Curriculum Committee Approval: 09/01/2020

Lecture Contact Hours: 32-36; Homework Hours: 64-72; Total Student Learning Hours: 96-108
Laboratory Contact Hours: 48-54; Homework Hours: 0; Total Student Learning Hours: 48-54

CUYAMACA COLLEGE
COURSE OUTLINE OF RECORD

COMPUTER AND INFORMATION SCIENCE 272 – PALO ALTO NETWORKS FIREWALL CONFIGURATION, MANAGEMENT, AND THREAT PREVENTION

2 hours lecture, 3 hours laboratory, 3 units

Catalog Description

Palo Alto Networks firewalls are leaders in Cybersecurity. This is the third course designed to teach students how to plan for security, design and implement Palo Alto firewalls for optimum protection. Students will learn to build and deploy high availability firewalls for the defense of Enterprise network architecture. Students will also learn features necessary for setting up traffic handling, advanced content and user identification, quality of service, GlobalProtect, monitoring and reporting, and high availability of next-generation firewalls. This course prepares students to take the Palo Alto Certified Network Security Engineer (PCNSE) exam.

Prerequisite

"C" grade or higher or "Pass" in CIS 270 and CIS 271 or equivalent

Entrance Skills

Without the following skills, competencies and/or knowledge, students entering this course will be highly unlikely to succeed:

1) Define an appropriate network security solution
2) Design the necessary policies for the proposed security solution
3) Implement the Design in two different models of Palo Alto appliances
4) Test the security policies and implementation of the installed Palo Alto appliance

Course Content

1) Security Architecture Planning
2) Infrastructure Device Configuration
3) Cybersecurity Policy
4) Application Software Identification
5) Antivirus, Anti-Spyware, and File Blocking
6) Uniform Resource Locator Filtering
7) Decryption and Certificate Management
8) Virus Analysis and Mitigation
9) End-User Identification
10) Remote Access Security
11) Security Monitoring and Reporting
12) Security Device High Availability

Course Objectives

Students will be able to:

1) Formulate an industry-standard design to protect infrastructure against cybersecurity threats.
2) Apply advanced filtering methodologies, such as user, application, and content identification, to protect against all known and unknown attack vectors.
3) Describe the basics of cryptography, including synchronous and asynchronous encryption, public key infrastructure, and certificates.
4) Assess and harden endpoints based on security policies.

5) Describe the uses of advanced malware research and analysis that provide enhanced protection for enterprise networks.
6) Examine mobile- and cloud-based connection technologies.
7) Compare industry-leading firewall platforms, architecture, and defense capability related to Zero Trust security approaches and public cloud security.
8) Demonstrate and apply configuration of firewall initial access, interfaces, security zones, routing, etc.
9) Analyze security policy administrative concepts related to source and destination network address translation (NAT).
10) Outline and construct security policies to identify known and unknown application software.
11) Differentiate, configure, and deploy filtering technologies such as antivirus, anti-spyware, and file blocking.
12) Construct and deploy URL profiles for attachment to next-generation firewall security policies.

Method of Evaluation

A grading system will be established by the instructor and implemented uniformly. Grades will be based on demonstrated proficiency in the subject matter determined by multiple measurements for evaluation, one of which must be essay exams, skills demonstration or, where appropriate, the symbol system.

Special Materials Required of Student

Portable Flash drive and internet access

Minimum Instructional Facilities

Laboratory equipped with Palo Alto security devices, computers, and internet access

Method of Instruction

Assignments, Quizzes, Final Project, and Exams.

Out-of-Class Assignments

Labs that are completed using the Netlab virtualized environment.

Texts and References

1) Required (representative example): Palo Alto Academy online curriculum, August 2019.
2) Supplemental: The Cybersecurity Survival Guide, September 2018, PDF, Palo Alto Networks.

Student Learning Outcomes

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

1) Collaborate in teams to design, implement and document a security plan for an Enterprise level network.
2) Collaborate in teams to develop and implement a response plan for threat intrusion and detection.
3) Configure networks to protect against cybersecurity threats.