シスコ セキュア アクセス ハウツー ガイド: 中央 Web 認証

現在のドキュメント バージョン: 4.0

2013 年 9 月 2 日

目次

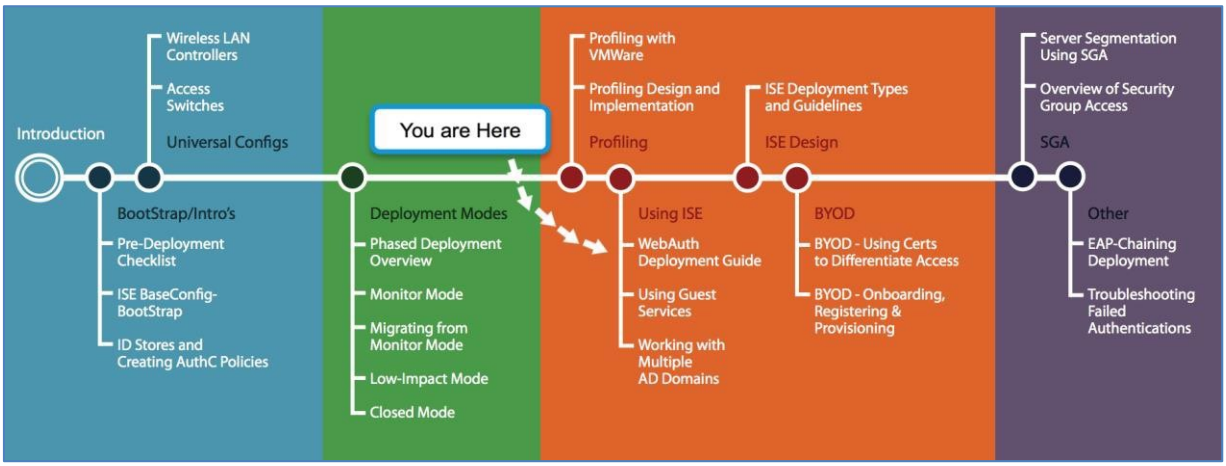
はじめに

シスコ セキュア アクセスを実現するハウツー ガイドについて

シリーズのハウツー ドキュメントは、シスコ セキュア アクセスの導入におけるベスト プラクティスを説明するために、シスコ セキュア アクセス チームによって作成されています。このシリーズのドキュメントは相互に関連して作られており、シスコ セキュア アクセス システムの導入を成功させるのに役立ちます。これらのドキュメントを参照することで、所定のパスに従ってシステム全体を展開したり、もしくは特定のニーズに合う個別の使用例を調べたりすることができます。

それぞれのガイドは、地下鉄の「現在地表示」の地図のようなスタイルをとっており、ドキュメントの扱う内容がどの段階にあたるのか、シスコ セキュア アクセスの導入手順のどこに該当するのかがわかりやすくなっています（図 1）。

図 1：ハウツー ガイドのナビゲーション マップ



シスコ セキュア アクセス認定の意義

シスコ セキュア アクセスの各バージョン番号（たとえば、シスコ セキュア アクセス バージョン 2.0、バージョン 2.1 など）は、設計またはアーキテクチャが認定済みであることを示しています。アーキテクチャを構成するすべてのテクノロジーは、完全なアーキテクチャ設計に基づく開発、および、ラボでのテストを経たものです。「シスコ セキュア アクセス認定」のマークがついたハウツー ガイドにおいては、ドキュメント内で言及されるすべての要素は次の基準を満たしている必要があります。

- 設計に組み込まれている製品は、一般的に使用できるものでなければならない。
- システム内のコンポーネントの導入、運用、管理については、繰り返し実施可能な手順を示さなければならない。
- 設計内で使用されているすべての設定と製品は、統合ソリューションとして完全にテスト済みでなければならない。

導入に役立つ可能性のある多くの機能がありますが、テスト済みのソリューションでない場合には、「シスコ セキュア アクセス認定」のマークがつくことはありません。シスコ セキュア アクセス チームは、新しい機能が利用できるようになった際に、ドキュメントにそれらの機能を加えられるように定期的に更新しています。また、シスコ セキュア アクセスのテスト計画、パイロット導入、システム リビジョンに統合しています。（たとえば、シスコ セキュア アクセス認定 2.2）。

