Configuring IP Source Guard

This chapter contains the following sections:

Information About IP Source Guard

IP Source Guard (IPSG) 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. This feature enables you to control the egress network traffic at the source point. You can configure IPSG in two modes: IP-only mode and IP-MAC mode. The IP-only mode allows you to filter the traffic based on the IP address. The IP address and MAC address combination is used to filter traffic in the IPSG IP-MAC mode. Starting with Cisco Nexus 1000V switch, Release 5.2(1)SV3(2.1), you can now bind multiple IP addresses to a single MAC address for traffic filtering. The multi-IP per MAC functionality enables you to manage traffic from multiple trusted VLANs in a network.

IPSG multi-IP per MAC feature is required to manage traffic when multiple IP addresses are originating from the same interface. For example, you need IPSG multi-IP per MAC feature to source guard a router configured behind a Nexus 1000V switch on a virtual ethernet (veth) trunk port.

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 a source whose static IP entries are configured in the Cisco Nexus 1000V.

The device permits IP packets if the IP address and MAC address of the packet matches a binding table entry or a static IP source entry in the DHCP binding table.

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      vEthernet3
```

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.

Starting with Release 4.2(1)SV2(1.1), you can filter the IP traffic based on the source IP address only as opposed to filtering the traffic based on the IP-MAC Address pair. For more information, refer to Enabling Source IP-Based Filtering.

Prerequisites for IP Source Guard

- You should be familiar with DHCP snooping before you configure IP Source Guard.
- DHCP snooping is enabled.

Guidelines and Limitations for IP Source Guard

- 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 might experience disruption in the IP traffic until the hosts on the interface receive a new IP address from a DHCP server.
- When the IP Source Guard (IPSG) functionality is enabled on the Cisco Nexus 1000V switch and whenever a duplicate IP address is detected on a port, it is error-disabled.
- 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 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.
- You can attach a maximum of 30 static IP addresses to a single MAC address with mult-IP-per-MAC feature enabled.
- Multi-IP per MAC feature is supported only for static IPSG entries in the DHCP snooping table.

Default Settings for IP Source Guard

Parameters	Default
IP Source Guard	Disabled on each interface.

Parameters	Default
IP source entries	None. No static or default IP source entries exist by default.

Configuring IP Source Guard Functionality

Enabling or Disabling IP Source Guard on a Layer 2 Interface

By default, IP Source Guard is disabled on all interfaces. You can configure IP Source Guard on either an interface or a port profile.

Before you begin

Ensure that DHCP snooping is enabled.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **interface vethernet** *interface-number*	Enters interface configuration mode, where *interface-number* is the vEthernet interface that you want to configure as trusted or untrusted for DHCP snooping.
Step 3	switch(config)# **port-profile** *profilename*	Places you in port profile configuration mode for the specified port profile.
Step 4	switch(config-if)# [**no**] **ip verify source dhcp-snooping-vlan**	Enables IP Source Guard on the interface. The **no** option disables IP Source Guard on the interface.
Step 5	(Optional) switch(config-if)# **show ip verify source interface vethernet interface number**	Displays the IP Source Guard configuration.
Step 6	(Optional) switch(config-if)# **copy running-config startup-config**	Copies the running configuration to the startup configuration.

Example

This example shows how to enable IP Source Guard on a Layer 2 interface:

```
switch# configure terminal
switch(config)# interface vethernet 3
switch(config-if)# ip verify source dhcp-snooping-vlan
switch (config-if)# show ip verify source interface vethernet 3

Filter Mode(for static bindings): IP-MAC
IP source guard is  enabled on this interface.
```

```
Interface         Filter-mode             IP-address     Mac-address       Vlan
----------    -----------           ----------     -----------    ----
Vethernet3        active                   1.182.56.137    00:50:56:82:56:3e  1053
```

Configuring Multi-IP per MAC feature

Use this procedure to configure multi-IP per MAC feature on IPSG on an interface.

Before you begin

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

- Ensure that IP Source Guard feature is enabled.
- Ensure that DHCP snooping is enabled.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **feature dhcp**	Enters global configuration mode.
Step 3	switch(config)# **ip source binding allow multi-ip-per-mac**	Enables multi-IP per MAC address functionality.
Step 4	switch(config)# **ip source binding** *ip_address mac_address* **vlan** *vlan_Number***interface vethernet***vethernet_number*	Enables multi-IP per MAC address functionality.
Step 5	switch(config)# **port-profile port_profile_Name**	Enables multi-IP per MAC address functionality.
Step 6	Required: switch(config-port-prof))# **ip verify source dhcp-snooping-vlan**	Copies the running configuration to the startup configuration.
Step 7	Required: switch(config-port-prof))# **end**	Copies the running configuration to the startup configuration.
Step 8	switch(config)# **copy running-config start-config**	(Optional) Displays the running configuration for DHCP snooping, including the IP Source Guard configuration.
Step 9	switch(config)# **show running-config dhcp**	(Optional) Displays the running configuration for DHCP snooping, including the IP Source Guard configuration.

Example

The following example shows how to configure multi-IP per MAC feature on IPSG:

```
switch# configure terminal
switch(config)# feature dhcp
switch(config)# ip source binding 1.1.1.1 0050.5695.ae38 vlan 2611 interface vethernet 1
switch(config)# ip source binding 1.1.1.2 0050.5695.ae38 vlan 2611 interface vethernet 1
switch(config)# ip source binding 1.1.1.3 0050.5695.ae38 vlan 2611 interface vethernet 1
switch(config)# port-profile port_profile_1
switch(config-port-prof)# ip verify source dhcp-snooping-vlan
switch(config-port-prof)# end
switch(config)# copy running-config startup-config
switch(config)#
```

Configuration Example for IP Source Guard

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

```
switch# configure terminal
switch(config)# ip source binding 10.5.22.17 001f.28bd.0013 vlan 100 interface vethernet 3
switch(config)# interface Vethernet 3
switch(config)# ip verify source dhcp-snooping-vlan
switch(config-port-prof)# show ip verify source interface vethernet 3
Filter Mode(for static bindings): IP-MAC
IP source guard is  enabled on this interface.

