Identity Services Engine を使用したワイヤレス BYOD

目次

概要

Cisco Identity Services Engine（ISE）は、Cisco TrustSec ソリューションに認証および許可のインフラストラクチャを提供するシスコの次世代のポリシー サーバです。 また、これは次の他の 2 つの重要なサービスを提供します。

- 最初のサービスは、Cisco ISE がさまざまな情報源から受信した属性に基づいてエンドポイント デバイスのタイプを自動的にプロファイルする方法を提供することです。 このサービス（プロファイラと呼ばれる）は、シスコが以前に Cisco NAC Profiler アプライアンスによって提供していた機能に相当する機能を提供します。
- Cisco ISE が提供するもう 1 つの重要なサービスは、エンドポイントのコンプライアンス、たとえば AV/AS ソフトウェアのインストールおよびその定義ファイルの有効性（ポスチャとして既知）をスキャンすることです。 シスコでは、以前に Cisco NAC アプライアンスでのみこの追加のポスチャ機能が提供されています。

Cisco ISE は同等のレベルの機能を提供し、802.1X 認証メカニズムと統合されます。

ワイヤレス LAN コントローラ（WLC）に付属している Cisco ISE は、Apple iDevice（iPhone、iPad、および iPod）、Android ベースのスマートフォンなどのモバイル デバイスのプロファイル メカニズムを提供できます。 802.1X ユーザのために、Cisco ISE は同じレベルのプロファイルおよびポスチャ スキャンなどのサービスを提供できます。 Cisco ISE のゲスト サービスも、認証用の Cisco ISE に Web 認証要求をリダイレクトすることでの方向を変更することで Cisco WLC と統合されることもできます。

このドキュメントでは、既知のエンドポイントおよびユーザ ポリシーに基づいた区別されたアクセスの提供などの、Bring Your Own Device（BYOD; 個人所有デバイス持ち込み）のワイヤレス ソリューションを説明します。 このドキュメントでは、BYOD の完全なソリューションは提供しませんが、ダイナミック アクセスの簡単な使用例を示します。 他の設定例は、特権ユーザがワイヤレス ゲスト アクセスをプロビジョニングするためにゲストに保証できる ISE スポンサー ポータルの使用などです。

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。

- ソフトウェア バージョン 7.2.103 を搭載した Cisco Wireless LAN Controller 2504 または 2106
- Catalyst 3560：8 ポート
- WLC 2504
- Identity Services Engine 1.0MR（VMware サーバ イメージのバージョン）
- Windows 2008 サーバ（VMware のイメージ）：512 M、20 GB ディスクActive DirectoryDNSDHCP証明書サービス

トポロジ

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。

ワイヤレス LAN コントローラ RADIUS NAC および CoA の概要

この設定は、ISE RADIUS サーバからの URL リダイレクトの AV-Pair を WLC が探すことを可能にします。 これは、有効な RADIUS NAC 設定のあるインターフェイスに関連付けられている WLAN 上だけです。 URL リダイレクトのための Cisco AV ペアが受信されると、クライアントは POSTURE_REQD の状態になります。 これは基本的に、コントローラ内の WEBAUTH_REQD 状態と内部的に同じです。

ISE RADIUS サーバがクライアントが Posture_Compliant だとみなすと、CoA ReAuth を発行します。 Session_ID が共に関連付けられるために使用されます。 この新しい AuthC（re-Auth）によって、URL Redirec AV-Pair が送信されません。 URL リダイレクト AV-Pairs がないので、WLC はクライアントがもうポスチャを必要としていないことを確認します。

RADIUS NAC の設定が有効になっていない場合、WLC は URL リダイレクト VSA を無視します。

CoA-ReAuth： これは RFC 3576 設定で有効になります。 ReAuth 機能は、以前にサポートされる既存の CoA コマンドに追加されました。

RADIUS NAC の設定は CoA が機能するように要求されますが、この機能から相互に排他的です。

Pre-Posture ACL： クライアントが POSTURE_REQ 状態にある場合、WLC のデフォルトの動作は DHCP/DNS を除くすべてのトラフィックを妨げることです。 Pre-Posture ACL（url-redirect-acl AV-Pair での呼び名）はクライアントに適用され、ACL で許可されるものはクライアントが到達できるものです。

Pre-Auth ACL と VLAN オーバーライド： 検疫または Access-VLAN とは異なる AuthC VLAN は 7.0MR1 ではサポートされません。 ポリシー サーバからの VLAN を設定した場合は、セッション全体に対する VLAN です。 最初の AuthZ 後は VLAN の変更は必要ありません。

ワイヤレス LAN コントローラ RADIUS NAC および CoA の機能のフロー

次の図は、クライアントがバックエンド サーバと NAC のポスチャ検証に対して認証された場合のメッセージ交換の詳細を説明しています。

1. クライアントは、dot1x の認証を使用して認証します。
2. RADIUS アクセス アクセプトは、ポート 80 のリダイレクトされた URL、および許可する IP アドレスおよびポート、または検疫 VLAN を含む pre-auth ACL を転送します。
3. クライアントはアクセス アクセプトで提供された URL にリダイレクトされ、ポスチャ検証が終了するまで新しい状態になります。 この状態のクライアントは ISE サーバと通信し、ISE NAC サーバで設定されたポリシーに対してそれ自身を検証します。
4. クライアントの NAC エージェントはポスチャ検証（ポート 80 へのトラフィック）を開始します。 エージェントは、アクセス アクセプトで提供される URL にコントローラをリダイレクトするポート 80 に HTTP Discovery リクエストを送信します。 ISE は、到達しようとしているクライアントを認識し、クライアントに直接応答します。 この方法でクライアントは ISE サーバ IP について学習し、それ以降クライアントは ISE サーバと直接通信します。
5. ACL はこのトラフィックを許可するように設定されているため、WLC はこのトラフィックを許可します。 VLAN オーバーライドの場合、トラフィックは ISE サーバに到達できるようにブリッジされます。
6. ISE クライアントが評価を完了すると、再認証サービス付きの RADIUS CoA Req が WLC に送信されます。 これは、クライアントの再認証を開始します（EAP-START を送信）。再認証が成功した場合は、ISE は新しい ACL（存在する場合）を使って URL のリダイレクトなしでアクセス アクセプトを送信するか、または VAN にアクセスします。
7. WLC は、RFC 3576 のとおりに CoA Req および Disconnect-Req をサポートします。 WLC は、RFC 5176 のとおりに再認証サービスに対する CoA-Req をサポートする必要があります。
8. ダウンロード可能 ACL の代わりに、事前設定された ACL が WLC で使用されます。 ISE サーバは、コントローラですでに設定されている ACL の名前だけを送信します。
9. この設計は、VLAN および ACL の両方のケースで動作します。 VLAN オーバーライドの場合は、ここではポート 80 をリダイレクトするだけで、検疫 VLAN の残りのトラフィックを許可（ブリッジ）します。 ACL については、アクセス アクセプトで受信される事前認証 ACL が適用されます。

