Cisco TrustSec

This chapter describes how to identify and resolve problems that might occur when configuring Cisco TrustSec.

This chapter includes the following sections:

Information About Cisco TrustSec

The Cisco TrustSec security architecture builds secure networks by establishing clouds of trusted network devices. Each device in the cloud is authenticated by its neighbors. Communication on the links between devices in the cloud is secured with a combination of encryption, message integrity checks, and data-path replay protection mechanisms.

Cisco TrustSec also uses the device and user identification information acquired during authentication for classifying, or coloring, the packets as they enter the network. This packet classification is maintained by tagging packets on ingress to the Cisco TrustSec network so that they can be properly identified for the purpose of applying security and other policy criteria along the data path. The tag, also called the security group tag (SGT), allows the network to enforce the access control policy by enabling the endpoint device to act upon the SGT to filter traffic.

See the *Cisco Nexus 1000V Security Configuration Guide* for more information on the Cisco TrustSec feature on Cisco Nexus 1000V.

Guidelines and Limitations for Troubleshooting Cisco TrustSec

The following guidelines and limitations apply when troubleshooting Cisco TrustSec SXP:

- In this release, SGT Exchange Protocol (SXP) is supported for Cisco Nexus 1000V.
- Cisco Nexus 1000V VSM will always be configured as the SXP speaker in all peer connections. Listener functionality is not supported in this release.
- A maximum of 2048 IP-SGT mappings can be learned system-wide in the DVS. This is a combined total for both entries learned via DHCP snooping as well as device tracking of individual virtual machines by ARP as well as IP traffic inspection.

- The IP-SGT mappings can be communicated to up to 64 SXP peer devices.
- In order to assign a SGT to a virtual machine, SGT interactions need to be manually configured in the port profile or vEthernet interface. This is not supported on a management interface or a ethernet interface.

Cisco TrustSec Troubleshooting Commands

This section contains the following topics:

Debugging Commands

Table 25-1 lists the available debugging commands.

Table 25-1 Cisco TrustSec Debugging Commands

Command	Purpose
debug cts authentication	Collect and view logs related to Cisco TrustSec authentication.
debug cts authorization	Collect and view logs related to Cisco TrustSec authorization.
debug cts errors	Collect and view logs related to Cisco TrustSec errors and warning messages.
debug cts messages	Collect and view logs related to Cisco TrustSec messages.
debug cts packets	Collect and view logs related to Cisco TrustSec packets.
debug cts relay	Collect and view logs related to Cisco TrustSec relay functionality.
debug cts sxp	Collect and view logs related to Cisco TrustSec SXP.
debug cts sap	Collect and view logs related to Cisco TrustSec security association protocol (SAP).
debug cts trace	Collect and view logs related to Cisco TrustSec trace functionality.
show cts internal debug-info	Displays Cisco TrustSec debug information.

Host Logging Commands

Table 25-2 lists the commands from the ESX host to collect and view logs related to Cisco TrustSec.

Table 25-2 ESX Host Commands

ESX Host Command	Description
echo "logfile enable" > /tmp/dpafifo	Enables DPA debug logging. Logs are output to **/var/log/vemdpa.log** file.
echo "debug sfctsagent all" > /tmp/dpafifo	Enables TrustSec SXP agent debug logging. Logs are output to **/var/log/vemdpa.log** file.
vemlog debug sfcts_config all	Enables datapath debug logging, and captures logs for the data packets sent between the client and the server.
vemlog debug sfdhcps_config all	Enables datapath debug logging, and captures logs for DHCP snooping configuration coming from the VSM. To view the logs DHCP snooping should be enable in Cisco Nexus 1000V.
vemlog debug sfdhcps_binding_table all	Enables datapath debug logging, and captures logs corresponding to binding database changes. To view the logs DHCP snooping should be enabled on Cisco Nexus 1000V.
vemlog debug sfipdb all	Enables datapath debug logging, and captures logs corresponding to IP database that maintains the IP addresses for all the virtual machines that are being tracked using Cisco TrustSec device tracking. To view the logs Cisco TrustSec device tracking should be enabled on Cisco Nexus 1000V.
vemcmd show learnt ip	Displays Cisco TrustSec configuration on Cisco Nexus 1000V.
vemcmd show cts global	Displays if Cisco TrustSec is enabled on Cisco Nexus 1000V.
vemcmd show cts ipsgt	Displays Cisco TrustSec configuration on Cisco Nexus 1000V.