また、テスト済みではあっても、ベスト プラクティスと見なされないために、このドキュメントに含まれていない多くの機能やシナリオがあります。たとえば、特定の IEEE 802.1X のタイマーや、ローカル Web 認証機能は含まれていません。

注：このマニュアルでは、推奨される導入方法と、お客様の環境で必要とされるセキュリティのレベルに応じたいくつかの異なるオプションについて説明します。これらの方法は、正常なプロジェクトの展開を支援するシスコのベスト プラクティスによって規定されたシスコ セキュア アクセスの導入に関する例であり、段階的な手順を示しています。

Web 認証

Web 認証を使用する理由

シスコ セキュア アクセス ソリューションでは、ユーザおよびデバイスの認証に 3 つのメカニズムを採用しています。

- IEEE 802.1X がプライマリの認証プロトコルとなり、サプリカントの組み込まれたエンドポイントとユーザに使用されます。
- IEEE 802.1X を実行できないエンドポイントの認証には、MAC 認証バイパス（MAB）が使用されます。この場合、すべての信頼済みエンドポイントについて、MAC アドレスのデータベースを維持することが必要です。
- Web 認証が 3 つ目のメカニズムになります。これは、Web ポータルがユーザに表示され、ユーザはそこで自分のクレデンシャルを送信し、ネットワークへの認証を受けます。

Web 認証は、主に次の状況で使用されます。

- 一時的なユーザの認証に使用

  組織は、ゲストや請負業者などの一時的なユーザにネットワーク アクセスを提供する必要があります。一時的なユーザは、多くの場合、組織の IT サービスでは制御できないデバイスを使用しています。その結果、一時的なユーザが IEEE 802.1X の設定されたエンドポイントを使用しないことになります。Web 認証は、このようなユーザを認証し、アクセプタブル ユース ポリシーへのユーザの同意を得る際に便利な方式です。一時的にアクセスするユーザを認証することで、そうしたユーザのアクティビティのモニタリングが可能になり、組織のコンプライアンス要件を遵守できるというメリットもあります。

- 通常のネットワーク ユーザに対する認証方式のフォールバックとして使用

  IEEE 802.1X が設定されているデバイスを使用する通常のネットワーク ユーザが認証に失敗することがよくあります。これは、パスワードや証明書の有効期限切れ、サプリカントの設定ミスなどさまざまな理由で発生する可能性があります。Web 認証を提供することで、そのようなユーザが自ら認証したり、IEEE 802.1X での認証を回避したりして問題を修正できるようになります。

- デバイス登録に使用

  ユーザがスマートフォンやタブレットなどの個人用デバイスを使用して、インターネットや他の企業アプリケーションにアクセスする場合があります。そのようなデバイスをすべてユーザと結び付け、ネットワーク リソースに適切にアクセスしていることを確認することは、IT 部門にとってますます重要になっています。Web 認証は、ユーザの個人用デバイスを登録するための手段として使用することができます。登録することで、そのデバイスに対して、組織のセキュリティ ポリシーや組織でのユーザ ロールに基づいて、ネットワーク リソースへのフル アクセスを認めたり、限定したりすることができます。

Web 認証のフロー

一般的な Web 認証のフローは、次のイベントで構成されます。

1. ユーザが、有線ネットワークに接続を試みます。ユーザは、ゲストや請負業者、もしくは IEEE 802.1X 認証に失敗した従業員になります。IEEE 802.1X 認証の失敗の理由としては、サプリカントの設定ミスやクレデンシャルの期限切れなどが挙げられます。
2. IEEE 802.1X がタイムアウトすると、スイッチは MAB を試行し、MAB にも失敗します。

3. この時点で、Web 認証が起動されます。Web 認証は、次の 2 つのいずれかの方法で行われます。

- ローカル Web 認証（LWA）

  LWA は、ネットワーク アクセス デバイス、スイッチ、ワイヤレス LAN コントローラ（WLC）が Web 認証をローカルで処理する際のプロセスです。この際、すべてのネットワーク アクセス デバイスは Web ポータルページで設定される必要があります。実稼働ネットワークのすべてのネットワーク アクセス デバイスで、Web ポータルの設定と制御を行うことは、難しい作業になります。LWA では、アクセス コントロール リスト（ACL）ベースの適用のみをサポートし、RADIUS の認可変更（CoA）はサポートしていません。RADIUS CoA には、プロファイルに基づいたポスチャの評価と適用が必要です。

