CCNP Security Certification (Coming Soon)

Modality: Self-Paced Learning

Duration: No

SUBSCRIPTION: Learn, Master, Master Plus

About this course:

The Cisco Certified Network Professional Security (CCNP Security) certification path shall cover the following courses:

- Implementing Cisco Secure Access Solutions (SISAS)
- Implementing Cisco Edge Network Security Solutions (SENSS)
- Implementing Cisco Secure Mobility Solutions (SIMOS)
- Implementing Cisco Threat Control Solutions (SITCS)

Implementing Cisco Secure Access Solutions (SISAS) provides you with foundational knowledge and the capabilities to implement and manage network access security by using a Cisco Identity Services Engine (ISE) appliance product solution. You gain experience with configuring various advanced Cisco security solutions for mitigating outside threats and securing devices connecting to the network. You shall also be exposed to the necessary knowledge and hands-on experience, so you can deploy Cisco ISE and 802.1X secure network access. This course shall act as the **exam prep** for **300-208 SISAS exam.**

Implementing Cisco Edge Network Security Solutions (SENSS) v1.0 has been designed to provide you with the necessary knowledge and skills needed to implement and manage security on Cisco ASA firewalls, Cisco Routers with the firewall feature set and Cisco Switches. In this course you will gain hands-on experience with configuring various perimeter security solutions to mitigate outside threats and secure network zones. At the end of the course, you should be able to reduce the risk to your IT infrastructures and applications and provide detailed operations support for Cisco Switches, Cisco ASA, and Router security appliance features. This course shall act as the **exam prep** for **300-206 SENSS exam.**

Implementing Cisco Secure Mobility Solutions (SIMOS) course is designed to prepare network security engineers with the knowledge and skills required to protect data traversing a public or shared infrastructure such as the Internet by implementing and maintaining Cisco VPN solutions. In this course you will gain hands-on experience with configuring and troubleshooting remote access and site-to-site VPN solutions, using Cisco ASA adaptive Security Appliances and Cisco IOS routers. This course shall act as the **exam prep** for **300-209 SIMOS exam.**

Implementing Cisco Threat Control Solutions (SITCS) course will teach you how to deploy Cisco's Email Security (ESA); Web Security (CWS, WSA); Advanced Malware Protection (AMP); and Next Generation Intrusion Prevention Systems (NGIPS). You will learn how to implement and manage security threat controls by leveraging the capabilities of Cisco's FirePOWER NGIPS, AMP, WSA, CWS, and ESA products and solutions. The hands-on labs enable to configure advanced Cisco security solutions for mitigating outside threats, and to secure traffic traversing the network and

security systems. This course shall act as the **exam prep** for **300-210 SITCS exam.**

This course supports a certification that is a DoD Approved 8570 Baseline Certification and meets DoD 8140/8570 training requirements.

This Course prepares you for the following exams:

- 300-208 SISAS
- 300-206 SENSS
- 300-209 SIMOS
- 300-210 SITCS

Course Objective:

Upon completing this course, you will be able to:

- Describe ISE architecture and access control capabilities
- Explain the 802.1X architecture, implementation and operation
- Describe the commonly implemented
- Extensible Authentication Protocols (EAP)
- Implement Public-Key Infrastructure with ISE
- Explain the implement Internal and External authentication databases
- Implement MAC Authentication Bypass
- Implement identity based authorization policies
- Describe Cisco TrustSec features
- Implement Web Authentication and Guest Access
- Implement ISE Posture service
- Implement ISE Profiling
- Explain Bring Your Own Device (BYOD) with ISE
- Troubleshoot ISE
- Understand current security threat landscape
- Understand and implement Cisco modular
- Network Security Architectures such as
- SecureX and TrustSec
- Deploy Cisco Infrastructure management and control plane security controls
- Configure Cisco layer 2 and layer 3 data plane security controls
- Implement and maintain Cisco ASA Network
- Address Translations (NAT)
- Design and deploy Cisco Threat Defense solutions on a Cisco ASA utilizing access policy and application and identity based inspection
- Implement Botnet Traffic Filters
- Deploy Cisco IOS Zone-Based Policy
- Firewalls (ZBFW)
- Configure and verify Cisco IOS ZBFW
- Application Inspection Policy
- 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
- Deploy Cisco FlexVPN in point-to-point, huband-spoke and spoke-to-spoke IPsec VPNs
- Implement Cisco clientless SSL VPNs
- Implement and maintain Cisco AnyConnect
- SSL and IPsec VPNs
- Deploy endpoint security and dynamic access policies (DAP)
- 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

