CHAPTER 8

Configuring wIPS and Profiles

This chapter describes how to configure wIPS profiles and those items that must be configured in conjunction to operate wIPS.

This chapter contains the following sections:

Guidelines and Limitations

- The mobility services engine can only be configured from the Cisco Prime Infrastructure.
- If your wIPS deployment consists of a controller, access point, and MSE, you must set all the three entities to the UTC timezone.
- A controller is associated to a single configuration profile. All wIPS mode access points connected to that controller share the same wIPS configuration.

Prerequisites

Before you can configure wIPS profiles you must do the following:

1. Install a mobility services engine (if one is not already operating in the network). See the *Cisco 3350 Mobility Services Engine Getting Started Guide* or *Cisco 3310 Mobility Services Engine Getting Started Guide*:

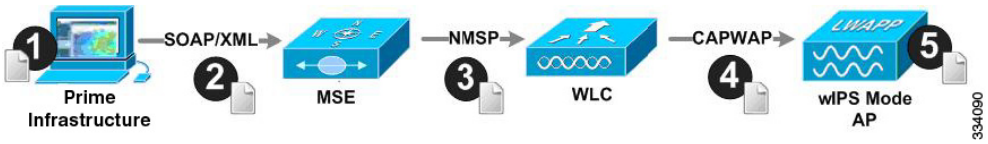
   http://www.cisco.com/en/US/products/ps9742/prod_installation_guides_list.html
2. Add the mobility services engine to the Prime Infrastructure (if not already added).
3. Configure access points to operate in wIPS monitor mode. See the "Configuring Access Points for wIPS Monitor Mode" section on page 8-2.
4. Configure wIPS profiles. See the "Configuring wIPS Profiles" section on page 8-4.

Information About wIPS Configuration and Profile Management

Configuration of wIPS profiles follows a chained hierarchy starting with the Prime Infrastructure, which is used for profile viewing and modification. The actual profiles are stored within the wIPS service running on the MSE.

From the wIPS service on the mobility services engine, profiles are propagated to specific controllers, which in turn communicate this profile transparently to wIPS mode access points associated to that respective controller. (See Figure 8-1).

Figure 8-1 Configuration and Update of wIPS Profiles



When a configuration change to a wIPS profile is made at the Prime Infrastructure and applied to a set of mobility services engines and controllers, the following occurs:

1. The configuration profile is modified on the Prime Infrastructure and version information is updated.
2. An XML-based profile is pushed to the wIPS engine running on the mobility services engine. This update occurs over the SOAP/XML protocol.
3. The wIPS engine on the mobility services engine updates each controller associated with that profile by pushing out the configuration profile over NMSP.
4. The controller receives the updated wIPS profile, stores it into NVRAM (replacing any previous revision of the profile) and propagates the updated profile to its associated wIPS access points using CAPWAP control messages.
5. A wIPS mode access point receives the updated profile from the controller and applies the modifications to its wIPS software engine.

This section contains the following topics:

Guidelines and Limitations

- Only Cisco Aironet 1130, 1140, 1240, 1250, 3502E and 3502I Series Access Points support wIPS monitor mode.
- The wIPS submode is supported only when the access point mode is Monitor, Local, or HREAP. But for 1130 and 1240 access points, wIPS is supported only in monitor mode.

Configuring Access Points for wIPS Monitor Mode

To configure an access point to operate in wIPS monitor mode, follow these steps:

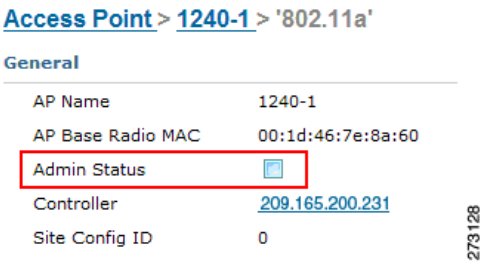
Step 1 Choose **Configure > Access Points**.

Step 2 Click the **802.11a** or **802.11b/g** radio link (see Figure 8-2).

