ISE を搭載した WLC 上で FlexConnect AP を使用した 中央 Web 認証の設定例

目次

概要

このドキュメントでは、ローカル スイッチング モードで Identity Services Engine（ISE）を搭載したワイヤレス LAN コントローラ（WLC）上の FlexConnect アクセス ポイント（AP）を使用した中央 Web 認証を設定する方法について説明します。

重要： この時点で、FlexAP のローカル認証は、このシナリオではサポートされません。

このシリーズの他のドキュメント

- スイッチおよび Identity Services Engine を使用した中央 Web 認証の設定例
- WLC と ISE での中央 Web 認証の設定例

前提条件

要件

このドキュメントに関しては個別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（ISE）リリース 1.2.1
- Wireless LAN Controller Software、リリース バージョン- 7.4.100.0

設定

ワイヤレス LAN コントローラ（WLC）の中央 Web 認証を設定するには複数の方法があります。最初の方法は、ユーザが認証の入力を促される内部または外部サーバに WLC によって HTTP トラフィックがリダイレクトされるローカル ネットワークの認証です。 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）または Cisco NAC ゲスト サーバ（NGS））が、デバイスの登録およびセルフプロビジョニングなどの機能を提供するポータルとして必要です。 このプロセスには、次の手順が含まれています。

1. Web 認証 SSID に関連付けます。
2. 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。

このプロセスには多くのリダイレクトが含まれます。 新しい方法では、ISE（1.1 より後のバージョン）および WLC（7.2 より後のバージョン）で機能する中央 Web 認証を使用します。 このプロセスには、次の手順が含まれています。

1. Web 認証 SSID に関連付けます。
2. 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、ユーザが有効であり最終的にアクセス コントロール リスト（ACL）などの RADIUS の属性をプッシュすることをコントローラに示すために RADIUS 認可変更（CoA から UDP のポート 1700）を送信します。
6. ユーザは元の URL の再試行を促されます。

この項では、WLC および ISE に中央 Web 認証を設定するために必要な手順について説明します。

ネットワーク図

この設定では、次のネットワーク設定を使用します。

WLC の設定

WLC の設定は比較的簡単です。「トリック」が使用され（スイッチと同様に）、ISE からダイナミックな認証 URL を取得します。（これが CoA を使用するため、セッションはセッション

ID が URL の一部であるように作成する必要があります）。 SSID は MAC フィルタリングを使用するように設定され、MAC アドレスが見つからない場合でも ISE は Access-Accept メッセージを返すように設定されます。このため、すべてのユーザにリダイレクト用の URL が送信されるように設定されます。

さらに、RADIUS ネットワーク アドミッション コントロール（NAC）と AAA オーバーライドを有効にする必要があります。 RADIUS NAC によって、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 リクエストを ISE が送信できるようになります。 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使用されます。

1. RADIUS サーバで RFC3576（CoA）が有効であることを確認します。これは、デフォルトです。

2. 新規 WLAN を作成してください。 この例では、*CWAFlex* という名前の新しい WLAN を作成し、vlan33 に割り当てます。（アクセス ポイントがローカル スイッチング モードであるため、大きな影響はない点に注意してください。）

3. [Security] タブで、レイヤ 2 セキュリティの MAC フィルタリングを有効にします。

4. [Layer 3] タブで、セキュリティが無効であることを確認します。（ネットワーク認証がレイヤ 3 で有効にされると、ローカル Web 認証は有効になり、中央 Web 認証は有効になりません。）

5. [AAA Servers] タブで、WLAN の RADIUS サーバとして ISE サーバを選択します。 オプションで、ISE での詳細情報を得るために会計用にこれを選択できます。

6. [Advanced] タブで、[Allow AAA Override] がオンで [NAC State] に対して [Radius NAC] が選択されていることを確認します。