- 中央 Web 認証（CWA）

  CWA は、Cisco Identity Services Engine（ISE）などのポリシー サーバが、Web 認証を通して中央でユーザを認証する際に使用されるプロセスです。Web 認証に中央ポリシー サーバを使用することで、運用面で導入がより簡単になります。CWA では、ACL と VLAN ベースでの適用の両方がサポートされます。また、RADIUS CoA もサポートされます。そのため、プロファイルに基づいたポスチャの評価と適用が可能となります。

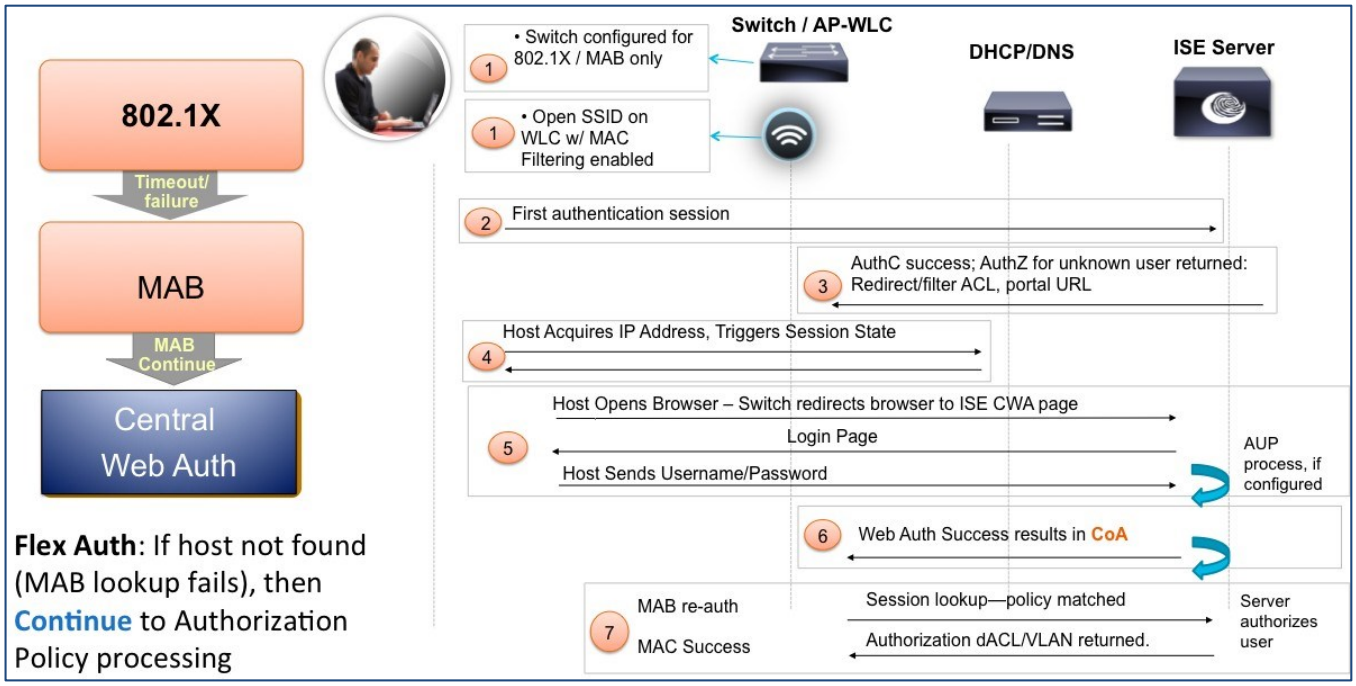
注：ワイヤレス ネットワークの CWA は、シスコ ワイヤレス LAN コントローラ ソフトウェア リリース 7.2 で導入されました

ワイヤレス ユーザの場合、Web 認証のフローが若干異なります。ワイヤレス ユーザは Web 認証のみ許可するように設定されたオープン SSID に接続します。つまり実質的には、ユーザがオープン SSID にアソシエーションした時点で、ユーザは Web 認証プロセスのステップ 3 を実施することになります。

シスコでは、CWA の使用を推奨しています。運用効率に優れていること、および、プロファイルに基づいたポスチャ評価や適用などの追加機能がサポートされていることがその理由です。本ドキュメントの範囲に限定して、ここでは CWA についてのみ説明します。ローカル Web 認証の詳細については、『Design and Implementation Guide』を参照してください。

