Washtenaw Community College Comprehensive Report

CSS 210 Network Perimeter Protection - CCNA Security
Effective Term: Winter 2022

Course Cover

College: Business and Computer Technologies
Division: Business and Computer Technologies
Department: Computer Science & Information Technology
Discipline: Computer Systems Security
Course Number: 210
Org Number: 13400
Full Course Title: Network Perimeter Protection - CCNA Security
Transcript Title: Network Perimeter Protection
Is Consultation with other department(s) required: No
Publish in the Following: College Catalog , Time Schedule , Web Page
Reason for Submission: Three Year Review / Assessment Report
Change Information:
Consultation with all departments affected by this course is required.
Course description
Rationale: Master syllabus update
Proposed Start Semester: Spring/Summer 2021
Course Description: In this course, students learn how to implement security solutions that reduce the vulnerability of computer networks. Topics include principles of network security, packet filtering with Access Control Lists (ACLs), configuring networks and deploying multiple firewall topologies using Cisco devices, implementing virtual private networks (VPNs) and user authentication. This course uses the Cisco Networking Academy curriculum.

Course Credit Hours

Variable hours: No
Credits: 4
Lecture Hours: Instructor: 60 **Student:** 60
Lab: Instructor: 0 **Student:** 0
Clinical: Instructor: 0 **Student:** 0

Total Contact Hours: Instructor: 60 **Student:** 60
Repeatable for Credit: NO
Grading Methods: Letter Grades
Audit
Are lectures, labs, or clinicals offered as separate sections?: NO (same sections)

College-Level Reading and Writing

College-level Reading & Writing

College-Level Math

Level 1

Requisites

Prerequisite
CNT 206 minimum grade "C"

and
Prerequisite
CNT 216 minimum grade "C"

General Education

General Education Area 7 - Computer and Information Literacy
Assoc in Arts - Comp Lit
Assoc in Applied Sci - Comp Lit
Assoc in Science - Comp Lit

Request Course Transfer

Proposed For:

Student Learning Outcomes

1. Configure router features to filter ingress and egress traffic.
   Assessment 1
   Assessment Tool: Outcome-related questions on the departmentally-developed final concepts and skills exam
   Assessment Date: Winter 2024
   Assessment Cycle: Every Three Years
   Course section(s)/other population: All sections
   Number students to be assessed: All students
   How the assessment will be scored: Departmentally-developed rubric
   Standard of success to be used for this assessment: At least 80% of students must score 70% or better
   Who will score and analyze the data: Department faculty

2. Configure firewalls to protect inside and demilitarized zone (DMZ) networks against external threats.
   Assessment 1
   Assessment Tool: Outcome-related questions on the departmentally-developed final concepts and skills exam
   Assessment Date: Winter 2024
   Assessment Cycle: Every Three Years
   Course section(s)/other population: All sections
   Number students to be assessed: All students
   How the assessment will be scored: Departmentally-developed rubric
   Standard of success to be used for this assessment: At least 80% of students must score 70% or better.
   Who will score and analyze the data: Department faculty

3. Implement various authentication methods on routers and firewalls.
   Assessment 1
   Assessment Tool: Outcome-related questions on the departmentally-developed final concepts and skills exam
   Assessment Date: Winter 2024
   Assessment Cycle: Every Three Years
   Course section(s)/other population: All sections
   Number students to be assessed: All students
   How the assessment will be scored: Departmentally-developed rubric
   Standard of success to be used for this assessment: At least 80% of students must score 70% or better.
   Who will score and analyze the data: Department faculty

4. Configure and implement Virtual Private Networks.

   Assessment 1

   Assessment Tool: Outcome-related questions on the departmentally-developed final concepts and skills exam
   Assessment Date: Winter 2024
   Assessment Cycle: Every Three Years
   Course section(s)/other population: All sections
   Number students to be assessed: All students
   How the assessment will be scored: Departmentally-developed rubric
   Standard of success to be used for this assessment: At least 80% of students must score 70% or better.
   Who will score and analyze the data: Department faculty

5. Implement 802.1x on switches.

   Assessment 1

   Assessment Tool: Outcome-related questions on the departmentally-developed final concepts and skills exam
   Assessment Date: Winter 2024
   Assessment Cycle: Every Three Years
   Course section(s)/other population: All sections
   Number students to be assessed: All students
   How the assessment will be scored: Departmentally-developed rubric
   Standard of success to be used for this assessment: At least 80% of students must score 70% or better.
   Who will score and analyze the data: Department faculty

Course Objectives

1. Describe security terminology and acronyms.
2. Describe security technologies, products, solutions and design.
3. Implement authentication and authorization on Cisco routers, security appliances and switches.
4. Implement layer 2 Identity Based Network Services and 802.1x.
5. Filter network traffic on switches, routers and adaptive security appliance (ASA) devices.
6. Explain VPN technologies including Internet Security Association and Key Management Protocol (ISAKMP) and Internet Protocol Security (IPSec).
7. Implement a site-to-site VPN using pre-shared keys and digital certificates.
8. Implement a remote access VPN.
9. Explain network threats, mitigation techniques and the basics of securing a network.
10. Configure IPS to mitigate attacks on the network.
11. Describe local area network (LAN) security considerations and implement endpoint and Layer 2 security features.
12. Describe methods for implementing data confidentiality and integrity.
13. Implement an ASA firewall configuration using the command line interface (CLI).
14. Implement an ASA firewall configuration and VPNs using an adaptive security device manager (ASDM).
15. Test network security and create a technical security policy.

New Resources for Course

Course Textbooks/Resources

Textbooks
Manuals
Periodicals
Software

Equipment/Facilities

Level III classroom
Computer workstations/lab

Reviewer	Action	Date
Faculty Preparer:		
Cyndi Millns	*Faculty Preparer*	*Jan 28, 2021*
Department Chair/Area Director:		
Cyndi Millns	*Recommend Approval*	*Jan 28, 2021*
Dean:		
Eva Samulski	*Recommend Approval*	*Jan 28, 2021*
Curriculum Committee Chair:		
Lisa Veasey	*Recommend Approval*	*Apr 21, 2021*
Assessment Committee Chair:		
Shawn Deron	*Recommend Approval*	*Apr 22, 2021*
Vice President for Instruction:		
Kimberly Hurns	*Approve*	*Apr 26, 2021*