CHAPTER 8

wIPS およびプロファイルの設定

この章では、wIPS プロファイルおよび wIPS を操作するために併せて設定する必要がある項目の設定方法について説明します。

この章は、次の内容で構成されています。

ガイドラインと制限事項

- モビリティ サービス エンジンは 1 つの NCS からのみ設定できます。
- ご使用の wIPS がコントローラ、アクセス ポイント、および MSE で構成されている場合、これら 3 つのエンティティをすべて UTC タイムゾーンに設定する必要があります。
- コントローラは 1 つの設定プロファイルに関連付けられます。そのコントローラに接続されている wIPS モード アクセス ポイントはすべて同じ wIPS 設定を共有します。

前提条件

wIPS プロファイルを設定する前に、次の手順を実行する必要があります。

1. モビリティ サービス エンジンをインストールします（まだネットワーク内で動作していない場合）。次の URL にある『*Cisco 3350 Mobility Services Engine Getting Started Guide*』または『*Cisco 3310 Mobility Services Engine Getting Started Guide*』を参照してください。

   http://www.cisco.com/en/US/products/ps9742/prod_installation_guides_list.html

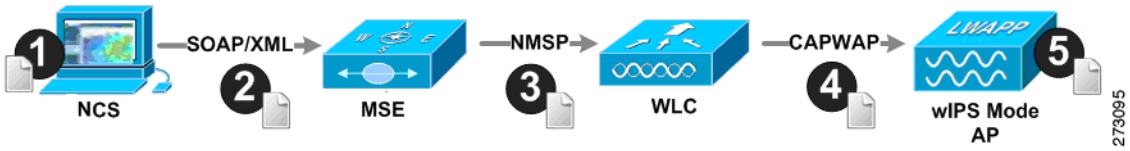
2. モビリティ サービス エンジンを NCS に追加します（まだ追加されていない場合）。
3. wIPS モニタ モードで動作するようにアクセス ポイントを設定します。「wIPS モニタ モードのアクセス ポイントの設定」（P.8-2）を参照してください。
4. wIPS プロファイルを設定します。「wIPS プロファイルの設定」（P.8-4）を参照してください。

wIPS 設定およびプロファイル管理について

wIPS プロファイルの設定は、プロファイルの表示と変更に使用される NCS から始まるチェーン階層を進みます。実際のプロファイルは、MSE で実行するワイヤレス IPS サービス内に保存されます。

プロファイルは、モビリティ サービス エンジン上の wIPS サービスから、特定のコントローラに伝播され、次に、その各コントローラに関連付けられている wIPS モード アクセス ポイントに透過的にこのプロファイルが伝達されます。（図 8-1 を参照）。

図 8-1　　wIPS プロファイルの設定および更新



NCS で wIPS プロファイルへの設定変更が行われ、一連のモビリティ サービス エンジンおよびコントローラに適用される場合、次のようになります。

1. NCS で設定プロファイルが変更され、バージョン情報が更新されます。
2. XML ベースのプロファイルがモビリティ サービス エンジンで実行する wIPS エンジンに適用されます。この更新は、SOAP/XML プロトコルを介して行われます。
3. モビリティ サービス エンジン上の wIPS は、NMSP を使用して設定プロファイルを適用することによって、そのプロファイルに関連付けられている各コントローラを更新します。
4. コントローラは更新された wIPS プロファイルを受け取り、それを NVRAM に保存し（以前のすべてのバージョンのプロファイルを置き換える）、CAPWAP 制御メッセージを使用して、更新されたプロファイルをそれに関連付けられた wIPS アクセス ポイントに伝播します。
5. wIPS モード アクセス ポイントはコントローラから更新されたプロファイルを受け取り、その wIPS ソフトウェア エンジンに変更を適用します。

この項では、次のトピックを扱います。

ガイドラインと制限事項

- wIPS モニタ モードをサポートしているのは、Cisco Aironet 1130、1140、1240、1250、3502E、および 3502I シリーズのアクセス ポイントだけです。
- wIPS サブモードがサポートされるのは、アクセス ポイント モードがモニタ、ローカル、または HREAP の場合だけです。ただし、1130 および 1240 アクセス ポイントの場合、wIPS はモニタ モードだけでサポートされます。

wIPS モニタ モードのアクセス ポイントの設定

wIPS モニタ モードで動作するようにアクセス ポイントを設定するには、次の手順に従います。

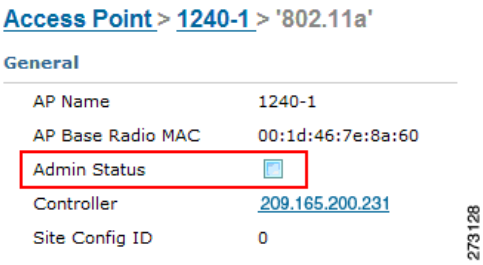
ステップ 1　[Configure] > [Access Points] の順に選択します。