Interface         Filter-mode             IP-address     Mac-address       Vlan
------      -----------             ----------     --------------    ----
Vethernet3        active              10.5.22.17     00:1f:28:bd:00:13  100
```

Configuration Example for Multi-IP per MAC Support

The following example shows how to configure multi-IP per MAC support on IP Source Guard on an interface:

```
switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# feature dhcp
switch(config)# ip source binding allow multi-ip-per-mac
switch(config)# ip source binding 1.1.1.1 0050.5695.ae38 vlan 2611 interface vethernet 1
switch(config)# ip source binding 1.1.1.1 0050.5695.ae38 vlan 2611 interface vethernet 1
switch(config)# ip source binding 1.1.1.1 0050.5695.ae38 vlan 2611 interface vethernet 1
switch(config)# port-profile port_profile_1
switch(config-port-prof)# ip verify source dhcp-snooping-vlan
switch(config-port-prof)# end
switch(config)# copy running-config startup-config
switch(config)#
```

Verifying the IP Source Guard Configuration

Use the following commands to display and verify the IPSG configuration:

Command	Purpose
show running-config dhcp	Displays DHCP snooping configuration, including the IP Source Guard configuration.

Command	Purpose
show ip verify source	Displays IP-MAC address bindings.
Show ip source binding filter-mode	Displays IPSG filtering mode configured on the interface.
Show ip dhcp snooping binding static	Displays IPSG static entries in DHCP snooping table.

The following example displays the DHCP snooping configuration including IPSG configuration:

```
Nexus-1000v# show running-config dhcp
!Command: show running-config dhcp
!Time: Tue Jun 21 10:30:16 2016

version 5.2(1)SV3(2.1)
feature dhcp


interface Vethernet1
  ip verify source dhcp-snooping-vlan
ip dhcp snooping
ip dhcp snooping vlan 2611
ip source binding allow multi-ip-per-mac
no ip dhcp relay
ip source binding 1.1.1.1 0050.5695.ae38 vlan 2611 interface Vethernet1
ip source binding 1.1.1.2 0050.5695.ae38 vlan 2611 interface Vethernet1
ip source binding 1.1.1.3 0050.5695.ae38 vlan 2611 interface Vethernet1
```

The following example displays the multi-IP per MAC support configuration on IP Source Guard on an interface:

```
Nexus-1000v# sh ip verify source
Filter Mode(for static bindings): IP-MAC
IP source guard is enabled on the following interfaces:
------------------------------------------------------
        Vethernet1


IP source guard operational entries:
-----------------------------------
Interface         Filter-mode             IP-address     Mac-address       Vlan
------------      -----------             ----------     --------------    ----
Vethernet1        active                  1.1.1.1        00:50:56:95:ae:38  2611
Vethernet1        active                  1.1.1.2        00:50:56:95:ae:38  2611
Vethernet1        active                  1.1.1.3        00:50:56:95:ae:38  2611
```

The following example displays IP Source Guard filtering mode configured on an interface:

```
Nexus-1000v# sh ip source binding filter-mode
DHCP Snoop Filter Mode(for static bindings) = IP-MAC
DHCP Snoop Multi IP Addresses Per MAC(for static bindings)= Allowed
Nexus-1000v#
```

The following example displays IP Source Guard static entries in DHCP snooping table:

```
MacAddress         IpAddress        LeaseSec     Type       VLAN  Interface
-----------------         ------------      --------   ----------   ----  -------------
00:50:56:95:ae:38          1.1.1.1          infinite    static      2611  Vethernet1
00:50:56:95:ae:38          1.1.1.2          infinite    static      2611  Vethernet1
00:50:56:95:ae:38          1.1.1.3          infinite    static      2611  Vethernet1
Nexus-1000v#
```

Monitoring IP Source Guard Bindings

Use the following command to monitor IP Source Guard Bindings.

Command	Purpose
show ip verify source	Displays IP-MAC address bindings

Feature History for IP Source Guard

This table only includes updates for those releases that have resulted in additions to the feature.

Feature Name	Releases	Feature Information
Mulit-IP per MAC Support	5.2(1)SV3(2.1)	Bind multiple IP addresses to a single MAC address for traffic filtering.
Licensing Changes	4.2(1)SV2(1.1)	IP Source Guard is available as an advanced feature. Use the **feature dhcp** command to enable the feature.
Enabling Source IP Based Filtering	4.2(1)SV2(1.1)	You can enable source IP-based filtering on the Cisco Nexus 1000V switch.
IP Source Guard	4.0(4)SV1(2)	This feature was introduced.