次の図に、この機能のフローを仮想的に表現します。

ISE のプロファイル概要

Cisco ISE プロファイラ サービスは、企業ネットワークへの適切なアクセスのセキュリティと保守を確保するために、デバイス タイプに関係なく、ネットワークに接続されたすべてのエンドポイントの機能を検出、検索、および判断する機能を提供します。 主にネットワーク上のすべてのエンドポイントの属性または一連の属性を収集し、エンドポイントをそのプロファイルに従って分類します。

プロファイラは次のコンポーネントから構成されます。

- センサーには、さまざまなプローブが含まれています。 プローブはネットワーク アクセス デバイスに問い合わせてネットワーク パケットをキャプチャし、収集した属性およびその属性値をエンドポイントからアナライザに転送します。
- アナライザは、収集した属性と属性値に一致するように設定したポリシーとアイデンティティ グループを使用してエンドポイントを評価し、エンドポイントを指定されたグループに分

類して一致したプロファイルを使用して Cisco ISE データベースにエンドポイントを保存します。

モバイル デバイスを検出するには、適切なデバイス ID に次のプローブの組み合わせを使用することが推奨されます。

- RADIUS Calling-Station-ID： MAC アドレス（OUI）を提供
- DHCP（ホスト名）： ホスト名：デフォルトのホスト名は、次の例のようなデバイス タイプを含めることができます。 例： jsmith-ipad
- DNS（逆 IP 参照）： FQDN：デフォルトのホスト名はデバイス タイプを含むことができます。
- HTTP（User-Agent）： 特定のモバイル デバイス タイプの詳細

iPad の例では、リクエスト メッセージからの HTTP 属性と同じように、プロファイラはユーザ エージェントの属性から Web ブラウザ情報をキャプチャし、それをエンドポイント属性のリストに追加します。

内部アイデンティティ ユーザの作成

MS Active Directory（AD）は、単純な概念検証には必要ありません。 ISE は唯一の ID ストアとして使用でき、アクセスおよびより細かい制御ポリシーに対するユーザ アクセスの区別を含みます。

ISE 1.0 のリリースでは、AD の統合を使用して、ISE は許可ポリシーで AD のグループを使用できます。 ISE 内部ユーザのストア（AD の統合のない）が使用されている場合、グループはデバイス ID のグループ（ISE 1.1 で解決される識別されたバグ）と組み合わせてポリシーに使用することはできません。 したがって、デバイス ID のグループに加えて使用すると、専用従業員または請負業者など個々のユーザのみに区別できます。

次の手順を実行します。

1. https://ISEip アドレスに対してブラウザ ウィンドウを開きます。
2. [Administration] > [Identity Management] > [Identities] の順に移動します。
3. [Users] を選択し、[Add] をクリックします（ネットワーク アクセスユーザ）。 これらのユーザの値を入力し、従業員のグループに割り当てます。[Name]： 従業員パスワード： XXXX
4. [Submit] をクリックします。[Name]： 建築業者パスワード： XXXX
5. 両方のアカウントを確認します。

ワイヤレス LAN コントローラの ISE への追加

ISE に RADIUS 要求を開始したデバイスは、ISE に定義がある必要があります。 これらのネットワーク デバイスは、IP アドレスに基づいて定義されます。 ISE ネットワーク デバイス定義には、複数の実際の機器を表すために定義する IP アドレス範囲を指定できます。

RADIUS の通信に必要なものを超えて、ISE ネットワーク デバイス定義は SNMP および SSH などの他の ISE/デバイス通信の設定を含みます。

ネットワーク デバイス定義のもう一つの重要な側面は、適切にグループ化して、これがネットワーク アクセス ポリシーに利用できるようにデバイスをグループ化しています。

この演習では、ラボに必要なデバイスの定義が設定されます。

次の手順を実行します。

1. ISE から [Administration] > [Network Resources] > [Network Devices] の順に移動します。
2. [Network Devices] で、[Add] をクリックします。 IP アドレスを入力し、[Authentication Setting] をマスク チェックし、次に共有秘密の「cisco」を入力します。
3. WLC エントリを保存し、リストのコントローラを確認します。

ISE のワイヤレス認証の設定

ISE は 802.1x ワイヤレス クライアントを認証するように設定され、ID ストアとして Active Directory を使用する必要があります。

次の手順を実行します。

1. ISE から [Policy] > [Authentication] に移動します。
2. 展開するために [Dot1x] > [Wired_802.1X (-)] の順にクリックします。
3. 歯車アイコンをクリックして [Add Condition from Library] に移動します。
4. 条件選択のドロップダウンから [Compound Condition] > [Wireless_802.1X] の順に選択します。
5. 式の条件を [OR] に設定します。
6. 許可プロトコル オプションの後で展開し、デフォルトの内部ユーザ (デフォルト) を受け入れます。
7. 他はすべてデフォルトのままにします。 手順を完了するには、[Save] をクリックします。

