CHAPTER 6

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:

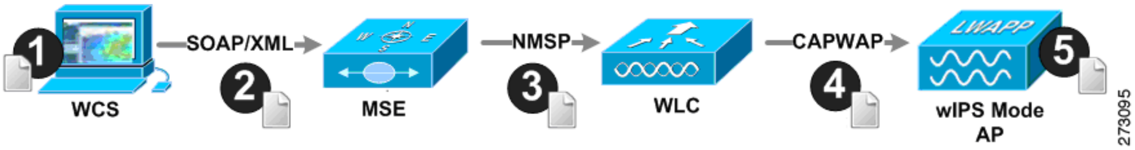
- "Configuring Access Points for wIPS Monitor Mode" section on page 6-3
- "Configuring wIPS Profiles" section on page 6-4

Overview of wIPS Configuration and Profile Management

Configuration of wIPS profiles follows a chained hierarchy starting with WCS which is used for profile viewing and modification. The actual profiles are stored within the wIPS service running on the mobility services engine (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.

Figure 6-1 Configuration and Update of wIPS Profiles



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

1. The configuration profile is modified on WCS 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.

Note A controller is associated to a single configuration profile. All wIPS mode access points connected to that controller share the same wIPS configuration.

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.

Note The mobility services engine can only be configured from one Cisco WCS.

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). Refer to the *Cisco 3350 Mobility Services Engine Getting Started Guide* or *Cisco 3350 Mobility Services Engine Getting Started Guide* at:
   http://www.cisco.com/en/US/products/ps9742/prod_installation_guides_list.html
2. Add the mobility services engine to Cisco WCS (if not already added). Refer to Chapter 2, "Adding and Deleting Systems"
3. Configure access points to operate in wIPS monitor mode. Refer to "Configuring Access Points for wIPS Monitor Mode" section on page 6-3.
4. Configure wIPS profiles. Refer to "Configuring wIPS Profiles" section on page 6-4.

Configuring Access Points for wIPS Monitor Mode

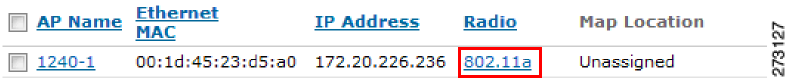
Note Only Cisco Aironet 1130, 1140, 1240 and 1250 Series Access Points support wIPS monitor mode.

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

Step 1 In Cisco WCS, click **Configure > Access Points**.

Step 2 Click on the 802.11a or 802.11b/g radio. (Figure 6-2).

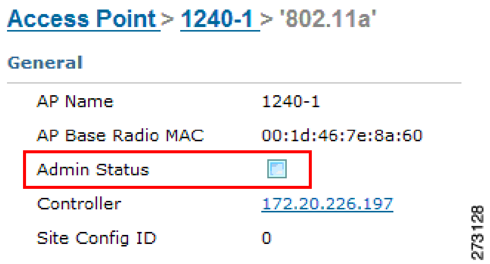
Figure 6-2 Configure > Access Points > Radio



□	AP Name	Ethernet MAC	IP Address	Radio	Map Location
□	1240-1	00:1d:45:23:d5:a0	172.20.226.236	802.11a	Unassigned

Step 3 On the access point window, uncheck **Admin Status** to disable the radio.

Figure 6-3 Access Points > Radio



Access Point > 1240-1 > '802.11a'

General

AP Name	1240-1
AP Base Radio MAC	00:1d:46:7e:8a:60
Admin Status	□
Controller	172.20.226.197
Site Config ID	0

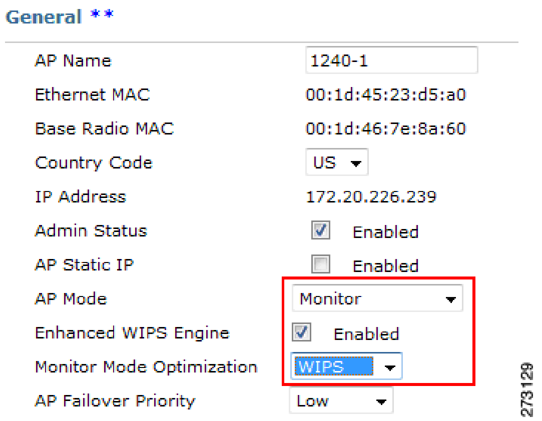
Step 4 Click **Save** (bottom).