Job Roles associated with CCNP Security Certification and their average pay

- Network Engineer **USD 76,034**
- Sr. Network Engineer **USD 98,455**
- Network Security Engineer **USD 88,108**
- Security Engineer **USD 86,097**

Audience:

The primary audience for this course is as follows:

- Network Security Engineers
- Network Engineers
- Network Designers and Administrators
- Network Managers
- System Engineers

Prerequisite:

Cisco recommends that you should have the following knowledge to benefit fully from this courses:

- Implementing Cisco Network Security v3.0 (IINS)
- Cisco Certified Network Associate (CCNA®) certification
- Cisco Certified Network Associate (CCNA®) Security certification
- Knowledge of Microsoft Windows operating system

Any CCIE certification can act as a prerequisite

Course Outline:

Module 1: Threat Mitigation through Identity

- Services
- Identity Services
- 802.1X and EAP
- 802.1X Components

Module 2: ISE Fundamentals

- Cisco ISE
- Technologies
- Operational Components
- Policy Platform
- Deployment Options
- Cisco ISE with PKI
- PKI Enrollment Procedure
- Cisco ISE Authentication
- Authentication Conditions
- Cisco ISE with External Authentication
- ISE Identity Source Sequence

Module 3: Advance Access Control

- Certificate Based User Authentication
- Authorization Policy and Configuration
- Cisco TrustSec
- MAC Security
- MACsec Cryptography

Module 4: Web Authentication and Guest

- Access
- Web Authentication
- WebAuth Process and Scenarios
- Guest Access Services
- Guest Policies

Module 5: Endpoint Access Control

- Enhancements
- Posture Service
- Profiler Policies and Conditions
- BYOD Solution elements

Module 6: Access Control Troubleshooting

- Troubleshooting Procedure
- Tools
- ISE
- 802.1X
- RADIUS Peering
- Authentication Protocol
- WebAuth
- Posture

Labs:

- Bootstrapping Identity System
- Enrolling Cisco ISE in PKI
- Implementing MAB and Internal
- Authentication
- Implementing External Authentication
- Implementing EAP-TLS
- Implementing Authorization
- Implementing Cisco TrustSec and MACsec
- Implementing WebAuth for Employees
- Implementing Guest Service
- Implementing Posture Service
- Implementing Profiler Service
- (Optional) Troubleshooting Prep
- (Optional) Troubleshooting Network Access
- Controls

300-206 SENSS

Module 1: Secure Design Principles

- Network Security Zoning implementation
- Zone interface Points
- Placement of Services
- Cisco Module Network Security Architecture
- and Principles
- Cisco SecureX Architecture and
- Components
- Cisco TrustSec Solution Architecture and
- Components

Module 2: Deploying Network Infrastructure

- Protection
- Cisco Network Infrastructure Architecture

- IOS Control Plane Security Controls
- IOS Management Plane Security Controls
- Configuring Cisco Traffic Telemetry Methods
- ASA Management Plane Security Controls
- Cisco Traffic Telemetry Methods
- Configuration
- Deploying Cisco IOS Layer 2 and Layer 3
- Data Plane Security Controls

Module 3: Deploying NAT on Cisco IOS and

- Cisco ASA
- Network Address Translation (NAT)
- ASA NAT configuration
- IOS Software NAT deployment

