CCNA Security 1.2
Scope and Sequence

Last Updated 25 June 2014

Target Audience

The Cisco CCNA® Security course is designed for Cisco Networking Academy® students seeking career-oriented, entry-level security specialist skills. This includes 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 Cisco CCENT® or CCNA Routing and Switching students who want to expand their skill set to prepare for a career in network security.

Prerequisites

CCNA Security students are expected to 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 IOS® Network Security (IINS) certification exam (640-554), which leads to the CCNA Security certification.

Curriculum Description

CCNA Security helps students prepare for entry-level security specialist careers by developing an in-depth understanding of network security principles and the tools and configurations needed to secure a network. This hands-on course emphasizes practical experience and blends both online and classroom learning.

Students complete hands-on activities ranging from procedural and troubleshooting labs to skills integration challenges and model building. All hands-on labs can be completed on physical equipment or in conjunction with the NDG NETLAB solution. Most chapters also include Cisco Packet Tracer-based skills integration challenges.

Curriculum Objectives

The goals of CCNA Security are as follows:

- Provide an in-depth, theoretical understanding of network security
- Equip students with the knowledge and skills needed to design and support network security
- Provide an experience-oriented course that employs industry-relevant instructional approaches to prepare students for entry-level IT security jobs
- Enable significant hands-on interaction with IT equipment to prepare students 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 Cisco routers

- Implement AAA on Cisco routers using a local router database and external ACS
- Mitigate threats to Cisco routers and networks using ACLs
- Implement secure network design, management, and reporting
- Mitigate common Layer 2 attacks
- Implement the Cisco IOS firewall feature set
- Implement the Cisco IOS IPS feature set
- Implement a site-to-site VPN
- Implement a remote access VPN

Minimum System Requirements

CCNA Security curriculum requirements:

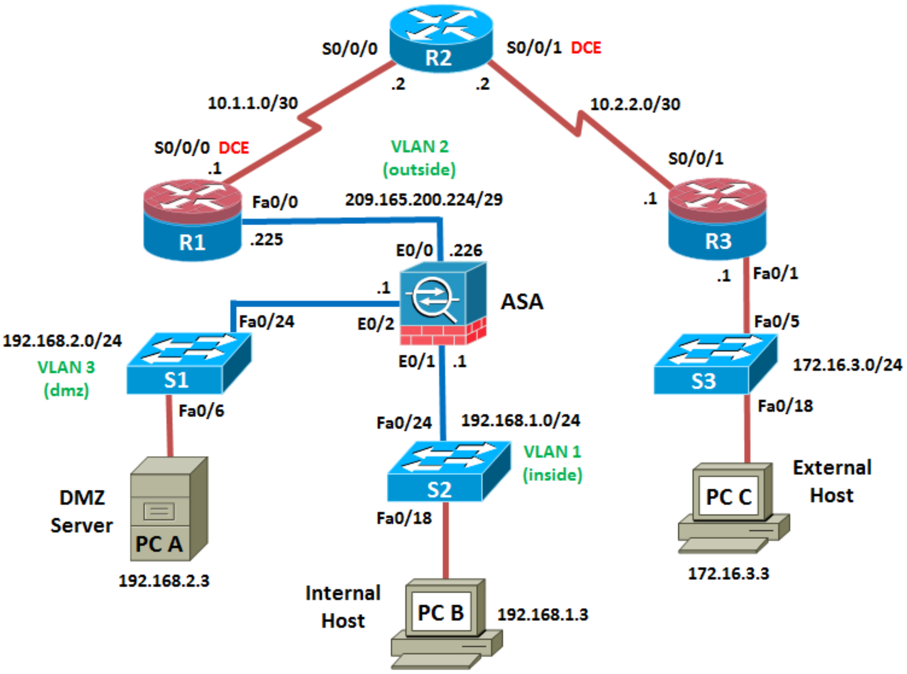
- 1 Student PC per student; 1 local curriculum server

CCNA Security lab bundle requirements:

