Configuring Adaptive Wireless Intrusion Prevention System

Finding Feature Information

Your software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Configuring wIPS

• The regular local mode access point has been extended with a subset of Wireless Intrusion Prevention System (wIPS) capabilities. This feature enables you to deploy your access points to provide protection without needing a separate overlay network.

How to Configure wIPS on Access Points

Configuring wIPS on an Access Point (CLI)

Procedure

	Command or Action	Purpose
Step 1	**ap name** *Cisco_AP* **mode local** **Example:** `Device# ap name AP01 mode local`	Configures an access point for monitor mode. A message appears that indicates that changing the AP's mode causes the access point to reboot. This message also displays a prompt that enables you to specify whether or not you want to continue with changing the AP mode. Enter **y** at the prompt to continue.
Step 2	**ap name** *Cisco_AP* **dot11 5ghz shutdown** **Example:** `Device# ap name AP01 dot11 5ghz shutdown`	Disables the 802.11a radio on the access point.
Step 3	**ap name** *Cisco_AP* **dot11 24ghz shutdown** **Example:** `Device# ap name AP02 dot11 24ghz shutdown`	Disables the 802.11b radio on the access point.
Step 4	**ap name** *Cisco_AP* **mode monitor submode wips** **Example:** `Device# ap name AP01 mode monitor submode wips`	Configures the wIPS submode on the access point. **Note** To disable wIPS on the access point, enter the **ap name** *Cisco_AP* **modemonitor submode none** command.
Step 5	**ap name** *Cisco_AP* **monitor-mode wips-optimized** **Example:** `Device# ap name AP01 monitor-mode wips-optimized`	Enables wIPS optimized channel scanning for the access point. The access point scans each channel for 250 milliseconds. It derives the list of channels to be scanned from the monitor configuration. You can choose the following options: • **All**—All channels supported by the access point's radio. • **Country**—Only the channels supported by the access point's country of operation. • **DCA**—Only the channel set used by the dynamic channel assignment (DCA)

	Command or Action	Purpose
		algorithm, which by default includes all of the nonoverlapping channels allowed in the access point's country of operation.
Step 6	**show ap dot11 24ghz monitor** **Example:** `Device# show ap dot11 24ghz monitor`	Displays the monitor configuration channel set. **Note** The 802.11b Monitor Channels value in the output of the command indicates the monitor configuration channel set.

Step 7	**ap name** *Cisco_AP* **no dot11 5ghz shutdown**
	
	Example:
	`Device# ap name AP01 no dot11`
	`5ghz shutdown`
		Enables the 802.11a radio on the access point.

Step 8	**ap name** *Cisco_AP* **no dot11 24ghz shutdown**
	
	Example:
	`Device# ap name AP01 no dot11`
	`24ghz shutdown`
		Enables the 802.11b radio on the access point.

Monitoring wIPS Information

Note   The procedure to perform this task using the device GUI is not currently available.

Procedure

	Command or Action	Purpose
Step 1	**show ap name** *Cisco_AP* **config general** **Example:** `Device# show ap name AP01 config general`	Displays information on the wIPS submode on the access point.
Step 2	**show ap monitor-mode summary** **Example:** `Device# show ap monitor-mode summary`	Displays the wIPS optimized channel scanning configuration on the access point.
Step 3	**show wireless wps wips summary** **Example:** `Device# show wireless wps wips summary`	Displays the wIPS configuration forwarded by NCS or Prime to the device.

	Command or Action	Purpose
Step 4	**show wireless wps wips statistics** **Example:** `Device# show wireless wps wips statistics`	Displays the current state of wIPS operation on the device.
Step 5	**clear wireless wips statistics** **Example:** `Device# clear wireless wips statistics`	Clears the wIPS statistics on the device.

Related Topics

Configuration Examples for Configuring wIPS on Access Points

Displaying the Monitor Configuration Channel Set: Example

This example shows how to display the monitor configuration channel set:

```
Device# show ap dot11 24ghz monitor
Default 802.11b AP monitoring
802.11b Monitor Mode........................... enable
802.11b Monitor Channels....................... Country channels
802.11b AP Coverage Interval................... 180 seconds
802.11b AP Load Interval....................... 60 seconds
802.11b AP Noise Interval...................... 180 seconds
802.11b AP Signal Strength Interval............ 60 seconds
```

Displaying wIPS Information: Examples

This example shows how to display information on the wIPS submode on the access point:

```
Device# show ap name AP01 config general
Cisco AP Identifier.............. 3
Cisco AP Name.................... AP1131:46f2.98ac
...
AP Mode ......................... Monitor
Public Safety ................... Disabled Disabled
AP SubMode ...................... WIPS
```

This example shows how to display the wIPS optimized channel scanning configuration on the access point:

```
Device# show ap monitor-mode summary
AP Name        Ethernet MAC    Status    Scanning
                                         Channel
                                         List
------------- -------------- -------- ---------
AP1131:4f2.9a 00:16:4:f2:9:a WIPS     1,6,NA,NA
```

This example shows how to display the wIPS configuration forwarded by WCS to the device:

```
Device# show wireless wps wips summary
Policy Name.............. Default
Policy Version........... 3
```

This example shows how to display the current state of wIPS operation on the device:

```
Device# show wireless wps wips statistics
Policy Assignment Requests............ 1
Policy Assignment Responses........... 1
Policy Update Requests................ 0
Policy Update Responses............... 0
Policy Delete Requests................ 0
Policy Delete Responses............... 0
Alarm Updates......................... 13572
Device Updates........................ 8376
Device Update Requests................ 0
Device Update Responses............... 0
Forensic Updates...................... 1001
Invalid WIPS Payloads................. 0
Invalid Messages Received............. 0
CAPWAP Enqueue Failed................. 0
NMSP Enqueue Failed................... 0
NMSP Transmitted Packets.............. 22950
NMSP Transmit Packets Dropped......... 0
NMSP Largest Packet................... 1377
```