ISE バージョン 1.3 ホットスポットの設定例

目次

概要

Cisco Identity Services Engine (ISE) バージョン 1.3 では、ホットスポットと呼ばれる新しいタイプのゲスト ポータルがあります。 このタイプのポータルでは、ネットワークへのゲスト アクセスを提供でき、ユーザに対してクレデンシャルの入力を強制しません。 このドキュメントでは、この機能の設定とトラブルシューティングの方法を説明します。

前提条件

要件

ISE 構成の経験と、次のトピックに関する基本的な知識があることが推奨されます。

- ISE の導入およびゲスト フロー
- ワイヤレス LAN コントローラ (WLC) の設定

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。

- Microsoft Windows 7
- Cisco WLC バージョン 7.6 以降
- ISE ソフトウェア バージョン 1.3 以降

トポロジとフロー

このシナリオは、アクセプタブル ユース ポリシー（AUP）に同意し、同意後にのみインターネットへのアクセス（またはその他の制限付きアクセス）が付与されるゲスト ユーザを対象としています。

ステップ 1：ゲスト ユーザがサービス セット識別子（SSID）： Hotspot にアソシエートします。 これは、認証に ISE を使用する MAC フィルタリングが設定されたオープン ネットワークです。 この認証では、ISE の 2 番目の認可ルールに一致し、認可プロファイルが Hotspot にリダイレクトします。 ISE から、2 つの cisco-av-pairs を使用した RADIUS Access-Accept が返されます。

- url-redirect-acl（リダイレクトする必要があるトラフィック、および WLC でローカルに定義されたアクセス コントロール リスト（ACL）の名前）
- url-redirect（そのトラフィックのリダイレクト先 - ISE）

ステップ 2： ゲスト ユーザは ISE にリダイレクトされ、AUP に同意し、オプションでシークレット アクセス コードを入力します。

ステップ 3：ISE が RADIUS 認可変更（CoA）Admin-Reset を WLC に送信します。 WLC は、RADIUS Access-Request の送信時に、ユーザを再認証します。 ISE は、WLC でローカルに定義されており、インターネットのみへのアクセスを提供する Access-Accept および Airespace ACL で応答します。

> **注:** CoA Admin-Reset はホットスポット機能に固有です。これについては Cisco Bug ID CSCus46754 で説明しています。 ゲスト ポータルでの ISE バージョン 1.2 の動作はこれとは異なり、 CoA Re-authenticate または Terminate が送信されました。

ステップ 4 ゲスト ユーザがネットワークへのアクセスを希望します。 ネットワーク管理者は、ユーザが AUP に同意したことを確認しています。 ゲスト ユーザは、元の URL、静的に設定された URL、または正常完了を示すページにリダイレクトされます。 ISE により示されるすべてのページは、カスタマイズ可能です。

オプションのポスチャ チェックとの統合については、最後の項で説明します。

設定

WLC

1. 認証とアカウンティングのために新しい RADIUS サーバを追加します。 RADIUS CoA（RFC 3576）を有効にするため、[Security] > [AAA] > [Radius] > [Authentication] に移動します。

   アカウンティングでも同様の設定があります。 また、[Called Station ID] 属性で SSID を送信するように WLC を設定することが推奨されます。これにより、ISE は SSID に基づいて

柔軟なルールを設定できます。

2. [WLANs] タブで無線 LAN（WLAN）ホットスポットを作成し、正しいインターフェイスを設定します。 MAC フィルタリングで Layer2 セキュリティを [None] に設定します。 [Security/Authentication, Authorization, and Accounting (AAA) Servers] で認証および認可の両方の ISE IP アドレスを選択します（アカウンティングはオプションです）。 [Advanced] タブで [AAA Override] を有効にし、[Network Admission Control (NAC) State] を [RADIUS NAC] に設定します（CoA サポート）。

3. [Security] > [Access Control Lists] > [Access Control Lists] の順に移動し、2 つのアクセス リストを作成します。

   HotspotRedirect：リダイレクトしてはならないトラフィックを許可し、その他のすべてのトラフィックをリダイレクトします。Internet：社内ネットワークについては拒否され、その他のすべてのネットワークについては許可されます。

   HotspotRedirect ACL の例を次に示します（ISE との間でのトラフィックをリダイレクトから除外する必要があります）。

ISE

1. [Guest Access] > [Configure] > [Guest Portals] に移動し、新しいポータル タイプとして Hotspot Guest Portal を作成します。

