SOUTHEAST COMMUNITY COLLEGE
CONSTRUCTION MANUFACTURING AND TECHNOLOGY DIVISION
Computer Information Technology Program
Revision Date: August 2024

I. CATALOG DESCRIPTION

Course Number:	INFO2581
Course Title:	Network Security Systems
Prerequisite(s):	INFO1491, INFO1494, ELEC2760
Catalog Description:	This course provides in-depth training in deploying and configuring enterprise-level security devices. Students gain an understanding of how Next-Generation Firewall (NFGW)/Unified Threat Management (UTM) defenses and countermeasures are used to protect today's networks and critical information systems.
Credit Hours:	3
Class Hours:	45
Lab Hours:	0
Total Contact Hours:	45

II. COURSE OBJECTIVES: *Course will:*

- **A.** Identify, install, and configure open-source Linux, Windows-based and Vendor-specific firewall solutions.
- **B.** Define essential components of Next-Generation Firewalls (NGFWs) and perform the initial configurations.
- **C.** Introduce Basic and Custom App-ID, Basic and Advanced Content-ID, and file blocking techniques used by NGFWs.
- **D.** Implement methods to inspect encrypted traffic on NGFWs.
- **E.** Introduce Basic and Advanced User-ID configurations.
- **F.** Provide procedures to establish Site-to-Site VPNs and Quality of Service (QoS) configuration on NGFWs.
- **G.** Examine NGFW Management, Monitoring, and Reporting options.
- **H.** Describe Active/Passive High Availability (HA) on NGFWs.

III. STUDENT LEARNING OUTCOMES AND GENERAL EDUCATION LEARNING OUTCOMES:

- **A.** Student Learning Outcomes: *Student will be able to:*
  - **1.** Differentiate among NGFW Platforms & Architectures.
  - **2.** Describe NGFW Flow Logic.
  - **3.** Perform Basic Interface and Network Address Translation (NAT) configurations.
  - **4.** Establish initial NGFW security policies.
  - **5.** Configure protocol decoders, application signatures, and traffic classifications.
  - **6.** Create custom application and threat signatures.
  - **7.** Distinguish among two categories of encryption algorithms used with SSL/TLS.
  - **8.** Construct outbound and inbound decryption policies to filter network traffic.
  - **9.** Create a NGFW security policy to examine certain types of file transfers.
  - **10.** Demonstrate how to incorporate user and group information into security policies.
  - **11.** Manage User-ID using Terminal Services, Captive Portal, and redistribution.
  - **12.** Set up a site-to-site VPN and troubleshoot IPSec issues.

13. Configure Quality of Service (QoS) policies, profiles, interfaces, and monitoring tools.
14. Implement filtering, reporting, and forwarding using integrated firewall logs.
15. Use Simple Network Management Protocol (SNMP) and syslog for monitoring.
16. Configure a basic Active/Passive High Availability (HA) architecture.

B. General Education Learning Outcomes (GELOs)

1. GELO #3: Critical Thinking & Problem Solving
Outcome 2: Synthesize information to arrive at reasoned solutions to problems.

IV. CONTENT/TOPICAL OUTLINE

A. Next-Generation Firewall (NGFW) essentials and initial firewall and interface configuration.

1. Firewall management using browser-based and client-based interfaces.
2. Establish zones and interface types.

B. Network Address Translation (NAT) and initial security policies.
C. Basic and custom App-ID and basic and advanced Content-ID.

1. Application identification and classification.
2. Custom spyware and vulnerability signatures.

D. Decryption on NGFWs.
E. File Blocking and Palo Alto Networks (PAN) WildFire configuration.

1. File blocking profiles and WildFire analysis.

F. Basic and Advanced User-ID.

1. Mapping users to IP addresses with User-ID.
2. Terminal Services agent and Captive Portal.

G. Site-to-Site VPNs
H. Quality of Service (QoS) on NGFWs.
I. Log management, reporting and advanced monitoring.

1. Dashboard, viewing and filtering logs, Panorama, and report creation.

J. Active/Passive High Availability (HA) on the PAN NGFW.

1. High Availability (HA) configuration, split brain management, and monitoring.

V. INSTRUCTIONAL MATERIALS

A. Required Text(s): None
B. Other Resources: Course Supplemental Materials, PAN Academy website course content, and Trial and shareware programs/utilities available from the Internet
C. Computer and Internet access

VI. METHODS OF PRESENTATION/INSTRUCTION

A. Methods of presentation typically include a combination of the following:

1. Technology enhanced lectures
2. ~~In-class~~ Hands-on activities
3. Engaged learning activities
4. Development of progressive projects using theories covered in class

VII. METHODS OF EVALUATION

A. Methods of evaluation, although determined by the individual instructor, traditionally includes a combination of the following:

1. Attendance
2. In-class participation activities
3. Homework assignments

4. Quizzes

VIII. SPECIFIC COURSE REQUIRMENTS

A. This course will not qualify as a prerequisite if the student receives a final grade below a C (70%).