COURSE OUTLINE: NASA204 - VIRTUAL PRIVATE NET

Prepared: Sam Laitinen
Approved: Corey Meunier, Chair, Technology and Skilled Trades

Course Code: Title	NASA204: VIRTUAL PRIVATE NETWORKS
Program Number: Name	2196: NETWRK ARCH & SEC AN
Department:	COMPUTER STUDIES
Semesters/Terms:	19W
Course Description:	This course will examine the use of virtual private network (VPN) technologies to provide secure communications, and the implementation and configuration of VPN technologies. The course explores site-to-site and multi-site VPN solutions using firewalls and routers, as well as several remote-access VPN solutions.
Total Credits:	4
Hours/Week:	4
Total Hours:	60
Prerequisites:	There are no pre-requisites for this course.
Corequisites:	There are no co-requisites for this course.
Essential Employability Skills (EES) addressed in this course:	EES 1 Communicate clearly, concisely and correctly in the written, spoken, and visual form that fulfills the purpose and meets the needs of the audience. EES 2 Respond to written, spoken, or visual messages in a manner that ensures effective communication. EES 3 Execute mathematical operations accurately. EES 4 Apply a systematic approach to solve problems. EES 5 Use a variety of thinking skills to anticipate and solve problems. EES 6 Locate, select, organize, and document information using appropriate technology and information systems. EES 7 Analyze, evaluate, and apply relevant information from a variety of sources. EES 8 Show respect for the diverse opinions, values, belief systems, and contributions of others. EES 9 Interact with others in groups or teams that contribute to effective working relationships and the achievement of goals. EES 10 Manage the use of time and other resources to complete projects. EES 11 Take responsibility for ones own actions, decisions, and consequences.
Course Evaluation:	Passing Grade: 50%,
Other Course Evaluation & Assessment Requirements:	NOTE: You must obtain a minimum mark of 50% in both the Theory portion and the Lab portion of the course. Failing to do so, will result in an overall failing grade (F). The professor reserves the right to adjust the mark up or down based on attendance, participation, leadership, creativity and whether there is an improving trend. • Students must complete and pass both the test and lab portion of the course in order to

pass the entire course.
- All Assignments must be completed satisfactorily to complete the course.
- A minimum of 80% attendance required in the lectures and labs.
- Makeup Tests are at the discretion of the instructor and will be assigned a maximum grade of 50%.
- The professor reserves the right to adjust the number of tests, practical tests and quizzes based on unforeseen circumstances. The students will be given sufficient notice to any changes and the reasons thereof.
- A student who is absent for 3 or more times without any valid reason or effort to resolve the problem will result in action taken.

NOTE: If action is to be taken, it will range from marks being deducted to a maximum of removal from the course.

Books and Required Resources:

Guide to Firewalls and VPNs by Michael Whitman, Herbert Mattord and Andrew Green
Publisher: Delmar Publishers Inc Edition: 3rd
ISBN: 9781111135393

Course Outcomes and Learning Objectives:

Course Outcome 1	**Learning Objectives for Course Outcome 1**
Develop an understanding of Information Security	• Describe the basics of Information Security • Reive examples of Network Infrastructures and Related Security Concerns • Enhancing the Security of Wired Versus Wireless LAN Infrastructures • Examine Common Network Security Components Used to Mitigate Threats
Course Outcome 2	**Learning Objectives for Course Outcome 2**
Develop an understanding of Firewall Fundamentals	• Describe the purpose of a Firewall. • Examine both software and hardware firewalls available • Determine when a Firewall is needed • Discuss how Firewalls work and what they do • Review TCP/IP Fundamentals
Course Outcome 3	**Learning Objectives for Course Outcome 3**
Review VPN Fundamentals	• Describe the purpose of a Virtual Private Network • Examine benefits of deploying a VPN • Examine the Relationship Between Encryption and VPNs • Review types of VPN authentication
Course Outcome 4	**Learning Objectives for Course Outcome 4**
Examine Network Security Threats and Issues	• Review Hacker threats and motivation • Examine Threats from Internal Personnel and External Entities • Review types of attacks • Examine varied threats over wired and wireless networks
Course Outcome 5	**Learning Objectives for Course Outcome 5**
Review Implementing Network Security	• Discuss Network Design and Defense in Depth • Discuss Authentication, Authorization, and Accounting • Examine Hosts: Local-Only or Remote and Mobile as related to VPNs
Course Outcome 6	**Learning Objectives for Course Outcome 6**
Explore Network Security	• Discuss Fail-Secure, Fail-Open, and Fail-Close Options

Management Best Practices	• Examine Physical vs Virtual Security • Example Securing the VPN • Review the Security Checklist
Course Outcome 7	**Learning Objectives for Course Outcome 7**
Review Firewall Basics	• Discuss Firewall Rules • Review Authentication, Authorization, and Accounting • Discuss Monitoring and Logging • Review Limitations of Firewalls • Discuss The Downside of Encryption with Firewalls • Review various Management Interfaces
Course Outcome 8	**Learning Objectives for Course Outcome 8**
Explore Firewall Deployment Considerations	• Discuss What Should You Allow and What Should You Block • Discuss Essential Elements of a Firewall Policy • Evaluating Needs and Solutions in Designing Security
Course Outcome 9	**Learning Objectives for Course Outcome 9**
Explore Firewall Management and Security	• Best Practices for Firewall Management • Security Measures in Addition to a Firewall • Testing Firewall Security • Proper Firewall Implementation Procedure
Course Outcome 10	**Learning Objectives for Course Outcome 10**
Explore Using Common Firewalls	• Uses for a Host Software Firewall • Examples of Software Firewall Products • Discuss Simple Firewall Techniques
Course Outcome 11	**Learning Objectives for Course Outcome 11**
Examine VPN Management Best Practice	• Examine Developing a VPN Policy • Explore Developing a VPN Deployment Plan • Discuss VPN Threats and Exploits • Commercial or Open Source VPNs • Review Differences Between Personal and Enterprise VPNs • Discuss VPN Troubleshooting
Course Outcome 12	**Learning Objectives for Course Outcome 12**
Explore VPN Technologies	• Examine Differences Between Software and Hardware Solutions • Examine Software VPNs • Examine Hardware VPNs • Review Differences Between Layer 2 and Layer 3 VPNs • Review Internet Protocol Security (IPSec) • Review Layer 2 Tunneling Protocol (L2TP) • Examine VPN and Virtualization
Course Outcome 13	**Learning Objectives for Course Outcome 13**
Explore Real World VPN Scenarios	• Examine Operating System-Based VPNs • Examine VPN Appliances • Discuss choosing Between IPSec and SSL Remote Access VPNs • Review DMZ, Extranet, and Intranet VPN Solutions

Evaluation Process and Grading System:	

Evaluation Type	Evaluation Weight
Attendance and Assignments	10%
Labs	30%
Quizzes	10%
Tests	50%

Date:	September 19, 2019
Addendum:	Please refer to the course outline addendum on the Learning Management System for further information.