Network Defense

Network Defense requires the IoT security technician to be familiar with the common vulnerability exploit database and numbering system (CVE). Network Defense also includes technologies like anti-virus protection, anti-spam, intrusion detection, network admission control and the establishment of user and group policies.
2.2 INFORMATION COMMUNICATION TECHNOLOGIES – NETWORK DEFENSE

Curriculum Resources

Videos
- CCNA Security Introduction
- CCNA Security Lab 4 - Configure an Intrusion Prevention System (IPS)
- CCNA Security Lab 1 - Securing the Router for Administrative Access
- CCNA Security Lab 5 - Securing Layer 2 Switches

Textbooks
- Practical Internet of Things Security
  Chapter 2, 3, 5, 6, 7, 10
- Internet of Things
  Chapter 10, 11, 13
- Raspberry Pi Networking Cookbook
  Chapter 5
- NIST Special Publication 800-82 Revision 2
- Guide to Industrial Control Systems (ICS) Security

Assessment Resources

Labs
- Lab-2.5.1.1 - Securing the Router for Administrative Access
- Lab-3.6.1.1 - Securing Administrative Access Using AAA and RADIUS
- Lab-4.4.1.1 - Configuring Zone Based Policy Firewalls
- Lab-5.5.1.1 - Configuring an Intrusion Prevention System IPS Using the CLI and CCP
- Lab-6.5.1.1 - Securing Layer 2 Switches

Quizzes/Exams
- Cisco CCNA – Chapter Exams
- CSSIA CISSP Course
- Security Operations – Chapter Exam

Quizlet.com
- CCNA Security
- CCNA Security Final
- CCNA Security Vocabulary

Existing Course Cross Reference

Cisco Networking Academy Courses
- Introduction to IoT
- Cisco Cybersecurity Essentials
- CCNA Security

Cisco Partner Courses
- Security+ (CSSIA.ORG)
- Python Programming Security Technicians (CSSIA.ORG)
- IoT and ICS Security Controls (CSSIA.ORG)
- ICS and SCADA Security (CSSIA.ORG)
- CISSP (CSSIA.ORG)