WLC と ISE での中央 Web 認証の設定例

目次

概要

このドキュメントでは、ワイヤレス LAN コントローラ（WLC）で中央 Web 認証（CWA）を実行するために使用する設定例を示します。

前提条件

要件

このドキュメントに関する固有の要件はありません。

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 1.2
- Cisco WLC ソフトウェア リリース 7.3.102.0

設定

Web 認証の最初の方法は、ローカル Web 認証です。 この場合、WLC は HTTP トラフィックを内部サーバまたは外部サーバにリダイレクトし、ここでユーザに認証を求めるプロンプトが表示されます。 次に、WLC はクレデンシャルを取得し（外部サーバの場合は HTTP GET リクエストで返信）し、RADIUS 認証を行います。 ゲスト ユーザの場合は、外部サーバ（Identity Services Engine（ISE）や NAC ゲスト サーバ（NGS））が必要です。これは、デバイス登録やセルフプロビジョニングなどの機能がポータルで提供されているためです。 フローには、次の手順が含まれます。

1. ユーザは、Web 認証 Service Set Identifier（SSID）に関連付けられています。
2. ユーザはブラウザを開きます。
3. URL を入力するとすぐに、WLC によってゲストのポータル（ISE または NGS など）にリダイレクトされます。
4. ポータルで認証します。
5. 入力されたクレデンシャルを持つ WLC にゲストのポータルによってリダイレクトして戻されます。
6. WLC は RADIUS を介してゲストのユーザを認証します。
7. WLC は元の URL にリダイレクトして戻します。

このフローには、複数のリダイレクションが含まれています。 新しいアプローチは、CWA を使用することです。 この方法は、ISE（バージョン 1.1 以降）と WLC（バージョン 7.2 以降）で動作します。 フローには、次の手順が含まれます。

1. ユーザは Web 認証 SSID に関連付けられています。これは、実際には open+macfiltering とレイヤ 3 セキュリティなしの SSID です。
2. ユーザはブラウザを開きます。
3. WLC はゲストのポータルにリダイレクトします。
4. ポータルで認証します。
5. ISE はコントローラにユーザが有効であることを示すために RADIUS の認可変更（CoA - UDP ポート 1700）を送信し、最後にアクセス コントロール リスト（ACL）などの RADIUS の属性をプッシュします。
6. ユーザは元の URL の再試行を促されます。

使用する設定は、次のとおりです。

WLC の設定

WLC の設定は比較的簡単です。 ISE からダイナミックな認証 URL を取得するために、**テクニック**（スイッチと同様）を使用します（これは、認可変更（CoA）を使用するためセッションを作成する必要があり、セッション ID が URL の一部になるためです）。 MAC フィルタリングを使用するために SSID を設定します。 MAC アドレスが見つからない場合も access-accept を返し、すべてのユーザにリダイレクション URL を送信するように ISE を設定します。

この他に、RADIUS ネットワーク アドミッション コントロール（NAC）および認証、許可、およびアカウンティング（AAA）オーバーライドを有効にする必要があります。 RADIUS NAC は、ユーザが認証されて、ネットワークにアクセスできることを示す CoA を要求を ISE が送信できるようにします。 また、ISE がポスチャ結果に基づいてユーザ プロファイルを変更するようにするポスチャ割り当てにも使用されます。

RADIUS サーバで RFC3576（CoA）がデフォルトで有効になっていることを確認します。

最後に、リダイレクト ACL を作成します。 この ACL は ISE の access-accept で参照され、どのトラフィックをリダイレクトする必要があるか（ACL によって拒否）、どのトラフィックをリダイレクトする必要がないか（ACL によって許可）を定義します。 ここでは、ISE に対するリダイレクション トラフィックを回避するだけです。 より具体的には、ポート 8443（ゲスト ポータル）で ISE が送受信するトラフィックのみを回避しますが、ユーザがポート 80/443 で ISE へのアクセスを試みた場合はリダイレクトされます。

