Cisco TrustSec VRF-Aware SGT

Revised: July 29, 2016

The Cisco TrustSec VRF-Aware SGT feature binds a Security Group Tag (SGT) Exchange Protocol (SXP) connection with a specific virtual routing and forwarding (VRF) instance.

This module consists of these sections:

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 at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About Cisco TrustSec VRF-Aware SGT

VRF-Aware SGT

Cisco TrustSec uses security group tags (SGTs) to ensure that packets passing through the Cisco TrustSec network can be properly identified and applied with security and other access control policies.

The SGT implementation of VRF binds a Security Group Tag (SGT) Exchange Protocol (SXP) connection to a specific VRF. The assumption is that the network topology is configured for Layer 2 or Layer 3 VPNs, with all VRFs configured before enabling Cisco TrustSec.

SXP VRF support can be summarized as follows:

- The same VRF can have multiple SXP connections, with different source and peer IP address. SXP has no limitation on the number of connections and number of IP–SGT mappings per VRF.
- Different VRFs may have overlapping SXP peer or source IP addresses.
- IP–SGT mappings learned (added or deleted) in one VRF can be updated only in the same VRF domain. The SXP connection cannot update a mapping bound to a different VRF. If no SXP connection exits for a VRF, IP–SGT mappings for that VRF is not updated by SXP.
- Multiple address families per VRF is supported. Therefore, one SXP connection in a VRF domain can forward both IPV4 and IPV6 IP-SGT mappings.

You can map an SGT to a VRF using the **cts role-based sgt-map vrf** *vrf-name* command.

VRF-to-Layer 2 VLAN assignments are specified with the **cts role-based l2-vrf** *vrf-name* **vlan-list** command. A VLAN is considered a Layer 2 VLAN when there is no switch virtual interface (SVI) with an IP address configured on the VLAN. The VLAN becomes a Layer 3 VLAN once an IP address is configured on its SVI.

VRF assignments configured by the **cts role-based l2-vrf** command are active as long as a VLAN remains a Layer 2 VLAN.

Note Cisco IOS XE 3.9.2E on Catalyst 4500 Series Switch supports VRF aware SGT only for Layer 3 VLAN.

The IP–SGT bindings learned while a VRF assignment is active are also added to the Forwarding Information Base (FIB) table associated with the VRF and the IP protocol version. If an SVI becomes active for a VLAN, the VRF-to-VLAN assignment becomes inactive and all bindings learned on the VLAN are moved to the FIB table associated with the SVI's VRF.

The VRF-to-VLAN assignment is retained even when the assignment becomes inactive. It is reactivated when the SVI is removed or when the SVI IP address is removed. When reactivated, the IP–SGT bindings are moved back from the FIB table associated with the SVI's VRF to the FIB table associated with the VRF assigned by the **cts role-based l2-vrf** command.

Starting with Cisco IOS XE 3.9.2E, you can assign SGT to End-point IDs (EIDs) in LISP configuration, with the VRF aware SGT feature.

How to Configure VRF-Aware SGT

Configuring VRF-to-Layer-2-VLAN Assignments

	Command or Action	Purpose
Step 1	`Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	`Switch# configure terminal`	Enters global configuration mode.
Step 3	`Switch(config)# interface type number`	Enables an interface and enters interface configuration mode.

	Command or Action	Purpose
Step 4	`Switch(config-if)# vrf forwarding vrf-name`	Associates a VRF instance or a virtual network with an interface or subinterface. **Note** Do not configure VRFs on the management interface.
Step 5	`Switch(config-if)# exit`	Exits interface configuration mode and returns to global configuration mode.
Step 6	`Switch(config)# cts role-based l2-vrf vrf1 vlan-list 20`	Selects a VRF instance for Layer 2 VLANs.
Step 7	`Switch(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Configuring VRF-to-SGT Mapping

	Command or Action	Purpose
Step 1	`Switch(config)# cts role-based sgt-map vrf vrf-name {ip4_netaddress | ipv6_netaddress | host {ip4_address | ip6_address }}] sgt sgt_number`	Applies the SGT to packets in the specified VRF. The IP-SGT binding is entered into the IP-SGT table associated with the specified VRF and the IP protocol version implied by the type of IP address.
Step 2	`Switch(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Configuration Examples for Cisco TrustSec VRF-Aware SGT

Example: Configuring VRF-to-Layer2-VLAN Assignments

```
Device> enable
Device# configure terminal
Device(config)# interface vlan 101
Device(config-if)# vrf forwarding vrf-intf
Device(config-if)# exit
Device(config)# cts role-based l2-vrf vrf1 vlan-list 20
Device(config)# end
```

Example: Configuring VRF-to-SGT Mapping

```
Device# configure terminal
Device(config)# cts role-based sgt-map vrf red 23.1.1.2 sgt 23
Device(config)# end
```

Additional References for Configuring Cisco TrustSec VRF-Aware SGT

Related Documents

Related Topic	Document Title
Cisco IOS commands	*Cisco IOS Master Commands List, All Releases*
Cisco TrustSec configuration guide	*Cisco TrustSec Switch Configuration Guide*
Managing Switch Stacks	"Managing Switch Stacks" chapter in the *Software Configuration Guide, Cisco IOS XE Denali 16.3.1 (Catalyst 3850 Switches)*

Standards & MIBs

MIB	MIBs Link
•	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Cisco TrustSec VRF-Aware SGT

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 1 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.

Table 1 Feature Information for Cisco TrustSec VRF-Aware SGT

Feature Name	Releases	Feature Information
Cisco TrustSec VRF-Aware SGT	Cisco IOS XE Denali 16.3.1	The Cisco TrustSec VRF-Aware SGT feature binds a Security Group Tag (SGT) Exchange Protocol (SXP) connection with a specific virtual routing and forwarding (VRF) instance. The **cts role-based l2-vrf** command was introduced on Cisco on Cisco Catalyst 3850 Series Switches and Cisco Catalyst 3650 Series Switches.
	Cisco IOS XE 3.9.2E	The following commands were implemented on Cisco Catalyst 4500-E Series Switches: • **cts role-based l2-vrf** • **cts role-based sgt-map vrf**