SSID に基づく ISE ポリシーの設定例

目次

概要

この文書では、さまざまなサービス セット ID（SSID）を区別するために Cisco Identity Services Engine（ISE）で認可ポリシーを設定する方法について説明します。 これは、さまざまな目的のためにワイヤレス ネットワークに複数の SSID がある組織にとって非常に一般的です。 最も一般的な目的の 1 つとして、従業員用に会社の SSID を使用し、会社への訪問者用にゲスト SSID を使用することがあります。

このマニュアルでは、以下の条件を想定しています。

1. ワイヤレス LAN コントローラ（WLC）が設定され、関係するすべての SSID で動作している。
2. 関係するすべての SSID で ISE に対する認証が動作している。

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
- RADIUS/802.1x 認証用の ISE ゲスト アカウントの設定例
- iPEP ISE および ASA を使用した VPN インライン ポスチャ

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。

- ワイヤレス LAN コントローラ リリース 7.3.101.0
- Identity Services Engine Release 1.1.2.145

先行バージョンにもこの両方の機能があります。

このドキュメントの情報は、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、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

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。

設定

この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

注: このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を使用してください。

設定

このドキュメントでは、次の設定を使用します。

- 方法 1： **Airespace-Wlan-Id**
- 方法 2： **Called-Station-ID**

一度に 1 つの設定方法のみを使用する必要があります。 両方の設定を同時に実装すると、ISE によって処理される量が増え、ルールの読みやすさに影響します。 この文書では、各設定方法の利点と欠点を説明します。

方法 1： Airespace-Wlan-Id

WLC に作成されたすべてのワイヤレス ローカル エリア ネットワーク（WLAN）に WLAN ID があります。 WLAN ID は WLAN 要約ページに表示されます。

クライアントが SSID に接続するとき、ISE への RADIUS 要求には Airespace-WLAN-ID 属性が含まれています。 この単純な属性は ISE でポリシー決定を行うために使用されます。 この属性の短所の 1 つは、複数のコントローラに分散している SSID で WLAN ID が一致しない場合があることです。 これに該当する導入の場合は、「メソッド 2」に進みます。

この場合、Airespace-Wlan-Id は基準として使用されます。 単純な条件として（単独で）または複合条件として（別の属性と組み合わせて）使用し、必要な結果を実現できます。 この文書では、両方の使用例について説明します。 上記の 2 個の SSID を使用して、次の 2 つのルールを作成できます。

A) ゲスト ユーザはゲスト SSID にログインする必要があります。

B) 企業ユーザは Active Directory（AD）のグループ「Domain Users」に含まれている必要があり

、会社の SSID にログインする必要があります。

ルール A

ルール A の要件は 1 つだけであるため、単純な条件（上記の値に基づく）を作成できます。

1. ISE で、[Policy] > [Policy Elements] > [Conditions] > [Authorization] > [Simple Conditions] に移動し、新しい条件を作成します。
2. [Name] フィールドに、条件名を入力します。
3. [Description] フィールドに説明を入力します（オプション）。
4. [Attribute] ドロップダウン リストから、[Airespace] > [Airespace-Wlan-Id--[1]] を選択します。
5. [Operator] ドロップダウン リストから、[Equals] を選択します。
6. [Value] ドロップダウン リストから、[2] を選択します。
7. [Save] をクリックします。

ルール B

ルール B には 2 つの要件があるため、複合条件を作成できます（上記の値に基づく）。

1. ISE で、[Policy] > [Policy Elements] > [Conditions] > [Authorization] > [Compound Conditions] に移動し、新しい条件を作成します。
2. [Name] フィールドに、条件名を入力します。
3. [Description] フィールドに説明を入力します（オプション）。
4. [Create New Condition (Advance Option)] を選択します。
5. [Attribute] ドロップダウン リストから、[Airespace] > [Airespace-Wlan-Id--[1]] を選択します。
6. [Operator] ドロップダウン リストから、[Equals] を選択します。
7. [Value] ドロップダウン リストから、[1] を選択します。
8. 右側の歯車をクリックし、[Add Attribute/Value] を選択します。
9. [Attribute] ドロップダウン リストから、[AD1] > [External Groups] を選択します。
10. [Operator] ドロップダウン リストから、[Equals] を選択します。
11. [Value] ドロップダウン リストから、必要なグループを選択します。 この例では、Domain Users に設定されています。
12. [Save] をクリックします。

