APPENDIX A

Notes for Catalyst 3000 and 2000 Series Switches and WLC 5700 Series Wireless LAN Controllers

Revised: October 16, 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

Configuration Guidelines and Restrictions

Global Cat3K Restrictions

- AAA for Cisco TrustSec requires RADIUS and is supported only by the Cisco Identity Services Engine (Cisco ISE), Release1.2 with patches or more recent, and Cisco Secure Access Control System (Cisco ACS), version 5.1 or more recent.
- Default for Cisco Trustsec is disabled.
- Default for SXP is disabled.

Catalyst 3850 and Catalyst 3650 Switches, and WLC 5700 Wireless LAN Controllers

- Cisco Trustsec can be configured only on physical interfaces; not on logical interfaces.
- Cisco TrustSec for IPv6 is not supported.
- Dynamic binding of IP-SGT is not supported for hosts on Layer 3 physical routed interfaces because the IP Device Tracking feature for L3 physical interfaces is not currently supported.
- Cisco TrustSec can not be configured on a pure bridging domain with IPSG feature enabled, user has to either enable ip routing, or disable IPSG feature in the bridging domain.
- Cisco TrustSec only supports up to 255 security group tag.

Catalyst 3750-X and Catalyst 3560-X switches

The following guidelines and limitations apply to configuring Cisco TrustSec SGT and SGACL:

- You cannot statically map an IP-subnet to an SGT. You can only map IP addresses to an SGT. When you configure IP address-to-SGT mappings, the IP address prefix must be 32.
- If a port is configured in Multi-Auth mode, all hosts connecting on that port must be assigned the same SGT. When a host tries to authenticate, its assigned SGT must be the same as the SGT assigned to a previously authenticated host. If a host tries to authenticate and its SGT is different from the SGT of a previously authenticated host, the VLAN port (VP) to which these hosts belong is error-disabled.
- Cisco TrustSec enforcement is supported only on up to eight VLANs on a VLAN-trunk link. If there are more than eight VLANs configured on a VLAN-trunk link and Cisco TrustSec enforcement is enabled on those VLANs, the switch ports on those VLAN-trunk links will be error-disabled.
- The switch can assign SGT and apply corresponding SGACL to end-hosts based on SXP listening only if the end-hosts are Layer2 adjacent to the switch.
- Port-to-SGT mapping can be configured only on Cisco TrustSec links (that is, switch-to-switch links). Port-to-SGT mapping cannot be configured on host-to-switch links.
- When port-to-SGT mapping is configured on a port, an SGT is assigned to all ingress traffic on that port. There is no SGACL enforcement for egress traffic on the port.