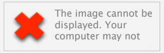
CCNP Security - SISAS
Security Group Tags - SGT

What is SGT ?

- A label / tag identifying a packet
- How is it different than a VLAN tag ?
  - It is a tag used for security purposes
  - It identifies the context of the user, because it is assigned based on
    - How did the user access the network
    - From which device did the user access the network
    - At what time did the user access the network
    - Was the user's device profiled
    - What is the posture of the user's machine



SGT Building Blocks

- Classification
  - SGT assignment, always done at the network ingress point
  - Can be static or dynamic
- Transport
  - Via inline tagging by the NAD
  - Via SXP protocol, a control-plane protocol
    - Used to propagate SGT across devices that do not support SGT inline tagging
    - Runs over TCP 64999
    - Connection can be unidirectional (speaker-listener)
    - Connection can be bidirectional, both devices can play both roles
- Enforcement
  - Policy is applied via SGACL or SGFW

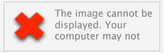
How does SGT help ?

- Used to configure firewall rules
  - Restrict network access
- Firewall rules
  - Configured on layer 3 switches, named SGACL
  - Configured on ASA firewall, named SGFW
  - Configured on IOS Zone-Based Firewall, named SGFW
- Why is it better than regular firewall rules ?
  - The tag identifies much more than the user, it identifies the health state of the user/device
  - A user can have the same tag, regardless of point of connection, thus regardless of its IP address
  - In the BYOD context, a user may actually have 1-10 IP addresses assigned, which presents a scalability problem with firewall rules

The image cannot be displayed. Your computer may not

SGT Overview

- SGT
  - Layer 2 tag, by default
  - Can be copied and carried in the layer 3 header by using ESP encapsulation
    - Helps keep the security tag across routing domains
- SGT is dynamically assigned by ISE as part of the authorization policy
  - For authenticated endpoints
- SGT is statically assigned by NAD
  - For non-authenticated endpoints, like servers
  - It can be assigned per VLAN, per IP, per subnet
- SGT is always applied to the packet by the NAD
  - Requires both hardware and software capabilities



SGT Configuration Steps

- Configure TrustSec (CTS) between ISE and NAD
- Configure ISE dynamic SGT classification
- Configure NAD static SGT classification
- Configure SGACL on ISE
- Configure SGACL and SGFW enforcement
- Optionally configure SXP session between network devices

Q&A