ステップ 2　[802.11a] または [802.11b/g] 無線リンクをクリックします（図 8-2 を参照）。

図 8-2　[Configure] > [Access Points] > [Radio]

ステップ 3　[Access Point] ページで、[Admin Status] チェックボックスをオフにして無線を無効にします。

図 8-3　[Access Points] > [Radio]



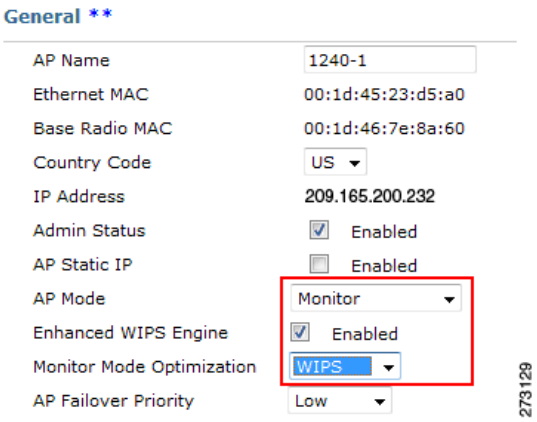
ステップ 4　[Save] をクリックします。

（注）　wIPS モニタ モードに設定されるアクセス ポイント上の各無線について、これらの手順を繰り返します。

ステップ 5　無線が無効になると、[Configure] > [Access Points] の順に選択し、無効にした無線のアクセス ポイントの名前をクリックします。

ステップ 6　アクセス ポイントのダイアログボックスで、[AP Mode] ドロップダウン リストから [Monitor] を選択します（図 8-4 を参照）。

図 8-4　[Configure] > [Access Points] > アクセス ポイントの詳細



ステップ 7　[Enhanced WIPS Engine] の [Enabled] チェックボックスをオンにします。

ステップ 8　[Monitor Mode Optimization] ドロップダウン リストから [WIPS] を選択します。

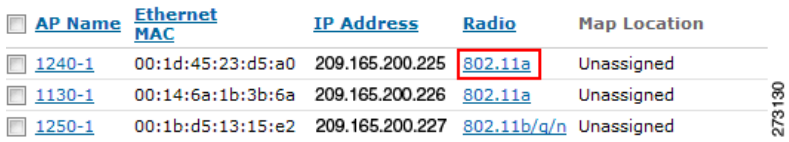
ステップ 9　[Save] をクリックします。

ステップ 10　アクセス ポイントをリブートするように求められたら、[OK] をクリックします。

ステップ 11　アクセス ポイント無線を再度有効にするには、[Configure] > [Access Points] の順に選択します。

ステップ 12　該当するアクセス ポイント無線をクリックします（図 8-5 を参照）。

図 8-5　[Configure] > [Access Points] > [Radio]



ステップ 13　[Radio Detail] ページで、[Admin Status] の [Enabled] チェックボックスをオンにします。

ステップ 14　[Save] をクリックします。

wIPS モニタ モードに設定した各アクセス ポイントおよびその各無線について、この手順を繰り返します。

wIPS プロファイルの設定

デフォルトで、モビリティ サービス エンジンと対応する wIPS アクセス ポイントは NCS からデフォルトの wIPS プロファイルを継承します。このプロファイルは、デフォルトで有効にされている大部分の攻撃アラームによってあらかじめ調整されており、wIPS アクセス ポイントと同じ RF グループ内のアクセス ポイントに対する攻撃を監視します。このように、システムは WLAN インフラストラクチャと wIPS アクセス ポイントの両方が同じコントローラ上に混合されている統合ソリューションを利用する構成モデルに対する攻撃を監視するようにあらかじめ設定されています。

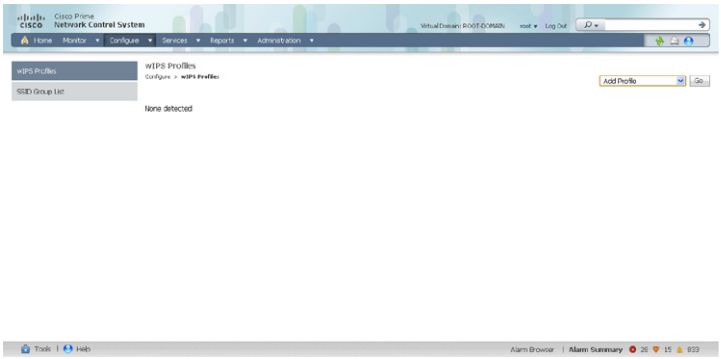
（注）　次の設定手順の一部は*オーバーレイだけ*としてマークされており、Autonomous や完全に個別のコントローラベースの WLAN などの既存の WLAN インフラストラクチャを監視するように適応型 wIPS ソリューションを導入している場合にだけ実行されます。