図 2 は、CWA のフローの詳細について示しています。

図 2 中央 Web 認証プロセスのフロー



ステップ 1：シスコのスイッチで IEEE 802.1X と MAB が設定されています。Cisco WLC は、MAC フィルタリングが有効になった状態で、オープン SSID が設定されています。

注：スイッチと CWA 用の Cisco WLC の設定の詳細な手順については、次のハウツー ガイドを参照してください。

HowTo-10-Universal_Switch_Configuration

HowTo-11-Universal_WLC_Configuration

ステップ 2：ユーザが有線ポートに接続するか、ワイヤレスのオープン SSID とアソシエーションします。ユーザが有線ポートに接続する場合は、まず IEEE 802.1X がタイムアウトするか、失敗します。シスコ スイッチが MAB にフォールバックします。Cisco ISE は、内部のエンドポイントの ID ストアにエンドポイントを見つけられません。この時点で、Cisco ISE は、RADIUS のアクセス拒否メッセージをスイッチに送信する代わりに、アクセス許可メッセージを送信します。

ステップ 3：RADIUS のアクセス許可に沿って、Cisco ISE も、フィルタ ACL **PERMIT_ALL_TRAFFIC**、リダイレクト ACL **ACL-WEBAUTH-REDIRECT**、Web ポータルの URL をプッシュ ダウンします。RADIUS のアクセス許可により、スイッチは通常のネットワーク トラフィックに対してポートを開きますが、同時にポートとリダイレクト ACL に基づいて制限されます。

ステップ 4：エンドポイントは IP アドレスを取得し、DNS クエリを解決できるようになります。また、ISE の新しいセッションをトリガーします。このセッションは、一意なセッション ID を保持します。

ステップ 5：ユーザが Web ブラウザを起動させると、スイッチもしくは Cisco WLC が、ブラウザを ISE CWA の Web ポータル URL にリダイレクトします。この時点で、ユーザはクレデンシャルを入力し、設定されたアクセプタブル ユース ポリシー（AUP）を受け入れます。

ステップ 6：Cisco ISE が RADIUS の CoA メッセージをネットワーク アクセス デバイスに送信します。

ステップ 7：ネットワーク アクセス デバイスがエンドポイントを再認証し、前回作成されたものと同じセッションで接続させます。Cisco ISE は、ネットワーク アクセス デバイスに適切なアクセス ポリシーを送信します。

CWA 設定の説明

この項では、さまざまなリダイレクト/フィルタ ACL や Cisco ISE、シスコ スイッチ、シスコ ワイヤレス LAN コントローラで設定されたリダイレクト ポリシーがどのように動作して、CWA を有効にするかについて説明します。

注：詳細な設定手順については、次を参照してください。

スイッチ：『Global Switch Configuration』

WLC：『Base configuration for the Wireless LAN Controller』

シスコ スイッチで定義された CWA 用アクセス コントロール リスト

スイッチポート ACL

モニタ モード、低影響モードのどちらで導入しているかによって、**ACL-ALLOW** もしくは **ACL-DEFAULT** のいずれかになります。この ACL によって、リダイレクトの前に、どのトラフィックがポートを通過できるかが制御されます。この ACL は、Cisco IOS® ソフトウェアのデバイスに固有のものです。主に、**Authentication Open** コマンドが使用された際のトラフィックの制限に使用されます。

シスコ スイッチのリダイレクト ACL

リダイレクト ACL は **ACL-WEBAUTH-REDIRECT** になり、スイッチで次のように定義されています。

```
C3750X(config)#ip access-list ext ACL-WEBAUTH-REDIRECT
C3750X(config-ext-nacl)#remark explicitly deny DNS from being redirected to address a bug
C3750X(config-ext-nacl)#deny udp any any eq 53
C3750X(config-ext-nacl)#remark redirect all applicable traffic to the ISE Server
C3750X(config-ext-nacl)#permit tcp any any eq 80
C3750X(config-ext-nacl)#permit tcp any any eq 443
C3750X(config-ext-nacl)#remark all other traffic will be implicitly denied from the
redirection
```