注: このドキュメント全体で、[Policy] > [Policy Elements] > [Results] > [Authorization] > [Authorization Profiles] の下で設定した単純な許可プロファイルを使用します。 これらは [Permit Access] に設定されますが、導入のニーズに合うように変更できます。

これで条件を作成したため、ここでは許可ポリシーに適用できます。 [Policy] > [Authorization] に移動します。 ルールを挿入するリスト上の場所を決めるか、既存のルールを編集します。

ゲスト ルール

1. 既存ルールの右にある下矢印をクリックし、[Insert a new rule] を選択します。
2. ゲスト ルールの名前を入力し、[Identity Groups] フィールドを [Any] に設定したままにします。
3. [Conditions] の下で、プラスをクリックし、[Select Existing Condition from Library] をクリックします。
4. [Condition Name] の下で、[Simple Condition] > [GuestSSID] を選択します。

5. [Permissions] の下で、ゲスト ユーザの適切な許可プロファイルを選択します。
6. [Done] をクリックします。

企業ルール

1. 既存ルールの右にある下矢印をクリックし、[Insert a new rule] を選択します。
2. 企業ルールの名前を入力し、[Identity Groups] フィールドを [Any] に設定したままにします。
3. [Conditions] の下で、プラスをクリックし、[Select Existing Condition from Library] をクリックします。
4. [Condition Name] の下で、[Compound Condition] > [CorporateSSID] を選択します。
5. [Permissions] の下で、企業ユーザの適切な許可プロファイルを選択します。
6. [Done] をクリックします。

注: [Policy List] の下部にある [Save] をクリックするまで、この画面で行った変更は、導入に適用されません。

方法 2： Called-Station-ID

WLC は RADIUS の Called-Station-ID 属性に入れて SSID 名を送信するように設定できます。次に、ISE で条件としてこれを使用できます。 この属性の利点は、WLC での WLAN ID の設定にかかわらず使用できることです。 デフォルトでは、WLC は Called-Station-ID 属性で SSID を送信しません。 WLC でこの機能をイネーブルにするには [Security] > [AAA] > [RADIUS] > [Authentication] に移動し、[Call Station ID Type] を [AP MAC Address: SSID] に設定します。 これにより、Called-Station-ID の形式が *<MAC of the AP the user is connecting to>: <SSID Name>* に設定されます。

送信されている SSID 名は WLAN 要約ページから確認できます。

Called-Station-Id 属性には、AP の MAC アドレスも含まれているため、ISE ポリシーの SSID の名前との照合には、正規表現（REGEX）が使用されます。 条件設定の演算子の「Matches」では、[Value] フィールドから正規表現を読み取ることができます。

正規表現の例

'「**Starts with**」では、たとえば、正規表現値 **^(Acme)*? を使用します。この条件は CERTIFICATE:** Organization MATCHES 'Acme'（「Acme」で始まる条件とのすべての一致）として設定されます。

'「**Ends with**」では、たとえば、正規表現値***(.*(mktg)$** を使用します。この条件は CERTIFICATE: Organization MATCHES 'mktg'（「mktg」で終了する条件とのすべての一致）として設定されます。

'「**Contains**」では、たとえば、正規表現値 .*(1234).* を使用します。この条件は CERTIFICATE: Organization MATCHES '1234'（Eng1234、1234Dev、Corp1234Mktg など「1234」を含む条件とのすべての一致）として設定されます。

'「**Does not start with**」では、たとえば、正規表現値 **^(?! LDAP).*? を使用します。この条件は CERTIFICATE:** Organization MATCHES 'LDAP'（usLDAP、CorpLDAPmktg など、「LDAP」で始まっていない条件とのすべての一致）として設定されます。

Called-Station-ID は SSID 名で終了するため、この例で使用する正規表現は、**.*(:*(: <SSID NAME>)$** です。 設定を行うときは、この点に留意してください。

上記の 2 個の SSID を使用すると、次の要件を持つ 2 つのルールを作成できます。

A) ゲスト ユーザはゲスト SSID にログインする必要があります。

B) 企業ユーザは AD グループ「Domain Users」に含まれている必要があり、会社の SSID にログインする必要があります。

ルール A

ルール A の要件は 1 つだけであるため、単純な条件（上記の値に基づく）を作成できます。

1. ISE で、[Policy] > [Policy Elements] > [Conditions] > [Authorization] > [Simple Conditions] に移動し、新しい条件を作成します。
2. [Name] フィールドに、条件名を入力します。
3. [Description] フィールドに説明を入力します（オプション）。
4. [Attribute] ドロップダウン リストから、[Radius] -> [Called-Station-ID--[30]] を選択します。
5. [Operator] ドロップダウン リストから、[Matches] を選択します。
6. [Value] ドロップダウン リストから、[.*(:*(: Guest)$] を選択します。 これは大文字と小文字が区別されます。
7. [Save] をクリックします。

