CS 82.59 Course Outline as of Fall 2022

CATALOG INFORMATION

Dept and Nbr: CS 82.59 Title: FIREWALLS
Full Title: Firewalls and Network Security
Last Reviewed: 5/10/2021

Units		Course Hours per Week		Nbr of Weeks	Course Hours Total	
Maximum	3.00	Lecture Scheduled	3.00	17.5	Lecture Scheduled	52.50
Minimum	3.00	Lab Scheduled	0	8	Lab Scheduled	0
		Contact DHR	0		Contact DHR	0
		Contact Total	3.00		Contact Total	52.50
		Non-contact DHR	0		Non-contact DHR	0

Total Out of Class Hours: 105.00 Total Student Learning Hours: 157.50

Title 5 Category:	AA Degree Applicable
Grading:	Grade or P/NP
Repeatability:	00 - Two Repeats if Grade was D, F, NC, or NP
Also Listed As:	
Formerly:	

Catalog Description:
Survey of topics in field of firewall, advanced threats and their characteristics. Students will learn how to manage firewalls and advanced threats using security policies, profiles and signatures to protect networks against emerging threats. Knowledge of the operation of firewalls is essential to the person who wants to ensure network security. The student will be introduced to the concepts, principles, types and topologies of firewalls to include packet filtering, proxy firewalls, application gateways, circuit gateways and stateful packet inspection. Additionally, the course provides the broad-based knowledge necessary to prepare students for further study in other specialized security fields. Cisco ASA and Palo Alto Networks, and other industry leading firewalls, will be examined and configured.

Prerequisites/Corequisites:
Course completion of CS 82.58 and CS 82.22C

Recommended Preparation:
Eligibility for ENGL 100 or ESL 100

Limits on Enrollment:

Schedule of Classes Information:

Description: Survey of topics in field of firewall, advanced threats and their characteristics. Students will learn how to manage firewalls and advanced threats using security policies, profiles and signatures to protect networks against emerging threats. Knowledge of the operation of firewalls is essential to the person who wants to ensure network security. The student will be introduced to the concepts, principles, types and topologies of firewalls to include packet filtering, proxy firewalls, application gateways, circuit gateways and stateful packet inspection. Additionally, the course provides the broad-based knowledge necessary to prepare students for further study in other specialized security fields. Cisco ASA and Palo Alto Networks, and other industry leading firewalls, will be examined and configured. (Grade or P/NP)
Prerequisites/Corequisites: Course completion of CS 82.58 and CS 82.22C
Recommended: Eligibility for ENGL 100 or ESL 100
Limits on Enrollment:
Transfer Credit: CSU;
Repeatability: Two Repeats if Grade was D, F, NC, or NP

ARTICULATION, MAJOR, and CERTIFICATION INFORMATION:

AS Degree:	**Area**			Effective:	Inactive:
CSU GE:	**Transfer Area**			Effective:	Inactive:
IGETC:	**Transfer Area**			Effective:	Inactive:
CSU Transfer:	Transferable	Effective:	Fall 2022	Inactive:	
UC Transfer:		Effective:		Inactive:	

CID:

Certificate/Major Applicable:
Both Certificate and Major Applicable

COURSE CONTENT

Student Learning Outcomes:
At the conclusion of this course, the student should be able to:
1. Demonstrate methods and techniques used by firewalls to counteract vulnerabilities
2. Describe basic network security vulnerabilities

Objectives:
At the conclusion of this course, the student should be able to:
1. Describe basic network security vulnerabilities
2. Explain firewalls and their features
3. Apply techniques used by firewalls to counteract vulnerabilities
4. Incorporate common solutions and strategies
5. Apply different Business Models and appropriate solutions
6. Describe a firewall's use of digital signature authentication
7. Explain the operation of firewalls with Built-in Virus Scanning
8. Perform installation and configuration of common firewalls
9. Demonstrate appropriate and ethical behavior and good work habits

Topics and Scope:

1. Security Platform and Architecture
2. Initial Configuration
3. Interface Configuration
4. Security and NAT Policies
5. URL Filtering
6. Decryption
7. Site-to-Site VPNs
8. Monitoring and Reporting
9. Active/Passive High Availability
10. Security Practices, Industry Ethical Standards of Behavior

Assignment:

Reading assignments include:
1. Online research of security devices and deployment practices
2. Approximately 50 pages weekly from the textbook

Homework problems include:
1. Weekly online discussion thread participation
2. Hands-on exercises to demonstrate proficiency with topics
3. Online quizzes (5 - 12)
4. Assignments for configuring and deploying firewalls

Other assignments include:
1. Skill demonstration examinations
2. Classroom scenario-based exercises

Methods of Evaluation/Basis of Grade:

Writing: Assessment tools that demonstrate writing skills and/or require students to select, organize and explain ideas in writing.

Weekly written online discussions	Writing 5 - 10%

Problem Solving: Assessment tools, other than exams, that demonstrate competence in computational or non-computational problem solving skills.

Homework problems, assignments for configuring and deploying firewalls.	Problem solving 15 - 30%

Skill Demonstrations: All skill-based and physical demonstrations used for assessment purposes including skill performance exams.

Class performances of configurating and deploying firewalls, and skill demonstration examinations	Skill Demonstrations 20 - 30%

Exams: All forms of formal testing, other than skill performance exams.

Quizzes and skill demonstration examinations	Exams 20 - 30%

Other: Includes any assessment tools that do not logically fit into the above categories.

Attendance and participation in scenario-based exercises	Other Category 5 - 20%

Representative Textbooks and Materials:
Cisco Next-Generation Security Solutions: All-in-one Cisco ASA Firepower Services, NGIPS, and AMP. Santos, Omar and Kampanakis, Panos and Woland, Aaron. Cisco Press. 2016 (classic)

Mastering Palo Alto Networks. Piens, Tom. Packet Publishing. 2020