CIS 343 – Implementing Internet/Intranet Firewalls

Course Description

This course provides students with an in-depth look at firewall technologies and how these technologies are incorporated into the information security policy of an organization. It introduces the student to different varieties of firewall configurations and describes popular firewall tools by CheckPoint, Cisco, and other vendors. It takes the student through the steps involved in installation, configuration, and administration of firewalls on a network system. The course culminates with a project in which the student constructs and implements a sophisticated firewall. Students must come to the course with a basic understanding of the Internet and networking concepts such as TCP/IP, gateways, routers, and Ethernet. This course helps students prepare for CheckPoint’s CCSA Certification.

Instructional Materials


Course Learning Outcomes

1. Describe the types of firewall protection, understand what a firewall does, and understand the limitations of firewalls
2. Describe why a security policy is an important part of a firewall implementation, understand what it takes to build a security policy, and define responses to security violations
3. Establish firewall rules, understand the goals of firewall’s configuration, and identify firewall configuration strategies
4. Describe packets and packet filtering, set up filtering rules, and explain approaches to packet filtering
5. Describe how proxy servers work, understand the uses of reverse proxy, and make decision about proxy server configurations
6. Explain why authentication is a critical part of network security, describe user, client, and session authentication, and understand the use of password security tools
7. Discuss the role encryption plays in a firewall architecture, know how digital certificates work, and understand popular encryption schemes
8. Describe and select the attributes of a bastion host, configure the bastion host, and establish a baseline performance level and audit procedures
9. Describe the different types of VPNs, create VPN setups for mesh or hub-and-spoke configurations, establish best practices for configuring and maintaining VPNs
10. Explain how enterprise firewalls work
11. Explain how to meet the needs for firewalls, use a remote management interface, track log files for security, and adhere to security principals
12. Synthesize current information related to topics in this course using the APA format