Paris Session 2022

SD-WAN & Cybersecurity

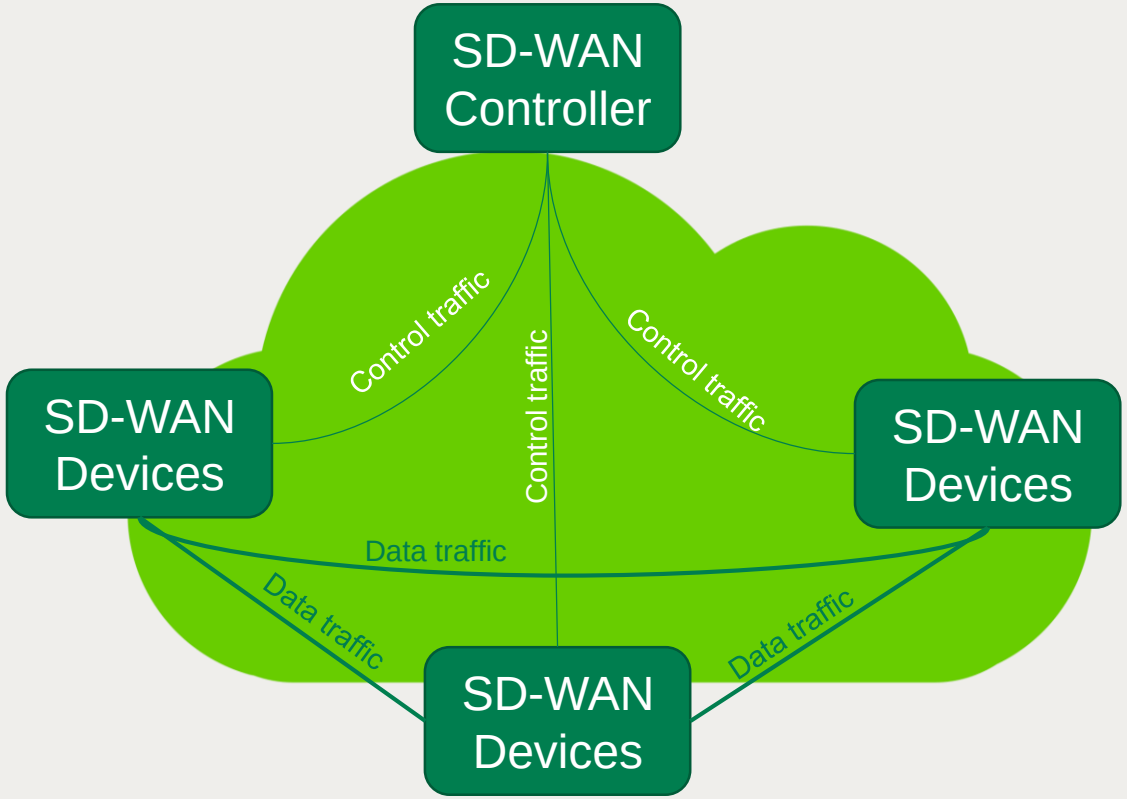
SC D2: Information Systems and Telecommunication

Question 3.3: SD-WAN's clear advantage including rapid service provisioning, often with the use of a centralised control hosted in the public cloud. Discuss the potential cybersecurity concerns and methods to address these concerns, especially when SD-WAN is used to carry sensitive and critical operational data such as SCADA and substation asset access including remote protection relay management access.

