Cisco Networking Academy
Mind Wide Open

CCNA Security 2.0 Overview

Sew Hoon Yeo
Product Manager
July 2015

Contents

CCNA Security 2.0 Course Overview

DESCRIPTION
- Understand core security concepts and develop skills in implementing security policies to mitigate risks
- Prepare for the Cisco CCNA Security certification exam

FEATURES
- Eleven modules of interactive instructional content
- Activities, including Packet Tracer activities
- Assessments include a pre-test, module quizzes, practice exams and final exam
- Estimated time to complete: 70 hours / full semester course
- Certificate of Completion and CEO Letter
- Prerequisites: CCENT-level networking knowledge and skills

TARGET AUDIENCE
- Students seeking career-oriented, entry-level security specialist skills
- IT professionals wishing to broaden skills or add specialized technology expertise
- Current Cisco CCENT or CCNA Certification holders who wish to build CCNA knowledge

AVAILABILITY
- Language: English
- Instructor-Led
- Available Sept 2015

CCNA Security Course Goals

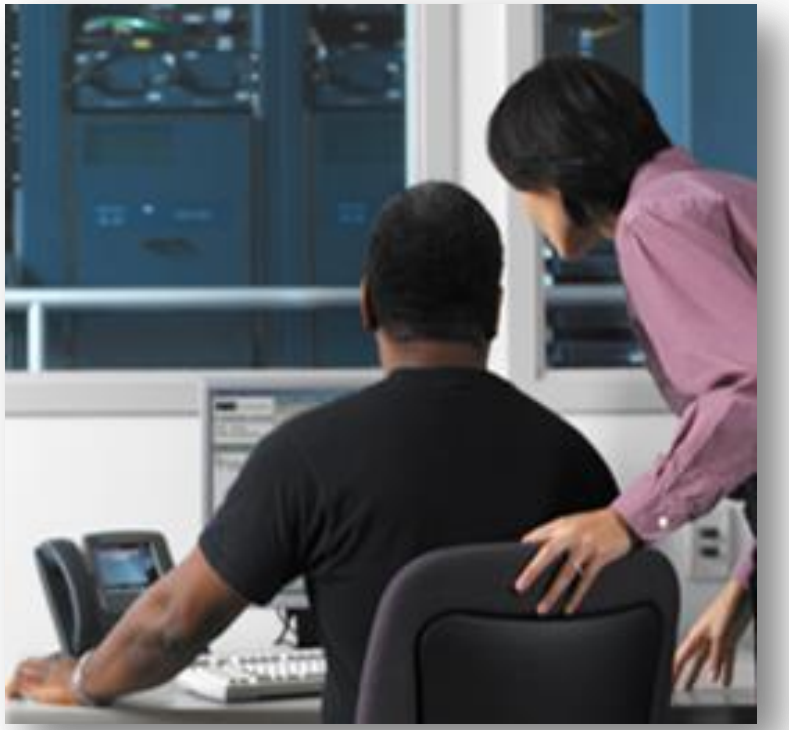
CCNA Security helps students:

- Understand core security concepts and how to develop and implement security policies to mitigate risks
- Acquire skills needed to configure, monitor, and troubleshoot network security
- Prepare for the Cisco CCNA Security certification exam
- Start or advance a career in network security
- Differentiate themselves in the market with specialized skills and expertise to achieve success

CCNA Security 2.0 Key Competencies

Upon completion of this course, students will be able to:

- Describe security threats facing modern network infrastructures
- Secure Cisco routers and switches
- Describe AAA functionalities and implement AAA on Cisco routers using local router database and server-based ACS or ISE
- Mitigate threats to networks using ACLs and stateful firewalls
- Implement IPS and IDS to secure networks against evolving attacks
- Mitigate threats to email, web based and endpoints attacks and common Layer 2 attacks
- Secure communications to ensure integrity, authenticity and confidentiality.
- Describe the purpose of VPNs, and implement Remote Access and Site-to-Site VPNS.
- Secure networks using ASA



New in Version 2.0

- Aligns with updated CCNA Security (IINS) Certification Exams (210-260)
- Focus on router and switch CLI-based configurations
- Updated and expanded content : IPS (next-generation IPS), Firewall (next-generation FW), VPNs, End-point Security, Web Security
- New topics added to align with certification changes:
  - Introductory / No labs :
    - Cisco Identity Service Engine (ISE)
    - 802.1x
    - BYOD and MDM
    - Network Topologies
    - Cisco Cloud Web Security
    - Network Security for a virtual environment
  - ASA configuration using ASDM (Chapter 10)

- Aligns to latest version of Packet Tracer, PT 6.2
- Cisco Configuration Professional content removed.
- Reduced ACL content covered in CCNA R&S ITN and RSE.

