Configuring IP Source Guard

This chapter describes how to configure IP Source Guard on Cisco NX-OS devices.

This chapter includes the following sections:

About IP Source Guard

IP Source Guard is a per-interface traffic filter that permits IP traffic only when the IP address and MAC address of each packet matches one of two sources of IP and MAC address bindings:

- Entries in the Dynamic Host Configuration Protocol (DHCP) snooping binding table
- Static IP source entries that you configure

Filtering on trusted IP and MAC address bindings helps prevent spoofing attacks, in which an attacker uses the IP address of a valid host to gain unauthorized network access. To circumvent IP Source Guard, an attacker would have to spoof both the IP address and the MAC address of a valid host.

You can enable IP Source Guard on Layer 2 interfaces that are not trusted by DHCP snooping. IP Source Guard supports interfaces that are configured to operate in access mode and trunk mode. When you initially enable IP Source Guard, all inbound IP traffic on the interface is blocked except for the following:

- DHCP packets, which DHCP snooping inspects and then forwards or drops, depending upon the results of inspecting the packet
- IP traffic from static IP source entries that you have configured on the Cisco NX-OS device

The device permits the IP traffic when DHCP snooping adds a binding table entry for the IP address and MAC address of an IP packet or when you have configured a static IP source entry.

The device drops IP packets when the IP address and MAC address of the packet do not have a binding table entry or a static IP source entry. For example, assume that the **show ip dhcp snooping binding** command displays the following binding table entry:

```
MacAddress         IpAddress    LeaseSec   Type           VLAN    Interface
-----------------  ----------   ---------  -------------  ----    ---------
00:02:B3:3F:3B:99  10.5.5.2     6943       dhcp-snooping  10      Ethernet2/3
```

If the device receives an IP packet with an IP address of 10.5.5.2, IP Source Guard forwards the packet only if the MAC address of the packet is 00:02:B3:3F:3B:99.

Prerequisites for IP Source Guard

IP Source Guard has the following prerequisites:

- You must enable the DHCP feature and DHCP snooping before you can configure IP Source Guard. See Configuring DHCP.
- You must configure the ACL TCAM region size for IP Source Guard using the **hardware access-list tcam region ipsg** command. See Configuring ACL TCAM Region Sizes.

Note By default the ipsg region size is zero. You need to allocate enough entries to this region for storing and enforcing the SMAC-IP bindings.

Guidelines and Limitations for IP Source Guard

IP Source Guard has the following configuration guidelines and limitations:

- IP Source Guard limits IP traffic on an interface to only those sources that have an IP-MAC address binding table entry or static IP source entry. When you first enable IP Source Guard on an interface, you may experience disruption in IP traffic until the hosts on the interface receive a new IP address from a DHCP server.
- IP Source Guard is dependent upon DHCP snooping to build and maintain the IP-MAC address binding table or upon manual maintenance of static IP source entries.
- IP Source Guard is not supported on fabric extender (FEX) ports or generic expansion module (GEM) ports.
- The following guidelines and limitations apply to the Cisco Nexus 9200 Series switches:
  - IPv6 adjacency is not formed with IPSG enabled on the incoming interface.
  - IPSG drops ARP packets at HSRP standby.
  - With DHCP snooping and IPSG enabled, if a binding entry exists for the host, traffic is forwarded to the host even without ARP.

- Beginning with Cisco NX-OS Release 9.3(5), IP Source Guard is supported on Cisco Nexus 9364C-GX, Cisco Nexus 9316D-GX, and Cisco Nexus 93600CD-GX switches.
- IP Source Guard does not require TCAM carving on the Cisco Nexus 9300-X Cloud Scale Switches.

Default Settings for IP Source Guard

This table lists the default settings for IP Source Guard parameters.

Table 1: Default IP Source Guard Parameters

Parameters	Default
IP Source Guard	Disabled on each interface
IP source entries	None. No static or default IP source entries exist by default.

