# CLEVELAND INSTITUTE OF ELECTRONICS SYLLABUS

**Course Number**: S370

**Course Name**: Firewalls and VPNs

**Course Clock Hours**: 90

**Course Prerequisites**: S360 Computer Security

**Course Co-requisites**: None

**Course Contact Information**: www.cie-wc.edu faculty@cie-wc.edu
1-800-243-6446 (216) 781-9400 (216) 781-0331 (fax)

**Course Description**: General introduction to firewalls and VPNs along with techniques used to attack hosts and networks, the TCP/IP protocol suite, basic firewall requirements and step-by-step guidelines for installation, designing and implementing a virtual private network, and analyzing log files for network forensics.

**Course Objectives**: Upon completion of this course the student will:

- Define security in basic terms
- Describe the TCP/IP stack
- Explain how MAC address filtering works and where it is useful
- Outline the basic types of hardware and software firewalls
- Recognize the role of IPTABLES and access control lists (ACLs)
- List and describe the basic components of a firewall policy

**Course Readings**: The required readings will be drawn from the textbook Guide to Firewalls and VPNs (ISBN: 978-1-111-13539-3). The authors are Michael E. Whitman, Herbert J. Mattford, and Andrew Green and the publisher is Course Technology / Cengage Learning. The study guide was written by Bruce Coscia. Students should complete the required readings and solve all problems in the exercise sections before continuing to the next topic.

**Student Evaluation and Grading**: There are twelve lessons in this course. The lessons are broken into nine exams and three projects. The nine lessons conclude with an examination; all examinations are open book. The minimum passing score of 70% must be achieved but if the score is less than 70%, the lesson must be retaken to earn a passing score of 70% overall. The twelve scores are averaged together and constitute 100% of the course grade.

| | | | |
|---|---|---|---|
| 93% - 100% | A | The final grade for this course will be determined as follows: | |
| 86% - 92.9% | B | 9 examinations + 3 projects = | 100% |
| 78% - 85.9% | C | | |
| 70% - 77.9% | D | | |

**Course Schedule**: You should complete the following lessons in the order shown in the table. It is best to complete 1-2 lessons per week to maintain your schedule.

| Lesson Number | Title of Lesson | Topics Covered |
|---|---|---|
| 3701C | Introduction to Information Security | • Define the key terms and critical concepts of information and network security<br>• Identify and differentiate the threats posed to information and network security, as well as the common attacks associated with those threats |
| 3702C | Security Policies and Standards | • Explain the three types of information security policy and list the critical components of each<br>• Describe the fundamental elements of key information security management practices |
| 3703C | Authenticating Users | • Explain why authentication is a critical aspect of perimeter defense and the process of firewall authentication<br>• List the advantages and disadvantages of popular centralized authentication systems |
| 3704C | Project 1 | • Case problems from preceding chapters |
| 3705C | Introduction to Firewalls | • Identify common misconceptions about firewalls<br>• Understand what a firewall does and describe the types of protection |
| 3706C | Packet Filtering | • Describe packets and packet filtering and the approaches to packet filtering<br>• Configure specific filtering rules based on business needs |
| 3707C | Firewall Configuration and Administration | • Identify and implement different firewall configuration strategies<br>• Adhere to proven security principles to help the firewall protect network resources<br>• Track firewall log files and follow the basic initial steps in responding to security incidents |
| 3708C | Project 2 | • Case problems from preceding chapters |
| 3709C | Working with Proxy Servers and Application-Level Firewalls | • Describe proxy servers and their function<br>• Discuss critical issues in proxy server configurations<br>• Determine when a proxy server is not the correct choice |
| 3710C | Implementing the Bastion Host | • Describe the general requirements for installing a bastion host<br>• Evaluate different options for positioning the bastion host, both physically and within the network<br>• Establish a baseline performance level and audit procedures |
| 3711C | Encryption – The Foundation for the Virtual Private Network | • Describe the role encryption plays in firewall and VPN architectures<br>• Discuss Internet Protocol Security (IPSec) and identify its protocols and modes |
| 3712C | Setting Up a Virtual Private Network / Project 2 | • Explain the components and essential operations of virtual private networks (VPNs)<br>• Discuss best practices for effective configuration and maintenance of VPNs<br>• Case problems from preceding chapters. |