Secured Enterprise Networks

1. **Course number and name:** 020RESES5/020SENES5 Secured Enterprise Networks

2. **Credits and contact hours:** 4 ECTS credits, 2x1:15 contact hours

3. **Name of course coordinator:** Tony Feghali

4. **Instructional materials:** Course handouts; technical documentation best practices documentation

5. **Specific course information**
    a. **Catalog description:**
    Understanding security services used when designing a secure enterprise network. Packet and content filtering, Security zones, Intrusion prevention techniques, Public Key Infrastructures, Virtual Private Networks, Network Access control, Data Leak Prevention, Network Management, Security Events and Information Management, SOC tools, SDN security, Design principles of a secure network. Case studies on designing an enhanced secure network design, dimensioning principles of security controls and appliances.

    b. **Prerequisites:** 020RCOES2/020NRSES2 Network Routing and Switching

    c. **Required** for CCE Telecommunication Networks Option students; **Selected Elective** for students in the CCE Artificial Intelligence and Software Engineering Options.

6. **Educational objectives for the course**
    a. **Specific outcomes of instruction:**
    – Understand the security requirement for an enterprise network.
    – Identify the benefits of the usage of security protocols.
    – Identify weakness in a network design.
    – Propose and design a secure solution for an enterprise network.
    – Dimension appliances and services to be implemented in a secure design.

    b. **PI addressed by the course:**

PI	1.1	1.2	1.3	2.1	2.2	2.3	2.4	3.1	3.2	5.1	6.4
Covered	x	x	x	x	x	x	x				x
Assessed	x	x	x	x	x	x	x	x	x	x	x

7. **Brief list of topics to be covered**
    – Security services + Example of secure messages exchange. (1 lecture)
    – Public Key Infrastructures + Lab. (3 lectures)

- Packet and Content level filtering. (1 lecture)
- FW-UTM-NGFW. (1 lecture)
- Intrusion prevention - IPS – WAF – Honeypot. (1 lecture)
- Security Zones concept and Design. (1 lecture)
- VPN + Tunneling concepts + Lab. (1 lecture)
- Comparison between different protocols (Layer 2 – IPsec – SSL VPN- SSTP)
- PPTP/L2TP – IPsec + Lab. (1 lecture)
- SSL + Lab. (1 lecture)
- Identity Management. (1 lecture)
- 802.1x + NAC. (1 lecture)
- Data Leak Prevention. (1 lecture)
- Network Management. (2 lectures)
- Centralized Logging – SEIM – SOC tools (2 lectures)
- Traffic flow matrix + Case study. (1 lecture)
- Case study: studying an existent design + defining the Flow Matrix. (1 lecture)
- Case study: Designing internal security Zones. (1 lecture)
- Case study: Designing Internet Access protection. (1 lecture)
- Case study: Designing a VPN solution. (1 lecture)
- Case study: choosing the Appliances (based on datasheets). (1 lecture)
- Case study: NAC solution. (1 lecture)
- SDN Security + Lab. (2 lectures)