CHAPTER 1

Cisco TrustSec

Cisco TrustSec provides security improvements to Cisco network devices based on the capability to strongly identify users, hosts, and network devices within a network. TrustSec provides topology independent and scalable access controls by uniquely classifying data traffic for a particular role. TrustSec ensures data confidentiality and integrity by establishing trust among authenticated peers and encrypting links with those peers.

The key component of Cisco TrustSec is the Cisco Identity Services Engine (ISE). Cisco ISE can provision switches with TrustSec Identities and Security Group ACLs (SGACLs), though these may be configured manually on the switch.

For details on ISE, refer to the following URL:

http://www.cisco.com/en/US/products/ps11640/index.html

To configure Cisco Trustsec on the switch, see the Cisco TrustSec Switch Configuration Guide at the following URL:

http://www.cisco.com/en/US/docs/switches/lan/trustsec/configuration/guide/trustsec.html

Release notes for Cisco TrustSec General Availability releases are at the following URL:

http://www.cisco.com/en/US/docs/switches/lan/trustsec/release/notes/rn_cts_crossplat.html

Additional information about the Cisco TrustSec solution, including overviews, datasheets, and case studies, is available at:

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

Table 1-1 lists the TrustSec features to be eventually implemented on TrustSec-enabled Cisco switches. Successive general availability releases of TrustSec will expand the number of switches supported and the number of TrustSec features supported per switch.

See the "Configuration Guidelines and Limitations"section for more information about the limitations of TrustSec features on Catalyst 4500 series switches.

Table 1-1 Cisco TrustSec Key Features

Cisco TrustSec Feature	Description
802.1AE Tagging (MACSec)	Protocol for IEEE 802.1AE-based wire-rate hop-to-hop Layer 2 encryption. Between MACSec-capable devices, packets are encrypted on egress from the transmitting device, decrypted on ingress to the receiving device, and in the clear within the devices. This feature is only available between TrustSec hardware-capable devices.
Endpoint Admission Control (EAC)	EAC is an authentication process for an endpoint user or a device connecting to the TrustSec domain. Usually EAC takes place at the access level switch. Successful authentication and authorization in the EAC process results in Security Group Tag assignment for the user or device. Currently EAC can be 802.1X, MAC Authentication Bypass (MAB), and Web Authentication Proxy (WebAuth).
Network Device Admission Control (NDAC)	NDAC is an authentication process where each network device in the TrustSec domain can verify the credentials and trustworthiness of its peer device. NDAC utilizes an authentication framework based on IEEE 802.1X port-based authentication and uses EAP-FAST as its EAP method. Successful authentication and authorization in NDAC process results in Security Association Protocol negotiation for IEEE 802.1AE encryption.
Security Group Access Control List (SGACL)	A Security Group Access Control List (SGACL) associates a Security Group Tag with a policy. The policy is enforced upon SGT-tagged traffic egressing the TrustSec domain.
Security Association Protocol (SAP)	After NDAC authentication, the Security Association Protocol (SAP) automatically negotiates keys and the cipher suite for subsequent MACSec link encryption between TrustSec peers. SAP is defined in IEEE 802.11i.
Security Group Tag (SGT)	An SGT is a 16-bit single label indicating the security classification of a source in the TrustSec domain. It is appended to an Ethernet frame or an IP packet.
SGT Exchange Protocol (SXP)	Security Group Tag Exchange Protocol (SXP). With SXP, devices that are not TrustSec-hardware-capable can receive SGT attributes for authenticated users or devices from the Cisco Secure Access Control System (ACS). The devices can forward the sourceIP-to-SGT binding to a TrustSec-hardware-capable device for tagging and SGACL enforcement.

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.