wIPS プロファイルを設定するには、次の手順に従います。

ステップ 1　[Configure] > [wIPS Profiles] を選択します。

[wIPS Profiles] ページが表示されます（図 8-6 を参照）。

図 8-6　[wIPS Profiles] > プロファイル リスト



ステップ 2　[Select a command] ドロップダウン リストから、[Add Profile] を選択し、[Go] をクリックします。

ステップ 3　[Profile Parameters] ダイアログボックスで、[Copy From] ドロップダウンリストからプロファイル テンプレートを選択します。

（注）　適応型 wIPS には一連のプロファイル テンプレートがあらかじめ定義されており、お客様はそれらをベースとして使用して、独自のカスタム プロファイルを作成できます。各プロファイルは、そのプロファイルで有効な特定のアラームと同様に、特定の業務または用途に合わせて作成されています。

（注）　デフォルト プロファイルは編集できません。

（注）　プロファイルをコントローラに適用するために NMSP セッションがアクティブなことを確認します。

ステップ 4　プロファイルを選択し、プロファイル名を入力したら、[Save and Edit] をクリックします。

ステップ 5　（任意）[SSID Group List] ページで SSID を設定します。

デフォルトで、ローカル ワイヤレス LAN インフラストラクチャ（同じ RF グループ名を持つ AP によって定義された）に対して仕掛けられた攻撃が監視されます。オーバーレイ構成モデルで構成する場合など、他のネットワークに対する攻撃を監視させる必要がある場合は、SSID グループ機能を使用する必要があります。

（注）　この手順が必要ない場合は、単に [Next] をクリックします。

a.　[MyWLAN] 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 [Edit Group] を選択して、[Go] をクリックします。

b. 監視する SSID を入力します。

c. SSID 名を入力し（複数の名前を入力する場合は 1 つのスペースで区切る）、**[Save]** をクリックします。

SSID が正常に追加されたことを確認する [SSID Groups] ページが表示されます。

d. [Next] をクリックします。

[Select Policy] および [Policy Rules] 概要ペインが表示されます。

（注） [Select Policy] ペインで、検出および報告対象の攻撃を有効または無効にすることができます。アラームのしきい値を編集し、フォレンジックを有効にすることもできます。

ステップ 6　検出および報告対象の攻撃を有効または無効にするには、[Select Policy] ペインでその攻撃タイプの横にあるチェックボックスをオンにします。

ステップ 7　プロファイルを編集するには、攻撃タイプの名前（DoS：アソシエーション フラッドなど）をクリックします。

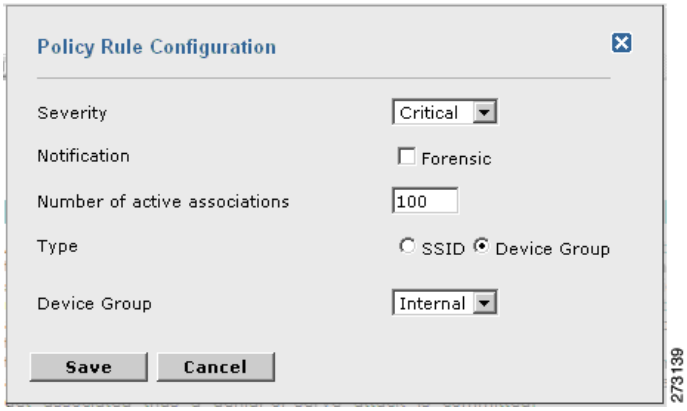
その攻撃タイプの設定ペインが、ポリシー ルールの説明の上の右側のペインに表示されます。

ステップ 8　ポリシー ルールを変更するには、次の手順に従います。

a. [Policy Rules] ペインで、ポリシー ルールの横にあるチェックボックスをオンにし、[Edit] をクリックします。

[Policy Rule Configuration] ダイアログボックスが表示されます（図 8-7 を参照）。

図 8-7　[Policy Rule Configuration] ダイアログボックス



b. アラームの重大度を選択します。

c. このアラームのパケットをキャプチャする場合は、[Forensic] チェックボックスをオンにします。

d. 必要に応じて、アクティブなアソシエーションの数を変更します。（この値はアラーム タイプによって異なります）。

e. 攻撃を監視する WLAN インフラストラクチャのタイプ（[SSID] または [Device Group]）を選択します。

1. [SSID] を選択した場合は、ステップ 9 に進みます。
2. [Device Group] を選択した場合は、ステップ 10 に進みます。

（注）　[Device Group]（[Type]）および [Internal] はデフォルトです。*Internal* は、同じ RF グループ内のすべてのアクセス ポイントを示します。タイプに [SSID] を選択すると、オーバーレイ構成に一般的な個別ネットワークを監視できます。