Figure 8-2 Configure > Access Points > Radio

Step 3 In the Access Point page, unselect the **Admin Status** check box to disable the radio.

Figure 8-3 Access Points > Radio



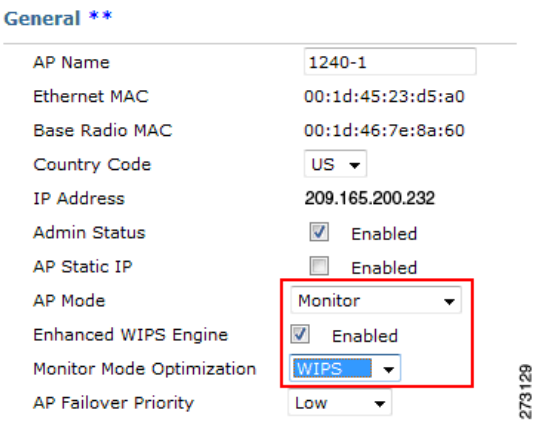
Step 4 Click **Save**.

Note Repeat these steps for each radio on an access point that is to be configured for wIPS monitor mode.

Step 5 Once the radios are disabled, choose **Configure** > **Access Points** and then click the name of the access point of the radio you just disabled.

Step 6 In the access point dialog box, choose **Monitor** from the AP Mode drop-down list (see Figure 8-4).

Figure 8-4 Configure > Access Points > Access Point Detail



Step 7 Select the **Enabled** check box for the Enhanced WIPS Engine.

Step 8 From the Monitor Mode Optimization drop-down list, choose **WIPS**.

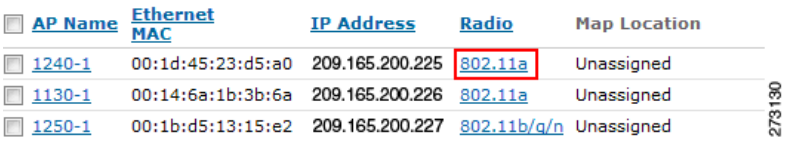
Step 9 Click **Save**.

Step 10 Click **OK** when prompted to reboot the access point.

Step 11 To reenable the access point radio, choose **Configure > Access Points**.

Step 12 Click the appropriate access point radio (see Figure 8-5).

Figure 8-5 Configure > Access Points > Radio



Step 13 In the Radio Detail page, select the Admin Status **Enabled** check box.

Step 14 Click **Save**.

Repeat this procedure for each access point and each respective radio configured for wIPS monitor mode.

Configuring wIPS Profiles

By default, the mobility services engine and corresponding wIPS access points inherit the default wIPS profile from the Prime Infrastructure. This profile comes pre-tuned with a majority of attack alarms enabled by default and monitors attacks against access points within the same RFGroup as the wIPS access points. In this manner, the system comes pre-setup to monitor attacks against a deployment model that utilizes an integrated solution in which both the WLAN infrastructure and wIPS access points are intermixed on the same controller.

Note Some of the configuration steps that follow are marked as *Overlay-Only* and are only to be undertaken when deploying the Adaptive wIPS solution to monitor an existing WLAN Infrastructure such as an autonomous or completely separate controller-based WLAN.

To configure wIPS profiles, follow these steps:

Step 1 Choose **Configure > wIPS Profiles**.

The wIPS Profiles page appears.

Step 2 From the Select a command drop-down list, choose **Add Profile**, and click **Go**.

Step 3 In the Profile Parameters dialog box, choose a profile template from the Copy From drop-down list.

Note The Adaptive wIPS comes with a pre-defined set of profile templates from which customers can choose or use as a basis for their own custom profiles. Each profile is tailored to either a specific business or application as are the specific alarms enabled on that profile.

Note You cannot edit the default profile.

Note Ensure that the NMSP session is active to push the profile to the controller.

Step 4 After selecting a profile and entering a profile name, click **Save and Edit**.

Step 5 (Optional) Configure SSIDs in the SSID Group List page.

