CHAPTER 14

# Configuring IP Source Guard

This chapter describes how to configure IP Source Guard on Cisco Nexus 1000Vs.

This chapter includes the following sections:



## Information 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 the IP and MAC address bindings of dynamic or static IP source entries in the Dynamic Host Configuration Protocol (DHCP) snooping binding table.

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 in the Cisco Nexus 1000V.

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:

Send document comments to nexus1k-docfeedback@cisco.com.

```
MacAddress          IpAddress    LeaseSec   Type         VLAN      Interface
----------          ----------   ---------  ------       -------    ----------
00:02:B3:3F:3B:99   10.5.5.2       6943    dhcp-snooping  10      vEthernet3
```

If the device receives an IP packet with an IP address of 10.5.5.2, IP Source Guard forward 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 should be familiar with DHCP snooping before you configure IP Source Guard.
- DHCP snooping is enabled (see the "Configuring DHCP Snooping" section on page 12-4).

# Guidelines and Limitations

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. For more information on DHCP snooping, see Chapter 12, "Configuring DHCP Snooping."
- For seamless IP Source Guard, Virtual Service Domain (VSD) service VM ports are trusted ports by default. If you configure these ports as untrusted, this setting is ignored.

# Default Settings

Table 14-1 lists IP Source Guard defaults.

***Table 14-1 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

This section includes the following topics:

Send document comments to nexus1k-docfeedback@cisco.com.

# Enabling or Disabling IP Source Guard on a Layer 2 Interface

Use this procedure to enable or disable IP Source Guard on a Layer 2 interface.

## BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- By default, IP Source Guard is disabled on all interfaces.
- Ensure that DHCP snooping is enabled. For more information, see the "Enabling or Disabling the DHCP Feature" section on page 12-5.

## SUMMARY STEPS

1. **config t**
2. **interface vethernet** *interface-number*

   **port-profile** *profilename*
3. **[no] ip verify source dhcp-snooping-vlan**
4. **show running-config dhcp**
5. **copy running-config startup-config**

## DETAILED STEPS

| | Command | Purpose |
|---|---|---|
| **Step 1** | **config t**<br><br>**Example:**<br>switch# config t<br>switch(config)# | Enters global configuration mode. |
| **Step 2** | **interface vethernet** *interface-number*<br><br>**Example:**<br>switch(config)# interface vethernet 3<br>switch(config-if)# | Enters interface configuration mode, where *interface-number* is the vEthernet interface that you want to configure as trusted or untrusted for DHCP snooping. |
| | **port-profile** *profilename*<br><br>**Example:**<br>switch(config)# port-profile vm-data<br>switch(config-port-prof)# | Enters port profile configuration mode for the specified port profile, where *profilename* is a unique name of up to 80 characters. |
| **Step 3** | **[no] ip verify source dhcp-snooping-vlan**<br><br>**Example:**<br>switch(config-if)# ip verify source dhcp-snooping vlan | Enables IP Source Guard on the interface. The **no** option disables IP Source Guard on the interface. |
| **Step 4** | **show running-config dhcp**<br><br>**Example:**<br>switch(config-if)# show running-config dhcp | (Optional) Displays the running configuration for DHCP snooping, including the IP Source Guard configuration. |

Send document comments to nexus1k-docfeedback@cisco.com.

| | Command | Purpose |
|---|---|---|
| Step 5 | **copy running-config startup-config**<br><br>**Example:**<br>`switch(config-if)# copy running-config startup-config` | (Optional) Copies the running configuration to the startup configuration. |

# Adding or Removing a Static IP Source Entry

Use this procedure to add or remove a static IP source entry on a device.

## BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- By default, there are no static IP source entries on a device.

## SUMMARY STEPS

1. **config t**
2. [**no**] **ip source binding** *IP-address MAC-address* **vlan** *vlan-ID* **interface vethernet** *interface-number*
3. **show ip dhcp snooping binding [interface vethernet** *interface-number*]
4. **copy running-config startup-config**

## DETAILED STEPS

| | Command | Purpose |
|---|---|---|
| Step 1 | **config t**<br><br>**Example:**<br>`switch# config t`<br>`switch(config)#` | Enters global configuration mode. |
| Step 2 | [**no**] **ip source binding** *IP-address MAC-address* **vlan** *vlan-ID* **interface vethernet** *interface-number*<br><br>**Example:**<br>`switch(config)# ip source binding 10.5.22.17 001f.28bd.0013 vlan 100 interface ethernet 3` | Creates a static IP source entry for the current interface, or if you use the **no** option, removes a static IP source entry. |
| Step 3 | **show ip dhcp snooping binding** [**interface vethernet** *interface-number*]<br><br>**Example:**<br>`switch(config)# show ip dhcp snooping binding interface ethernet 3` | (Optional) Displays IP-MAC address bindings for the interface specified, including static IP source entries. Static entries appear with the term “static” in the Type column. |
| Step 4 | **copy running-config startup-config**<br><br>**Example:**<br>`switch(config)# copy running-config startup-config` | (Optional) Copies the running configuration to the startup configuration. |

Send document comments to nexus1k-docfeedback@cisco.com.

# Verifying the IP Source Guard Configuration

To display IP Source Guard configuration information, use one of the following commands:

| Command | Purpose |
|---|---|
| **show running-config dhcp** | Displays DHCP snooping configuration, including the IP Source Guard configuration. |
| **show ip verify source** | Displays IP-MAC address bindings. |

For detailed information about command output, see the *Cisco Nexus 1000V Command Reference, Release 4.2(1)SV1(4)*.

# Displaying IP Source Guard Bindings

Use the **show ip verify source** command to display IP-MAC address bindings.

# Example Configuration for IP Source Guard

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

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

# Additional References

For additional information related to implementing IP Source Guard, see the following sections:

- Related Documents, page 14-5
- Standards, page 14-6

## Related Documents

| Related Topic | Document Title |
|---|---|
| Information About DHCP Snooping, page 12-1 | *Cisco Nexus 1000V Security Configuration Guide, Release 4.2(1)SV1(4a), Chapter 12, "Configuring DHCP Snooping"* |
| IP Source Guard commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples | *Cisco Nexus 1000V Command Reference, Release 4.2(1)SV1(4)* |
| DHCP snooping commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples | *Cisco Nexus 1000V Command Reference, Release 4.2(1)SV1(4)* |

Send document comments to nexus1k-docfeedback@cisco.com.

## Standards

| Standards | Title |
|---|---|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | — |

# Feature History for IP Source Guard

Table 14-2 lists the release history for this feature.

*Table 14-2 Feature History for IP Source Guard*

| Feature Name | Releases | Feature Information |
|---|---|---|
| IP Source Guard | 4.0(4)SV1(2) | This feature was introduced. |