Notes for Catalyst 4500 Series Switches

Revised: April 24, 2013, OL-22192-02

Supported Hardware and Software

For a complete table of features, platforms, and IOS images supported see the latest Product Bulletins at the following URL:

http://www.cisco.com/en/US/netsol/ns1051/index.html

See also, the Matrix of Cisco TrustSec-Enabled Infrastructure at the following URL:

http://www.cisco.com/en/US/solutions/ns170/ns896/ns1051/trustsec_matrix.html

TrustSec SGT and SGACL Configuration Guidelines and Limitations

The following guidelines and limitations apply to configuring Cisco TrustSec SGT and SGACL on Catalyst WS-X45-SUP7-E/SUP7L-E and WS-C4500X-32 switches:

- Propagation of Security Group Tag in the CMD header is supported on the supervisor engine uplink ports, the WS-X47xx series line cards, and the WS-X4640-CSFP-E linecard.
- The way Destination Security tag (DGT) is derived for *switched traffic* (i.e. traffic forwarded between ports in the same VLAN or subnet) is restricted:
  - A maximum of 2000 IP-SGT mappings exists for DGT derivation. Though you can configure IP-SGT mappings above this limit, such mappings cannot be used to derive DGT for switched traffic. You can, however, use them to derive DGT for other types of traffic (e.g. routed traffic).
- The IP-SGT mappings that are downloaded through SGT Exchange Protocol (SXP) are programmed into the TCAM and the Security Group Access Control List (SGACL) enforcement is performed in the hardware.

Note None of the previous restrictions exist for deriving either Source Security Tag for any type of traffic, or DGT for *routed traffic* (i.e. traffic forwarded between ports of different VLANs or subnets).

- The **platform-cts subnet-sgt l2traffic** command enables support for subnet based DGT derivation for switched (Layer 2) traffic. See the **platform-cts** command in the *Cisco TrustSec Command Summary* section in this document for detailed usage guidelines.
- In Cisco IOS XE 3.8.xE and earlier releases, IP-SGT mappings are not VRF-aware.
- The Time-To-Live (TTL) configuration is not supported for SGACL.
- The TCP flags supported by SGACL is similar to what the other ACLs support.
- The maximum number of access control entries (ACEs) supported in the default/(*,*) SGACL policy is 512.
- The IP-SGT mapping (based on the Source IP address in the packet) takes precedence over the SGT tag present in the CMD header of incoming traffic even if the ingress port is in trusted state. This deviates from the default behavior, which dictates that if the port is trusted the packet SGT is used for enforcing the SGACL policy.
- Every IP-SGT mapping learnt on the device is added to both the source lookup table and the destination lookup table.
- In Cisco IOS XE Release 3.9xE and later releases, a switched virtual interface (SVI) on a data VLAN is required to derive the source user group for switched (Layer 2) traffic.

  Cisco TrustSec depends on the routing table (Routing Information Base [RIB]/Forwarding Information Base [FIB]/FLC) to derive the source user group for switched traffic. Prior to Cisco IOS XE Release 3.9.xE, only one instance of the routing table was by default attached to all VLANs. In Cisco IOS XE Release 3.9.xE, with the introduction of virtual routing and forwarding (VRF) support, mapping a routing table instance to a VLAN is done only after the creation of an SVI.

  The following example shows how to configure the SVI:

```
Switch(config)# interface vlan 1
Switch(config-if)# no shutdown
```

Note An SVI is required for routed (Layer 3) IPv4/IPv6 traffic also. However, router traffic will always have an SVI that is up and running.

- In Cisco IOS XE 3.10.xE and later releases, IPv6 unicast routing must be enabled to derive source user group and destination user group for IPv6 Layer 2 traffic.

  The **ipv6 unicast-routing** command must be enabled to use Cisco TrustSec, and derive source user group and destination user group for Layer 2 clients. For IPv6 routing, routing entries are added only if the **ipv6 unicast-routing** command is enabled. This routing entry is used to derive the source user group for Layer 2 traffic. After updating the routing table, details are passed to the access control list (ACL) manager to create Content-Addressable Memory (CAM) entries to derive the destination user group for switched IPv6 traffic.

Note IPv6 unicast routing must be enabled for routed (Layer 3) IPv6 traffic also. However; for routed traffic the **ipv6 unicast-routing** command is enabled by default.

- Subnet Security Group Tag (SGT) entries will create entries with network prefix, broadcast address and matching unicast IP or IPv6 addresses in the Layer 2 destination user group derivation TCAM block, if these entries are already available in the FIB.
- The IP-SGT mapping configured on a switch takes precedence over the source user group value present in the command header of the incoming traffic, even if the ingress port is in the trusted state.

- Cisco TrustSec enforcement is not supported on logical interfaces in Cisco IOS XE Release 3.8.5E and later releases.
- The limit for Layer 2 destination user group derivation is given below:

Table B-1 In Cisco IOS XE Release 3.10.2E and Later Releases

	IPv4	**IPv6**
Software Hash	2500	1500
TCAM	2000	1000

Table B-2 In Cisco IOS XE Release 3.9xE and Previous Releases

	IPv4
Software Hash	2000
TACM	2000

- IPv6 Layer 2 destination user-group derivation will not work on an interface, if an IPv6 ACL that has ACEs configured with partially-masked lower 48 bit source address is applied in the ingress direction.
- By default, both IPv4 and IPv6 SGACL enforcement is disabled on all interfaces. It can be enabled by specifying a VLAN ID with the **cts role-based enforcement vlan-list** *vlan-id* command. This command will enable IPv4/IPv6 SGACL enforcement on all ports on the VLAN.
- The **cts role-based sgt-map vlan-list all** command binds the SGT with the full range of VLANs supported by the switch and is not preserved in the nonvolatile generation (NVGEN) process. The specified SGT is bound to incoming packets received in any of the specified VLANs. The system uses discovery methods such as DHCP or ARP snooping (also known as IP device tracking) to discover active hosts in any of the VLANs mapped by this command. Alternatively, the system could map the subnet associated with the SVI of each VLAN to the specified SGT.
- IPv6 SGACL enforcement and IPv6 ACEs that have partially-masked lower 48 bit source address in the egress direction cannot co-exist on an interface.
- In the case of IPv6 fragmented Cisco TrustSec packets without an encapsulating security protocol (ESP) header, there is a chance of packet parse errors happening, and packets getting dropped.
- A host that is marked as untrusted and authenticated in Cisco ISE is assigned the device SGT on the authentication switch. However, when the same host is marked as trusted, and re-authenticated, the existing device SGT mapping is not removed from the switch, and the new mapping does not come into effect until the port is shutdown and brought up again.