CCNA Security
Who Should Enroll?

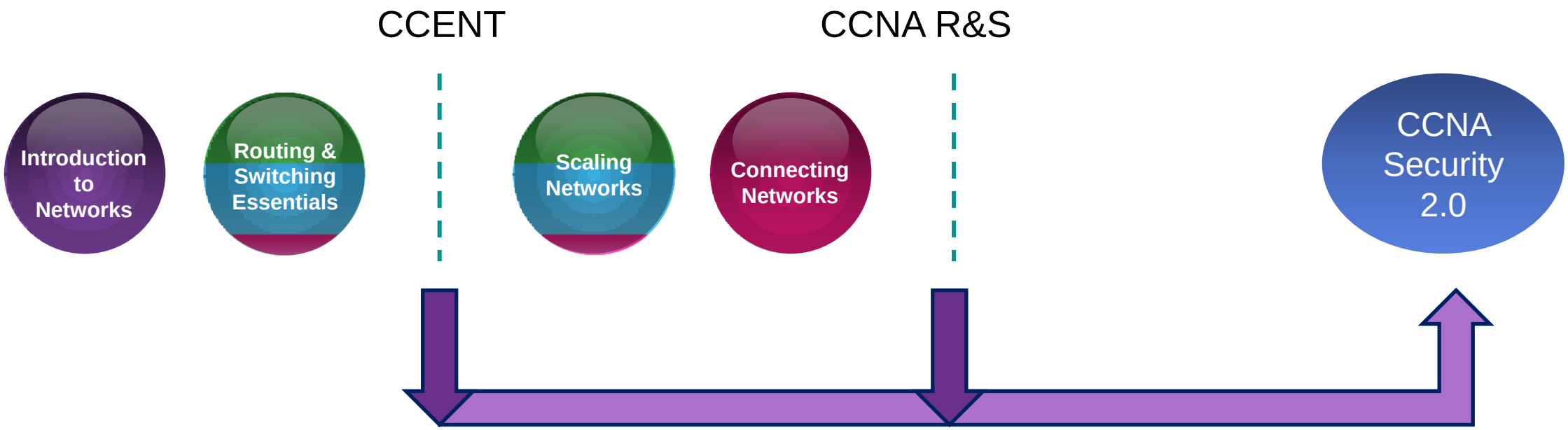
- College and university-level students seeking career-oriented, entry-level security specialist skills
- IT professionals wishing to broaden skills or add specialized technology expertise
- Current CCENT or CCNA Certification holders who wish to build CCNA knowledge
- Prerequisites: CCENT-level networking knowledge and skills

CCNA Security Certification
Meets Growing Demand

- Verifies an individual's skills in the following roles:
  - Network Security Specialist
  - Security Administrator
  - Network Security Support Engineer
- Prerequisite for CCNP Security certification
- Potential employers can be confident that candidates have the skills needed to install, troubleshoot, and monitor Cisco security technologies.
- The U.S. Department of Defense (DoD) has certified that the Cisco CCNA Security certification complies with DoD8570.01-M. The certification also meets the ISO 17024 standard accredited by ANSI. (learn more)

Move from CCENT Courses to CCNA Security 2.0

- Students can complete CCENT courses, then enroll in CCNA Security
- Students can also complete all 4 CCNA R&S courses, then enroll in CCNA Security



CCNA Security Certification Prerequisite is CCENT

- To achieve Cisco CCNA Security certification, a candidate must pass the IINS exam
- As of March 2013, the prerequisite for the CCNA Security certification is a valid CCENT certification

  CCNA Routing and Switching or any CCIE certification can also satisfy the prerequisite
- BENEFIT: candidates can pursue CCNA Security certification by meeting the minimal prerequisite of possessing a CCENT certification (ICND1 exam)

- CCNA Security 2.0 adds some CCNA Routing and Switching topics aligning with the certification changes
- CCNA Security 2.0 fully aligns to the new IINS exam (210-260)

