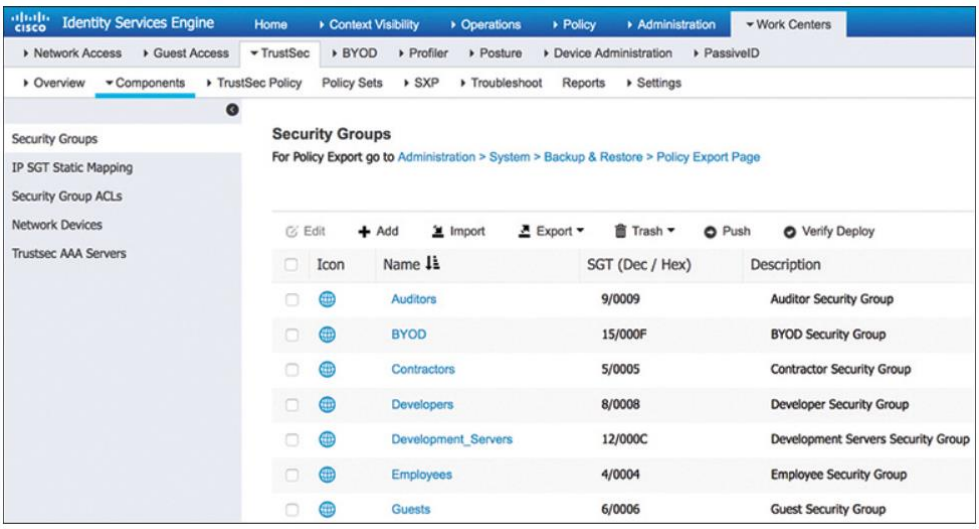
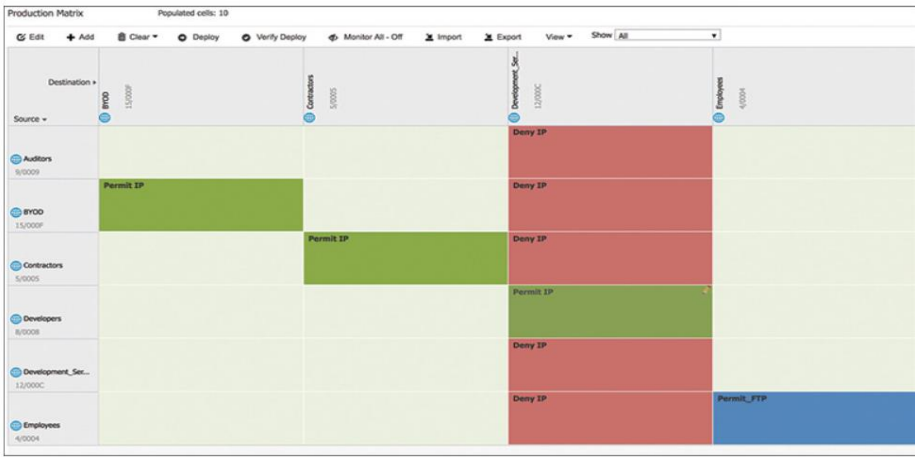
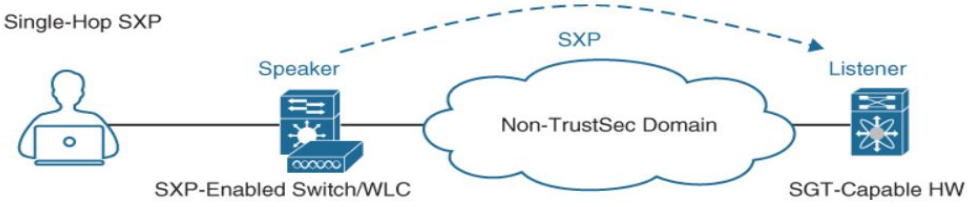
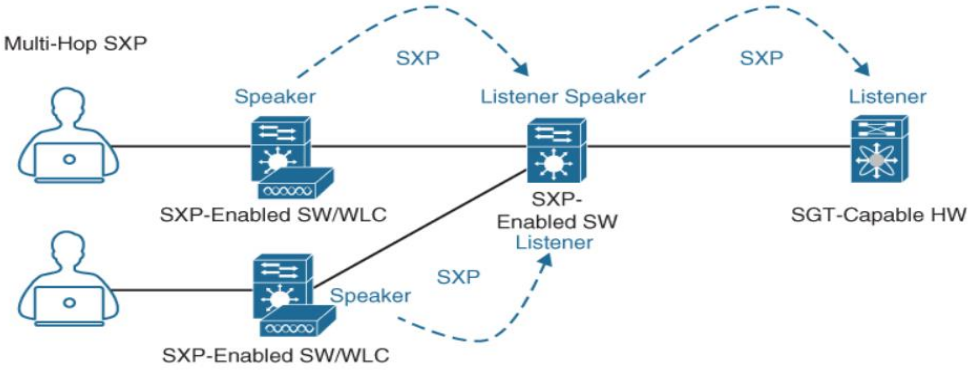
TrustSec:

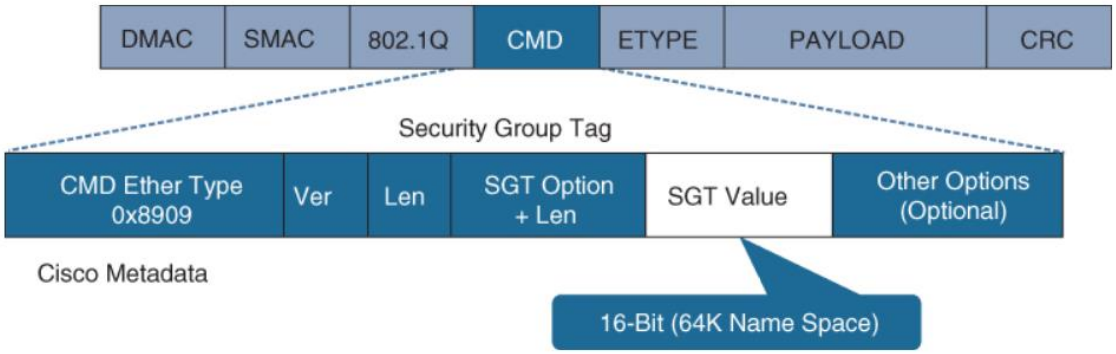
- TrustSec is next-generation access control enforcement solution developed by Cisco.
- To address the growing operational challenges related to maintaining firewall rules.
- To maintaining the Firewall rules and ACLs by using Security Group Tag (SGT) tags.
- It uses SGT tags perform ingress tagging & egress filtering enforce access control policy.
- Cisco ISE assigns the SGT tags to users or devices that are successfully authenticated.
- Cisco ISE assigns the SGT tags to users authorized through 802.1x, MAB, or WebAuth.
- The SGT tag assignment is delivered to the authenticator as an authorization option.
- After SGT tag is assigned, an access enforcement policy allow or drop based on SGT tag.
- After SGT tag is assigned SGT Tag can be applied at any egress point of TrustSec network.
- The SGT tags represent the context of the user, device, use case, or the function.
- This means SGT tags are often named after particular roles or business use cases.
- The SGT name is available on Cisco ISE and the network devices to create policies.
- What is actually inserted into a Layer 2 frame SGT tag is basically a numeric value.
- It Config occurs three phases Ingress classification, Propagation & Egress enforcement.

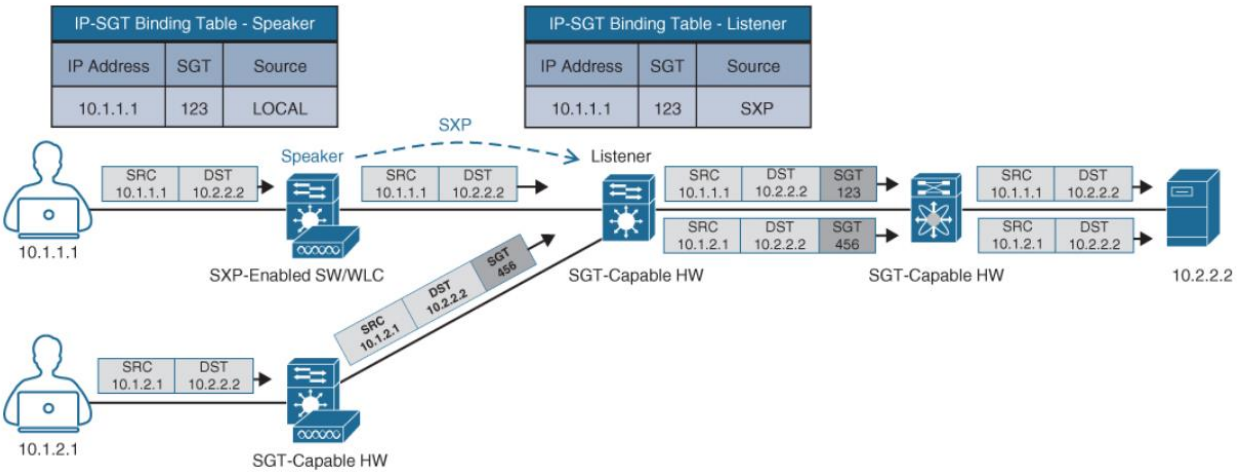












MACsec:

- MACsec is an IEEE 802.1AE standards-based Layer 2 hop-by-hop encryption method.
- In MACsec the traffic is encrypted only on the wire between two MACsec peers.
- In MACsec the traffic is unencrypted as it is processed internally within the switch.
- This allows the Cisco switch to look into the inner packets for things like SGT tags.
- To perform packet enforcement or Quality of Service (QoS) etc prioritization.
- MACsec also leverages onboard ASICs to perform the encryption and decryption.
- Rather than having to offload to a crypto engine, as with Internet Protocol Security.
- It is based on Ethernet frame format; an additional 16-byte MACsec Security Tag field.
- MACsec provides authentication using Galois Method Authentication Code (GMAC).
- Authenticated encryption using Galois/Counter Mode Advanced Encryption Standard.