CHAPTER 16

Cisco TrustSec

This chapter describes how to identify and resolve problems that might occur when configuring Cisco TrustSec and includes the following sections:

- Information About Cisco TrustSec, page 16-1
- Cisco TrustSec Troubleshooting Commands, page 16-1
- Problems with Cisco TrustSec, page 16-5

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 1000 Virtual Edge for VMware vSphere Security Configuration Guide* for more information on the Cisco TrustSec feature on Cisco Nexus 1000VE.

Cisco TrustSec Troubleshooting Commands

This section contains the following topics:

- Debugging Commands, page 16-2
- VSE Logging Commands, page 16-2
- show Commands, page 16-4

Debugging Commands

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

VSE Logging Commands

You can use the commands in this section to troubleshoot commands related to VSE logging. Logging commands needs to be executed directly by login to VSE..

VSE Command	Description
echo "logfile enable" >/var/tmp/dpafifo	Enables DPA debug logging. Logs are output to the **/var/log/vemdpa.log** file.
echo "debug sfctsagent all" > /var/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.

VSE 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 the Cisco Nexus 1000VE.
vemcmd show learnt ip	Displays the Cisco TrustSec configuration on the Cisco Nexus 1000VE. See Example 16-1 on page 16-3
vemcmd show cts global	Displays if Cisco TrustSec is enabled on the Cisco Nexus 1000VE. See Example 16-2 on page 16-3
vemcmd show cts ipsgt	Displays the Cisco TrustSec configuration command specific to IP-to-SGT mapping on Cisco Nexus 1000VE. See Example 16-3 on page 16-4
vemcmd show cts subnet-sgt-map ip	Displays the Cisco TrustSec configuration specific to Subnet-to-SGT mapping on Cisco Nexus 1000VE. See Example 16-4 on page 16-4
vemcmd show cts access-list	Displays the Cisco TrustSec Role-Based access-list names and counters matching the ACEs in the access-list. (Permit/Deny/No-Match). See Example 16-5 on page 16-4
vemcmd show cts policy	Displays the Cisco TrustSec Role-Based policies where source sgt to destination sgt mapping with RBACL. See Example 16-6 on page 16-4.

Example

vemcmd can be executed by directly logging in to VSE or directly from VSM using **module vse #vse-module-number execute** vemcmd complete command.

Example 16-1 vemcmd show learnt ip Command

```
cisco-vse:~$ vemcmd show learnt ip
IP Address LTL VLAN BD
/SegID
10.78.1.76 49 353 7
switch#
```

Example 16-2 vemcmd show cts global Command

```
cisco-vse:~$ vemcmd show cts global
CTS Global Configuration:
CTS is: Enabled
CTS Device Tracking is: Enabled
```

```
switch#
```

Example 16-3 vemcmd show cts ipsgt Command

```
cisco-vse:~$ vemcmd show cts ipsgt
IP Address LTL VLAN BD SGT Learnt
10.78.1.76 49 353 7 6766 Device Tracking
switch#
```

Example 16-4 v**emcmd show cts subnet-sgt-map ip**

```
Example 16-4 vemcmd show cts subnet-sgt-map ip

cisco-vse:~$ vemcmd show cts subnet-sgt-map ip
Key (tid, ip/mask) : Data (SGT)
**** Dumping all subnet SGT entries ****
(0, 192.168.0.0/24) : 200
cisco-vse:~$
```

Example 16-5 vemcmd show cts access-list

```
cisco-vse:~$ vemcmd show cts access-list
Global RBACL List Permit/Deny/No-Match

------ ----- ---- --------------------
ise_permit_icmp 0/0/0
ise_permit_icmp_ret 4/0/0
test 0/0/0
cisco-vse:~$
```

Example 16-6 vemcmd show cts policy

```
isco-vse:~$ vemcmd show cts policy
SGT DGT RBACL
700 800 ise_permit_icmp
800 700 ise_permit_icmp_ret
cisco-vse:~$
```

show Commands

See the *Cisco Nexus 1000VE Command Reference* for more information on 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.

Command	Purpose
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 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 Cisco TrustSec.

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