Module 4: Deploying Threat Controls on Cisco

- ASA
- Cisco Firewall Threat Controls
- ASA Basic Access Policies
- ASA Application Inspection Policies
- ASA Botnet Traffic Filtering
- ASA Identity Based Firewall

Module 5: Deploying Threat Controls on Cisco

- IOS Software
- IOS Zone-Based Policy Firewall (ZBFW)
- Access Policies
- Zones and Zone Pairs configuration and
- verification
- ZBFW troubleshooting
- IOS Software ZBFW with Application
- Inspection Policies
- Advanced Access Policies
- Application-Layer Access Policies
- Peer-to-Peer Protocols Inspection
- ZBFW URL Filtering Methods

Labs:

- Configure Control and Management Plane
- Security Controls
- Configure Traffic Telemetry Methods

- Configure Layer 2 Data Plane Security
- Controls
- Configure Layer 3 Data Plane Security
- Controls
- Configure Cisco ASA NAT
- Configure Cisco IOS Software NAT
- Configure Basic Cisco ASA Access Policies
- Configure Advanced Cisco ASA Access
- Policies

- Configure Cisco ASA Botnet Traffic Filter
- Configure Cisco ASA Identity Firewall
- Configure Basic Cisco IOS Zone-Based
- Policy Firewall Access Policies
- Configure Advanced Cisco IOS Zone-Based
- Policy Firewall Access Policies

300-209 SIMOS

Module 1: The Role of VPNs in Network Security

- VPN Definition
- Key Threats to WANs and Remote Access
- Cisco Modular Network Architecture and

- VPNs
- VPN Types
- VPN Components
- Secure Communication and Cryptographic Services
- Cryptographic Algorithms
- Cryptography and Confidentiality
- Cryptography and Integrity
- Cryptography and Authentication
- Cryptography and Nonrepudiation
- Keys in Cryptography
- Public Key Infrastructure
- Next-Generation Encryption
- Dependencies in Cryptographic Services
- Cryptographic Controls Guidelines

Module 2: Secure Site-to-Site Connectivity Solutions

- Site-to-Site VPN Topologies and Technologies
- IPsec VPN Overview
- Internet Key Exchange v1 and v2
- Security Payload Encapsulation

- IPsec Virtual Tunnel Interface
- Dynamic Multipoint VPN
- Cisco IOS FlexVPN
- Overview of Point-to-Point IPsec VPNs on the Cisco ASA
- Configuration Tasks for Basic Point-to-Point Tunnels on the Cisco ASA
- Enable IKE on an Interface
- Configure IKE Policy
- Configure PSKs
- Choose Transform Set and VPN Peer
- Choose Traffic for VPN
- Configure Site-to-Site VPN with Connection Profiles Menu
- Verify and Troubleshoot Basic Point-to-Point Tunnels on the Cisco ASA
- Overview of Cisco IOS VTIs
- Configure Static VTI Point-to-Point Tunnels
- Verify Static VTI Point-to-Point Tunnels
- Configure Dynamic VTI Point-to-Point Tunnels
- Verify Dynamic VTI Point-to-Point Tunnels
- Overview of Cisco IOS DMVPN
- DMVPN Solution Components
- GRE
- NHRP
- DMVPN
- Types of Authentication
- Configure DMVPN on Hub
- Configure DMVPN on Spoke
- Configure Routing in DMVPN
- Verify DMVPN

Module 3: Cisco IOS Site-to-Site FlexVPN Solutions

- FlexVPN Overview
- Public Key Infrastructure (PKI)
- Site-to-Site VPN Topologies
- FlexVPN Architecture
- FlexVPN Configuration Overview
- FlexVPN Capabilities
- IKEv2 vs. IKEv1 Overview
- IKEv2 Message Exchange
- IKEv2 DoS Prevention
- IKEv1 and IKEv2 Comparison
- FlexVPN Use Cases
- Point-to-Point FlexVPN
- FlexVPN Configuration Blocks
- IKEv2 Profile
- Smart Defaults
- Manipulating Default Values
- Negotiating IKEv2 Proposals
- Point-to-Point VPN Scenario with IPv4 Static Routes