7. リダイレクト ACL を作成します。

   この ACL は ISE の Access-Accept メッセージで参照され、リダイレクトすべきトラフィック（ACL によって拒否される）、およびリダイレクトすべきでないトラフィック（ACL によって許可される）を定義します。 基本的には、DNS および ISE との間でやり取りされるトラフィックを許可する必要があります。 **注:** FlexConnect の AP に関する問題は、通常の ACL から切り離して FlexConnect ACL を作成する必要があることです。 この問題は Cisco

Bug ID CSCue68065 で文書化されており、リリース 7.5 で解決されています。 WLC 7.5 以降では、FlexACL だけが必要であり、非標準 ACL は必要ありません。 ISE によって返されるリダイレクト ACL が標準 ACL であると WLC では考えます。 しかし、そのように機能することを保証するには、FlexConnect ACL として適用されている同一の ACL が必要です。
次の例では、*flexred* という名前の FlexConnect ACL の作成方法を示しています。

ISE へのトラフィックと同様に DNS トラフィックを許可し残りを拒否するルールを作成します。

最高レベルのセキュリティを必要とする場合は、ISE へのポート 8443 だけを許可できます。（ポスチャする場合は、8905、8906、8909、8910 などの一般的なポスチャ ポートを追加する必要があります。）

（CSCue68065 が原因でバージョン 7.5 よりも前のコードについてのみ）[Security] > [Access Control Lists] を選択して、同じ名前の同一の ACL を作成します。

特定の FlexConnect AP を用意します。 より大規模な導入の場合、通常は FlexConnect グループを使用し、拡張性の理由から、次の項目を AP 単位で実行しないことに注意してください。

[Wireless] をクリックして、特定のアクセス ポイントを選択します。[FlexConnect] タブをクリックし、[External Webauthentication ACLs] をクリックします。（バージョン 7.4 以前は、このオプションの名前は *Web ポリシー* でした。）

Web ポリシー領域に ACL（この例では *flexred* いう名前）を追加します。 これにより、この ACL がアクセス ポイントに事前にプッシュされます。 この ACL はまだ適用されていませんが、必要な場合に適用できるように、ACL の内容が AP に提供されます。

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

許可プロファイルを作成するには、次の手順を実行します。

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「*CentralWebauth*」という名前を使用します。
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 Authentication] 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 WLC 上の ACL の名前を入力します。 この例では *flexred* 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。

[Redirect] 属性は、ISE がデフォルトの Web ポータルと ISE 管理者が作成したカスタム Web ポータルのいずれを参照するかを定義します。 たとえば、この例の *flexred* ACL はクライアントから Anywhere への HTTP トラフィックのリダイレクトをトリガーします。

認証ルールの作成

認証プロファイルを使用して認証ルールを作成するには、次の手順を実行します。

1. [Policy] メニューで [Authentication] をクリックします。 この図は、認証ポリシー ルールの設定方法の例を示します。 この例では、MAC フィルタが検出されるとトリガーされるようにルールが設定されています。

2. 認証ルールの名前を入力します。 この例では、*Wireless mab* を使用します。
3. [If] 条件フィールドで、プラス ([+]) アイコンをクリックします。
4. [Compound condition] を選択し、次に [Wireless_MAB] を選択します。
5. 許可されたプロトコルとして [Default network access] を選択します。
6. 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。
7. [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。
8. [If user not found] ドロップダウン リストから [Continue] を選択します。

このオプションにより、MAC アドレスが不明な場合でも、webauth によってデバイスが認証済みとなります。 Dot1x クライアントはクレデンシャルを使用して認証できるので、この設定で考慮する必要はありません。

許可ルールの作成

ここでは、許可ポリシーでいくつかのルールを設定します。 PC は関連付けられると、MAC フィルタリングに移動します。 この例では MAC アドレスを不明と想定しているので、webauth と ACL が返されます。 この*MAC not known* (MAC が既知でない) のルールは、次の画像に示され、このセクションで設定されます。