ブートストラップ ワイヤレス LAN コントローラ

WLC のネットワークへの接続

Cisco 2500 ワイヤレス LAN コントローラ導入ガイドは、『Cisco 2500 シリーズ ワイヤレス コントローラ導入ガイド』でも使用できます。

スタートアップ ウィザードを使用したコントローラの設定

```
(Cisco Controller)
 Welcome to the Cisco Wizard Configuration Tool Use the '-' character to backup
 Would you like to terminate autoinstall? [yes]: yes AUTO-INSTALL: process terminated
-- no configuration loaded System Name [Cisco_d9:24:44] (31 characters max):
   ISE-Podx Enter Administrative User Name (24 characters max): admin
   Enter Administrative Password
   (3 to 24 characters): Cisco123
   Re-enter Administrative Password: Cisco123
Management Interface IP Address: 10.10.10.5
Management Interface Netmask: 255.255.255.0
Management Interface Default Router: 10.10.10.1
Management Interface VLAN Identifier (0 = untagged): 0
Management Interface Port Num [1 to 4]: 1
Management Interface DHCP Server IP Address: 10.10.10.10
 Virtual Gateway IP Address: 1.1.1.1
Mobility/RF Group Name: ISE
```

```
 Network Name (SSID): PODx
Configure DHCP Bridging Mode [yes][NO]: no
Allow Static IP Addresses [YES][no]: no
 Configure a RADIUS Server now? [YES][no]: no
Warning! The default WLAN security policy requires a RADIUS server.
Please see documentation for more details.
 Enter Country Code list (enter 'help' for a list of countries) [US]: US

Enable 802.11b Network [YES][no]: yes
Enable 802.11a Network [YES][no]: yes
Enable 802.11g Network [YES][no]: yes
Enable Auto-RF [YES][no]: yes
 Configure a NTP server now? [YES][no]: no
Configure the ntp system time now? [YES][no]: yes
Enter the date in MM/DD/YY format: mm/dd/yy
Enter the time in HH:MM:SS format: hh:mm:ss
Configuration correct? If yes, system will save it and reset. [yes][NO]: yes
 Configuration saved!
 Resetting system with new configuration...
Restarting system.
```

ネイバー スイッチの設定

コントローラは、ネイバー スイッチ (ファスト イーサネット 1) のイーサネット ポートに接続されています。 ネイバー スイッチのポートは 802.1Q トランクとして設定され、そのトランク上のすべての VLAN を許可します。 ネイティブ VLAN 10 により、WLC の管理インターフェイスが接続できます。

802.1Q スイッチ ポートの設定は次のとおりです。

```
switchport
switchport trunk encapsulation dot1q
switchport trunk native VLAN 10
switchport mode trunk
end
```

WLC への認証サーバ (ISE) の追加

ISE は、ワイヤレス エンドポイントの 802.1X および CoA の機能を有効にするために、WLC に追加する必要があります。

次の手順を実行します。

1. ブラウザを開き、次に POD WLC (セキュア HTTP を使用して) に接続した後 https://wlc に接続します。
2. [Security] > [Authentication] > [New] の順に移動します。
3. 次の値を入力してください。[Server IP address]： 10.10.10.70 (チェックの割り当て) [Shared Secret]： cisco[Support for RFC 3576 (CoA)]： Enabled (デフォルト) その他すべて： デフォルト
4. [Apply] をクリックして継続します。
5. [RADIUS Accounting] > [add NEW] の順に選択します。
6. 次の値を入力してください。[Server IP address]： 10.10.10.70[Shared Secret]： ciscoその他すべて： デフォルト
7. [Apply] をクリックし、WLC の設定を保存します。

WLC の従業員のダイナミック インターフェイスを作成

WLC 用の新しいダイナミック インターフェイスを追加し、従業員 VLAN にマッピングするには、次の手順を実行してください。

1. WLC で、[Controller] > [Interfaces] の順に移動します。 次に [New] をクリックします。
2. WLC で、[Controller] > [Interfaces] の順に移動します。 次の内容を入力します。[Interface Name]： Employee[VLAN ID]： 11
3. [Enter the following for Employee interface]：[Port Numbe]： 1[VLAN Identifier]： 11IP アドレス： 10.10.11.5[Netmask]： 255.255.255.0ゲートウェイ： 10.10.11.1DHCP: 10.10.10.10
4. 新規従業員のダイナミック インターフェイスが作成されたことを確認します。

WLC のゲストのダイナミック インターフェイスを作成

WLC 用の新しいダイナミック インターフェイスを追加し、ゲスト VLAN にマッピングするには、次の手順を実行してください。

1. WLC で、[Controller] > [Interfaces] の順に移動します。 次に [New] をクリックします。
2. WLC で、[Controller] > [Interfaces] の順に移動します。 次の内容を入力します。[Interface Name]： ゲスト[VLAN ID]： 12
3. [Enter these for Guest interface]：[Port Numbe]： 1[VLAN Identifier]： 12IP アドレス： 10.10.12.5[Netmask]： 255.255.255.0ゲートウェイ： 10.10.12.1DHCP: 10.10.10.10
4. ゲストのインターフェイスが追加されたことを確認します。

802.1x WLAN の追加

WLC の初期ブートストラップから、デフォルト WLAN が作成されてる場合があります。 その場合は、修正するか、またはガイドの手順に従ってワイヤレス 802.1X 認証をサポートする新しい WLAN を作成します。

次の手順を実行します。

1. WLC で、[WLAN] > [Create New] に移動します。
2. WLAN の場合、次のように入力してください.[Profile Name]： pod1x[SSID]： 同左
3. [WLAN setting] の [General] タブで、次を使用します。[Radio Policy]： All[Interface/Group]： 管理その他すべて： デフォルト
4. [WLAN] の [Security] タブの [Layer 2] で、次を設定します。[Layer 2 Security]：WPA + WPA2WPA2 Policy / Encryption： Enabled / AES[Auth Key Mgmt]： 802.1X
5. [WLAN] の [Security] タブの [AAA Servers] で、次を設定します。[Radio Server Overwrite Interface]： Disabled[Authentication/Accounting Servers]： Enabled[Server 1]： 10.10.10.70
6. [WLAN] の [Advanced] タブで、次を設定します。[Allow AAA Override]： Enabled[NAC State]： RADIUS NAC（選択済み）
7. [WLAN] に戻り、[General] タブで [Enable WLAN]（チェックボックス）をオンにします。