- Configure and Verify Point-to-Point VPN with IPv4 Static Routes
- Point-to-Point VPN Scenario with OSPFv3
- Configure and Verify Point-to-Point VPN with OSPFv3
- Enroll Devices to ECDSA PKI
- Configure Router for ECDSA
- Configure ASA for ECDSA
- Verify EC Key Pairs and Certificates
- Verify IKEv2 SA
- Verify IPsec SA

- Verify Point-to-Point FlexVPN (just flowchart and important show/debug command output)
- Cisco IOS FlexVPN
- IKEv2 Configuration Payload
- Locally Managed Hub-and-Spoke Scenario
- Configure a Spoke in a Hub-and-Spoke Scenario
- Configure a Hub in a Hub-and-Spoke Scenario
- Configuration Exchange
- Verify and Troubleshoot Hub-and-Spoke FlexVPN
- Spoke-to-Spoke Shortcut Scenario NHRP in FlexVPN
- Configure and Verify a Spoke in a Spoke-to- Spoke Shortcut Scenario
- Configure and Verify a Hub in a Spoke-to- Spoke Shortcut Scenario
- RADIUS-Managed FlexVPN Scenario
- Verify Spoke-to-Spoke Shortcut Switching
- Troubleshoot Spoke-to-Spoke Shortcut
- Switching (just flowchart and important show/debug command output)
- Module 4: SSL VPNs
- Components
- SSL/TLS
- Overview of group policies and connection profiles
- Basic Cisco Clientless SSL VPN
- Solution Components
- Configure ASA gateway
- Configure basic authentication
- Configure access control (including URL entry and bookmarks)
- Verify basic clientless SSL VPN
- Troubleshoot basic clientless SSL VPN
- Deploying Application Access options (plugins, smart tunnels)
- Configure and verify plugins
- Configure and verify smart tunnels
- Troubleshoot plugins and smart tunnel
- Advanced Authentication in Cisco Clientless
- SSL VPN Solution Components
- Configure and verify Certificate based Authentication
- Configure and Verify External Authentication
- roubleshoot Advanced Authentication in Clientless SSL VPN

Module 5: Cisco AnyConnect VPNs

- IP Address assignment
- Split Tunneling
- Basic Cisco AnyConnect SSL VPN
- Solution Components
- SSL VPN Server Authentication
- SSL VPN Clients Authentication
- SSL VPN Clients IP Address Assignment
- SSL VPN Split Tunneling
- Configure ASA for Basic AnyConnect SSL VPN
- Configure Basic Cisco Authentication
- Configure Access Control
- Verify and Troubleshoot Basic Cisco
- AnyConnect SSL VPN
- DTLS Overview
- Parallel DTLS and TLS Tunnels
- Configure DTLS
- Verify DTLS
- Cisco AnyConnect Client Configuration Management
- Cisco AnyConnect Client Operating System Integration Options
- Cisco AnyConnect Start Before Logon
- Cisco AnyConnect Trusted Network Detection
- Configure, Verify and Troubleshoot Cisco
- AnyConnect Start Before Logon
- Cisco AnyConnect Trusted Network Detection
- AnyConnect Support for IPSec/IKEv2
- Configure a Cisco AnyConnect IPsec/IKEv2
- VPNs on a Cisco ASA Adaptive Security Appliance
- Verify and Troubleshoot Cisco AnyConnect
- IPsec/IKEv2 VPNs on Cisco ASA
- Cisco AnyConnect Advanced Authentication Scenarios External Authentication
- Certificate-Based Server Authentication
- Configure and Verify Certificate-Based Client Authentication
- SCEP Proxy
- Connection Flow
- Configuration Procedure
- Local Authorization
- External Authentication and Authorization Scenario
- Configure External Authentication and Authorization
- Troubleshoot Advanced Authentication and Authorization in Cisco AnyConnect VPNs Accounting