許可ルールを作成するには、次の手順を実行します。

1. 新しいルールを作成し、名前を入力します。 この例では、「*MAC not known*」という名前を使用します。
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] ページで、単語 [then] の右側フィールドの [CentralWebauth]（[Authorization Profile]）を選択します。この手順により、ユーザ（または MAC アドレス）が不明でも、ISE を続行することができます。不明なユーザには、ここで [Login] ページが表示されます。 しかし、ユーザがいったんクレデンシャルを入力しても、ISE の認証要求が再度表示されます。 そのため、ゲスト ユーザの場合に満たされる条件を使用して、別のルールを設定する必要があります。 この例では、[If UseridentityGroup equals Guest] を使用し、すべてのゲストがこのグループに属すると想定されています。
8. [MAC not known] ルールの末尾にあるアクション ボタンをクリックして、上で説明した新しいルールを挿入します。**注:** この新しいルールは、[MAC not known] ルールの前に挿入することが重要です。
9. 名前フィールドに、「**2nd AUTH**」と入力します。
10. 条件として ID グループを選択します。 この例では、[Guest] を選択します。

11. 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。

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

13. 演算子として [Equals] を選択します。

14. 右のオペランドとして [GuestFlow] を選択します。 これは、Web ページでログインしたばかりで、認可変更（ルールのゲスト フローの部分）の後に戻ってきたユーザを捕捉することを意味し、これはゲスト ID グループに属している場合にのみ実行されます。

15. 許可ページで [then] の隣にあるプラス（[+]）アイコンをクリックし、ルールの結果を選択します。

    この例では、事前に設定されたプロファイル（vlan34）が割り当てられます。 この設定はこのドキュメントには示されていません。

    [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。

重要： ISE バージョン 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。

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、*2nd AUTH* ルールに VLAN を設定していない場合は、このステップを省略できます。

FlexConnect AP では、VLAN が AP 自体に事前に存在している必要があることに注意してください。 したがって、VLAN が事前に存在しない場合、AP 自体、または作成する新規 VLAN に ACL をなにも適用しない Flex グループに VLAN-ACL マッピングを作成することができます。 これにより、VLAN が実際に作成されます (その VLAN に ACL なしで)。

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。

Traffic flow

このシナリオでは、どのトラフィックがどこに送信されるかを理解することが難しいように思われる可能性があります。 再確認のために以下に簡単にまとめます。

- クライアントが無線で SSID のアソシエーション要求を送信します。
- WLC が ISE を使用して MAC フィルタリング認証を処理します (WLC がリダイレクト属性を受信する場合)。
- クライアントが、MAC フィルタリングの完了後にアソシエーション応答を受信します。
- クライアントが DHCP 要求を送信し、リモート サイトの IP アドレスを取得するために、アクセス ポイントによってその要求が**ローカルに**スイッチ
- Central_webauth 状態では、リダイレクト ACL で拒否とマークされたトラフィック (通常 HTTP) は**中央に**スイッチ このため、リダイレクションを実行するのは、AP ではなく WLC です。 たとえば、クライアントが任意の Web サイトを要求すると、AP でその要求を CAPWAP でカプセル化して WLC に送信し、WLC でその Web サイトの IP アドレスをスプーフィングして ISE へリダイレクトします。
- クライアントが ISE のリダイレクト URL にリダイレクトされます。 このリダイレクトは、再度**ローカルに**スイッチされます (このリダイレクトが Flex のリダイレクト ACL で許可にヒットするため)。
- 一度 RUN 状態になると、トラフィックはローカルにスイッチされます。

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。

下から上に、CWA の属性を返す MAC アドレスのフィルタリング認証を確認できます。 ユーザ名を使用したポータルのログインを次に示します。 次に。ISE は WLC に CoA を送信し、最後の認証は WLC 側のレイヤ 2 の MAC フィルタリング認証ですが、ISE はクライアントとユーザ名を記憶していてこの例で設定した必要な VLAN に適用します。

このクライアントでいずれかのアドレスが開くと、ブラウザは ISE にリダイレクトされます。 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。

コントローラで、ポリシー マネージャの状態および RADIUS NAC の状態が [POSTURE_REQD] から [RUN] に変わります。