# Cisco CCNP Security Bootcamp

Length: 14 days
Format: Bootcamp
Time: Day

## About This Course

Cisco Certified Network Professional Security (CCNP Security) Boot Camp program is aligned specifically to the job role of the Cisco Network Security Engineer responsible for Security in Routers, Switches, Networking devices and appliances, as well as choosing, deploying, supporting and troubleshooting Firewalls, VPNS, and IDS/IPS solutions for their networking environments.

## Required Exams

300-208:Implementing Cisco Secure Access Solutions (SISAS)/

300-206:Implementing Cisco Edge Network Security Solutions (SENSS)/

300-207:Implementing Cisco Threat Control Solutions (SITCS)

## Audience Profile

The CCNP Security certification is for IT professionals looking to expand upon and document their existing skills in CISCO technology. This boot camp is intended for students seeking to earn their CCNP Security certification and who need an expert instructor to guide them throughout the training and exam preparation process.

## Course Objectives

Implementing Cisco Secure Access Solutions (SISAS)

Implementing Cisco Secure Access Solutions (SISAS) is part of the curriculum path leading to the Cisco Certified Network Professional Security (CCNP Security) certification. Additionally, it is designed to prepare security engineers with the knowledge and hands-on experience so that they can deploy Cisco's Identity Services Engine and 802.1X secure network access. The goal of the course is to provide students with foundational knowledge and the capabilities to implement and managed network access security by utilizing Cisco ISE appliance product solution.

Upon completing this course, the learner will be able to meet these overall objectives:

* Understand Cisco Identity Services Engine architecture and access control capabilities.
* Understand 802.1X architecture, implementation and operation.
* Understand commonly implemented Extensible Authentication Protocols (EAP).
* Implement Public-Key Infrastructure with ISE.
* Understand the implement Internal and External authentication databases.
* Implement MAC Authentication Bypass.
* Implement identity based authorization policies.
* Understand Cisco TrustSec features.
* Implement Web Authentication and Guest Access.
* Implement ISE Posture service.
* Implement ISE Profiling.
* Understand Bring Your Own Device (BYOD) with ISE.
* Troubleshoot ISE

## Outline

Implementing Cisco Edge Network Security Solutions (SENSS)

Implementing Cisco Edge Network Security Solutions (SENSS) is part of the curriculum path leading to the Cisco Certified Network Professional Security (CCNP Security) certification. Additionally, it is designed to prepare security engineers with the knowledge and hands-on experience to prepare them to configure Cisco perimeter edge security solutions utilizing Cisco Switches, Cisco Routers, and Cisco Adaptive Security Appliance (ASA) Firewalls. The goal of the course is to provide students with foundational knowledge and the capabilities to implement and managed security on Cisco ASA firewalls, Cisco Routers with the firewall feature set, and Cisco Switches.

Course Objectives

* Understanding and implementing Cisco modular Network Security Architectures such as SecureX and TrustSec.
* Deploy Cisco Infrastructure management and control plane security controls.
* Configuring Cisco layer 2 and layer 3 data plane security controls.
* Implement and maintain Cisco ASA Network Address Translations (NAT).
* Implement and maintain Cisco IOS Software Network Address Translations (NAT).
* Designing and deploying Cisco Threat Defense solutions on a Cisco ASA utilizing access policy and application and identity based inspection.
* Implementing Botnet Traffic Filters.
* Deploying Cisco IOS Zone-Based Policy Firewalls (ZBFW).
* Configure and verify Cisco IOS ZBFW Application Inspection Policy.

SIMOS Course Objectives and OutlineImplementing Cisco Secure Mobility Solutions (SIMOS)

Implementing Cisco Secure Mobility Solutions (SIMOS) is part of the curriculum path leading to the Cisco

Certified Network Professional Security (CCNP Security) certification. This course is designed to prepare network security engineers with the knowledge and skills they need to protect data traversing a public or shared infrastructure such as the Internet by implementing and maintaining Cisco VPN solutions.

Course Objectives

Upon completing this course, the learner will be able to meet these overall objectives:

* Describe the various VPN technologies and deployments as well as the cryptographic algorithms and protocols that provide VPN security.
* Implement and maintain Cisco site-to-site VPN solutions.
* Implement and maintain Cisco FlexVPN in point-to-point, hub-and-spoke, and spoke-to-spoke IPsec VPNs.
* Implement and maintain Cisco clientless SSL VPNs.
* Implement and maintain Cisco AnyConnect SSL and IPsec VPNs.
* Implement and maintain endpoint security and dynamic access policies (DAP).

SITCS Course Objectives and OutlineImplementing Cisco Threat Control Solutions (SITCS)

Implementing Cisco Threat Control Solutions (SITCS) is part of the curriculum path leading to the Cisco Certified Network Professional Security (CCNP Security) certification. Additionally, it is designed to prepare security engineers with the knowledge and hands-on experience so that they can deploy Cisco’s Next Generation Firewall (NGFW) as well as Web Security, Email Security and Cloud Web Security. The goal of the course is to provide students with foundational knowledge and the capabilities to implement and managed security on Cisco ASA firewalls utilizing Cisco Next Generation product solution which integrates Cisco Prime Security Manager for managing identity policies.

Course Objectives

Upon completing this course, the learner will be able to meet these overall objectives:

* Understand Cisco ASA Next-Generation Firewall (NGFW)
* Deploy Cisco Web Security appliance to mitigate malware
* Configure Web Security appliance for acceptable use controls
* Configure Cisco Cloud Web Security Connectors
* Describe Cisco Email Security Solution
* Configure Cisco Email Appliance Incoming and Outgoing Policies
* Describe IPS Threat Controls
* Configure and Implement Cisco IPS Sensor into a Network.