Detailed equipment information, including descriptions and part numbers, is available in the official CCNA Security Equipment List on the Cisco NetSpace™ learning environment. 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 Chapter Outline

Chapter/Section	Goals/Objectives
Chapter 1. Modern Network Security Threats	**Describe security threats facing modern network infrastructures**
1.1 Fundamental Principles of a Secure Network	Describe the fundamental principles of securing a network
1.2 Viruses, Worms, and Trojan Horses	Describe common network attack methodologies and mitigation techniques such as Reconnaissance, Access, Denial of Service, and DDoS
1.3 Attack Methodologies	Describe the characteristics of Worms, Viruses, and Trojan Horses and mitigation methods
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 basic security for local and remote administrative access
2.2 Assigning Administrative Roles	Configure command authorization using privilege levels and role-based CLI
2.3 Monitoring and Managing Devices	Implement secure management, monitoring, and resiliency of network devices
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 and protocols for implementing AAA
3.2 Local AAA Authentication	Implement AAA on Cisco routers using the local router database
3.3 Server-Based AAA	Implement server-based AAA
3.4 Server-Based AAA Authentication	Implement server-based AAA authentication using TACACS+ and RADIUS protocols
3.5 Server-Based AAA Authorization and Accounting	Implement server-based AAA authorization and accounting
Chapter 4. Implementing Firewall Technologies	**Implement firewall technologies to secure the network perimeter**
4.1 Access Control Lists	Mitigate threats to Cisco routers and networks using ACLs
4.2 Firewall Technologies	Implement classic firewall to mitigate network attacks
4.3 Zone-Based Policy Firewall	Implement Zone-Based Policy Firewall
Chapter 5. Implementing Intrusion Prevention	**Configure IPS to mitigate attacks on the network**
5.1 IPS Technologies	Describe network-based and host-based intrusion detection and prevention
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 protective measures
6.2 Layer 2 Security Considerations	Describe Layer 2 vulnerabilities and implement security measures
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 Wireless, VoIP, and SAN security considerations
Chapter 7. Cryptographic Systems	**Describe methods for protecting data confidentiality and integrity**
7.1 Cryptographic Services	Describe how the types of encryption, hashing, and digital signatures

	provide confidentiality, integrity, authentication, and non-repudiation
7.2 Basic Integrity and Authenticity	Describe the mechanisms used 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 in a public key cryptography
Chapter 8. Implementing Virtual Private Networks	**Implement secure virtual private networks**
8.1 VPNs	Describe the purpose and operation of VPNs
8.2 GRE VPNs	Implement a site-to-site VPN GRE tunnel
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	Use CLI to configure and verify a site-to-site IPSec VPN with pre-shared key authentication
8.5 Implementing Site-to-Site IPSec VPNs with CCP	Use CCP to configure and verify a site-to-site IPSec VPN with pre-shared key authentication
8.6 Implementing Remote-Access VPNs	Configure and verify a remote-access VPN
Chapter 9. Implementing the Cisco Adaptive Security Appliance (ASA)	**Given the security needs of an enterprise, create and implement a comprehensive security policy**
9.1 Introduction to the ASA	Describe the ASA as an advanced stateful firewall
9.2 ASA Firewall Configuration	Implement an ASA Firewall configuration
9.3 ASA VPN Configuration	Configure and verify a remote access VPN on an ASA
Chapter 10. Managing a Secure Network	**Implement firewall technologies using the ASA to secure the network perimeter**
10.1 Principles of Secure Network Design	Describe the principles of secure network design
10.2 Security Architecture	Describe the Cisco SecureX Architecture
10.3 Operations Security	Describe the implementation of a comprehensive security policy
10.4 Network Security Testing	Describe the various techniques and tools used for network security testing
10.5 Business Continuity Planning and Disaster Recovery	Describe the principles of business continuity planning and disaster recovery
10.6 System Development Life Cycle	Describe SDLC and how to use it to design a Secure Network Life Cycle management process
10.7 Developing a Comprehensive Security Policy	Describe the functions, goals, role, and structure of 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.**