> **注:** 7.2 や 7.3 などの以前のバージョンの WLC ソフトウェアでは DNS を指定するようには要求されませんでしたが、より新しいコード バージョンでは、そのリダイレクト ACL で DNS トラフィックを許可するように要求されます。

WLC の設定は以上で完了です。

ISE 設定

許可プロファイルの作成

ISE で許可プロファイルを作成する必要があります。 次に、認証および認可ポリシーを設定します。 WLC はネットワーク デバイスとして設定済みである必要があります。

許可プロファイルに WLC で以前に作成された ACL の名前を入力します。

1. [Policy] をクリックし、次に [Policy Elements] をクリックします。
2. [Results] をクリックします。
3. [Authorization] を展開して、[Authorization profile] をクリックします。
4. [Add] ボタンをクリックして、中央 webauth の新しい許可プロファイルを作成します。
5. [Name] フィールドに、プロファイルの名前を入力します。 この例では、**WLC_CWA** を使用します。
6. [Access Type] ドロップダウン リストから [ACCESS_ACCEPT] を選択します。

7. [Web Redirection] チェックボックスをオンにし、ドロップダウン リストから [Centralized Web Auth] を選択します。

8. [ACL] フィールドに、リダイレクトされるトラフィックを定義するスイッチ上の ACL の名前を入力します。 この例では、**cwa_redirect** を使用します。

9. [Redirect] ドロップダウン リストで [Default] を選択します。（デフォルト以外のカスタム ポータルを使用する場合は、デフォルト以外を選択します）。

認証ルールの作成

ISE が WLC からのすべての MAC 認証を受け入れることを確認し、ユーザが見つからない場合でも認証を続行することを確認します。

[Policy] メニューで [Authentication] をクリックします。

次の図は、認証ポリシー ルールを設定する方法の例を示します。 この例では、MAB の検出時にルールがトリガーされるように設定されています。

- 認証ルールの名前を入力します。 この例では、ISE のバージョン 1.2 ではデフォルトで存在する **MAB** を使用します。
- [If] 条件フィールドで、プラス（[+]）アイコンをクリックします。
- [Compound condition] を選択し、次に [Wired_MAB OR Wireless_MAB] を選択します。
- ルールをさらに展開するには [and ...] の横にある矢印をクリックします。
- [Identity Source] フィールドの [+] アイコンをクリックし、[Internal endpoints] を選択します。
- [If user not found] ドロップダウン リストから [Continue] を選択します。

許可ポリシーの作成

許可ポリシーを設定します。 2 つの認証と認可が存在することを理解することが重要です。

- 1 つ目は、ユーザが SSID に関連付けられて中央 Web 認証のプロファイルが返されるときの認証と認可です（未知の MAC アドレスため、リダイレクションのためにユーザを設定する必要があります）。
- 2 つ目はユーザは Web ポータルで認証を行う認証と認可です。 これは、この設定（ユーザの要件を満たすように設定可能）のデフォルト ルール（内部ユーザ）に一致します。 認可の部分は、中央 Web 認証のプロファイルに再び照合されないことが重要です。 それ以外の場合は、リダイレクションのループが発生します。 **Network Access: UseCase Equals Guest Flow** 属性は、この 2 つ目の認証を照合するために使用できます。 結果は、次のようになります。

注: ISE リリース 1.3 では、Web 認証のタイプに応じて、「Guest Flow」の使用例がヒットしなくなっていることがあります。 この場合、認可ルールには、唯一の使用可能な条件としてゲスト ユーザ グループを含める必要があります。

次のステップを実行し、前の図に示すように認可ルールを作成します。

1. 新しいルールを作成し、名前を入力します。 この例では **Guest Redirection** を使用します。

2. 条件フィールドでプラス ([+]) アイコンをクリックして、新しい条件を作成します。

3. [expression] ドロップダウン リストを展開します。

4. [Network Access] を選択し、展開します。

5. [AuthenticationStatus] をクリックし、[Equals] 演算子を選択します。

6. 右側のフィールドで [UnknownUser] を選択します。

7. [General Authorization] ページの [then] という単語の右側のフィールドで [WLC_CWA] (「許可プロファイル」) を選択します。