By default, the system monitors attacks launched against the local Wireless LAN Infrastructure (as defined by APs which have the same RF Group name). If the system should also be required to monitor attacks against another network, such as when deployed in an overlay deployment model, the SSID groups feature must be utilized.

Note If this step is not required, simply click **Next**.

a. Select the **MyWLAN** check box and choose **Edit Group** from the drop-down list, then click **Go**.

b. Enter SSIDs to Monitor.

c. Enter the SSID name (separate multiple entries by a single space), and click **Save**.

The SSID Groups page appears confirming that the SSIDs are added successfully.

d. Click **Next**.

The Select Policy and Policy Rules summary panes appear.

Note In the Select Policy pane, you can enable or disable attacks to be detected and reported. You can also edit specific thresholds for alarms and turn on forensics.

Step 6 To enable or disable attacks to be detected and reported, select the check box next to the specific attack type in question in the Select Policy pane.

Step 7 To edit the profile, click the name of the attack type (such as DoS: Association flood).

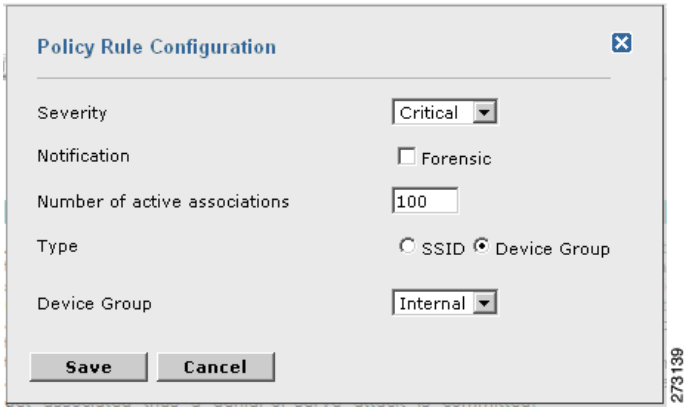
The configuration pane for that attack type appears in the right pane above the policy rule description.

Step 8 To modify a policy rule do the following:

a. In the Policy Rules pane, select the check box next to the policy rule, and click **Edit**.

The Policy Rule Configuration dialog box appears (see Figure 8-6).

Figure 8-6 Policy Rule Configuration Dialog Box



b. Choose the severity of the alarm.

c. Select the **Forensic** check box if you want to capture packets for this alarm.

d. Modify the number of active associations, if desired. (This value varies by alarm type).

e. Select the type of WLAN infrastructure (SSID or Device Group) that the system monitors for attacks.

1. If you select SSID, continue with Step 9.
2. If you select Device Group, continue with Step 10.

Note Device Group (Type) and Internal are the defaults. *Internal* indicates all access points within the same RF Group. Selecting SSID as the type, allows you to monitor a separate network, which is typical of an overlay deployment.

Step 9 (Optional), For overlay deployments only, to add a policy rule for an SSID, do the following:

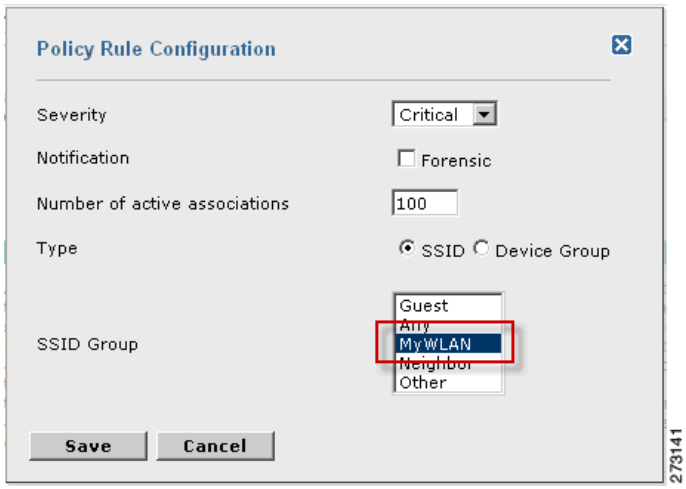
a. To add a policy rule, click **Add** (see Figure 8-7).

