Cisco | Networking Academy
Mind Wide Open™

CCNA Security v1.1 Scope and Sequence

Last updated December 21, 2011

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 CCNA Discovery or CCNA Exploration students who want to expand their CCNA-level skill set to prepare for a career in network security.

Prerequisites

CCNA Security has no Networking Academy course prerequisites.

Students should have the following skills and knowledge:

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

While there are no *required* course prerequisites, students are encouraged to complete the CCNA Discovery or CCNA Exploration curricula to acquire the fundamental CCNA-level routing and switching skills needed for success in this course.

Target Certifications

The CCNA Security curriculum prepares students for the Implementing Cisco IOS® Network Security (IINS) certification exam (640-554), 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:

- Describe the security threats facing modern network infrastructures
- Secure network device access
- Implement AAA on network devices
- Mitigate threats to networks using ACLs
- Implement secure network management and reporting
- Mitigate common Layer 2 attacks
- Implement the Cisco IOS firewall feature set
- Implement an ASA
- Implement the Cisco IOS IPS feature set
- Implement site-to-site IPSec VPNs
- Administer effective security policies

Minimum System Requirements

CCNA Security curriculum requirements:

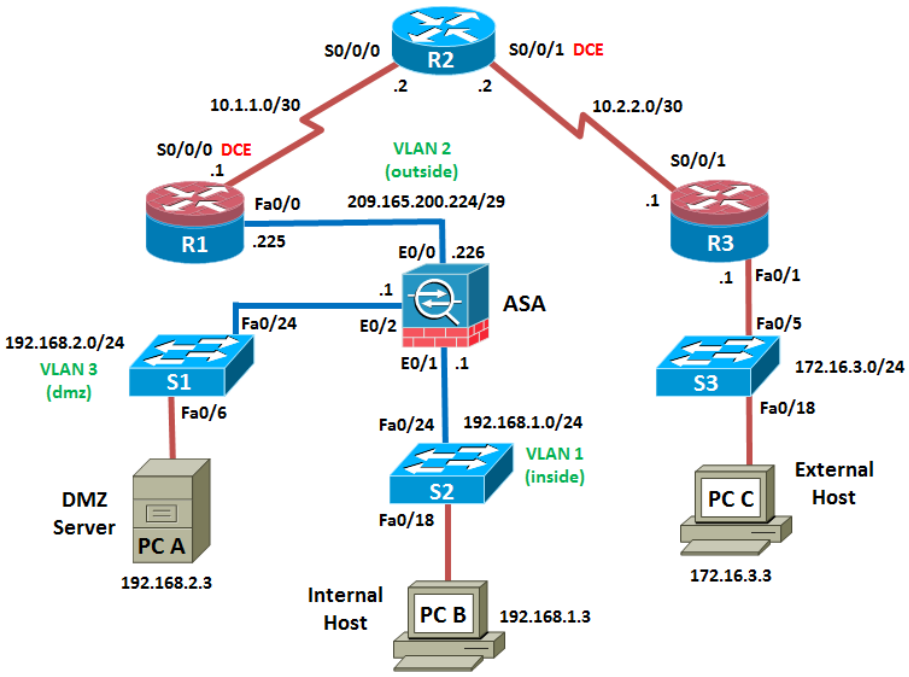
- 1 Student PC per student; 1 local curriculum server

Lab bundle requirements for CCNA Security:

Detailed equipment information, including descriptions and part numbers, is available in the official CCNA Security Equipment List on Academy Connection. 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

Chapter/Section	Goals/Objectives
Chapter 1. Modern Network Security Threats	**Explain network threats, mitigation techniques, and the basics of securing a network**
1.1 Fundamental Principles of a Secure Network	Describe the fundamental principles of securing a network
1.2 Viruses, Worms and Trojan Horses	Describe the characteristics of worms, viruses, and Trojan horses and mitigation methods
1.3 Attack Methodologies	Describe common network attack methodologies and mitigation techniques such as Reconnaissance, Access, Denial of Service, and DDoS
1.4 Cisco Network Foundation Protection Framework	Describe the Cisco Network Foundation Protection framework to include the control, management, and data (forwarding) planes.
Chapter 2. Securing Network Devices	**Secure administrative access on Cisco routers**
2.1 Securing Device Access	Configure secure administrative access on Cisco routers
2.2 Assigning Administrative Roles	Configure command authorization using privilege levels and role-based CLI
2.3 Monitoring and Managing Devices	Enable secure management and monitoring of network devices and router resiliency.
2.4 Using Automated Security Features	Secure IOS-based routers using automated features
Chapter 3. Authentication, Authorization and Accounting	**Secure administrative access with AAA**
3.1 Purpose of AAA	Describe the purpose of AAA and the various implementation techniques
3.2 Local AAA Authentication	Implementing AAA using the local database
3.3 Server-Based AAA	Describe the characteristics and protocols of server-based AAA
3.4 Server-Based AAA Authentication	Implementing server-based AAA authentication using TACACS+ and RADIUS protocols.
3.5 Server-Based AAA Authorization and Accounting	Implementing 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 ACLs
4.2 Firewall Technologies	Describe the purpose and operation of firewall technologies