ルール B

ルール B には 2 つの要件があるため、複合条件を作成できます（上記の値に基づく）。

1. ISE で、[Policy] > [Policy Elements] > [Conditions] > [Authorization] > [Compound Conditions] に移動し、新しい条件を作成します。
2. [Name] フィールドに、条件名を入力します。
3. [Description] フィールドに説明を入力します（オプション）。
4. [Create New Condition (Advance Option)] を選択します。
5. [Attribute] ドロップダウン リストから、[Radius] -> [Called-Station-Id--[30]] を選択します。
6. [Operator] ドロップダウン リストから、[Matches] を選択します。
7. [Value] ドロップダウン リストから、[.*(:*(: Corporate)$] を選択します。 これは大文字と小文字が区別されます。
8. 右側の歯車をクリックし、[Add Attribute/Value] を選択します。
9. [Attribute] ドロップダウン リストから、[AD1] > [External Groups] を選択します。
10. [Operator] ドロップダウン リストから、[Equals] を選択します。
11. [Value] ドロップダウン リストから、必要なグループを選択します。 この例では、Domain Users に設定されています。
12. [Save] をクリックします。

注: このドキュメント全体で、[Policy] > [Policy Elements] > [Results] > [Authorization] > [Authorization Profiles] の下で設定した単純な許可プロファイルを使用します。 これらは [Permit Access] に設定されますが、導入のニーズに合うように変更できます。

これで条件を設定したため、許可ポリシーに適用します。 [Policy] > [Authorization] に移動します。 ルールを適切なロケーションのリストに挿入するか、既存のルールを編集します。

ゲスト ルール

1. 既存ルールの右にある下矢印をクリックし、[Insert a new rule] を選択します。
2. ゲスト ルールの名前を入力し、[Identity Groups] フィールドを [Any] に設定したままにしま

す。
3. [Conditions] の下で、プラスをクリックし、[Select Existing Condition from Library] をクリックします。
4. [Condition Name] の下で、[Simple Condition] > [GuestSSID] を選択します。
5. [Permissions] の下で、ゲスト ユーザの適切な許可プロファイルを選択します。
6. [Done] をクリックします。

企業ルール

1. 既存ルールの右にある下矢印をクリックし、[Insert a new rule] を選択します。
2. 企業ルールの名前を入力し、[Identity Groups] フィールドを [Any] に設定したままにします。
3. [Conditions] の下で、プラスをクリックし、[Select Existing Condition from Library] をクリックします。
4. [Condition Name] の下で、[Compound Condition] > [CorporateSSID] を選択します。
5. [Permissions] の下で、企業ユーザの適切な許可プロファイルを選択します。
6. [Done] をクリックします。
7. [Policy] リストの下部にある [Save] をクリックします。

注: [Policy List] の下部にある [Save] をクリックするまで、この画面で行った変更は、導入に適用されません。

確認

現在、この設定に使用できる確認手順はありません。

トラブルシューティング

ここでは、設定のトラブルシューティングに役立つ情報について説明します。

ポリシーが正しく作成されたことを確認し、ISE で適切な属性を受信しているかどうかを確認するには、成功または失敗したユーザ認証の詳細な認証レポートを調べます。 [Operations] > [Authentications] を選択してから認証の [Details] アイコンをクリックします。

まず、[Authentication Summary] を確認します。 これはユーザに示された許可プロファイルを含む認証の基本を示します。

ポリシーが正しくない場合、WLC から送信された [Airespace-Wlan-Id] および [Called-Station-Id] が [Authentication Details] に表示されます。 ルールを適宜調整します。 [Authorization Policy Matched Rule] で、認証が目的のルールに一致しているかどうかを確認します。

これらのルールは、誤設定の多いルールです。 設定の問題を特定するためには、認証の詳細に表示される内容とルールを照合します。 [Other Attributes] フィールドに属性が表示されない場合は、WLC が正しく設定されていることを確認します。

関連情報

- テクニカルサポートとドキュメント - Cisco Systems