Cisco Security Certifications

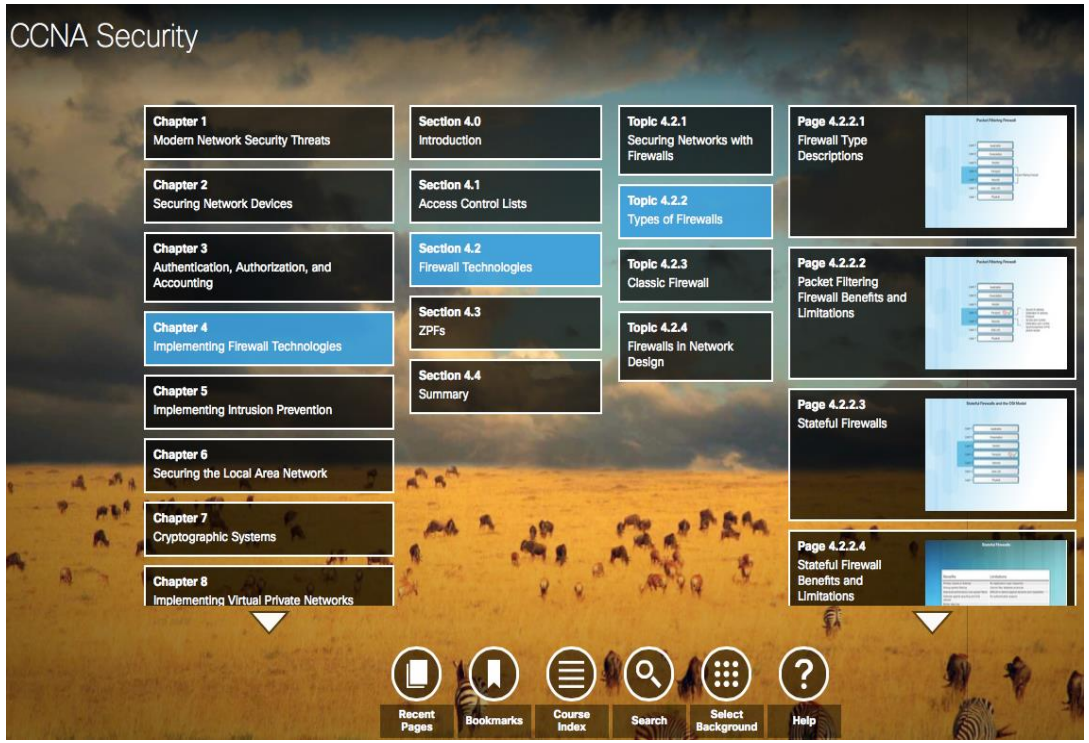
Certification Name	Years of Experience	Job Roles	Number of Exams	Prerequisites
CCNA Security	1-3	• Network Security Specialist • Security Administrator • Network Security Support Engineer	1	• Valid Cisco CCENT, CCNA Routing and Switching, or any CCIE certification
CCNP Security	3 – 5	• Network Security Engineer	4	• Valid CCNA Security or any CCIE Certification
CCIE Security	5-7	• Network Security Engineer	2	• No formal prerequisite

Source : http://www.cisco.com/web/learning/certifications/associate/ccna_security/comparison_chart.html

Course Design

CCNA Security 2.0
Course Design

- Easy-to-navigate graphical user interface
- 11 chapters, modifiable chapter quizzes and chapter exams
- 41 Syntax Checker activities
- 13 Cisco Packet Tracer activities, require PT 6.2.x or above
- 16 hands-on labs
- 1 Packet Tracer Practice skills-based assessment
- 1 pre-test, 1 practice final exam practice certification exam, 1 final exam
- Balance of theory, hands-on practice, and application
- 11 chapters containing accessible text and media text videos with closed captioning.
- Available in English only, no translated versions are planned
- Certificate of Completion



Assessments

- Pre-test
- Chapter quizzes at the end of each chapter
- Chapter exams at the end of each chapter
- Checkpoint (section) quizzes for self-assessment (if appropriate)
- Practice End-Of-Course (EOC) final exam
- EOC final exam
- Certification practice exam
- 1 student SBA and 1 instructor SBA with answer keys
- 1 PTSBA
- Rubrics for self-assessment, project-based activities, and peer review of activities
- EOC assessment to provide evidence of completion and mastery of content
- EOC Survey