ステップ 9　（任意）オーバーレイ構成に限り、SSID のポリシー ルールを追加するには、以下の手順に従います。

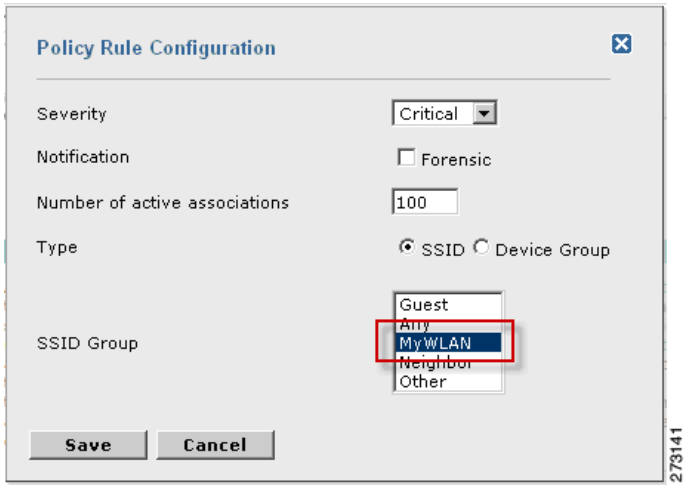
a. ポリシー ルールを追加するには、[Add] をクリックします（図 8-8 を参照）。

図 8-8　ポリシー ルールの追加

b. [Policy Rule Configuration] ダイアログボックスで、[SSID Group] リストから [MyWLAN] を選択します（図 8-9 を参照）。

（注）　タイプに SSID がすでに選択されています。

図 8-9　SSID の [Policy Rule Configuration] ダイアログボックス

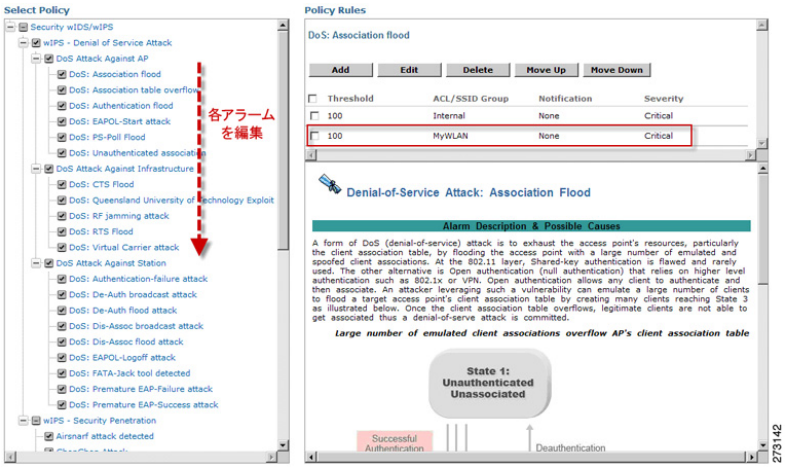


c. すべての変更が完了したら、[Save] をクリックします。

d. 各ポリシー ルールを変更します。すべての変更が完了したら、ステップ 10 に進みます。（図 8-10 を参照）。

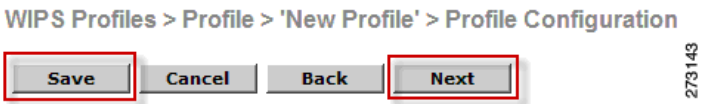
（注）　SSID によって別の WLAN インフラストラクチャを監視するようにシステムを設定する場合、監視するすべてのポリシー ルールごとに変更する必要があります。個別の各アラームに、システムで以前に作成した SSID グループに対する攻撃を監視するように定義したポリシー ルールを作成する必要があります。

図 8-10　SSID モニタリングに関するポリシー ルールの編集



ステップ 10　[Profile Configuration] ダイアログボックスで、[Save] をクリックしてプロファイル（SSID またはデバイス グループ）を保存します。[Next] をクリックします（図 8-11 を参照）。

図 8-11　[Profile Configuration] ダイアログボックス



ステップ 11　プロファイルを適用する MSE/ コントローラの組み合わせを選択して、[Apply] をクリックします（図 8-12 を参照）。

図 8-12　[Apply Profile] ダイアログボックス