Mr. Thanyapatt Srijanthub, Thailand

SD-WAN & Cybersecurity

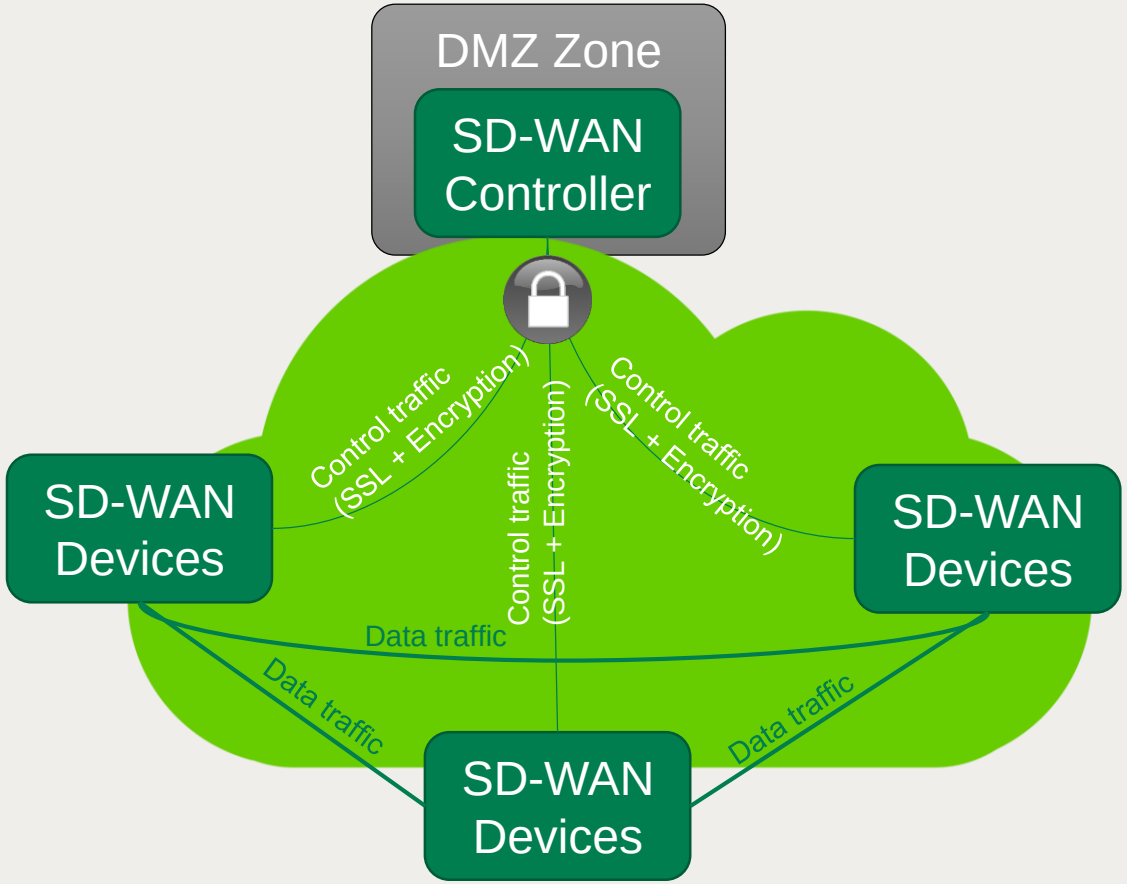
- *Potential cybersecurity concerns*
  - Control traffic between SD-WAN devices and SD-WAN Controller
  - Data traffic between SD-WAN devices
  - Cybersecurity objectives: CIA
  - The Example of possible attack
    - Man-in-the-middle
    - Packet Sniffing
    - Denial of Service



SD-WAN & Cybersecurity

- *Proposed solution: On-premise vs. On-Cloud*
  - On-premise controller: more control but overhead cost
  - On-Cloud controller: more features & less time to deploy but less control

- *Proposed solution: To secure the control traffic*
  - SD-WAN devices use secure tunnel to communication between the controller and devices: SSL port 541 and encryption options (3 levels: low, medium, high)
  - Place the controller in a DMZ: vendor's cloud, contractor's cloud or on premise cloud



SD-WAN & Cybersecurity

- *Proposed solution: To secure the data traffic*
  - SD-WAN devices use IPSec encryption for tunnels
  - Security policy to permit only traffic from SD-WAN devices
  - Security features on SD-WAN devices to protect network system and WAN connectivity (L3-L7) mainly IPSec VPN, NGFW
  - Security for access control: Multi-factor authentication (MFA), OT Active directory, Jump host
  - Other security feature: IDS, VA (Vulnerability Assessment)