IP Source Guard

Information About IP Source Guard

IP Source Guard (IPSG) is a Layer 2 security feature in the Cisco Catalyst 9800 Series Wireless Controller . It supports both IPv4 and IPv6 wireless clients.

The IPSG feature prevents the wireless controller from forwarding the packets, with the source IP addresses that are not known to it. This security feature is not enabled by default and has to be explicitly configured. It is enabled on a per WLAN basis, and all the wireless clients joining that WLAN inherits this feature.

The wireless controller maintains an IP/MAC pair binding table for the IPSG feature. Using this table, the wireless controller keeps track of IP and MAC address combination (binding) information for all the wireless clients. This binding information is captured as part of the IP learning process. When the feature is enabled on a WLAN, the wireless controller forwards the incoming packets (from the wireless clients) only if it finds a matching binding table entry corresponding to the source IP and MAC address combination of those packets. Otherwise, the packets are dropped.

Configuring IP Source Guard (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **WLANs**.

Step 2 Click the WLAN.

Step 3 In the **Advanced** tab, check the **IP Source Guard** checkbox.

Step 4 Click **Update & Apply to Device**.

Configuring IP Source Guard

Follow the procedure given below to configure IPSG:

Before you begin

Cisco Catalyst 9800 Series Wireless Controller supports only one IPv4 address for a client and up to 8 IPv6 addresses (including link local addresses) per client.

Procedure

	Command or Action	Purpose
Step 1	**wlan** *profile-name wlan-id ssid* **Example:** `Device(config)# wlan mywlan 34 mywlan-ssid`	Specifies the WLAN name and ID to use. **Note** If a WLAN is not already configured, this step creates the WLAN.
Step 2	**shutdown** **Example:** `Device(config-wlan)# shutdown`	Disables the WLAN.
Step 3	**ip verify source mac-check** **Example:** `Device(config-wlan)# ip verify source mac-check`	Enables the IP Source Guard feature.
Step 4	**no shutdown** **Example:** `Device(config-wlan)# no shutdown`	Enables the WLAN.