SGT Based PBR

The SGT Based PBR feature supports classification of packets based on Security Group for grouping the traffic into roles to match the defined policies in Policy-Based Routing (PBR).

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to https://cfnng.cisco.com/. An account on Cisco.com is not required.

Restrictions for SGT Based PBR

- SGT Based PBR feature supports policy configuration using number based tagging and does not support name based tagging.
- SGT Based PBR feature is not supported for IPV6 traffic on IOS XE.
- Dynamic route-map overrides static route-map when both are associated with the same interface. A warning message is issued during an override. The static route-map is enabled when the dynamic route-map is deleted.
- We recommend disassociating the route-map before it is deleted. You cannot configure static PBR if the route-map is deleted before disassociating it from the interface.

Information About SGT Based PBR

Cisco TrustSec

Cisco TrustSec assigns a Security Group Tag, (SGT) to the user's or device's traffic at ingress and applies the access policy based on the assigned tag. SGT Based PBR feature allows you to configure PBR based on Security Group classification enabling you to group users or devices into a role to match the defined policies.

SGT Based PBR

Security Group classification includes both Source and Destination Group, which is specified by source SGT and DGT. SGT Based PBR feature provides the PBR route-map match clause for SGT/DGT based packet classification. SGT Based PBR feature supports configuration of unlimited number of tags, but it is recommended to configure the tags based on memory available in the platform. SGT Based PBR supports VPN routing and forwarding (VRF) selection match criteria which can be used for policy based classification and forwarding of Virtual Private Network (VPN) traffic.

How to Configure SGT Based PBR

Configuring Match Security Group Tag

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **route-map** *map-tag*
4. **match security-group source tag** *sgt-number*
5. **set ip next-hop** *ip-address*
6. **match security-group destination tag** *sgt-number*
7. **set ip next-hop** *ip-address*
8. **end**

DETAILED STEPS

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

	Command or Action	Purpose
Step 3	**route-map** *map-tag* **Example:** `Device(config)# route-map policy_security`	Specifies the route-map and enters route-map configuration mode.
Step 4	**match security-group source tag** *sgt-number* **Example:** `Device(config-route-map)# match security-group source tag 100`	Configures the value for security-group source security tag.
Step 5	**set ip next-hop** *ip-address* **Example:** `Device(config-route-map)# set ip next-hop 71.71.71.6`	Specifies the next hop for routing packets.
Step 6	**match security-group destination tag** *sgt-number* **Example:** `Device(config-route-map)# match security-group destination tag 150`	Configures the value for security-group destination security tag.
Step 7	**set ip next-hop** *ip-address* **Example:** `Device(config-route-map)# set ip next-hop 72.72.72.6`	Specifies the next hop for routing packets.
Step 8	**end** **Example:** `Device(config-route-map)# end`	Exits route-map configuration mode and returns to privileged EXEC mode.

Assigning Route-Map to an Interface

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *typeslot/ subslot/ port*[. *subinterface-number*]
4. **ip policy route-map** *map-tag*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *typeslot/ subslot/ port*[. *subinterface-number*] **Example:** `Device(config)#interface gigabitEthernet0/0/0`	Specifies the interface information and enters interface configuration mode.
Step 4	**ip policy route-map** *map-tag* **Example:** `Device(config-if)#ip policy route-map policy_security`	Assigns the route-map configured in the previous task to the interface.

Displaying and Verifying SGT Based PBR Configuration

SUMMARY STEPS

1. **enable**
2. **show ip policy**
3. **show route-map** *map-tag*
4. **show route-map dynamic**

DETAILED STEPS

Step 1 **enable**

Example:

```
Device> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 **show ip policy**

Example:

```
Device# show ip policy

Interface      Route map
Gi0/0/1.77     test
```

Displays IP policy information.

Step 3 **show route-map** *map-tag*

Example:

```
Device# show route-map test

route-map test, permit, sequence 10
```

```
  Match clauses:
    security-group source tag 100 111
  Set clauses:
    ip next-hop 71.71.71.6
  Policy routing matches: 0 packets, 0 bytes
route-map test, permit, sequence 20
  Match clauses:
    security-group destination tag 200 222
  Set clauses:
    ip next-hop 72.72.72.6
  Policy routing matches: 0 packets, 0 bytes
```

Displays route-map configuration.

Step 4 **show route-map dynamic**

Example:

```
Device# show route-map dynamic

route-map AAA-02/11/15-12:32:52.955-1-test, permit, sequence 0, identifier 2818572289
Match clauses:
    Security-group source tag 100 300
Set clauses:
 ip next-hop 3.3.3.2
Nexthop tracking current: 3.3.3.2
3.3.3.2, fib_nh:7FDE41661370,oce:7FDE4C540AD0,status:1

 Policy routing matches: 1012 packets, 83458 bytes
Current active dynamic routemaps = 1
```

Displays information about dynamic PBR route-map.

Configuration Examples for SGT Based PBR

Example: SGT Based PBR

The following example shows how to configure SGT Based PBR:

Example: SGT Based PBR

```
enable
 configure terminal
 route-map policy_security
 match security-group source tag 100
 match security-group source tag 111
 set ip next-hop 71.71.71.6
 match security-group destination tag 200
 match security-group destination tag 222
 set ip next-hop 72.72.72.6
 end
 interface gigabitEthernet0/0/0
 ip policy route-map policy_security
```

Additional References for SGT Based PBR

Related Documents

Related Topic	Document Title
Cisco IOS IP Routing Protocol Independent commands	Cisco IOS IP Routing Protocol Independent Command Reference
Cisco TrustSec Overview	Understanding Cisco TrustSec

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for SGT Based PBR

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to https://cfnng.cisco.com/. An account on Cisco.com is not required.

Table 1: Feature Information for SGT Based PBR