Note Repeat these steps for each and every radio on an access point that is to be configured for wIPS monitor mode. For example, an Aironet 1130 requires this step to be performed on both its 802.11a and 802.11b/g radios.

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

Step 6 At the access point configuration window, select **Monitor Mode** from the AP Mode drop-down menu. (Figure 6-4)

Figure 6-4 Configure > Access Points > AP Name



General **

AP Name	1240-1
Ethernet MAC	00:1d:45:23:d5:a0
Base Radio MAC	00:1d:46:7e:8a:60
Country Code	US
IP Address	172.20.226.239
Admin Status	☑ Enabled
AP Static IP	□ Enabled
AP Mode	Monitor
Enhanced WIPS Engine	☑ Enabled
Monitor Mode Optimization	WIPS
AP Failover Priority	Low

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

Step 8 Select **WIPS** from the Monitor Mode Optimization drop-down menu.

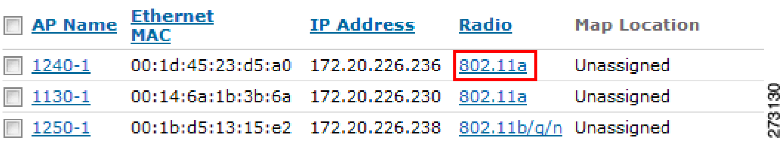
Step 9 Click **Save**.

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

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

Step 12 Click on the appropriate access point radio.

Figure 6-5 Configure > Access Points > Radio



□	AP Name	Ethernet MAC	IP Address	Radio	Map Location
□	1240-1	00:1d:45:23:d5:a0	172.20.226.236	802.11a	Unassigned
□	1130-1	00:14:6a:1b:3b:6a	172.20.226.230	802.11a	Unassigned
□	1250-1	00:1b:d5:13:15:e2	172.20.226.238	802.11b/g/n	Unassigned

Step 13 At the radio configuration panel, check the Admin Status **Enabled** check box.

Step 14 Click **Save**.

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

Configuring wIPS Profiles

By default, the MSE and corresponding wIPS access points inherit the default wIPS profile from WCS. This profile comes pre-tuned with a majority of attack alarms enabled by default and will monitor attacks against access points within the same RF-Group 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.

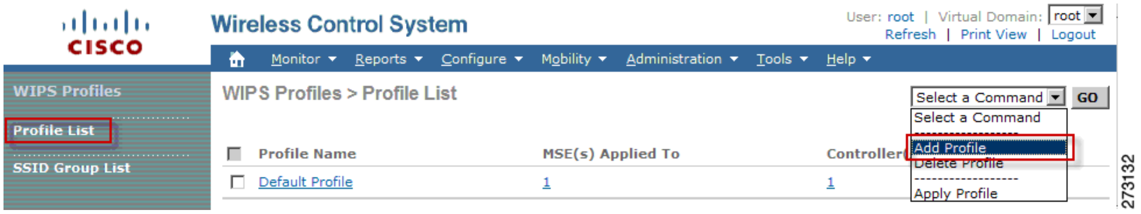
Note Some of the configuration steps that follow are marked as *Overlay-Only* and are only to be undertaken when deploying the Adaptive wIPS solution to monitor an existing WLAN Infrastructure such as an autonomous or completely separate controller-based WLAN.

To configure wIPS profiles, follow these steps:

Step 1 In Cisco WCS, click **Configure > WIPS Profiles**.

Step 2 In the window that appears (Figure 6-6), select **Profile List** (left panel).

Figure 6-6 WIPS Profiles > Profile List

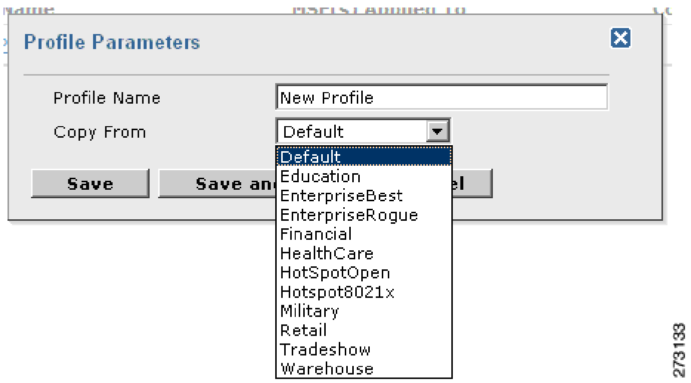


Step 3 Select **Add Profile** from the Select a command drop-down menu.