Figure 8-7 Adding a Policy Rule

b. In the Policy Rule Configuration dialog box, choose **MyWLAN** from the SSID Group list (see Figure 8-8).

Note SSID is already selected as the type.

Figure 8-8 Policy Rule Configuration Dialog Box for SSIDs

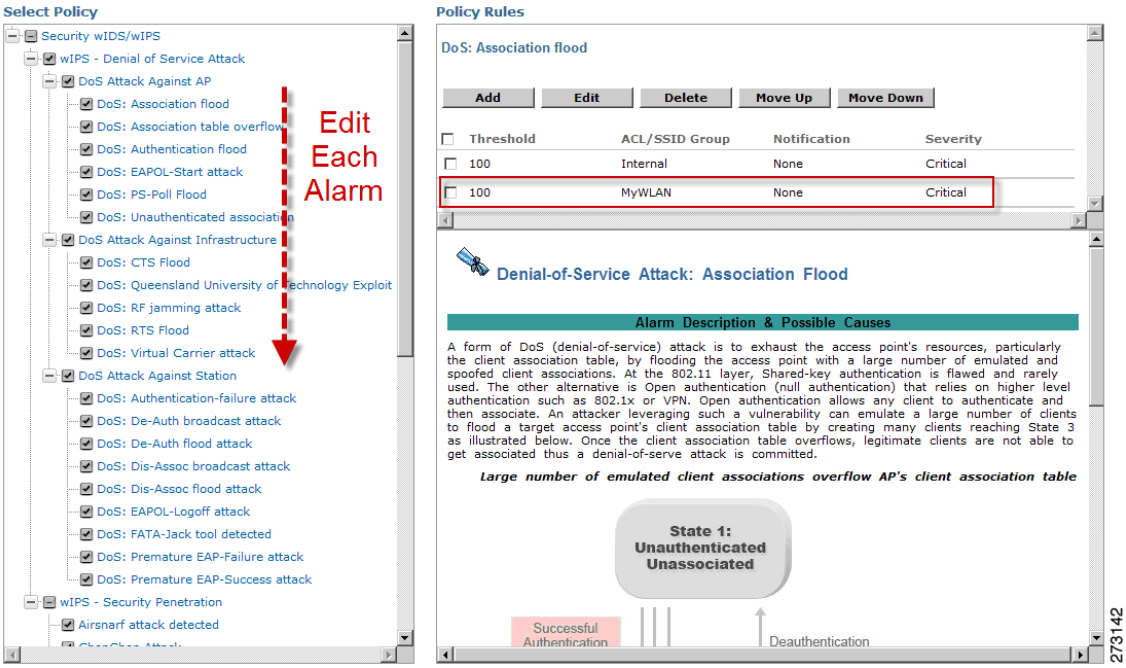


c. Click **Save** after all changes are complete.

d. Modify each policy rule. Continue with Step 10 when all modifications are complete. (See Figure 8-9).

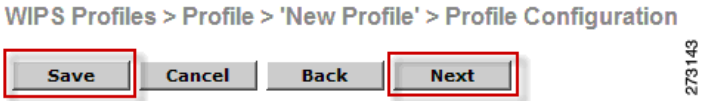
Note When you configure a system to monitor another WLAN infrastructure by SSID, changes must be made for each and every policy rule to monitor. You must create a policy rule under each separate alarm which defines the system to monitor attacks against the SSID Group created earlier.

Figure 8-9 Edit Policy Rules for SSID Monitoring



Step 10 In the Profile Configuration dialog box, click **Save** to save the Profile (SSID or Device Group). Click **Next** (see Figure 8-10).

Figure 8-10 Profile Configuration Dialog box



Step 11 Select the MSE/Controller combinations to apply the profile to and then click **Apply** (see Figure 8-11).

Figure 8-11 Apply Profile Dialog Box