WLC ダイナミック インターフェイスのテスト

有効な従業員とゲストのインターフェイスの簡易チェックを行う必要があります。 WLAN に関連

付けられているデバイスを使用し、WLAN インターフェイスの割り当てを変更します。

1. WLC で、[WLAN] > [WLANs] に移動します。 以前の演習で作成されたセキュアな SSID を編集するためにクリックします。
2. インターフェイスまたはインターフェイス グループを [Employee] に変更し、[Apply] をクリックします。
3. 正しく設定されている場合、デバイスは従業員 VLAN (10.10.11.0/24) から IP アドレスを受け取ります。 この例では新しい IP アドレスを取得する iOS のデバイスを示しています。
4. 前のインターフェイスが確認されたら、WLAN インターフェイスの割り当てを [Guest] に変更し、[Apply] をクリックします。
5. 正しく設定されている場合、デバイスはゲスト VLAN (10.10.12.0/24) から IP アドレスを受け取ります。 この例では新しい IP アドレスを取得する iOS のデバイスを示しています。
6. **重要：** 元の管理にインターフェイスの割り当てを戻します。
7. [Apply] クリックし、WLC の設定を保存します。

iOS (iPhone または iPad) のワイヤレス認証

iPhone、iPad、または iPod のような iOS デバイスを使用している内部ユーザ (または統合された、AD ユーザ) を認証された SSID で WLC に関連付けます。 適応しない場合は、次の手順をとばしてください。

1. iOS デバイスで、[WLAN setting] に移動します。 WiFi を有効にし、前のセクションで作成した 802.1X が有効な SSID を選択します。
2. 接続するには次の情報を提供してください。ユーザ名： employee (内部：従業員) または contractor (内部：契約作業員) パスワード： XXXX
3. ISE 証明書を受け入れるようにクリックします。
4. iOS デバイスが管理 (VLAN10) インターフェイスから IP アドレスを取得していることを確認します。
5. [WLC] > [Monitor] > [Clients] で、使用、国家、および EAP タイプなどのエンドポイント情報を確認します。
6. 同様に、クライアント情報は、[ISE] > [Monitor] > [Authentication] ページで提供されている可能性があります。
7. [Details] アイコンをクリックして、セッションの詳細情報のセッションまでドリルダウンます。

ポスチャ リダイレクト ACL の WLC への追加

ポスチャのリダイレクト ACL は、ISE がポスチャのクライアントをリダイレクトするために使用する WLC で設定されます。 効果的にそして最小限で ACL は ISE との間のトラフィックを許可します。 任意選択ルールは、この ACL で必要に応じて追加できます。

1. [WLC] > [Security] > [Access Control Lists] > [Access Control Lists] に順に移動します。 [New] をクリックします。
2. ACL に名前 (ACL-POSTURE-REDIRECT) を入力します。
3. 新しい ACL で [Add New Rule] をクリックします。 ACL シーケンス #1 に次の値を設定します。 最後に、[Apply] をクリックします出典： [Any]Destination： IP Address 10.10.10.70, 255.255.255.255プロトコル： [Any]アクション： 許可

4. シーケンスが追加されていることを確認します。
5. [Add New Rule] をクリックします。 ACL シーケンス #2 に次の値を設定します。 最後に、[Apply] をクリックします出典： IP Address 10.10.10.70, 255.255.255.255Destination：[Any]プロトコル： [Any]アクション： 許可
6. シーケンスが追加されていることを確認します。
7. ACL シーケンス #3 に次の値を設定します。 最後に、[Apply] をクリックします出典：[Any]Destination： [Any]プロトコル： UDP[Source Port]： DNS[Destination Port]： [Any]アクション： 許可
8. シーケンスが追加されていることを確認します。
9. [Add New Rule] をクリックします。 ACL シーケンス #4 に次の値を設定します。 最後に、[Apply] をクリックします出典： [Any]Destination： [Any]プロトコル： UDP[Source Port]：[Any][Destination Port]： DNSアクション： 許可
10. シーケンスが追加されていることを確認します。
11. 現在の WLC の設定を保存します。

ISE のプロファイル プローブの有効化

ISE は、効果的にエンドポイントのプロファイルを作成するプローブとして設定する必要があります。 デフォルトでは、これらのオプションは無効になります。 この項では、プローブに ISE を設定する方法を示します。

1. ISE 管理から、[Administration] > [System] > [Deployment] の順に移動します。
2. [ISE] を選択します。 [Edit ISE host] をクリックします。
3. [Edit Node] ページから [Profiling Configuration] を選択し、次の設定を行います。DHCP: Enabled、All（またはデフォルト）[DHCPSPAN]： Enabled、All（またはデフォルト）HTTP: Enabled、All（またはデフォルト）RADIUS: Enabled、N/A[DNS]： Enabled、N/A
4. デバイス（iPhone/iPad/Droid/Mac など）を再関連付けします。
5. ISE エンドポイントのアイデンティティを確認します。 [Administration] > [Identity Management] > [Identities] の順に移動します。 [Endpoints] をクリックし何がプロファイルにあるかリストします。**注:** 最初のプロファイルは RADIUS プローブからです。

デバイスの ISE プロファイル ポリシーの有効化

すぐに使用可能で、ISE はさまざまなエンドポイント プロファイルのライブラリを提供します。デバイスのプロファイルを有効にするには、次の手順を実行してください。

1. ISE から、[Policy] > [Profiling] の順に移動します。
2. 左側のペインで、[Profiling Policies] を展開します。
3. [Apple Device] > [Apple iPad] の順にクリックし、次の設定を行います。[Policy Enabled]：Enabled[Create Matching Identity Group]： オン
4. [Apple Device] > [Apple iPhone] の順にクリックし、次の設定を行います。[Policy Enabled]： Enabled[Create Matching Identity Group]： オン
5. [Android] をクリックし、次の設定を行います。[Policy Enabled]： Enabled[Create Matching Identity Group]： オン

ポスチャ検出リダイレクトのための ISE 許可プロファイル

適切な検索とプロファイルのために新しいデバイスが ISE にリダイレクトできる許可ポリシーのポスチャのリダイレクトを設定するには、次の手順を実行してください:

1. ISE から、[Policy] > [Policy Elements] > [Results] の順に移動します。
2. [Authorization] を展開します。 [Authorization Profiles] (左のペイン) をクリックし、[Add] をクリックします。
3. 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。[Name] : Posture_Remediation[Access Type] : Access_Accept[Common Tools] : Posture Discovery、EnabledPosture Discovery、ACL ACL-POSTURE-REDIRECT
4. この作業を完了するには、[Submit] をクリックします。
5. 新しい許可プロファイルが追加されていることを確認します。

