。 コントローラに内部 DHCP スコープを設定するときに、このコマンドを適用できます。 デフォルトでは、ゲスト ユーザは、Web 認証のタイマーが切れた場合、別のゲスト ユーザがその IP アドレスを取得する前に、ただちに同じ IP アドレスに再アソシエートできます。 ゲスト ユーザの数が多い場合、または DHCP プールの IP アドレスが限れられている場合、一部のゲスト ユーザが IP アドレスを取得できなくなる可能性があります。

ゲスト WLAN でこの機能を有効にした場合、Web 認証ポリシーのタイマーが切れると、ゲスト ユーザの IP アドレスが解放され、このゲスト ユーザは 3 分間 IP アドレスの取得から除外されます。 その IP アドレスは、別のゲスト ユーザが使用できます。 3 分経つと、除外されていたゲスト ユーザは、可能であれば、再アソシエートし、IP アドレスを取得できるようになります。

ステップ 3 次のコマンドを入力して、Web 認証のステータスを表示します。
show wlan *wlan_id*