Cisco TrustSec VRF-Aware SGT

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

Information About Cisco TrustSec VRF-Aware SGT

VRF-Aware SXP

The SXP implementation of Virtual Routing and Forwarding (VRF) binds an SXP connection with a specific VRF. It is assumed that the network topology is correctly configured for Layer 2 or Layer 3 VPNs, with all VRFs configured before enabling Cisco TrustSec.

SXP VRF support can be summarized as follows:

- Only one SXP connection can be bound to one 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 won't be 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.
- SXP has no limitation on the number of connections and number of IP–SGT mappings per VRF.

How to Configure VRF-Aware SGT

Configuring VRF-to-Layer-2-VLAN Assignments

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **vrf forwarding** *vrf-name*
5. **exit**
6. **cts role-based l2-vrf vrf1 vlan-list 20**
7. **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.
Step 3	**interface** *type number* **Example:** `Device(config)# interface vlan 101`	Enables an interface and enters interface configuration mode.
Step 4	**vrf forwarding** *vrf-name* **Example:** `Device(config-if)# vrf forwarding vrf-intf`	Associates a VRF instance or a virtual network with an interface or subinterface. **Note** Do not configure VRFs on the management interface.
Step 5	**exit** **Example:** `Device(config-if)# end`	Exits interface configuration mode and returns to global configuration mode.
Step 6	**cts role-based l2-vrf vrf1 vlan-list 20** **Example:**	Selects a VRF instance for Layer 2 VLANs.

	Command or Action	Purpose
	`Device(config)# cts role-based l2-vrf vrf1 vlan-list 20`	
Step 7	**end** **Example:** `Device(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Configuring VRF-to-SGT Mapping

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **cts role-based sgt-map vrf vrf-name** {**ip4_netaddress** | *ipv6_netaddress* | **host** {*ip4_address* | *ip6_address*}}] **sgt** *sgt_number*
4. **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.
Step 3	**cts role-based sgt-map vrf vrf-name** {**ip4_netaddress**	*ipv6_netaddress*	**host** {*ip4_address*	*ip6_address*}}] **sgt** *sgt_number* **Example:** `Device(config)# cts role-based sgt-map vrf red 10.0.0.3 sgt 23`	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 4	**end** **Example:** `Device(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-Layer2-VLAN Assignments

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