Step 4 At the profile parameters panel, select a profile template from the Copy From drop-down menu. (Figure 6-7)

Note Cisco's Adaptive wIPS comes with a pre-defined set of profile templates from which customers can choose from 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.

Figure 6-7 Profile Parameters Configuration Panel



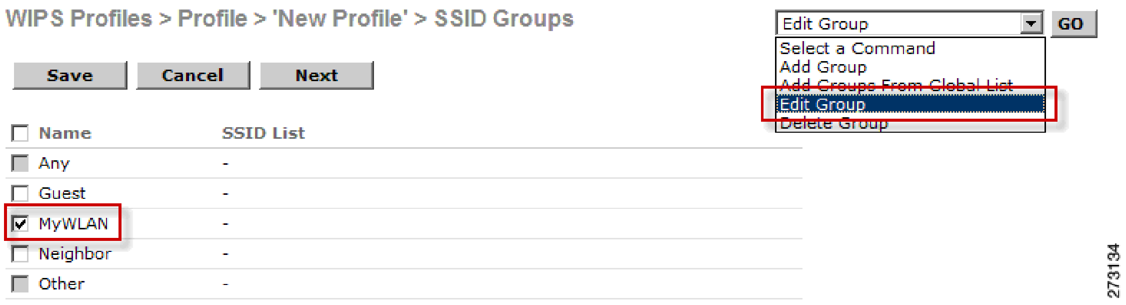
Step 5 After selecting a profile and entering a profile name, click **Save and Edit**.

Step 6 (Optional) Configure the SSIDs to Monitor.

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**.

Figure 6-8 SSID Groups Summary Panel


WIPS Profiles > Profile > 'New Profile' > SSID Groups
Save
Cancel
Next
Edit Group
GO
Select a Command
Add Group
Add Groups From Global List
Edit Group
Delete Group
273134

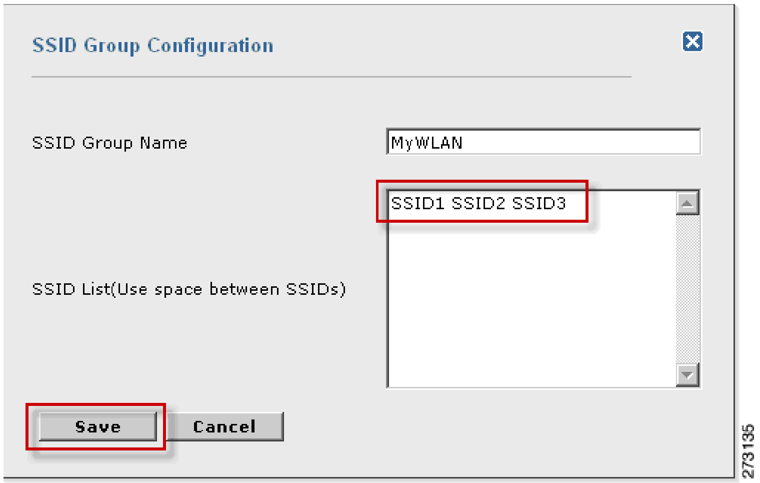
☐ Name	SSID List
☐ Any	-
☐ Guest	-
☑ MyWLAN	-
☐ Neighbor	-
☐ Other	-

a. Check the box next to **MyWLAN** and select **Edit Group** from the drop down in the upper right hand corner then click **GO.**

b. Enter SSIDs to Monitor.