CCNA Security 2.0
Equipment Requirements

No Hardware Changes from v1.2

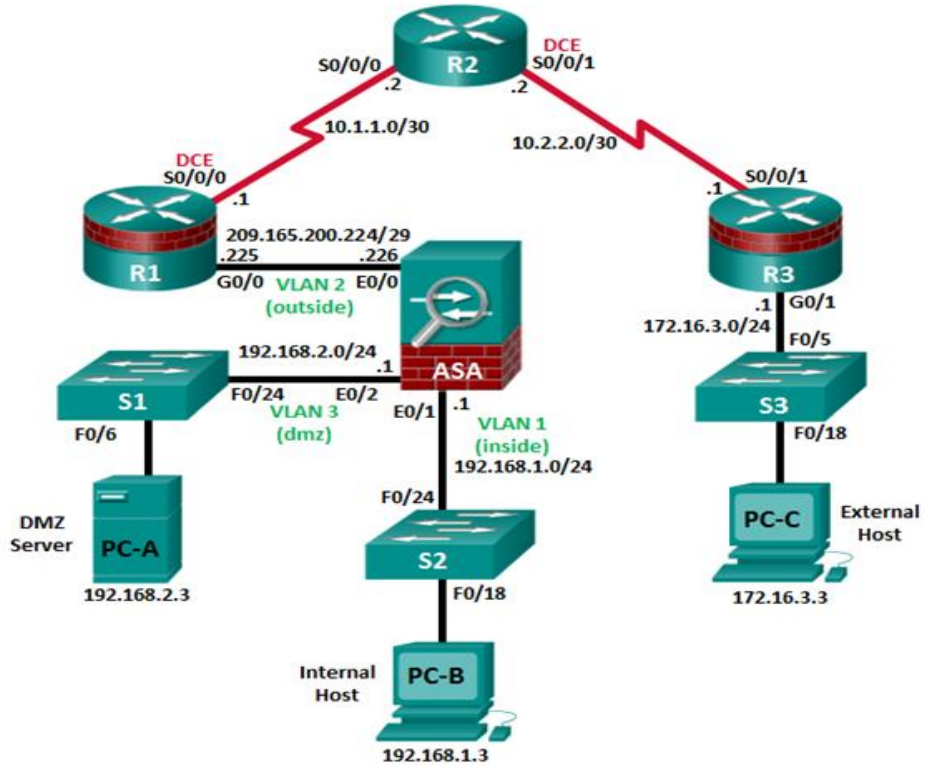
- Leverages CCNA Routing and Switching equipment bundle and topology
- NDG NETLAB+ can be enabled for remote lab equipment operation.
- The required Advanced IP Services feature set (ISR G2) and the Security (SEC) technology package license are available for academies that are part of Networking Academy Maintenance

Minimum Requirements

Curriculum requirements:
1 Student PC per student

Lab bundle requirements :
3 Cisco routers, 2 with the SEC technology package
3 two-port serial WAN interface cards
3 Cisco switches
1 Cisco Adaptive Security Appliance (ASA)
Assorted Ethernet and Serial cables and hubs

Detailed equipment information is available in the Instructor Lab Manual and the CCNA Security Equipment List located in the CCNA Security resources folder .



CCNA Security 2.0 Course Outline

Course Chapters and Goals	
Chapter 1	**Modern Network Security Threats** Goal: Explain security threats in modern network infrastructures and how to mitigate them.
Chapter 2	**Securing Network Devices** Goal: Secure Cisco routers.
Chapter 3	**Authentication, Authorization and Accounting** Goal: Implement AAA on Cisco routers using local router database and server-based ACS or Identity Service Engine (ISE).
Chapter 4	**Implementing Firewall Technologies** Goal: Implement firewall technologies to secure network perimeter.
Chapter 5	**Implementing Intrusion Prevention** Goal: Implement IPS to mitigate attacks on networks.
Chapter 6	**Securing the Local Area Network** Goal: Secure endpoints and mitigate common Layer 2 attacks.
Chapter 7	**Cryptographic Systems** Goal: Secure communications to ensure integrity, authenticity and confidentiality.
Chapter 8	**Implementing Virtual Private Networks** Goal: Implement secure Virtual Private Networks.
Chapter 9	**Implementing the Cisco Adaptive Security Appliance (ASA)** Goal: Implement an ASA firewall configuration using the CLI.
Chapter 10	**Advanced Cisco Adaptive Security Appliance (ASA)** Goal: Implement an ASA firewall configuration and VPNs using ASDM.
Chapter 11	**Managing a Secure Network** Goal: Test network security and create a technical security policy.

End-of-Life for CCNA Security 1.2

Course	Language	Last Class Start Date	Last Class End Date
CCNA Security 1.1	English	July 31, 2015	January 29, 2016

Course	Language	Last Class Start Date	Last Class End Date
CCNA Security 1.2	English	July 29, 2016	January 27, 2017