IP Source Guard for an Interface

An IP source guard filters a source IP address on a layer 2 port and prevents malicious hosts from impersonating a legitimate host. The feature uses dynamic DHCP snooping and static IP source binding to match IP addresses to hosts on untrusted layer 2 access ports.

Initially, all IP traffic on the bridge domain associated with the DHCP snooping in a particular interface is blocked except for DHCP packets that are captured by DHCP snooping. After a client receives an IP address from the DHCP server, or after static IP source binding is configured by the administrator, the IP source guard feature automatically creates TCAM entries to permit that traffic. Traffic from other hosts is denied. This filtering limits the ability of a host to attack the network by claiming the IP address of a neighbor host.

Restrictions for IP Source Guard

- IP Source Guard (IPSG) configuration is supported only on interface level at 12 bridge domain interfaces.
- IPSG configuration works only if DHCP snooping binding is enabled.
- Only IP filtering is supported. IP MAC filter mode is not supported.
- IPSG configuration is not supported on port-channels, trunk EFP, and on BDI interfaces.
- IPSG is not supported on routed interfaces, layer2 and layer3 VPN and VRF.
- IPSG is supported only on video template.
- The IPSG entries are in IPv4 Tunnel TCAM region of ASIC. Since this a sharing model, any feature contributing more entries in this region impacts the scalability of other features.
- IPv6 is not supported. IPv4 and IPv6 packets that have IPv6 as first header is included under this restriction.

- Due to IPv4 tunnel TCAM region space limitation, only 1000 TCAM entries are supported. So, only 1000 IPSG entries are supported (including permit and deny entry). This impacts only the IP packets. Layer2 packets flow is not affected.
- If PBR and IPSG are enabled in a node at the same time, 1000 entries are shared by PBR and IPSG based on first come, first serve basis. If PBR is not enabled in the node, IPSG can be scaled to 1000.
- As IPSG and PBR share the same region, for a particular interface, these features are mutually exclusive.
- PBR is not supported on BDI that is associated with the IPSG enabled interface.
- ACL on EFP and IPSG perform the same functionality, that is, to deny or permit traffic on the EFP. So, when both of these features are enabled in the same EFP, both lookups are launched in parallel. So, either of the features deny the non-matching traffic. When ACL gives permit action and IPSG gives deny action for the same traffic, packets get denied, and vice versa. Only when both the features give permit action, traffic is permitted. Hence, though there is no restriction for configuring both the features on the same EVC, ideally these two features should be considered mutually exclusive.

Configuring IP Source Guard

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface gigabitethernet** *slot/port* or **interface tengigabitethernet** *slot/port* or **interface port-channel** *type*
4. **ip verify source bridge-domain dhcp-snooping**
5. [**no**] **service instance** id **ethernet** [service-name]
6. **encapsulation dot1q** *vlan-id*
7. **rewrite ingress tag** {**push** {**dot1q** *vlan-id* | **dot1q** *vlan-id* **second-dot1q** *vlan-id* | **dot1ad** *vlan-id* **dot1q** *vlan-id*} | **pop** {**1** | **2**} | **translate** {**1-to-1** {**dot1q** *vlan-id* | **dot1ad** *vlan-id*} | **2-to-1 dot1q** *vlan-id* | **dot1ad** *vlan-id}*| 1-to-2 {dot1q *vlan-id* **second-dot1q** *vlan-id* | **dot1ad** *vlan-id* **dot1q** *vlan-id*} | **2-to-2** {**dot1q** *vlan-id* **second-dot1q** *vlan-id*}} **symmetric**
8. [**no**] **bridge-domain** *bridge-id*
9. **exit**
10. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**interface gigabitethernet** *slot/port* or **interface tengigabitethernet** *slot/port* or **interface port-channel** *type* **Example:** `Switch(config)# interface gigabitethernet 0/1`	Specifies the interface to configure. • *slot/port* - Specifies the location of the interface. • *type* - Specifies the port channel interface.
Step 4	**ip verify source bridge-domain dhcp-snooping** **Example:** `Switch(config-if)# ip verify source bridge-domain dhcp-snooping`	Enables the IP source guard states. The **dhcp-snooping** option applies the feature to all VLANs on the interface that have DHCP snooping enabled.
Step 5	[**no**] **service instance** id **ethernet** [service-name] **Example:** `Switch(config-if)# service instance 101 ethernet`	Defines the matching criteria to be used in order to map ingress dot1q frames on an interface to the appropriate service instance.
Step 6	**encapsulation dot1q** *vlan-id* **Example:** `Switch(config-if-srv)# encapsulation dot1q 13`	Defines the matching criteria to be used in order to map ingress dot1q frames on an interface to the appropriate service instance.
Step 7	**rewrite ingress tag** {**push** {**dot1q** *vlan-id* | **dot1q** *vlan-id* **second-dot1q** *vlan-id* | **dot1ad** *vlan-id* **dot1q** *vlan-id*} | **pop** {**1** | **2**} | **translate** {**1-to-1** {**dot1q** *vlan-id* | **dot1ad** *vlan-id*}| **2-to-1 dot1q** *vlan-id* | **dot1ad** *vlan-id}*| 1-to-2 {dot1q *vlan-id* **second-dot1q** *vlan-id* | **dot1ad** *vlan-id* **dot1q** *vlan-id*} | **2-to-2** {**dot1q** *vlan-id* **second-dot1q** *vlan-id*}} **symmetric** **Example:** `Switch(config-if-srv)# rewrite ingress tag pop 1 symmetric`	Specifies the tag manipulation that is to be performed on the frame ingress to the service instance. **Note** In order for the device to distinguish if the packet is DHCP, all tags must be in pop state ; push and translate states are not supported.
Step 8	[**no**] **bridge-domain** *bridge-id* **Example:** `Switch(config-if-srv)# bridge-domain 12`	Binds the service instance to a bridge domain instance where *bridge-id* is the identifier for the bridge domain instance.
Step 9	**exit** **Example:** `Switch(config-if-srv)# exit`	Exits service instance configuration mode.
Step 10	**end** **Example:** `Switch(config)# end`	Exits configuration mode.