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

Figure 6-9 SSID Group Configuration Panel

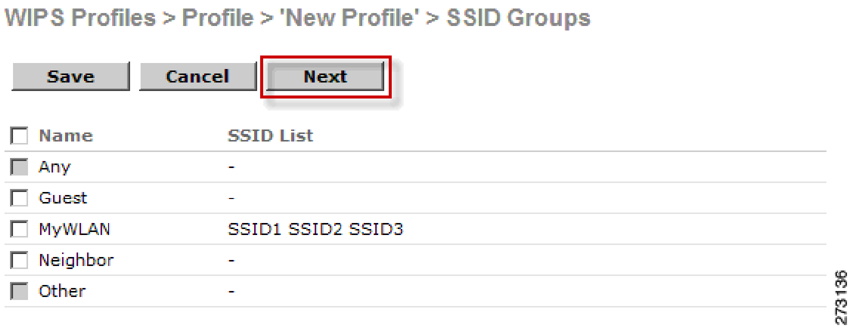


SSID Group Name: MyWLAN

SSID List(Use space between SSIDs): SSID1 SSID2 SSID3

The SSID Groups page appears confirming the SSID are added successfully. (Figure 6-10).

Figure 6-10 New Profile > SSID Groups Window

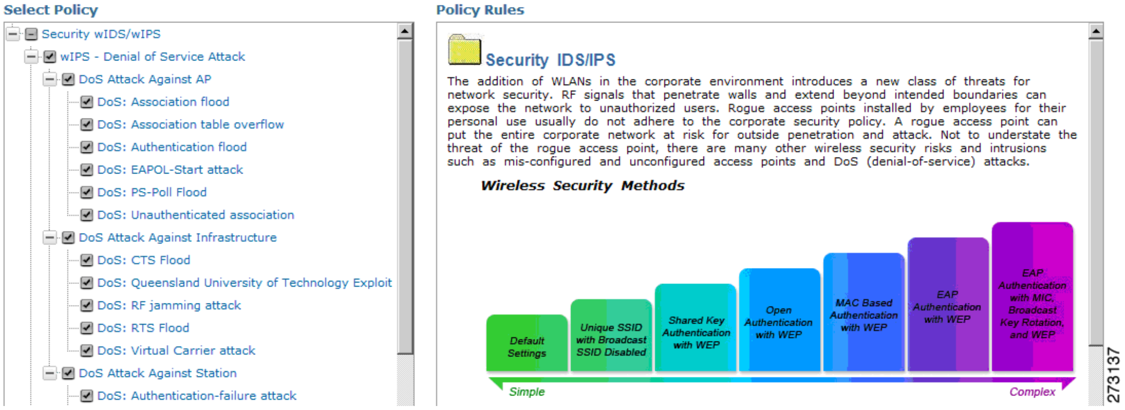


☐ Name	SSID List
☐ Any	-
☐ Guest	-
☐ MyWLAN	SSID1 SSID2 SSID3
☐ Neighbor	-
☐ Other	-

d. Click **Next**.

The Select Policy and Policy Rules summary window appears (Figure 6-11).

Figure 6-11 Next > Select Policy Summary Window



Select Policy

- ☑ Security wIDS/wIPS
  - ☑ wIPS - Denial of Service Attack
    - ☑ DoS Attack Against AP
      - ☑ DoS: Association flood
      - ☑ DoS: Association table overflow
      - ☑ DoS: Authentication flood
      - ☑ DoS: EAPOL-Start attack
      - ☑ DoS: PS-Poll Flood
      - ☑ DoS: Unauthenticated association
    - ☑ DoS Attack Against Infrastructure
      - ☑ DoS: CTS Flood
      - ☑ DoS: Queensland University of Technology Exploit
      - ☑ DoS: RF jamming attack
      - ☑ DoS: RTS Flood
      - ☑ DoS: Virtual Carrier attack
    - ☑ DoS Attack Against Station
      - ☑ DoS: Authentication-failure attack

Policy Rules

Security IDS/IPS

The addition of WLANs in the corporate environment introduces a new class of threats for network security. RF signals that penetrate walls and extend beyond intended boundaries can expose the network to unauthorized users. Rogue access points installed by employees for their personal use usually do not adhere to the corporate security policy. A rogue access point can put the entire corporate network at risk for outside penetration and attack. Not to understate the threat of the rogue access point, there are many other wireless security risks and intrusions such as mis-configured and unconfigured access points and DoS (denial-of-service) attacks.

