Cisco TrustSec

This chapter describes how to identify and resolve problems that might occur when configuring Cisco TrustSec. This chapter contains 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 about the Cisco TrustSec feature on Cisco Nexus 1000V.

Cisco TrustSec Troubleshooting Commands

Debugging Commands

Command	Purpose
debug cts authentication	Collects and displays logs related to Cisco TrustSec authentication.
debug cts authorization	Collects and displays logs related to Cisco TrustSec authorization.

Command	Purpose
debug cts errors	Collects and displays logs related to Cisco TrustSec errors and warning messages.
debug cts messages	Collects and displays logs related to Cisco TrustSec messages.
debug cts packets	Collects and displays logs related to Cisco TrustSec packets.
debug cts relay	Collects and displays logs related to Cisco TrustSec relay functionality.
debug cts sxp	Collects and displays logs related to Cisco TrustSec SXP.
debug cts sap	Collects and displays logs related to the Cisco TrustSec Security Association Protocol (SAP).
debug cts trace	Collects and displays logs related to Cisco TrustSec trace functionality.
show cts internal debug-info	Displays Cisco TrustSec debug information.

Host Logging Commands

ESX Host Command	Description
echo "logfile enable" > /tmp/dpafifo	Enables DPA debug logging. Logs are output to the `/var/log/vemdpa.log` file.
echo "debug sfctsagent all" > /tmp/dpafifo	Enables TrustSec SXP agent debug logging. Logs are output to the `/var/log/vemdpa.log` file.
vemlog debug sfcts_config all	Enables the data path debug logging and captures logs for the data packets sent between the client and the server.
vemlog debug sfdhcps_config all	Enables the data path debug logging and captures logs for DHCP snooping configuration coming from the VSM. To view the logs, enable DHCP snooping on Cisco Nexus 1000V.
vemlog debug sfdhcps_binding_table all	Enables the data path debug logging and captures logs corresponding to the binding database changes. To view the logs, enable DHCP snooping on Cisco Nexus 1000V.

ESX Host Command	Description
vemlog debug sfipdb all	Enables the data path debug logging and captures logs corresponding to the 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, enable Cisco TrustSec device tracking on Cisco Nexus 1000V.

vemcmd show learnt ip	Displays the Cisco TrustSec configuration on Cisco Nexus 1000V. Following is an example of this command:
	`switch# `**`vemcmd show learnt ip`**
	`IP Address LTL VLAN BD`
	`/SegID`
	`10.78.1.76 49 353 7`
	`switch#`

vemcmd show cts global	Displays if Cisco TrustSec is enabled on Cisco Nexus 1000V. Following is an example of this command:
	`switch# `**`vemcmd show cts global`**
	`CTS Global Configuration:`
	`CTS is: Enabled`
	`CTS Device Tracking is: Enabled`
	`switch#`

vemcmd show cts ipsgt	Displays the Cisco TrustSec configuration on Cisco Nexus 1000V. Following is an example of this command:
	`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

See the *Cisco Nexus 1000V Command Reference* for more information about the **show** commands for Cisco TrustSec.

Command	Purpose
show cts	Displays the 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.

Command	Purpose
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	Displays event logs for Cisco TrustSec.

Problems with Cisco TrustSec

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

Symptom	Possible Causes	Verification and Solution
Cisco Nexus 1000V is unable to form an SXP session with Cisco TrustSec.	There is no connection between Cisco Nexus 1000V and its peer.	Verify if Cisco Nexus 1000V is connected to its peer. **ping**
	The Cisco TrustSec SXP is not enabled on Cisco Nexus 1000V.	Verify if the Cisco TrustSec SXP is enabled on Cisco Nexus 1000V. **show cts sxp** If not, enable the Cisco TrustSec SXP. **cts sxp enable**
	The password configured on Cisco Nexus 1000V does not match the password configured on its peer.	Verify if the passwords configured onCisco Nexus 1000V matches its peer. **show cts sxp**
	The default source IPv4 address is not configured on Cisco Nexus 1000V.	Verify if the default source IPv4 address is not configured on 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**

Symptom	Possible Causes	Verification and Solution
Cisco TrustSec SXP is unable to learn any IP-SGT mappings on Cisco Nexus 1000V.	The Cisco TrustSec device tracking is not enabled on Cisco Nexus 1000V.	Verify if the Cisco TrustSec device tracking is enabled on Cisco Nexus 1000V. **show cts device tracking** If not, enable the Cisco TrustSec device tracking. **cts sxp device tracking**
	DHCP snooping is not enabled globally on Cisco Nexus 1000V.	Verify if DHCP snooping feature is enabled globally on Cisco Nexus 1000V. **show feature** If not, enable DHCP snooping globally. **feature dhcp** Verify if DHCP snooping is enabled on a VLAN on Cisco Nexus 1000V. **show ip dhcp snooping** If not, enable DHCP snooping on a VLAN. **ip dhcp snooping vlan** *vlan-list*