NAME : MR. THANYAPATT SRIJANTHUB
COUNTRY : THAILAND
REGISTRATION NUMBER : 6906

GROUP REF. : D2
PREF. SUBJECT : PS3
QUESTION N° : 3.3

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.

Potential cybersecurity concerns

- ❑ Control traffic between SD-WAN devices and SD-WAN Controller
- ❑ Data traffic between SD-WAN devices
- ❑ The main cybersecurity objectives in Smart Grids are availability, integrity and confidentiality. Availability provides to ensure authorized staff to access to the resource and asset. Integrity means to prevent unauthorized modification of critical data. Confidentiality means to ensure authorized access control to the stored data and transmitted data. The cyber-attack compromise those CIA. The Example of possible attack are the followings:
  - Man-in-the-middle – an attacker will connect to the communication channel for a jamming attack.
  - Packet Sniffing – an attacker overhear messages that transmit between any station over a communication network
  - Denial of Service – attempt to delay or damage information transmission and exchange between stations.

Proposed solution

- ❑ On-premise vs. On-cloud Controller
  - On-premise Controller: Give staffs more control to the system (if any incident occurs, staffs can suddenly access to the system) but there are overhead expenses on hardware server, power consumption, space, etc.
  - On-cloud Controller: Give staffs less control to the system but there are many advanced features on cloud.
- ❑ 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
- ❑ To secure the data traffic
  - SD-WAN devices use IPSec encryption for tunnels
  - Security policy to permit only traffic from SD-WAN devices, other traffic is denied, especially traffic from any sources in the Internet
  - Security features on SD-WAN devices to protect network system and WAN connectivity (L3-L7) mainly IPSec VPN, NGFW and other features such as Antivirus, IPS, Application Control, SSL Inspection and Web Filtering, special hardware (ASIC) to process security tasks, etc.
  - Security for access control:
    - ▪ OT Active directory: it provides central authentication and authorization services for OT application. It also enables Network Administrators to assign policies, deploy software, and apply critical updates to an organization. When a user attempts to log on to a OT system, the operating system automatically will verify the user's password with the Active Directory.
    - ▪ Multi-factor authentication (MFA) - Rather than just providing for a username and password to gain access to a resource such as an application, online account, or a VPN, MFA requires one or more additional verification factors, which decreases the likelihood of a successful cyber-attack.

  - Other security feature:
    - ▪ IDS - monitors network traffic for suspicious activity, harmful activity or policy breaching, then it will send notification to cybersecurity team. It is a software application that scans a network or a system for the harmful activity or policy breaching.
    - ▪ VA (Vulnerability Assessment) provides a review of security weakness in SD-WAN and communication system.