CCNA Security 2.01
Scope and Sequence

Last Updated April 19, 2019

Target Audience

The Cisco CCNA® Security course is designed for Cisco Networking Academy® students seeking career-oriented, entry-level security specialist skills. Target students include individuals enrolled in technology degree programs at institutions of higher education and IT professionals who want to enhance their core routing and switching skills.

CCNA Security provides a next step for CCENT or CCNA Routing and Switching students who want to expand their skill set to prepare for a career in network security.

Note: The course has been updated to include content that covers the Cisco ASA 5500-X with FirePOWER series and provides lab alternatives that use the newer ASA 5506-X devices.

Prerequisites

CCNA Security students should have the following skills and knowledge:

- CCENT-level networking concepts and skills
- Basic PC and Internet navigation skills

Target Certifications

The CCNA Security curriculum prepares students for the Implementing Cisco Network Security (IINS) certification exam (210-260), leading to the CCNA Security certification.

Curriculum Description

CCNA Security equips students with the knowledge and skills needed to prepare for entry-level security specialist careers. This course is a hands-on, career-oriented e-learning solution that emphasizes practical experience. It is a blended curriculum with both online and classroom learning. CCNA Security aims to develop an in-depth understanding of network security principles as well as the tools and configurations required to secure a network.

Various types of hands-on labs provide practical experience, including procedural and troubleshooting labs, skills integration challenges, and model building. All hands-on labs in the course can be completed on actual physical equipment or in conjunction with the NDG NETLAB solution. Most chapters include Packet Tracer-based skills integration challenges that are cumulative throughout the course.

Curriculum Objectives

CCNA Security helps students develop the skills needed for entry-level network security career opportunities and prepare for the CCNA Security certification. It provides a theoretically rich, hands-on introduction to network security, in a logical sequence driven by technologies.

The goals of CCNA Security are as follows:

- Provide an in-depth, theoretical understanding of network security
- Provide students with the knowledge and skills necessary to design and support network security
- Provide an experience-oriented course that employs industry-relevant instructional approaches to prepare students for entry-level jobs in the industry
- Enable students to have significant hands-on interaction with IT equipment to prepare them for certification exams and career opportunities

Upon completion of the CCNA Security course, students will be able to perform the following tasks:

- Explain network threats, mitigation techniques, and the basics of securing a network
- Secure administrative access on Cisco routers
- Secure administrative access with AAA
- Implement firewall technologies to secure the network perimeter
- Configure IPS to mitigate attacks on the network
- Describe LAN security considerations and implement endpoint and Layer 2 security features
- Describe methods for implementing data confidentiality and integrity
- Implement secure virtual private networks
- Implement an ASA firewall configuration using the CLI
- Implement an ASA firewall configuration and VPNs using ASDM
- Test network security and create a technical security policy

Minimum System Requirements

CCNA Security curriculum requirements:

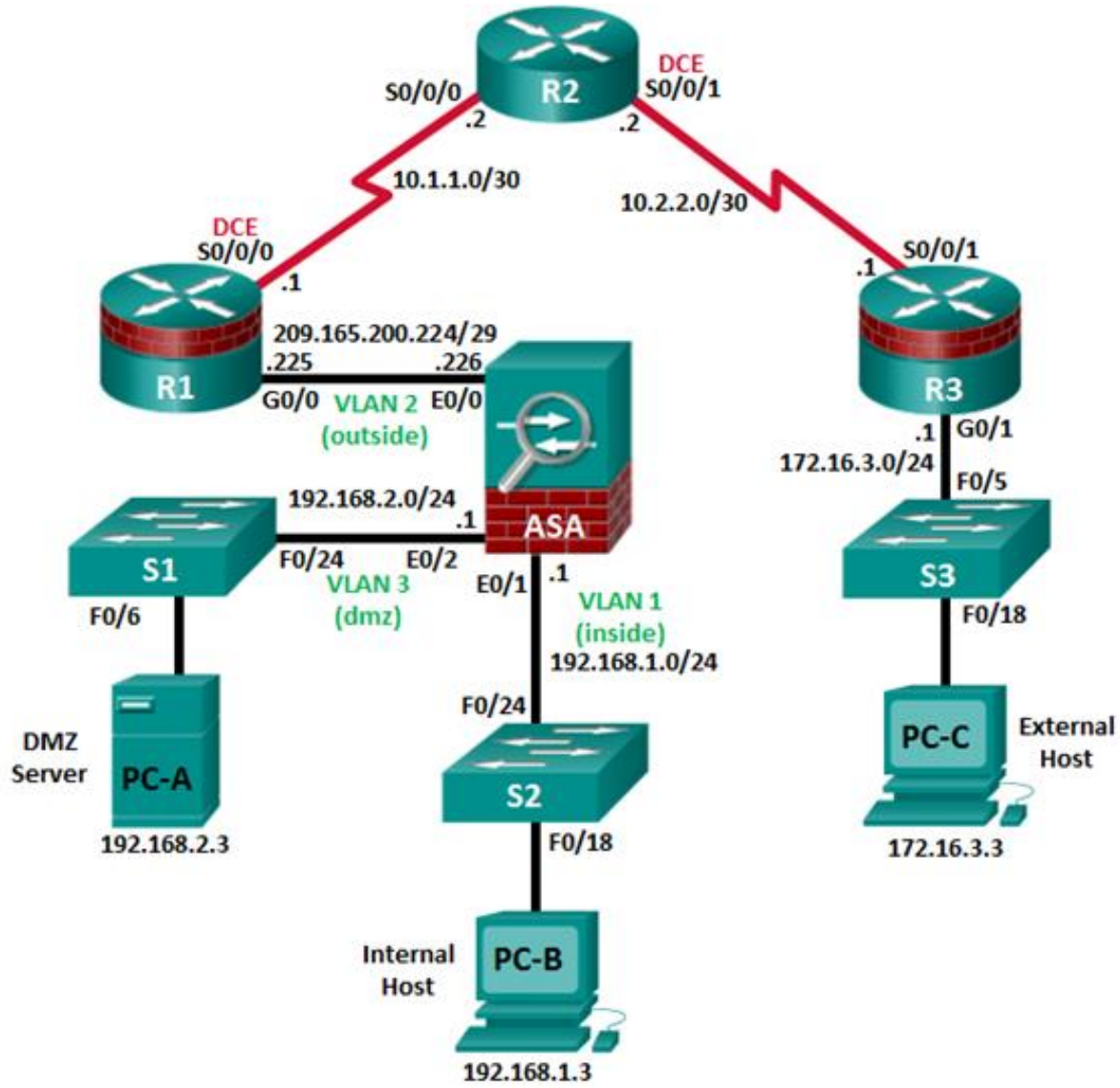
- 1 Student PC per student

Lab bundle requirements for CCNA Security:

Detailed equipment information, including descriptions and part numbers, is available on Cisco Netspace on the Equipment Information page. Please refer to that document for the latest information, which includes specifications for the following minimum equipment required:

- 3 Cisco routers, 2 with the Security Technology Package License
- 3 Two-Port Serial WAN Interface Cards
- 3 Cisco switches
- 1 Cisco Adaptive Security Appliance (ASA)
- Assorted Ethernet and Serial cables and hubs

The equipment should be set up in the following configuration:



CCNA Security Outline

This course teaches students the skills needed to obtain entry-level security specialist jobs. It provides a hands-on introduction to network security. Instructors are encouraged to provide outside-the-classroom learning experiences.

