Northwest Arkansas Community College

Business and Computer Information Systems Division

Discipline Code
NTWK

Course Number
2263

Course Title
Network Security Support

Catalog Description
Network Security Support is an advanced course that provides students with the knowledge to secure Cisco routers and switches and their associated networks. Students learn to configure, troubleshoot and monitor network devices to maintain integrity, confidentiality and availability of data and devices and develop competency in the technologies that Cisco uses in its security infrastructure. Some specific topics include: IPv4 to IPv6 transition, AAA, ACLs, secure network management and reporting, SD-WAN and Network Automation. This course is aligned with the CCNA Security and is recognized by the U.S. National Security Agency (NSA) and the Committee on National Security Systems (CNSS) to meet the CNSS 4011 training standard. Prerequisites: NTWK 2014, NTWK 2084, or equivalent knowledge.

Prerequisites
NTWK 2014 Network & Information Systems (CCNA1), and
NTWK 2084 Network Hardware Support (CCNA 2), or equivalent knowledge

Credit Hours
3 credit hours

Contact hours
45 lecture/lab contact hours

Load hours
3 load hours

Semesters Offered
On Demand

ACTS Equivalent
N/A

Grade Mode
A-F

Learning Outcomes

Students will:

- Describe security principles and concepts
- Describe Access controls and Security operations management
- Describe basic cryptography and PKI
- Describe and implement encryption on routers
- Implement VPNs and Tunneling
- Implement and configure Cisco Adaptive Security Appliance
- Host based Analysis using different Operating Systems Windows, Linux, Mac
- Describe Attack Vectors (Network Intrusion) and Threat Mitigation
- Describe Security monitoring and Operational Challenge
- Configure Zone-Based Policy Firewalls
- Configure and monitor Intrusion Prevention System
- Secure Layer 2 Switches
- Configure ASA settings and firewalls using CLI and ASDM
- Response strategy planning and response to security incidents
- Describe security policies and procedures in network security

General Education Outcomes Supported

- Students can write clear, coherent, well-organized documents, substantially free of errors.
- Students can use computers proficiently.
- Students can employ a variety of sources to locate, evaluate, and use Information.

Standard Practices

Topics list

- Security Teams
- Threat Vector
- Zero Trust
- Security Concepts
- Access Control Models
- Netflow
- TCP Dump
- Nxgen Firewall
- Data Visibility
- Session, transaction, statistical data
- Evasion and Obfuscation
- Adaptive Security Appliance

Learning activities

- Lab Assignments using Lab routers and Switches and Virtual NetLab
- Cisco Packet Tracer Activities
- Hands-on activities

- Quizzes
- Final Exam
- This course requires some in class, hands-on work and also additional hands-on work in a virtual or on-campus computer lab.

Assessments

- On-line chapter Exams in Netacad
- Hands-on lab assignments
- Packet Tracer Activities
- Hands on final Skill Based Assessment
- Comprehensive online final exam

Grading guidelines

Overall Score will be based on the below given grading scale.

A = 90-100
B = 80-89
C = 70-79
D = 60-69
F = 59 & below

In addition, students will demonstrate proficiency by scoring 70% or above on The Final Skill Based Assessment to pass the class.

Revision Date

May 27, 2020