Example

The following examples displays Cisco TrustSec specific information on Cisco Nexus 1000V.

```
switch# vemcmd show learnt ip
IP Address LTL VLAN BD
/SegID
10.78.1.76 49 353 7
switch#


switch# vemcmd show cts global
CTS Global Configuration:
CTS is: Enabled
CTS Device Tracking is: Enabled
switch#
```

```
switch# vemcmd show cts ipsgt
IP Address LTL VLAN BD SGT Learnt
10.78.1.76 49 353 7 6766 Device Tracking
switch#
```

Show Commands

Table 25-3 lists available Cisco TrustSec show commands. See the *Cisco Nexus 1000V Command Reference* for more information on the show commands for Cisco TrustSec.

Table 25-3 Cisco TrustSec Show Commands

Command	Purpose
show cts	Displays Cisco TrustSec configuration.
show cts sxp	Displays the SXP configuration for Cisco TrustSec.
show feature	Displays the features available, such as CTS, and whether they are enabled.
show running-configuration cts	Displays the running configuration information for Cisco TrustSec.
show cts device tracking	Displays the Cisco TrustSec device tracking configuration.
show cts ipsgt entries	Display the SXP SGT entries for Cisco TrustSec.
show cts role-based sgt-map	Displays the mapping of the IP address to SGT for Cisco TrustSec.
show cts sxp connection	Displays SXP connections for Cisco TrustSec.
show cts interface delete-hold timer	Displays the interface delete hold timer period for Cisco TrustSec.
show cts internal event-history [error |mem-stats | msgs | sxp]	Displays event logs for Cisco TrustSec.

Problems with Cisco TrustSec

This section includes symptoms, possible causes and solutions for the following problems with Ciso TrustSec.

Table 25-1 Problems with Cisco TrustSec

Symptom	Possible Causes	Verification and Solution
The Cisco Nexus 1000V is unable to form a SXP session with Cisco TrustSec.	There is no connection between Cisco Nexus 1000V and its peer.	Verify if the Cisco Nexus 1000V is connected to its peer. **ping**
	The Cisco TrustSec SXP is not enabled on the Cisco Nexus 1000V.	Verify if the Cisco TrustSec SXP is enabled on the Cisco Nexus 1000V. **show cts sxp** If not, enable the Cisco TrustSec SXP. **cts sxp enable**
	The password configured on the Cisco Nexus 1000V does not match the password configured on its peer.	Verify if the passwords configured on the Cisco Nexus 1000V matches its peer. **show cts sxp**
	The default source IPv4 address is not configured on the Cisco Nexus 1000V.	Verify if the default source IPv4 address is not configured on the Cisco Nexus 1000V. **show cts sxp**
	The SXP peer is not configured as the listener.	Verify that the SXP peer is configured as the listener. **show cts sxp connection**
Cisco TrustSec SXP is unable to learn any IP-SGT mappings on the Cisco Nexus 1000V.	The Cisco TrustSec device tracking is not enabled on the Cisco Nexus 1000V.	Verify if the Cisco TrustSec device tracking is enabled on the Cisco Nexus 1000V. **show cts device tracking** If not, enable the Cisco TrustSec device tracking. **cts sxp device tracking**
	The DHCP Snooping feature is not enabled globally and on a VLAN on the Cisco Nexus 1000V.	Verify if the DHCP Snooping feature is enabled globally on the Cisco Nexus 1000V. **show feature** If not, enable the DHCP Snooping feature globally. **feature dhcp** Verify if the DHCP Snooping feature is enabled on a VLAN on the Cisco Nexus 1000V. **show ip dhcp snooping** If not, enable the DHCP Snooping feature on a VLAN. **ip dhcp snooping vlan** *vlan-list*