SEC 175: PERIMETER DEFENSE

COURSE DESCRIPTION:

Prerequisites: None
Corequisites: None

This course introduces the principles of securing networks using routers and firewalls. Topics include networking protocols, threat mitigation, firewall configuration, authentication, authorization, intrusion detection, encryption, IPSec, VPNs, and remote access technologies. Upon completion, students should be able to secure internal networks using router and firewall technologies.
Course Hours per Week: Class, 1. Lab, 4. Semester Hours Credit, 3.

LEARNING OUTCOMES:

Upon completing requirements for this course, the student will be able to:

A. Identify core issues of network protection and perimeter defense.
    1. Explain and implement network defense fundamentals
    2. Design, apply, and search network traffic signatures
    3. Explain and identify types of intrusion detection systems
B. Deploy remote access technologies.
    1. Design and create virtual private networks (VPN)
C. Secure internal networks using router and firewall technologies.
    1. Choose, design, and implement firewalls using appropriate topology
    2. Strengthen and manage firewalls

OUTLINE OF INSTRUCTION:

I. Configure and manage firewalls
    A. Identify and recognize firewall platforms, architecture, and defense capability
    B. Review and apply initial configuration of firewall security zones, interfaces, and virtual routing
    C. Describe and practice the configuration of firewall source and destination Network Address Translation
    D. Recognize and demonstrate the use of management and reporting features available
II. Secure Internal networks
    A. Summarize, configure, and deploy basic filtering methodologies to protect against known and unknown attack vectors
    B. Discuss and configure firewall high availability to protect business critical infrastructure by minimizing downtime
III. Configure remote access technologies
    A. Configure firewall certificate management as well as inbound and outbound secure socket layer decryption
    B. Understand and implement site-to-site Virtual Private Networks through the use of IP Security Tunnels