   この手順では、ユーザ (または MAC アドレス) が不明な場合でも、ISE が続行されるようにします。

   不明なユーザには、ここで [Login] ページが表示されます。 ただし、クレデンシャルを入力すると、認証および認可ポリシーで設定された内容にもかかわらず、クライアント クレデンシャルが有効であれば認証に成功します。 ISE バージョン 1.1 と 1.2 では、ポータルの認証は認証および認可ルールに従わず、有効な場合は成功します。 したがって、ポータルのログインに成功する場合はアクセスを許可するルールを作成する必要はありません。

8. **Guest Redirection** ルールの最後にある [Actions] ボタンをクリックし、このルールの前に新しいルールを挿入することを選択します。

   注: この新しいルールが **Guest Redirection** ルールの前に位置することは非常に重要です。

9. 新しいルールの名前を入力します この例では **Guest Portal Auth** を使用します。

10. 条件フィールドで、プラス ([+]) アイコンをクリックし、新しい条件の作成を選択します。

11. [Network Access] を選択し、[UseCase] をクリックします。

12. 演算子として [Equals] を選択します。

13. 右のオペランドとして [GuestFlow] を選択します。 (この条件の ISE リリース 1.3 に関して、これらの手順の前に載せられた注を参照して下さい)。

14. 認可ページでプラス (+) アイコン ([then] の横にある) をクリックし、ルールの結果を選

択します。

[Permit Access] オプションを選択するか、カスタム プロファイルを作成し、VLAN または任意の属性に戻ることができます。 [If GuestFlow] の上では、ユーザ グループに基づいてさまざまな認可プロファイルを返すようにさらに条件を追加できます。 ステップ 7 で説明したように、この **Guest Portal Auth** ルールはポータルのログインに成功した後、およびクライアントを再認証するために ISE が CoA を送信した後に 2 つ目の MAC アドレスと照合されます。 この 2 つ目の認証の違いは、単に ISE の MAC アドレスが ISE に渡されるのではなく、ISE がポータルで提供されたユーザ名を記憶していることです。 この認可ルールに、ゲスト ポータルで数ミリ秒前に入力されたクレデンシャルを考慮させることができます。

注: プロファイリング機能が有効な場合、エンドポイントをデータベースに自動的に挿入できます。この場合、不明なユーザ（UnknownUser）の条件は一致しません。 この場合、Wireless_MAB（組み込みの条件）要求と照合することを推奨します。 コントローラ上での MAC 認証を使用する場合、さらに具体的な認可のためにエンドポイント グループを使用でき、またゲスト SSID と照合する条件を追加することもできます。

IP 更新の有効化（オプション）

VLAN を割り当てる場合、最後のステップとして、クライアント PC 用の IP アドレスを更新します。 このステップは、Windows クライアント用のゲスト ポータルによって実行できます。 前の手順で **2 つ目の認証**ルールのために VLAN を設定していない場合は、この手順をスキップすることができます。

VLAN を割り当てた場合は、次の手順を実行し、IP 更新を有効にします。

1. [Administration] をクリックし、[Guest Management] をクリックします。
2. [Setting] をクリックします。
3. [Guest] を展開し、次に [Multi-Portal Configuration] を展開します。
4. [DefaultGuestPortal] または作成したカスタム ポータルの名前をクリックします。
5. [VLAN DHCP Release] チェックボックスをクリックします。

   注: このオプションは Windows クライアントでのみ機能します。

Anchor-Foreign のシナリオ

この設定は、WLC の自動アンカーの機能でも使用できます。 唯一の問題点は、この Web 認証方式はレイヤ 2 であるため、すべての RADIUS 作業が外部 WLC で実行されることに注意する必要があります。 外部 WLC のみが ISE と通信し、リダイレクション ACL も外部 WLC 上にある必要があります。