Wireless Security Methods
Default Settings
Unique SSID with Broadcast SSID Disabled
Shared Key Authentication with WEP
Open Authentication with WEP
MAC Based Authentication with WEP
EAP Authentication with WEP
EAP Authentication with MIC, Broadcast Key Rotation, and WEP
Simple
Complex
273137

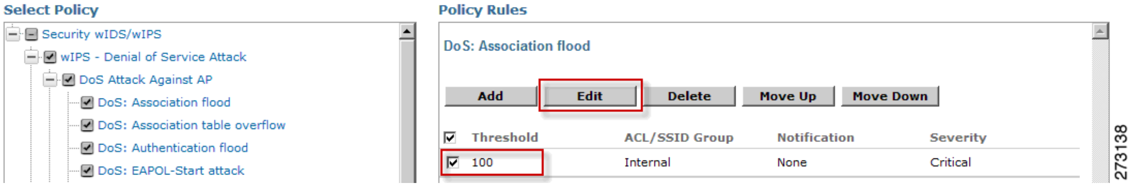
Note At the policy window (Figure 6-11), you can enable or disable attacks to be detected and reported. You can also edit specific thresholds for alarms and turn on forensics.

Step 7 To enable or disable attacks to be detected and reported, check the check box next to the specific attack type in question (left panel).

Step 8 To edit the profile, click on the name of the attack type (such as DoS: Association Flood).

The configuration panel for that attack type appears in the right panel above the policy rule description (Figure 6-12).

Figure 6-12 Policy Rules Panel



Select Policy

- ☑ Security wIDS/wIPS
  - ☑ wIPS - Denial of Service Attack
    - ☑ DoS Attack Against AP
      - ☑ DoS: Association flood
      - ☑ DoS: Association table overflow
      - ☑ DoS: Authentication flood
      - ☑ DoS: EAPOL-Start attack

Policy Rules

DoS: Association flood

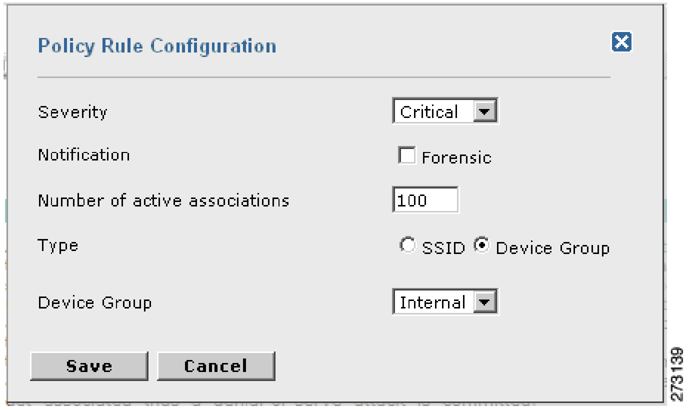
☑ Threshold	ACL/SSID Group	Notification	Severity
☑ 100	Internal	None	Critical

Step 9 To modify a policy rule do the following:

a. Check the check box next to the policy rule and click **Edit**.

The Policy Rule Configuration window appears. (Figure 6-13)

Figure 6-13 Policy Rule Configuration Panel



Policy Rule Configuration

Severity: Critical

Notification: □ Forensic

Number of active associations: 100

Type: ○ SSID ● Device Group

Device Group: Internal

b. Select the severity of the alarm.

c. Check 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 will monitor for attacks.

  1. If you select SSID, continue with Step 10.

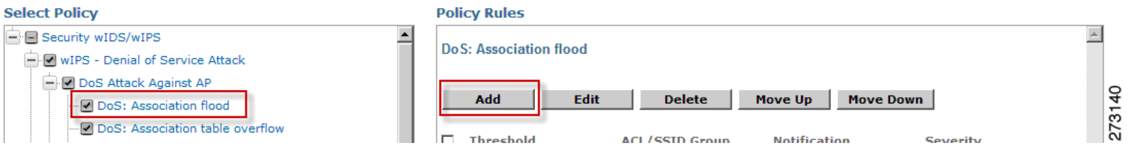
  2. If you select Device Group, continue with Step 11.

