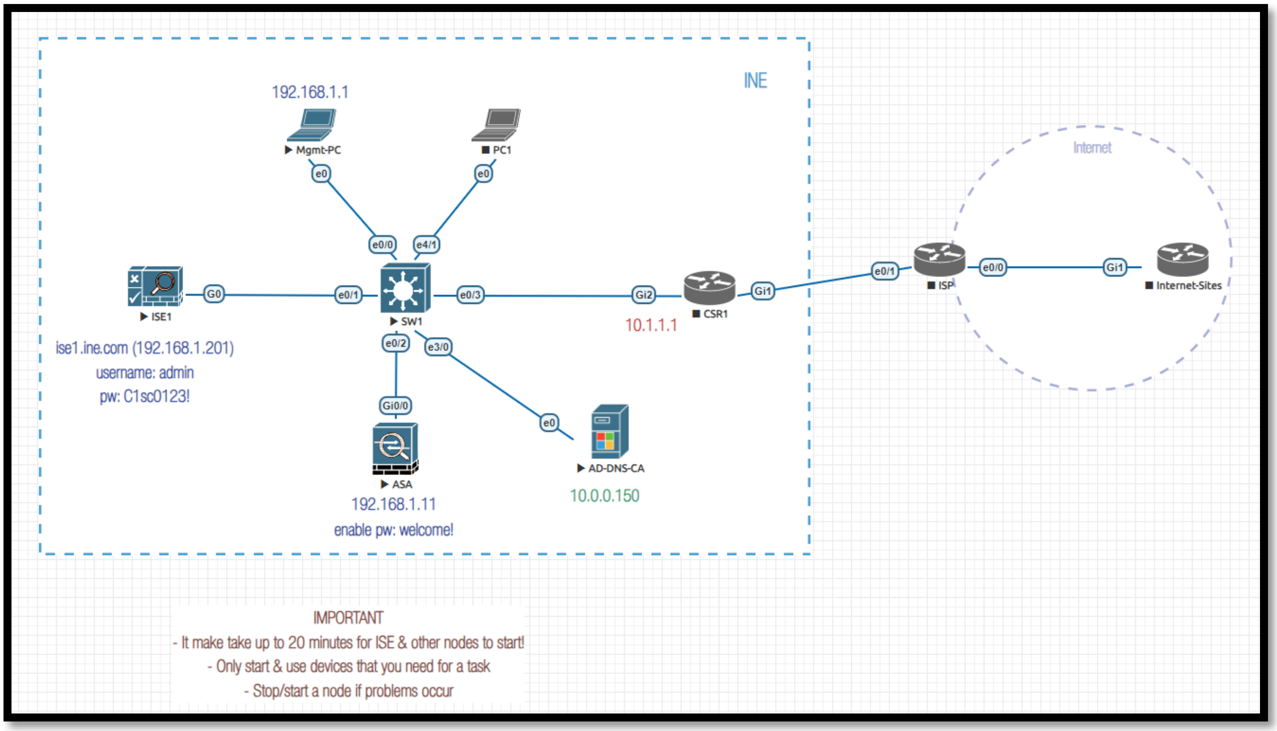

IMPORTANT

- It make take up to 20 minutes for ISE & other nodes to start!
- Only start & use devices that you need for a task
- Stop/start a node if problems occur

TASK 1 – TrustSec Propagation

- Configure a SXP session between SW1 & ASA in VLAN192
    - Make ASA the Listener
- Don’t use password for authentication
- Enable inline tagging on ASA’s G0/0
    - Untagged packets should be assigned SGT value 80
    - Traffic that is already tagged should retain the original number

TASK 2 – TrustSec on IOS

- Configure TrustSec components on ISE1
    - Delete default SGTs (except those in use)
    - Configure SGT for HR (100) and APPS (200)
- Integrate SW1 with ISE for TrustSec
    - SW1 & ISE are preconfigured for basic communication
    - Make sure SW1 downloads PAC & environment data from ISE
    - Use a local user account for SSH access
    - Use a password “cisco” for PAC provisioning
- Configure SGACL “HRAPPS” to only allow ICMP, TCP 5190 & UDP 17001
    - The SGACL should be used to restrict HR -> APPS communication

TASK 3 – TrustSec on ASA

- Configure ISE1 & ASA to integrate for TrustSec
    - Establish basic RADIUS communication
    - Generate a PAC on ISE1 and import it out of band from the Management PC via SCP
    - Authenticate as “cisco” with password “welcome!”
- Configure an ACL to deny all TCP traffic within the BYOD domain
    - Allow all other communication
    - Attach the ACL to the inside interface

TASK 4 – Preparing for Wireless TrustSec

- Assume there is a WLC configured as a SXP Speaker at 192.168.1.150
- Configure ISE to exchange SGT-IP mappings with the WLC
    - Enable the SXP service
    - Authenticate the session with a password “cisco123”