Chapter Outline

Table 1. Chapter Outline

Chapter /Section	Goals/Objectives
Chapter 1. Modern Network Security Threats	**Explain network threats, mitigation techniques, and the basics of securing a network**
1.1 Securing Networks	Explain network security
1.2 Network Threats	Describe various types of threats and attacks
1.3 Mitigating Threats	Explain tools and procedures to mitigate the effects of malware and common network attacks.
Chapter 2. Securing Network Devices	**Secure administrative access on Cisco routers**
2.1 Securing Device Access	Configure secure administrative access
2.2 Assigning Administrative Roles	Configure command authorization using privilege levels and role-based CLI
2.3 Monitoring and Managing Devices	Implement the secure management and monitoring of network devices.
2.4 Using Automated Security Features	Use automated features to enable security on IOS-based routers.
Chapter 3. Authentication, Authorization and Accounting	**Secure administrative access with AAA**
3.1 Purpose of AAA	Explain how AAA is used to secure a network.
3.2 Local AAA Authentication	Implement AAA authentication that validates users against a local database.
3.3 Server-Based AAA	Explain server-based AAA authentication and its communication protocols.
3.4 Server-Based AAA Authentication	Implement server-based AAA authentication using TACACS+ and RADIUS protocols.
3.5 Server-Based AAA Authorization and Accounting	Configure server-based AAA authorization and accounting
Chapter 4. Implementing Firewall Technologies	**Implement firewall technologies to secure the network perimeter**
4.1 Access Control Lists	Implement access control lists (ACLs) to filter traffic and mitigate network attacks on a network.
4.2 Firewall Technologies	Configure a classic firewall to mitigate network attacks.
4.3 Zone-Based Policy Firewalls	Implement Zone-Based Policy Firewall using CLI.
Chapter 5. Implementing Intrusion Prevention	**Configure IPS to mitigate attacks on the network**
5.1 IPS Technologies	Explain how network-based IPS is used to help secure a network.
5.2 IPS Signatures	Explain how signatures are used to detect malicious network traffic.
5.3 Implement IPS	Configure Cisco IOS IPS operations using CLI.

Chapter /Section	Goals/Objectives
Chapter 6. Securing the Local Area Network	**Describe LAN security considerations and implement endpoint and Layer 2 security features**
6.1 Endpoint Security	Explain endpoint vulnerabilities and protection methods.
6.2 Layer 2 Security Considerations	Implement Layer 2 security features.
Chapter 7. Cryptographic Systems	**Describe methods for implementing data confidentiality and integrity**
7.1 Cryptographic Services	Explain how the types of encryption, hashes, and digital signatures work together to provide confidentiality, integrity, and authentication.
7.2 Basic Integrity and Authenticity	Explain how cryptographic hashes are used to ensure data integrity and authentication.
7.3 Confidentiality	Explain how encryption algorithms are used to ensure data confidentiality.
7.4 Public Key Cryptography	Explain how a public key infrastructure is used to ensure data confidentiality and provide authentication.
Chapter 8. Implementing Virtual Private Networks	**Implement secure virtual private networks**
8.1 VPNs	Explain the purpose of VPNs.
8.2 IPsec VPN Components and Operation	Explain how IPsec VPNs operate.
8.3 Implementing Site-to-Site IPsec VPNs with CLI	Configure a site-to-site IPsec VPN, with pre-shared key authentication, using CLI.
Chapter 9. Implementing the Cisco Adaptive Security Appliance	**Implement an ASA firewall configuration using the CLI**
9.1 Introduction to the ASA	Explain how the ASA operates as an advanced stateful firewall.
9.2 ASA Firewall Configuration	Implement an ASA firewall configuration.
Chapter 10. Advanced Cisco Adaptive Security Appliance	**Implement an ASA firewall configuration and VPNs using ASDM**
10.1 ASA Security Device Manager	Implement an ASA firewall configuration.
10.2 ASA VPN Configuration	Configure remote-access VPNs on an ASA.
Chapter 11. Managing a Secure Network	**Test network security and create a technical security policy**
11.1 Network Security Testing	Explain the various techniques and tools used for network security testing.
11.2 Developing a Comprehensive Security Policy	Explain how to develop a comprehensive security policy.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**