従業員の ISE 許可プロファイルの作成

従業員に許可プロファイルを追加すると、ISE は許可され割り当てられている属性へのアクセスが許可されます。 この場合は、従業員 VLAN 11 が割り当てられます。

次の手順を実行します。

1. ISE から、[Policy] > [Results] の順に移動します。 [Authorization] を展開し、次に [Authorization Profiles] をクリックしてから [Add] をクリックします。
2. 従業員の許可プロファイルに次のように入力します。[Name] : Employee_Wireless[Common Tasks] : VLAN、EnabledVLAN、予備値 11
3. この作業を完了するには、[Submit] をクリックします。
4. 新規従業員の許可プロファイルが作成されたことを確認します。

契約作業員の ISE 許可プロファイルの作成

契約作業員に許可プロファイルを追加すると、ISE は許可され割り当てられている属性へのアクセスが許可されます。 この場合は、契約作業員 VLAN 12 が割り当てられます。

次の手順を実行します。

1. ISE から、[Policy] > [Results] の順に移動します。 [Authorization] を展開し、次に [Authorization Profiles] をクリックしてから [Add] をクリックします。
2. 従業員の許可プロファイルに次のように入力します。[Name] : Employee_Wireless[Common Tasks] : VLAN、EnabledVLAN、予備値 12
3. この作業を完了するには、[Submit] をクリックします。
4. 契約作業員の許可プロファイルが作成されたことを確認します。

デバイスのポスチャ/プロファイルのための許可ポリシー

新しいデバイスが初めてネットワークに現れたときはそのデバイスに関する情報はほとんどわからないので、管理者はアクセスを許可する前に未知のエンドポイントを識別できるように適切なポリシーを作成します。 この例では、新しいデバイスがポスチャ評価のために ISE にリダイレクトできるように許可ポリシーが作成されます (モバイル デバイスはエージェントがないのでプロファイルのみが関連します)。 エンドポイントは ISE キャプティブ ポータルにリダイレクトされ、識別されます。

次の手順を実行します。

1. ISE から、[Policy] > [Authorization] の順に移動します。
2. プロファイルの作成されたシスコの IP 電話のポリシーがあります。 これはすぐに使用できます。 ポスチャのポリシーとしてこれを編集します。
3. このポリシーに次の値を入力してください。[Rule Name]： Posture_Remediation[Identity Groups]： [Any][Other Conditions] > [Create New]： （詳細）[Session] > [PostureStatus][PostureStatus] > [Equals]： unknown
4. アクセス許可のために次の設定をします：[Permissions] > [Standard] Posture_Remediation
5. [Save] をクリックします。**注:** 代わりに、使いやすさを追加するカスタム ポリシーの要素を作成できます。

ポスチャ修復ポリシーのテスト

ISE が正しくポスチャのポリシーに基づいて新しいデバイスのプロファイルを作成していることを示すために簡単なデモンストレーションを実行できます。

1. ISE から、[Administration] > [Identity Management] > [Identities] の順に移動します。
2. [Endpoints] をクリックします。 デバイス（この例では iPhone）を関連付け、接続します。
3. エンドポイントのリストを更新します。 どのような情報が与えられているか確認します。
4. エンドポイント デバイスから、次を参照します。URL: http://www（または 10.10.10.10）デバイスがリダイレクトされます。 証明書のプロンプトを受け入れます。
5. モバイル デバイスが完全にリダイレクトされたら、ISE からエンドポイント リストが再び表示されます。 変更内容を確認します。 前のエンドポイント（たとえば、Apple-Device）は、「Apple-iPhone」などに変更する必要があります。 これは、キャプティブ ポータルにリダイレクトされるプロセスの一部として HTTP プローブが効果的にユーザ エージェント情報を取得したためです。

差別化したアクセスの許可ポリシー

正常にポスチャの許可をテストしてから、既知のデバイスを持ち、ユーザ ロール（この場合、従業員と契約作業員）に特化したさまざまな VLAN 割り当てのある従業員と契約作業員に区別されたアクセスをサポートするために続けてポリシーを作成します。

次の手順を実行します。

1. [ISE] > [Policy] > [Authorization] の順に移動します。
2. [Posture Remediation] ポリシー/行の上に新しいルールを追加または挿入します。
3. このポリシーに次の値を入力してください。[Rule Name]： Employee[Identity Groups (expand)]： Endpoint Identity Groups[Endpoint Identity Groups]： Profiled[Profiled]： Android、Apple iPad、または Apple iPhone
4. 追加デバイス タイプを指定するには、[+] をクリックしてさらにデバイスを追加します（必要な場合）。[Endpoint Identity Groups]： Profiled[Profiled]： Android、Apple iPad、または Apple iPhone
5. このポリシーの次のアクセス権限の値を指定します。[Other Conditions (expand)]： Create New Condition（[Advanced Option]）[Condition] > [Expression]（リストから）： [InternalUser] > [Name][InternalUser] > [Name]： 従業員

6. ポスチャ セッション コンプライアンスの条件の追加：[Permissions] > [Profiles] > [Standard]： Employee_Wireless
7. [Save] をクリックします。 ポリシーが正常に追加されたことを確認します。
8. 契約作業員のポリシーを追加して続行します。 このドキュメントでは、プロセスを容易にするために、前のポリシーが複製されます（つまり、適切な結果のために手動で設定できます）。[Employee policy] > [Actions] に移動し、[Duplicate Below] をクリックします。
9. このポリシー（重複コピー）の次のフィールドを編集します。[Rule Name]： Contractor[Other Conditions] > [InternalUser] > [Name]： 建築業者[Permissions]： Contractor_Wireless
10. [Save] をクリックします。 前の複製コピー（または新しいポリシー）が正しく設定されていることを確認します。
11. ポリシーをプレビューするには、[Policy-at-a-Glance] をクリックします。ポリシーの一覧では、統合され要約されポリシーが見やすくなっています。