2. 認証プロファイルで参照されるポータル名を選択します。 [Portal Behavior and Flow Settings] でポータルをカスタマイズするため、AUP とシークレット コード（オプション）を有効にします。

   [Portal Page Customization] では他にもさまざまなオプションを有効にすることができます。 表示されるすべてのページはカスタマイズ可能です。

3. [Policy] > [Results] > [Authorization] > [Authorization Profile] に移動し、認可プロファイルを設定します。

   HotSpot（Hotspot ポータル名へのリダイレクトと ACL として HotspotRedirect を設定）：

   Internet（[Airespace ACL] を [Internet] に設定）：

4. 認可ルールを確認するために、[Policy] > [Authorization] に移動します。 ISE バージョン 1.3 ではデフォルトで、MAC 認証バイパス（MAB）アクセスが失敗すると（MAC アドレスが見つからない場合）、認証が続行されます（拒否されません）。 これは、デフォルトの認証ルールで何も変更する必要がないため、ゲスト ポータルで非常に便利です。

   1 番目の MAB 認証では、2 番目のルールが一致します（エンドポイントが ID グループにまだ含まれていない）。 その後ユーザが Web ポータル（ホットスポット）にリダイレクトされ、ユーザは AUP に同意し、オプションで正しいシークレット アクセス コードを入力します。 ISE は RADIUS CoA を送信し、WLC は再認証を実行します。 2 番目の認証では、1 番目のルールが認可プロファイル PermitInternet に一致し、WLC に適用される ACL 名が戻されます（この時点では、エンドポイントがすでに GuestEndpoints グループに含まれています）。

   デフォルトでは、AUP に同意するゲストは GuestEndpoints ID グループに追加されます。これらのエンドポイントに割り当てられる ID グループは、ゲスト ポータル設定で設定されます。ゲスト ポータル設定はポータルによって異なります。

5. [Administration] > [Network Resources] > [Network Devices] で WLC をネットワーク アクセス デバイスとして追加します。

確認

このセクションでは、設定が正常に機能していることを確認します。

1. ゲスト ユーザが SSID ホットスポットにアソシエートし、URL を入力すると、AUP にリダイレクトされます。

2. ゲスト ポータルでアクセス コードが設定されている場合は、アクセス コードが必要です。ユーザが誤ったコードを入力すると、エラーが表示されます。

3. 正しいコードを入力すると、次の画面が表示されます。

4. 正しいコードの入力後に、WLC が再認証を実行し、セッションにアタッチされている Internet ACL を提供します。

追加ポスチャ

ゲスト ユーザが、最新のウイルス対策アップデートや Microsoft Windows アップデートなどの特定のポリシー（ポスチャ）を満たしている場合にだけゲスト ユーザにアクセスを提供する必要がある場合は、次のルールを使用してこれを実行できます。

HotSpot ルールではインターネットへのアクセスは提供されませんが、ポスチャ サービスへのリダイレクトが実行されます。 その後 Web エージェントをステーションにプッシュし（Client Provisioning ルール）、ポリシー チェックを実行することができます（Posture ルール）。 Web エージェントから ISE にレポート コンプライアンスが送信されます。 ステーションが準拠したら、ISE は別の CoA 再認証を送信し、これにより WLC で認可アップデートが実行されます。 次に HotSpot_Compliant ルールが検出され、インターネットへのアクセスが提供されます。

NAC または Web エージェントでのポスチャの設定は、ISE バージョン 1.2 の場合と非常に似ています。これについてはこのドキュメントでは説明しません（詳細については「関連情報」の項を参照）。

トラブルシューティング

このセクションでは、設定のトラブルシューティングに役立つ情報を提供します。

ISE で次のように表示されます。

ここで、フローを示します。

- ゲスト ユーザが 2 番目の認可ルールに一致し、ホットスポットにリダイレクトされます（「Authentication succeeded」）。
- ユーザが AUP に同意すると、ISE が CoA Admin-Reset を送信し、これが WLC により確認されます（「Dynamic Authorization succeeded」）。
- WLC は再認証を実行し、ACL 名が戻されます（「Authorize-Only succeeded」）。

[Operations] > [Reports] > [ISE Reports] > [Guest Access Reports] > [AUP Acceptance Status] に移動してこれを確認することもできます。

関連情報

- Cisco ISE コンフィギュレーション ガイドのポスチャ サービス
- Cisco ISE 1.3 アドミニストレータ ガイド
- WLC と ISE での中央 Web 認証の設定例
- 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
- テクニカルサポートとドキュメント - Cisco Systems