Cisco ISE はスイッチに指示を出し、このリダイレクト ACL をベンダー固有の属性を介して呼び出します。ベンダー固有属性（VSA）は、ISE の認証プロファイルの一部として定義されます。この ACL により、スイッチが ISE へリダイレクトするトラフィックを特定でき、中央 Web 認証（CWA）が許可されるようになります。

Web 認証を機能させるためには、ホスト マシンが DHCP や DNS などの基本的なネットワーク サービスにアクセスできるようにすることが必要です。そのため、DHCP および DNS トラフィックがリダイレクトされないようにしなければなりません。**deny udp any any eq 53** のステートメントを ACL に追加し、スイッチがポート 53 の User Datagram Protocol（UDP）トラフィックのリダイレクトを拒否するようにします。そうすることで、ホスト マシンが DNS サービスにアクセスできるようになります。

注：シスコ スイッチでは、既存のバグにより DNS トラフィックがリダイレクトされます。スイッチが DNS トラフィックをリダイレクトしないようにするための回避手順が別途用意されています。

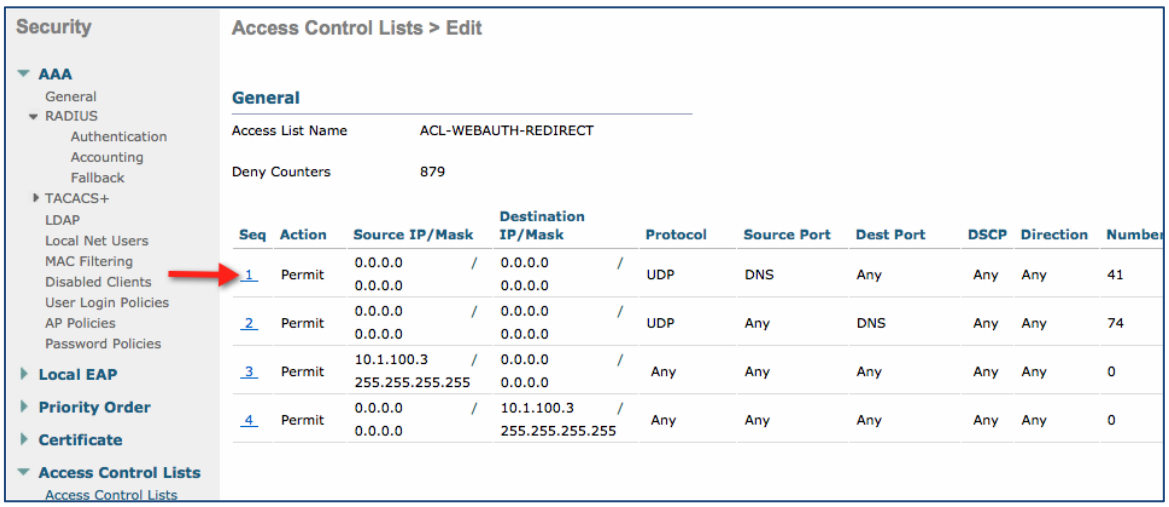
基本的なネットワーク サービスへのホスト マシンのアクセスを許可する一方で、ホストからのすべての Web トラフィックをリダイレクトする必要があります。**permit tcp any any eq 80** と **permit tcp any any eq 443** のステートメントを ACL に追加することで、スイッチが HTTP と HTTPS のトラフィックをリダイレクトするようにします。トラフィックのリダイレクト先の URL は、別の VSA で定義されており、それについては別途説明します。

シスコ WLC で定義された CWA 用アクセス コントロール リスト

1. Cisco WLC のリダイレクト ACL

Cisco WLC のリダイレクト ACL にも、**ACL-WEBAUTH-REDIRECT** という名前がつけられ、スイッチの設定との一貫性が確保されています。この ACL は、次に示すように定義されます。

図 3：Web 認証用のワイヤレス LAN コントローラの ACL



スイッチのリダイレクト ACL と WLC のリダイレクト ACL を比較すれば、その違いが確認できます。DNS トラフィックがリダイレクトされないようにするために、スイッチでは **deny udp any any eq 53** のステートメントを使用し、WLC では DNS トラフィックに対し、許可（permit）アクションを使用しています。これは、WLC のリダイレクト ACL が、標準ワイヤレス ACL であるためです。つまり、ACL ルールの許可（permit）ステートメントは、DNS や ISE（10.1.100.3）へのトラフィックのフローを許可するようになっているということです。そして、その他のすべてのトラフィックを、暗黙の拒否（deny）ステートメントで捕捉し、ISE で設定されているリダイレクト URL にリダイレクトします。この ACL は、ISE が認可プロファイルを利用して VSA を送信する際に呼び出されます。