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 10 (Optional, overlay deployments only) To add a policy rule for an SSID, do the following:

a. To add a policy rule, click **Add**. (Figure 6-14)

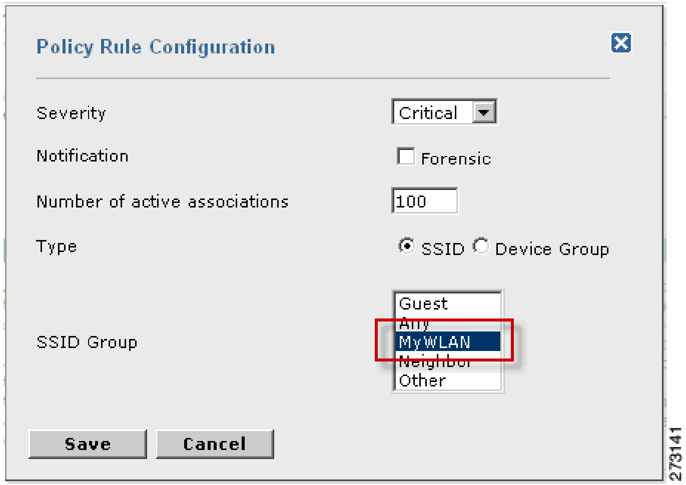
Figure 6-14 Adding a Policy Rule



b. In the policy rule configuration panel that appears, select **MyWLAN** from the SSID Group pull-down menu. (Figure 6-15)

Note SSID is already selected as the type.

Figure 6-15 Policy Configuration Panel for SSIDs



Policy Rule Configuration

Severity: Critical

Notification: □ Forensic

Number of active associations: 100

Type: ● SSID ○ Device Group

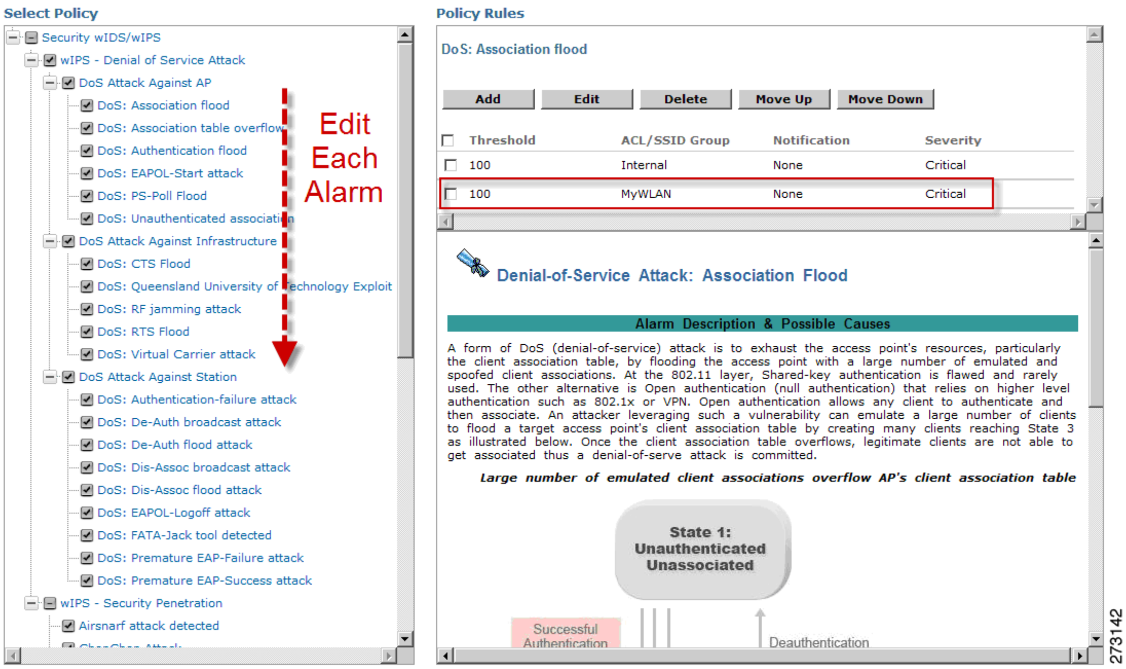
SSID Group: Guest, Any, MyWLAN, Neighbor, Other

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

d. Modify each policy rule.Continue to Step 11 when all edits are complete.

