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 271 – PALO ALTO NETWORKS – CERTIFIED NETWORK SECURITY ADMINISTRATOR (PCNSA)

2 hours lecture, 3 hours laboratory, 3 units

Catalog Description
Cybersecurity has become an essential survival skill for the modern world. The ability to secure information networks is increasing in demand every day. The Palo Alto Networks firewalls have become the industry standard for front-line Cybersecurity appliances. This course is designed to teach students to configure and manage next-generation firewalls. This is the second course in a series of three that trains students to become Network Security professionals. Students will learn to build and deploy Global Protect systems, manage and maintain high availability firewall protection, and monitor network traffic. Upon completion, students will be prepared to take the PCNSA exam for certification.

Prerequisite
None

Recommended Preparation
CIS 270

Entrance Skills
Without the following skills, competencies and/or knowledge, students entering this course will be highly unlikely to succeed:
1) Basic computer skills
2) Basic networking terminology
3) Subnetting

Course Content
1) Security Platform and Architecture
2) Initial Configuration
3) Interface Configuration
4) Security and NAT Policies
5) App-ID
6) Content-ID
7) URL Filtering
8) Decryption
9) WildFire
10) User-ID
11) GlobalProtect
12) Site-to-Site VPN
13) Monitoring and Reporting
14) Active/Passive High Availability
15) Next-generation Security Practice
16) NextSteps

Course Objectives
Students will be able to:
1) Configure and manage the essential feature of Palo Alto Networks next-generation firewalls
2) Configure and manage GlobalProtect to protect systems that are located outside of the data-center perimeter
3) Configure and manage firewall high availability
4) Monitor network traffic using the interactive web interface and firewall reports

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:
1) Essay exams
2) Skills demonstration
3) Labs
4) Final Project

Special Materials Required of Student
Internet access, Flash drive, Access to Cuyamaca Netlab

Minimum Instructional Facilities
Classroom equipped with computers and internet access.

Method of Instruction
Lecture, Labs, and Out-of-Class Assignments

Out-of-Class Assignments
Utilizing Cuyamaca Netlab as a virtual networking environment, students will compete labs designed to reinforce concepts and practices explained in the curriculum.

Texts and References
1) Required: Cybersecurity Survival Guide, Palo Alto Networks, August 2018, https://www.paloaltonetworks.com/resources/techbriefs/cybersecurity-survival-guide
2) Supplemental: Guide to Networking Essentials 7th edition, Cengage, e-publication, 2016; https://www.cengage.com/c/guide-to-networking-essentials-7e-tomsho/9781305105430/

Exit Skills
Students having successfully completed this course exit with the following skills, competencies and/or knowledge:
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

Student Learning Outcomes
Upon successful completion of this course, students will be able to:
1) Analyze a network security problem, and design, implement and test a solution through the successful completion of a semester-long project.
2) Collaborate in teams to allocate the responsibility of the analysis, design and implementation of a final project.