差別化したアクセスの CoA のテスト

アクセスを区別するために準備された許可プロファイルおよびポリシーを使って、テストします。 単一の安全な WLAN があり、1 人の従業員が従業員 VLAN に割り当てられ、1 人の契約作業者が契約作業員 VLAN に割り当てられます。 Apple の iPhone または iPad は、次の例で使用されます。

次の手順を実行します。

1. 安全な WLAN（POD1x）にモバイル デバイスで接続し、次のクレデンシャルを使用します。ユーザ名： 従業員パスワード： XXXXX
2. [Join] をクリックします。 従業員が割り当てられた VLAN 11（従業員 VLAN）であることを確認します。
3. [Forget this Network] をクリックします。 [Forget] をクリックして確認します。
4. WLC に移動し、既存のクライアント接続を削除します（同じものが前述のステップで使用している場合）。 [Monitor] > [Clients] > [MAC address] の順に移動し、[Remove] をクリックします。
5. 前のクライアント セッションを削除するもう一つの確実な方法は、WAN を無効化して有効化することです。[WLC] > [WLANs] > [WLAN] の順に移動し、[WLAN] をクリックして編集します。[Enabled] > [Apply] をオフにします（無効にします）。[Enabled] > [Apply] をオンにします（再度有効になります）。
6. モバイル デバイスに戻ります。 次のクレデンシャルを使用して同じ WLAN に再接続してください。ユーザ名： 建築業者パスワード： XXXX
7. [Join] をクリックします。 契約作業員のユーザが割り当てられた VLAN 12（契約作業員/ゲスト VLAN）であることを確認します。
8. [ISE] > [Monitor] > [Authorizations] で ISE のリアルタイム ログのビューを表示できます。 個々のユーザ（従業員、契約作業員）が異なる VLAN で区別された許可プロファイル（Employee_WirelessvsContractor_Wireless）を取得することが表示されます。

WLC のゲスト WLAN

ゲストが ISE スポンサーのゲスト ポータルにアクセスできるためにゲスト WLAN を追加するために、次の手順を実行してください。

1. WLC で、[WLANs] > [WLANs] > [Add New] に移動します。
2. 新しいゲスト WLAN のために、次のように入力してください。[Profile Name] : pod1guest[SSID] : pod1guest
3. [Apply] をクリックします。
4. ゲストの [WLAN] の [General] タブで、次を入力してください。Status: Disabled[Interface/Interface Group] : ゲスト
5. ゲストで [WLAN] > [Security] > [Layer2] の順に移動し、次を入力してください。[Layer 2 Security] : なし
6. ゲストの **[WLAN] > [Security] > [Layer3]** タブに移動し、次を入力してください。[Layer 3 Security] : なし[Web Policy] : Enabled[Web Policy sub value] : 認証[Preauthentication ACL] : ACL-POSTURE-REDIRECT[Web Auth type] : External (外部サーバへリダイレクト) URL: https://10.10.10.70:8443/guestportal/Login.action
7. [Apply] をクリックします。
8. **WLC の設定を保存**してください。

ゲスト WLAN とゲスト ポータルのテスト

ここでは、ゲスト WLAN の設定をテストできます。 これにより、ゲストが ISE ゲスト ポータルにリダイレクトされます。

次の手順を実行します。

1. iPhone のような iOS のデバイスから、[Wi-Fi Networks] > [Enable] に移動します。 次に、POD のゲスト ネットワークを選択します。
2. この iOS のデバイスは、ゲスト VLAN (10.10.12.0/24) で有効な IP アドレスで示されます。
3. Safari ブラウザを開き、次に接続します。URL: http://10.10.10.10Web 認証のリダイレクトが表示されます。
4. ISE ゲスト ポータル ページに到達したら、[Continue] をクリックします。次のサンプル スクリーン ショットは、ゲスト ポータルのログインでの iOS デバイスの表示です。 これで、WLAN の正しい設定および ISE ゲスト ポータルが動作していることを確認します。

ISE ワイヤレスのスポンサーされたアクセス

ISE はゲストをスポンサーできるように設定できます。 この場合、内部ユーザまたは AD ドメインのユーザ (統合されている場合) のどちらかがゲスト アクセスをスポンサーできるように ISE ゲスト ポリシーを設定します。 また、スポンサーがゲストのパスワード (任意選択) を表示できるように ISE を設定します。

次の手順を実行します。

1. SponsorAllAccount のグループに従業員のユーザを追加します。 これを行うさまざまな方法があります。 直接グループに移動するか、またはユーザを編集してグループを割り当てます。 この例では、[Administration] > [Identity Management] > [Groups] > [User Identity Groups] の順に移動します。 次に、[SponsorAllAccount] をクリックし、従業員のユーザを追加します。
2. [Administration] > [Guest Management] > [Sponsor Groups] の順に移動します。
3. [Edit] をクリックし、[SponsorAllAccounts] を選択します。

4. [Authorization Levels] を選択し、次の設定を行います。[View Guest Password]： ○
5. この作業を完了するには、[Save] をクリックします。

スポンサーしているゲスト

以前は、AD のドメイン ユーザが一時的にゲストをスポンサーできる適切なゲストのポリシーとグループを設定していました。 次に、スポンサー ポータルにアクセスし、一時的にゲスト アクセスを作成します。

次の手順を実行します。

1. ブラウザから、次の URL のいずれかに移動します。 http://<ise ip>:8080/sponsorportal/ **または** https://<ise ip>:8443/sponsorportal/。 次に、次のデータを使ってログインします。ユーザ名： aduser（実行中のディレクトリ）、employee（内部ユーザ）パスワード： XXXX
2. [Sponsor] ページで、[Create Single Guest User Account] をクリックします。
3. 一時ゲスト用に、次を追加します。[First Name]： 必要（たとえば sam）[Last Name]： 必須（たとえば Jones）[Group Role]： ゲスト[Time Profile]： DefaultOneHourタイム ゾーン：（Time Zone:） Any/Default
4. [Submit] をクリックします。
5. ゲスト アカウントは、前のエントリに基づいて作成されます。 パスワードはハッシュ***とは反対に表示される（前の演習から）ことに注意します。
6. ゲストのユーザ名とパスワードを表示しているこのウィンドウを開いたままにします。 ゲストのポータルのログインをテストするためにこれを使用します（次へ）。

