APPENDIX B

Notes for Catalyst 4500 Series Switches

Revised: April 24, 2013, OL-22192-01

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).
- We cannot derive the DGT using *IP subnet to SGT mapping*. It can be derived only from *IP address (with a /32 prefix) to SGT mapping*.

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

IP-SGT mappings are not VRF-aware.

The 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 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.