ここまでをまとめます。

a. リダイレクト ACL（ACL-WEBAUTH-REDIRECT）は、シスコ スイッチと Cisco WLC の両方で、事前に設定されている必要があります。

b. リダイレクト ACL は、ISE の認可プロファイルで定義された VSA を通じて呼び出されます。

c. トラフィックのリダイレクト先の URL も、VSA として ISE の認可プロファイルで指定されます。

d. スイッチのリダイレクト ACL の定義の際には、拒否（deny）ステートメントでトラフィックをリダイレクトから除外し、許可（permit）ステートメントで特定のトラフィックをリダイレクトします。

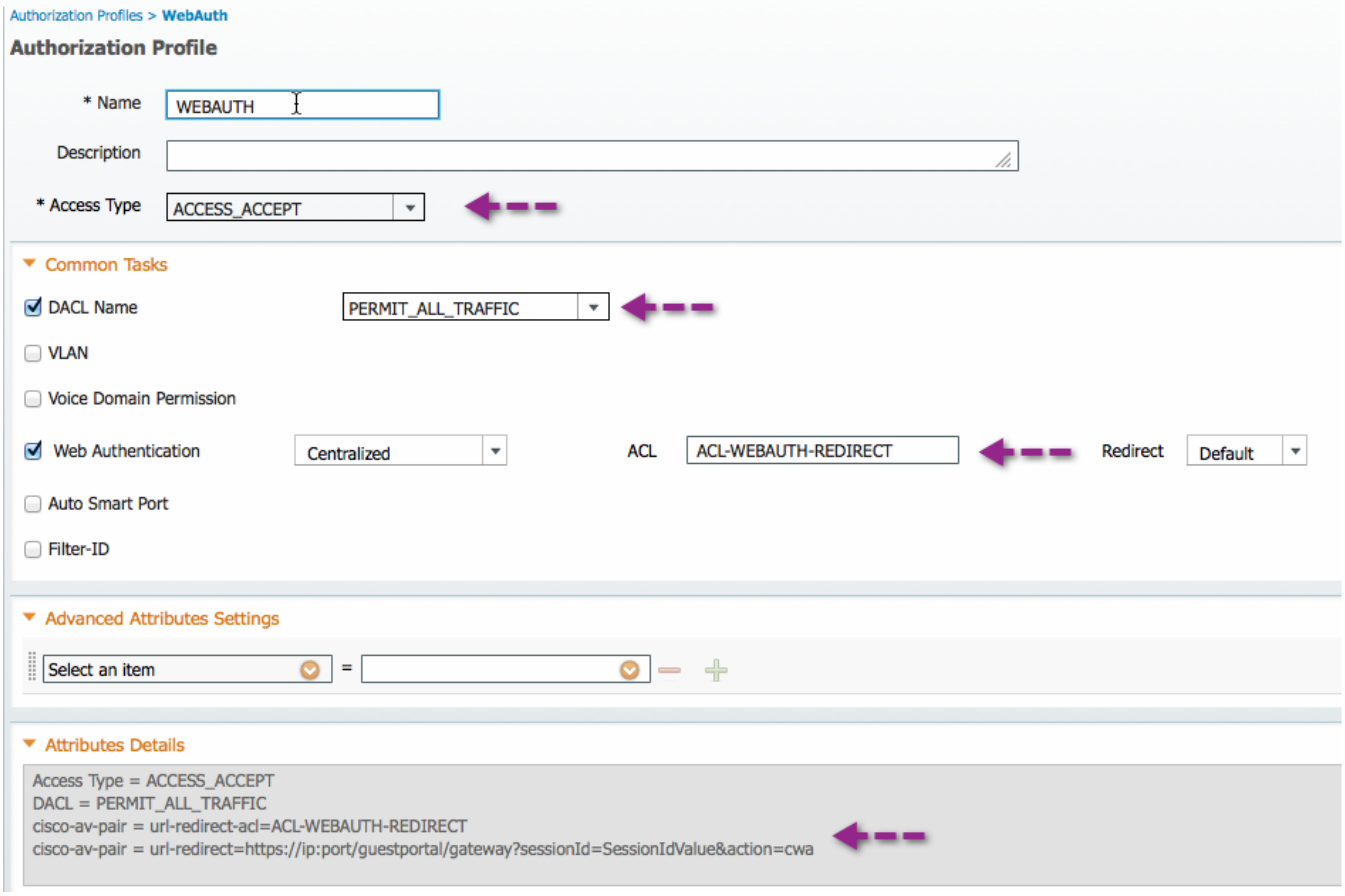
e. WLC のリダイレクト ACL は、標準のワイヤレス ACL です。許可ステートメントでトラフィックをリダイレクトから除外し、拒否（deny）ステートメントで特定のトラフィックをリダイレクトします。ACL の末尾には、暗黙的な拒否（deny）ステートメントがあります。