ゲスト ポータル アクセスのテスト

AD のユーザ/スポンサーによって作成した新しいゲスト アカウントを使用して、ゲスト ポータルとアクセスをテストします。

次の手順を実行します。

1. 優先するデバイス（この場合は Apple iOS または iPad）で、Pod ゲストの SSID に接続し、IP アドレスと接続性を確認します。
2. ブラウザを使用して、http://www にナビゲートしてみます。ゲスト ポータルのログイン ページにリダイレクトされます。
3. 前の演習で作成したゲスト アカウントを使用してログインします。成功した場合は、[Acceptable use policy] ページが表示されます。
4. [Accept terms and conditions] をチェックし、[Accept] をクリックします。元の URL が完了し、エンドポイントがゲストとしてアクセスを許可されます。

証明書の設定

ISE とセキュアな通信をするには、通信が認証関連か ISE 管理関連かを判断します。 たとえば、ISE Web UI を使用している設定では、X.509 証明書と証明書信頼のチェーンは非対称暗号化を有効にするように設定する必要があります。

次の手順を実行します。

1. 配線で接続されている PC から、ブラウザ ウィンドウで https://AD/certsrv を開きます。**注:** セキュア HTTP を使用します。**注:** ISE にアクセスするには、Mozilla Firefox または MS Internet Explorer を使用します。
2. administrator/Cisco123 でログインします。
3. [Download a CA certificate, certificate chain, or CRL] をクリックします。
4. [Download CA certificate] をクリックして、これを保存します（保存場所をメモしてください）。
5. ブラウザ ウィンドウで https://<Pod-ISE> を開きます。
6. [Administration] > [System] > [Certificates] > [Certificates Authority Certificates] の順に移動します。
7. [Certificate Authority Certificates] アクションを選択して、前にダウンロードした CA の証明書を参照します。
8. [Trust for client with EAP-TLS] を選択し、送信します。
9. CA がルート CA として信頼されて追加されたことを確認します。
10. ブラウザから、[Administration] > [System] > [Certificates] > [Certificates Authority Certificates] の順に移動します。
11. [Add] をクリックし、次に [Generate Certificate Signing Request] を選択します。
12. 次の値を送信します。[Certificate Subject]： CN=ise.corp.rf-demo.com[Key Length]： 2048
13. ISE が [CSR] ページに CSR が使用可能であることを表示します。 [OK] をクリックします。
14. CSR を [ISE CSR] ページから選択し、[Export] をクリックします。
15. 任意の場所にファイルを保存します（たとえば、[Downloads] など）
16. ファイルは *.pem として保存されます。
17. CSR ファイルを見つけ、メモ帳/ワードパッド/Textedit のどれかで編集します。
18. 内容をコピーします（[Select all] > [Copy]）。
19. ブラウザ ウィンドウで https://<Pod-AD>/certsrv を開きます。
20. [Request a certificate] をクリックします。
21. **advanced certificate request** をクリックして送信します。
22. [Saved Request] フィールドに CSR の内容を貼り付けます。
23. 証明書のテンプレートとして [Web Server] を選択し、[Submit] をクリックします。
24. [DER encoded] を選択し、[Download certificate] をクリックします。
25. ファイルを既知の場所（たとえば、[Downloads]）に保存します。
26. [Administration] > [System] > [Certificates] > [Certificates Authority Certificates] の順に移動します。
27. [Add] > [Bind CA Certificate] の順にクリックします。
28. 以前にダウンロードした CA 証明書を参照してください。
29. [Protocol EAP] および [Management Interface] の両方を選択し、次に [Submit] をクリックします。
30. CA がルート CA として信頼されて追加されたことを確認します。

Windows 2008 Active Directory との統合

ISE はユーザまたはマシンの認証情報のユーザ属性を検索するための Active Directory（AD）と直接通信できます。 AD と通信するには、ISE は AD のドメインに「結合」する必要があります。この例では、AD のドメインに ISE を結合して、AD の通信が正しく動作していることを確認します。

次の手順を実行します。

1. ISE から AD のドメインに結合するために、ISE から [Administration] > [Identity Management] > [External Identity Sources] に移動します。
2. 左側のペイン（外部 ID ソース）から、[Active Directory] を選択します。
3. 右側で、[Connection] タブを選択し、次のように入力します。[Domain Name]： corp.rf-demo.com[Identity Store Name]： AD1
4. [Test Connection] をクリックします。 AD のユーザ名（aduser/Cisco123）を入力し、[OK] をクリックします。
5. [Test Status] に [Test Succeeded] と表示されていることを確認します。
6. [Show Detailed Log] を選択し、トラブルシューティングに有用な詳細情報を確認します。[OK] をクリックして、次に進みます。
7. [Save Configuration] をクリックします。
8. [Join] をクリックします。 AD のユーザ（管理者/Cisco123）を入力し、[OK] をクリックします。
9. [Join Operation Status] に [Succeeded] と表示されていることを確認してから、[OK] をクリックします。[Server Connection Status] には [CONNECTED] と表示されます。 この時点でこのステータスが変化すれば、テスト接続は AD アクションでの問題のトラブルシュートに役立ちます。

Active Directory グループの追加

AD のグループが追加されると、ISE ポリシーを介してより細かい制御ができます。 たとえば、ポリシーがユーザだけに限定された前の ISE 1.0 の演習で経験した関連するバグがなければ、従業員または契約作業者グループのような機能ロールによって AD グループは区別できます。

このラボでは、ドメイン ユーザまたは従業員のグループだけが使用されます。

次の手順を実行します。

1. ISE から、[Administration] > [Identity Management] > [External Identity Sources] の順に移動します。
2. [Active Directory] の [Groups] タブを選択します。
3. [+Add] をクリックし、[Groups From Directory] を選択します。
4. 後続のウィンドウで、（[Select Directory Groups]）で、ドメイン（corp-rf-demo.com）とフィルタ（*）のデフォルトを受け入れます。 次に、[RetrieveGroups] をクリックします。
5. [Domain Users] グループと [Employee] グループのボックスを選択します。 完了したら、[OK] をクリックします。
6. グループがリストに追加されたことを確認します。