Configuring IP Source Guard

Enabling or Disabling IP Source Guard on a Layer 2 Interface

You can enable or disable IP Source Guard on a Layer 2 interface. By default, IP Source Guard is disabled on all interfaces.

Before you begin

Make sure that the DHCP feature and DHCP snooping are enabled.

Make sure that the ACL TCAM region size for IPSG (ipsg) is configured.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**interface ethernet** *slot/port*
	Example:
	`switch(config)# interface ethernet 2/3`
	`switch(config-if)#`
		Enters interface configuration mode for the specified interface.

Step 3	[**no**] **ip verify source dhcp-snooping-vlan** **Example:** `switch(config-if)# ip verify source dhcp-snooping vlan`	Enables IP Source Guard on the interface. The **no** form of this command disables IP Source Guard on the interface.

	Command or Action	Purpose
Step 4	(Optional) **show running-config dhcp** **Example:** `switch(config-if)# show running-config dhcp`	Displays the running configuration for DHCP snooping, including the IP Source Guard configuration.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch(config-if)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Adding or Removing a Static IP Source Entry

You can add or remove a static IP source entry on the device. By default, there are no static IP source entries.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	[**no**] **ip source binding** *ip-address mac-address* **vlan** *vlan-id* **interface** *interface-type slot/port* **Example:** `switch(config)# ip source binding 10.5.22.17 001f.28bd.0013 vlan 100 interface ethernet 2/3`	Creates a static IP source entry for the current interface. The **no** form of this command removes the static IP source entry.
Step 3	(Optional) **show ip dhcp snooping binding** [**interface** *interface-type slot/port*] **Example:** `switch(config)# show ip dhcp snooping binding interface ethernet 2/3`	Displays IP-MAC address bindings for the interface specified, including static IP source entries. Static entries appear with the term in the Type column.
Step 4	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Configuring IP Source Guard for Trunk Ports

When IP Source Guard is configured on a port, traffic coming on that port will be dropped unless there is a DHCP snooping entry to allow it in the TCAM. However, when IP Source Guard is configured on trunk ports and you do not want traffic coming on certain VLANs to undergo this check (even if DHCP snooping is not enabled on them), you can specify a list of VLANs to exclude.

Before you begin

Make sure that the DHCP feature and DHCP snooping are enabled.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	[**no**] **ip dhcp snooping ipsg-excluded vlan** *vlan-list* **Example:** `switch(config)# ip dhcp snooping ipsg-excluded vlan 1001-1256,3097`	Specifies the list of VLANs to exclude from the DHCP snooping check for IP Source Guard on trunk ports.
Step 3	(Optional) **show ip ver source** [**ethernet** *slot/port* | **port-channel** *channel-number*] **Example:** `switch(config)# show ip ver source`	Displays which VLANs are excluded.
Step 4	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Displaying IP Source Guard Bindings

Use the **show ip ver source** [**ethernet** *slot/port* | **port-channel** *channel-number*] command to display the IP-MAC address bindings.

Clearing IP Source Guard Statistics

To clear IP Source Guard statistics, use the commands in this table.

Command	Purpose
clear access-list ipsg stats [**instance** *number* | **module** *number*]	Clears IP Source Guard statistics.

Configuration Example for IP Source Guard

This example shows how to create a static IP source entry and enable IP Source Guard on an interface:

```
ip source binding 10.5.22.17 001f.28bd.0013 vlan 100 interface ethernet 2/3
interface ethernet 2/3
  no shutdown
  ip verify source dhcp-snooping-vlan
  show ip ver source

  IP source guard excluded vlans:
  -------------------------------------------------------
  None

  -----------------------------------
  IP source guard is enabled on the following interfaces:
  -------------------------------------------------------
        ethernet2/3
```

Additional References

Related Documents

Related Topic	Document Title
ACL TCAM regions	Configuring IP ACLs
DHCP and DHCP snooping	Configuring DHCP