Module 6: Endpoint Security and Dynamic

- Access Policies
- Cisco HostScan Overview
- Cisco HostScan Prelogin Assessment
- Install Cisco HostScan
- Configure Prelogin Criteria and Prelogin Policy

- Configure Host Scan Endpoint Assessment
- Configure Host Scan Advanced Endpoint Assessment
- DAP
- Integrate with Host Scan Configure
- Verifying and Troubleshooting

Labs

- Site to Site Secure Connectivity on Cisco
- ASA
- Implement a Cisco IOS static VTI point-topoint tunnel
- Site-to-Site Secure Connectivity Using Cisco IOS FlexVPN
- Hub-to-Spoke Secure Connectivity Using Cisco IOS Flex VPN
- Spoke-to-Spoke Secure Connectivity Using Cisco IOS Flex VPN
- Cisco Clientless SSL VPN on Cisco ASA
- Application Access clientless SSL
- Advanced AAA Clientless SSL
- Implement Basic AnyConnect SSL VPN on Cisco ASA
- Advanced AnyConnect SSL VPN on Cisco ASA
- AnyConnect IPsec/IKEv2 VPNs on Cisco ASA
- Hostscan and DAP for AnyConect SSL VPNs

300-210 SITCS

Module 1: Cisco Web Security Appliance

- Lesson 1: Describing the Cisco Web Security Appliance Solutions
- Lesson 2: Integrating the Cisco Web Security Appliance
- Lesson 3: Configuring Cisco Web Security Appliance Identities and User Authentication Controls
- Lesson 4: Configuring Cisco Web Security Appliance Acceptable Use Controls
- Lesson 5: Configuring Cisco Web Security Appliance Anti-Malware Controls
- Lesson 6: Configuring Cisco Web Security Appliance Decryption
- Lesson 7: Configuring Cisco Web Security Appliance Data Security Controls

Module 2: Cisco Cloud Web Security

- Lesson 1: Describing the Cisco Cloud Web Security Solutions
- Lesson 2: Configuring Cisco Cloud Web Security Connectors
- Lesson 3: Describing the Web Filtering Policy in Cisco ScanCenter

Module 3: Cisco Email Security Appliance

- Lesson 1: Describing the Cisco Email Security Solutions
- Lesson 2: Describing the Cisco Email Security Appliance Basic Setup Components

- Lesson 3: Configuring Cisco Email Security Appliance Basic Incoming and Outgoing Mail Policies

Module 4: Advanced Malware Protection for Endpoints

- Lesson 1: AMP for Endpoints Overview and Architecture
- Lesson 2: Customizing Detection and AMP Policy
- Lesson 3: IOCs and IOC Scanning

- Lesson 4: Deploying AMP Connectors
- Lesson 5: AMP Analysis Tools

Module 5: Cisco FirePOWER Next-Generation IPS

- Lesson 1: Describing the Cisco FireSIGHT System
- Lesson 2: Configuring and Managing Cisco FirePOWER Devices
- Lesson 3: Implementing an Access Control Policy
- Lesson 4: Understanding Discovery Technology
- Lesson 5: Configuring File-Type and Network Malware Detection
- Lesson 6: Managing SSL Traffic with Cisco FireSIGHT
- Lesson 7: Describing IPS Policy and Configuration Concepts
- Lesson 8: Describing the Network Analysis Policy
- Lesson 9: Creating Reports

- Lesson 10: Describing Correlation Rules and Policies
- Lesson 11: Understanding Basic Rule Syntax and Usage

Module 6: Cisco ASA FirePOWER Services Module

- Lesson 1: Installing Cisco ASA 5500-X Series FirePOWER Services (SFR) Module