他のシナリオと同様、外部 WLC ではクライアントが短時間で **RUN** 状態になったと表示されます

が、これは必ずしも正しくはありません。 これは、単にトラフィックが外部 WLC からアンカーに送信されたことを意味しています。 実際のクライアントの状態は、アンカーで確認できます。そこには、**CENTRAL_WEBAUTH_REQD** と表示されるはずです。

> **注:** 中央 Web 認証（CWA）を使用するアンカーと外部のセットアップは、リリース 7.3 以降でのみ動作します。

> **注:** Cisco Bug ID CSCuo56780 により（修正が含まれたバージョンでも）、IP と MAC のバインドの欠如の可能性があるため、アカウンティングでプロファイリングが不正確になるので、アンカーと外部の両方でアカウンティングを実行できません。 また、アカウンティングではゲスト ポータルのセッション ID に関する問題も多数発生します。 アカウンティングを設定したい場合は、外部コントローラでアカウンティングを設定します。

確認

ユーザが SSID に関連付けられると、認可が [ISE] ページに表示されます。

WLC のクライアントの詳細に、リダイレクション URL と ACL が適用されたことが表示されます。

これで、クライアントで任意のアドレスを開くと、ブラウザが ISE にリダイレクトされるようになります。 ドメイン ネーム システム（DNS）が正しく設定されていることを確認します。

ユーザがポリシーを受け入れるとネットワーク アクセスが許可されます。

ISE の例に示すように、適用される認証、認可変更、およびプロファイルは permitAccess です。

前のスクリーンショットは、個々の認証手順を明確に示す ISE バージョン 1.1.x のスクリーンショットです。

次のスクリーンショットは、同じクライアントで実行される複数の認証を ISE が 1 行にまとめた ISE バージョン 1.2 のスクリーンショットです。 実際には後者が実用的ですが、バージョン 1.1.x のスクリーンショットはこの例で厳密に何が起きているのかをわかりやすく表示しています。

コントローラでは、ポリシー マネージャの状態と RADIUS NAC の状態が **POSTURE_REQD** から **RUN** に変わります。

> **注:** リリース 7.3 以降では、この状態は **POSTURE_REQD** と呼ばれず、**CENTRAL_WEBAUTH_REQD** と呼ばれるようになりました。

トラブルシューティング

CWA の問題のトラブルシューティングまたは分離を行うには、次の手順を実行します。

1. コントローラで **debug client <mac address of client>** コマンドを入力し、クライアントが **CENTRAL_WEBAUTH_REQD** 状態に達するかどうかを判断するためにモニタします。 ISE

から WLC に存在しない（または正しく入力されていない）リダイレクト ACL が返される場合、一般的な問題が検出されます。 この場合は、**CENTRAL_WEBAUTH_REQD** 状態に達するとクライアントは認証解除され、これによってプロセスが再度開始されます

2. 正しいクライアントの状態に達することができた場合、WLC の Web GUI で [monitor] > [clients] に移動し、正しいリダイレクト ACL と URL がクライアントに適用されていることを確認します。

3. 正しい DNS が使用されていることを確認します。 クライアントは、インターネットの Web サイトと ISE のホスト名を解決できる必要があります。 これは、nslookup で確認できます。

4. すべての認証手順が ISE 上で実行されていることを確認するために次の点をチェックします。

   CWA 属性が返される MAC 認証が最初に実行されている必要がある。

   ポータルのログイン認証が実行されている。

   ダイナミック認可が実行されている。

   最後の認証が ISE 上のポータルのユーザ名を示す MAC 認証である。この認証に対して最終的な認可結果が返される（最後の VLAN と ACL など）。

アンカーのシナリオに関する特別な考慮事項

モビリティ シナリオでの CWA プロセスの効率を制限する、次の Cisco Bug ID を考慮してください（特にアカウンティングが設定されている場合）。

- CSCuo56780：*ISE RADIUS サービスの Denial of Service の脆弱性*
- CSCul83594：*ネットワークが開いている場合に、セッション ID がモビリティ全体で同期されない*