4.3 Context-Based Access Control	Implement CBAC
4.4 Zone-Based Policy Firewall	Implement Zone-Based Policy Firewall using CLI and CCP
Chapter 5. Implementing Intrusion Prevention	**Configure IPS to mitigate attacks on the network**
5.1 IPS Technologies	Describe the purpose and operation of network-based and host-based Intrusion Prevention Systems
5.2 IPS Signatures	Describe how signatures are used to detect malicious network traffic.
5.3 Implementing IPS	Implement Cisco IOS IPS operations using CLI and CCP
5.4 Verify and Monitor IPS	Verify and monitor the Cisco IOS IPS operations using CLI and CCP.
Chapter 6. Securing the Local Area Network	**Describe LAN security considerations and implement endpoint and Layer 2 security features**
6.1 Endpoint Security	Describe endpoint vulnerabilities and protection methods
6.2 Layer 2 Security Considerations	Describe the vulnerabilities of and mitigation techniques for securing the Layer 2 infrastructure.
6.3 Configuring Layer 2 Security	Configure and verify switch security features, including port security and storm control
6.4 Wireless, VoIP, and SAN Security	Describe the fundamentals of Wireless, VoIP, and SANs, and the associated security considerations.
Chapter 7. Cryptography	**Describe methods for implementing data confidentiality and integrity**
7.1 Cryptographic Services	Describe how different types of encryption, hashes, and digital signatures work together to provide confidentiality, integrity, and authentication
7.2 Basic Integrity and Authenticity	Describe the mechanisms to ensure data integrity and authentication
7.3 Confidentiality	Describe the mechanisms used to ensure data confidentiality
7.4 Public Key Cryptography	Describe the mechanisms used to ensure data confidentiality and authentication using a public key
Chapter 8. Implementing Virtual Private Networks	**Implement secure virtual private networks**
8.1 VPNs	Describe the purpose and operation of VPN types
8.2 GRE VPNs	Describe and configure a GRE VPN
8.3 IPSec VPN Components and Operation	Describe the components and operations of IPSec VPNs
8.4 Implementing Site-to-Site IPSec VPNs with CLI	Configure and verify a site-to-site IPSec VPN, with pre-shared key authentication. using CLI
8.5 Implementing Site-to-Site IPSec VPNs with CCP	Configure and verify a site-to-site IPSec VPN, with pre-shared key authentication, using CCP
8.6 Implementing Remote-Access VPNs	Configure and verify a remote-access VPN

Chapter 9. Managing a Secure Network	**Given the security needs of an enterprise, create and implement a comprehensive security policy**
9.1 Principles of Secure Network Design	Describe the principles of secure network design
9.2 Security Architecture	Describe the components and benefits of the Cisco SecureX Architecture
9.3 Operations Security	Describe the role of operations security in a network
9.4 Network Security Testing	Describe the various techniques and tools used for network security testing
9.5 Business Continuity Planning and Disaster Recovery	Describe the principles of business continuity planning and disaster recovery
9.6 System Development Life Cycle	Describe the SDLC and how to use it to design a Secure Network Life Cycle management process
9.7 Developing a Comprehensive Security Policy	Describe the functions, goals, role, and structure of a comprehensive security policy
Chapter 10. Implementing the Cisco Adaptive Security Appliance (ASA)	**Implement firewall technologies using the ASA to secure the network perimeter**
10.1 Introduction to the ASA	Describe the ASA as an advanced stateful firewall
10.2 ASA Firewall Configuration	Implement an ASA firewall configuration
10.3 ASA VPN Configuration	Implement remote-access VPNs on an ASA