Configuring IP Source Guard With Static IP

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip source binding** *mac-address* **bridge-domain** *bridge-id* **interface** *type mod /port*
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 3	**ip source binding** *mac-address* **bridge-domain** *bridge-id* **interface** *type mod /port* **Example:** `Switch(config)# ip source binding 000A.000A.000A bridge-domain 52 1.1.1.163 interface Gi0/0/0`	Adds the static entry.
Step 4	**end** **Example:** `Switch(config)# end`	Exits configuration mode.

Example

This example shows how to configure IP source guard:

```
Switch# enable
Switch# configure terminal
Switch(config)# interface Gigabitethernet0/0/1
Switch(config-if)# service instance 71 ethernet
Switch(config-if-srv)# encapsulation dot1q 71
Switch(config-if-srv)# rewrite ingress tag pop 1 symmetric
Switch(config-if-srv)# bridge-domain 10
Switch(config-if-srv)#exit
Switch(config-if)# ip verify source bridge-domain dhcp-snooping
```

Verification

Use the **show ip verify source** to verify the configuration:

```
router# show ip verify source
Interface  Filter-type  Filter-mode  IP-address       Mac-address        BD
---------  -----------  -----------  ---------------  -----------------  ----------
Gi0/0/5    ip           active       10.0.0.2                            10
Gi0/0/5    ip           active       10.0.0.3                            10
Gi0/0/5    ip           active       10.0.0.4                            10
Gi0/0/5    ip           active       10.0.0.5                            10
Gi0/0/5    ip           active       10.0.0.6                            10
Gi0/0/5    ip           active       10.0.0.7                            10
Gi0/0/5    ip           active       10.0.0.8                            10
```

Displaying IP Source Guard Information

To display IP Source Guard PACL information for all interfaces, perform this task:

Command	Purpose
Router# **show ip verify source** [**interface** *interface-name*]	Displays IP Source Guard PACL information for all interfaces on a switch or for a specified interface.

```
Router# show ip verify source interface gig0/0/1
Interface  Filter-type  Filter-mode  IP-address       Mac-address        Vlan
---------  -----------  -----------  ---------------  -----------------  ----
Gi0/0/7    ip           active       deny-all                            10
```

Displaying IP Source Binding Information

To display all IP source bindings on all interfaces, perform this task:

Command	Purpose
Router#show ip source binding [dhcp-snooping]	Displays all IP source bindings. The dhcp-snooping filter displays all VLANs on the interface that have DHCP snooping enabled.

This example shows how to display all IP source bindings configured on all the interfaces:

```
Router#show ip source binding
MacAddress          IpAddress        Lease(sec)  Type           BD    Interface
------------------  ---------------  ----------  -------------  ----  --------------------
04:62:73:2B:2A:3F   10.0.0.32        105         dhcp-snooping   10
GigabitEthernet0/0/4+Efp1 tag 10
Total number of bindings: 1
```

This example shows how to display only dynamic IP source bindings configured on all the interfaces:

```
Router#show ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           BD    Interface
```

```
------------------  ---------------  ----------  -------------  ----  ----------------------
00:00:00:4A:67:F4   30.0.0.188       44          dhcp-snooping   30
GigabitEthernet0/0/5+Efp3 tag 30
00:00:00:4A:65:8B   10.0.0.173       14          dhcp-snooping   10
GigabitEthernet0/0/5+Efp1 tag 10
00:00:00:4A:66:4B   20.0.0.184       51          dhcp-snooping   20
GigabitEthernet0/0/5+Efp2 tag 20
00:00:00:4A:66:D6   20.0.0.125       47          dhcp-snooping   20
GigabitEthernet0/0/5+Efp2 tag 20
00:00:00:4A:67:37   30.0.0.199       37          dhcp-snooping   30
GigabitEthernet0/0/5+Efp3 tag 30
```

Troubleshooting

Troubleshooting scenarios for IP Source Guard feature:

Problem	Solution
IP source guard not enabled	Use **show ip verify source** command to check if the entries exist.
DHCP snooping failures	1. Verify whether or not the issues are specific to DHCP snooping or IP source guard. Use the show **ip dhcp snooping binding** command to check the DHCP snooping bindings. If the expected entry is missing, debug the DHCP snooping sessions and share the output with TAC. 2. If the entry is displayed then check IP source guard configuration on the interface. If the issue persists, contact TAC.