f. また、ISE の認可ポリシーでは、DACL を送信して既存の事前認証スイッチポート ACL を置き換えることもできます。

CWA 用の Cisco ISE 認可プロファイル

この項では、さまざまな ACL やリダイレクト URL を Cisco ISE の認可ポリシー内でどのように定義するかについて説明します。『Low-Impact how to guide』での設定に基づいた場合、WEBAUTH の ISE 認可プロファイルは、下の図のようになります。

図 4：ISE で定義された Web 認証の認可プロファイル



認可プロファイルには、次の設定がされています。

a. RADIUS access_accept

これは、スイッチポートに認証の成功を伝えるものです。その結果、スイッチがポートを開き、トラフィックの通過を許可します。

b. PERMIT_ALL_TRAFFIC DACL

これは、ダウンロード可能なスイッチポート ACL です。この ACL により、スイッチポートで設定された事前認証 ACL が置き換えられます。

c. Web 認証パラメータ

ここでは、3 つの異なるパラメータが存在します。まず、Web 認証方式に [中央（Centralized）] を設定します。次に、適用する ACL を指定します。スイッチではリダイレクト ACL を呼び出し、WLC ではワイヤレス ACL を呼び出します。[リダイレクト（redirect）] フィールドで、リダイレクト URL を指定します。今回は、デフォルトの ISE ゲスト ポータルを使用します。

なお、ポスチャの評価、サプリカントのプロビジョニング、デバイス登録に Web 認証を使用する際にも同じパラメータ セットを使用します。内容はそれぞれ変更する必要があります。

d. 属性の詳細

このセクションは、自動的に入力されます。使用されるベンダー固有属性が表示されます。ACL-WEBAUTH-REDIRECT を url-redirect-acl としてリストする方法を確認してください。url-redirect の値には、トラフィックのリダイレクト先の URL が指定されます。

付録 A:参考資料

セキュア アクセス システム:

http://www.cisco.com/en/US/products/ps11640/products_implementation_design_guides_list.html

デバイス設定ガイド:

Cisco Identity Services Engine User Guides:
http://www.cisco.com/en/US/products/ps11640/products_user_guide_list.html

Cisco IOS ソフトウェア、Cisco IOS XE ソフトウェア、および Cisco NX-OS ソフトウェアの各リリースの詳細情報については、次の URL を参照してください。

- Cisco Catalyst 2900 シリーズ スイッチの場合:
  http://www.cisco.com/en/US/products/ps6406/products_installation_and_configuration_guides_list.html
- Cisco Catalyst 3000 シリーズ スイッチの場合:
  http://www.cisco.com/en/US/products/ps7077/products_installation_and_configuration_guides_list.html
- Cisco Catalyst 3000-X シリーズ スイッチの場合:
  http://www.cisco.com/en/US/products/ps10745/products_installation_and_configuration_guides_list.html
- Cisco Catalyst 4500 シリーズ スイッチの場合:
  http://www.cisco.com/en/US/products/hw/switches/ps4324/products_installation_and_configuration_guides_list.html
- Cisco Catalyst 6500 シリーズ スイッチの場合:
  http://www.cisco.com/en/US/products/hw/switches/ps708/products_installation_and_configuration_guides_list.html
- Cisco ASR 1000 シリーズ ルータの場合:
  http://www.cisco.com/en/US/products/ps9343/products_installation_and_configuration_guides_list.html

Cisco Wireless LAN Controller の場合:http://www.cisco.com/en/US/docs/wireless/controller/7.2/configuration/guide/cg.html