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 by SSID. You must create a policy rule under each separate alarm which defines the system to monitor attacks against the SSID Group created earlier.

Figure 6-16 Edit Policy Rules for SSID Monitoring



Select Policy

- ☐ Security wIDS/wIPS
  - ☑ wIPS - Denial of Service Attack
    - ☑ DoS Attack Against AP
      - ☑ DoS: Association flood
      - ☑ DoS: Association table overflow
      - ☑ DoS: Authentication flood
      - ☑ DoS: EAPOL-Start attack
      - ☑ DoS: PS-Poll Flood
      - ☑ DoS: Unauthenticated association
    - ☑ DoS Attack Against Infrastructure
      - ☑ DoS: CTS Flood
      - ☑ DoS: Queensland University of Technology Exploit
      - ☑ DoS: RF jamming attack
      - ☑ DoS: RTS Flood
      - ☑ DoS: Virtual Carrier attack
    - ☑ DoS Attack Against Station
      - ☑ DoS: Authentication-failure attack
      - ☑ DoS: De-Auth broadcast attack
      - ☑ DoS: De-Auth flood attack
      - ☑ DoS: Dis-Assoc broadcast attack
      - ☑ DoS: Dis-Assoc flood attack
      - ☑ DoS: EAPOL-Logoff attack
      - ☑ DoS: FATA-Jack tool detected
      - ☑ DoS: Premature EAP-Failure attack
      - ☑ DoS: Premature EAP-Success attack
  - ☐ wIPS - Security Penetration
    - ☑ Airsnarf attack detected

Edit Each Alarm

Policy Rules

DoS: Association flood

□	Threshold	ACL/SSID Group	Notification	Severity
□	100	Internal	None	Critical
□	100	MyWLAN	None	Critical

Denial-of-Service Attack: Association Flood

Alarm Description & Possible Causes

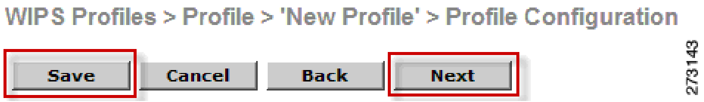
A form of DoS (denial-of-service) attack is to exhaust the access point's resources, particularly the client association table, by flooding the access point with a large number of emulated and spoofed client associations. At the 802.11 layer, Shared-key authentication is flawed and rarely used. The other alternative is Open authentication (null authentication) that relies on higher level authentication such as 802.1x or VPN. Open authentication allows any client to authenticate and then associate. An attacker leveraging such a vulnerability can emulate a large number of clients to flood a target access point's client association table by creating many clients reaching State 3 as illustrated below. Once the client association table overflows, legitimate clients are not able to get associated thus a denial-of-serve attack is committed.

Large number of emulated client associations overflow AP's client association table

State 1: Unauthenticated Unassociated
Successful Authentication
Deauthentication
273142

Step 11 Click **Save** to save the Profile (SSID or Device Group). Click **Next**. (Figure 6-17)

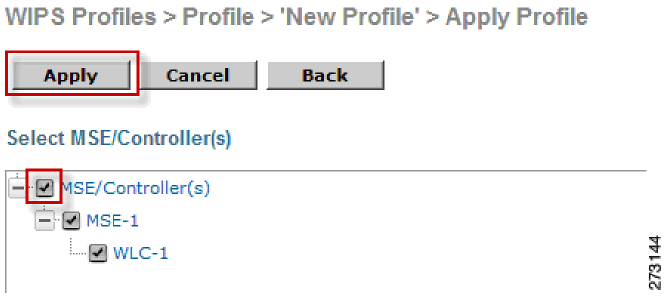
Figure 6-17 Saving Profile Configuration



WIPS Profiles > Profile > 'New Profile' > Profile Configuration

Step 12 Select the MSE/Controller combinations to apply the profile to and then click **Apply**. (Figure 6-18)

Figure 6-18 Applying Profile Configuration.



WIPS Profiles > Profile > 'New Profile' > Apply Profile

Select MSE/Controller(s)

- ☑ MSE/Controller(s)
  - ☑ MSE-1
    - ☑ WLC-1