Cybersecurity Infrastructure Configuration

Industry Partner: Palo Alto Networks

This course provides the student with a general understanding of how to install, configure, and manage firewalls for defense of enterprise network architecture. Students will learn the theory and configuration steps for setting up the security, networking, threat prevention, logging, and reporting features of next generation firewall technologies.

Pre-requisite: Basic Computer Knowledge

Course Objective:

Upon completion of this course, students will be able to:

- Compare and contrast industry leading firewall platforms, architecture, and defense capability related to zero trust security models and public cloud security.
- Demonstrate and apply configuration of firewall initial access, interfaces, security zones, virtual routing, filtering, licensing, service routes, software updates, and Policy-based forwarding.
- Analyze security policy administrative concepts related to source and destination network address translation.
- Outline and construct security policies to identify known and unknown application software running on the service network.
- Differentiate, configure, and deploy filtering technologies such as anti-virus, antispyware, and file blocking, to protect against telemetry induced attack vectors.

Course Outline:

1. Computer Physical Hardware Components
2. Networking Concepts
3. Basics of Firewall and Types
4. Virtualization Fundamentals
5. Introduction to Cybersecurity
6. Security Architecture Planning
7. Initial Configuration
8. Interface Configuration and Security Policies
9. App – ID & Content ID
10. URL Filtering

Hardware & Software Requirements

- 8 GB RAM, i3/i5 Processor, 200GB HDD, High Speed Internet connectivity
- Operating System: Windows 7 or later
- VMware Workstation 12 or later