アイデンティティ シーケンスの追加

デフォルトでは、ISE は認証ストアの内部ユーザを使用するように設定されています。 AD を追加すると、ISE が認証を確認するために使用する AD を含めるために、シーケンスの優先順位を作成できます。

次の手順を実行します。

1. ISE から、[Administration] > [Identity Management] > [Identity Source Sequences] の順に移動します。

2. [+Add] をクリックして新しいシーケンスを追加します。
3. 次の新しい名前を入力します。 **AD_Internal**。 [Selected] フィールドに、利用可能なすべての発信元を追加します。 次の、AD1 がリストの先頭に移動するように並び替えが必要です。 [Submit] をクリックします。
4. シーケンスがリストに追加されていることを確認します。

統合 AD を使用した ISE ワイヤレス スポンサー ゲスト アクセス

AD のドメイン ユーザがゲスト アクセスをスポンサーできるために、ポリシーを使用してゲストがスポンサーされることができるように ISE を設定することができます。

次の手順を実行します。

1. ISE から、[Administration] > [Guest Management] > [Settings] の順に移動します。
2. [Sponsor] を展開し、[Authentication Sourcen] をクリックします。 次に、ID ストア シーケンスとして [AD_Internal] を選択します。
3. ID ストア シーケンスとして [AD_Internal] を確認します。 [Save] をクリックします。
4. [Administration] > [Guest Management] > [Sponsor Groups Policy] の順に移動します。
5. 最初のルールの新しいポリシーを挿入します (右から [Actions] アイコンをクリックします)。
6. 新しいスポンサーのグループ ポリシーについて、次を作成します。[Rule Name]： ドメインユーザ[Identity Groups]： [Any][Other Conditions]： (Create New / Advanced) > AD1[AD1] : External Groups[AD1 External Groups] > [Equals] > [corp.rf-demo.com/Users/Domain Users]
7. スポンサー グループでは、次の設定を行います。[Sponsor Groups]： SponsorAllAccounts
8. [Administration] > [Guest Management] > [Sponsor Groups] の順に移動します。
9. [Edit] > [SponsorAllAccounts] の順に選択します。
10. [Authorization Levels] を選択し、次の設定を行います。[View Guest Password]： ○

スイッチでの SPAN の設定

SPAN の設定：ISE mgt/プローブのインターフェイスは、WLC 管理インターフェイスに隣接する L2 です。 スイッチは、SPAN、および従業員およびゲストのインターフェイス VLAN などの外部インターフェイスに対して設定することができます。

```
Podswitch(config)#monitor session 1 source vlan10 , 11 , 12
Podswitch(config)#monitor session 1 destination interface Fa0/8
ISE virtual probe interface.
```

参照： Apple MAC OS X のワイヤレス認証

Apple Mac OS X ワイヤレス ラップトップを使用している内部ユーザ (または統合された、AD ユーザ) を認証された SSID で WLC に関連付けます。 適応しない場合は、とばしてください。

1. Mac で、[WLAN setting] に移動します。 WiFi を有効にし、前の演習で作成した 802.1X が有効な POD SSID を選択し接続します。
2. 接続するには、次の情報を入力します。ユーザ名： aduser (AD を使用している場合)、employee (内部：従業員)、contractor (内部：契約作業員) パスワード： XXXX[802.1X]： 自動 (Automatic) [TLS Certificate]： なしこの時点で、ラップトップは接

続されていない場合があります。 また、ISE は次のように障害イベントをスローすることができます。

```
Authentication failed :12514 EAP-TLS failed SSL/TLS handshake because of
an unknown CA in the client certificates chain
```

3. [System Preference] > [Network] > [Airport] の [802.1X] 設定に移動して、新しい POD SSID/WPA のプロファイルの認証を次のように設定します。TLS： Disabled[PEAP]： Enabled[TTLS]： Disabled[EAP-FAST]： Disabled
4. [OK] をクリックして次に進み、設定を保存できます。
5. [Network] 画面で、適切な SSID + 802.1X WPA のプロファイル選択して [Connect] をクリックします。
6. システムはユーザ名とパスワードの入力を促す可能性があります。 AD のユーザおよびパスワード（aduser/XXXX）を入力し、[OK] をクリックします。クライアントは、有効な IP アドレスを使用して PEAP 経由での**接続済み**を表示する必要があります。

参照： Microsoft Windows XP のワイヤレス認証

Windows XP ワイヤレス ラップトップを使用している内部ユーザ（または統合された、AD ユーザ）を認証された SSID で WLC に関連付けます。 適応しない場合は、とばしてください。

次の手順を実行します。

1. ラップトップで、[WLAN setting] に移動します。 WiFi を有効にし、前の演習で作成した 802.1X が有効な POD SSID に接続します。
2. WiFi インターフェイスのネットワーク プロパティにアクセスします。
3. [Wireless Networks] タブまで移動します。 [pod SSID network properties] の [Authentication] タブで [EAP type] に [Protected EAP (PEAP)] を選択します。
4. EAP のプロパティをクリックします。
5. 次の設定を行います。[Validate server certificate]： Disabled[Authentication Method]： Secured password（EAP-MSCHAP v2）
6. この設定作業を完了するには、すべてのウィンドウで [OK] をクリックします。
7. Windows XP のクライアントがユーザ名とパスワードの入力画面を表示します。 この例では、「aduser/XXXX」です。
8. ネットワークの接続性および IP アドレス指定（v4）を確認します。

参照： Microsoft Windows 7 のワイヤレス認証

Windows 7 ワイヤレス ラップトップを使用している内部ユーザ（または統合された、AD ユーザ）を認証された SSID で WLC に関連付けます。

1. ラップトップで、[WLAN setting] に移動します。 WiFi を有効にし、前の演習で作成した 802.1X が有効な POD SSID に接続します。
2. Wireless Manager にアクセスし、新しい POD のワイヤレス プロファイルを編集します。
3. 次の設定を行います。[Authentication Method]： PEAP[Remember my credentials…]： Disabled[Validate server certificate (advanced setting)]： Disabled[Authentication Method (adv. Setting)]： EAP-MSCHAP v2[Automatically use my Windows logon…]： Disabled

関連情報

- テクニカル サポートとドキュメント – Cisco Systems