THINQTANK® LEARNING

CISCO CCNP SECURITY
Cisco Certified Network Professional Security Part 1 (SENSS and SIMOS)

Our Learning Exclusive

- Custom exam prep software and materials
- Exam delivery in classroom with 98% success
- Course specific thinQtank® Learning publications to promote a fun exciting learning
- Extended hours of training including immersive hands-on exercises
- WE DO NOT "TEACH THE TEST" We always deliver valuable hands-on experience
- Receive all reading material and study guides when you register
- All courses taught by CCIE expert instructors

Course Duration

- Seven days of instructor-led training
- 40% Lecture and 60% Hands-On Labs

Prerequisites

- Cisco Certified Network Associate certification
- Cisco Certified Network Associate Security certification
- Knowledge of Microsoft Windows operating systems
- General security architectures knowledge

Target Audience

- Senior Network Design Engineers, Principle System Engineer, Network/Solution Architects
- Security designers, planners and implementers
- Anyone wishing to attain the CCNP Security certification

Exam Information

- 300-206 – Implementing Cisco Edge Network Security Solutions (SENSS)
- 300-209 – Implementing Cisco Secure Mobility Solutions (SIMOS)

Delivery Methods

- Instructor-Led Training
- Immersive Live-Online Training
- On-Site and Custom Delivery

Exclusives for Certification Success

- Class recordings so you can review your course any time
- Practice labs to continue your learning beyond the classroom
- Unlimited retakes of course for 24 months
- An exam voucher so you have everything you need to take the exam
- Digital courseware for 24/7 access to authorized course materials, including changes and updates
- Pre-built vmware deployments of security platforms

Course Overview

thinQtank® Learning is offering an industry unique seven-day training camp in which students can receive the first half of the Cisco CCNP Security certification. As with all of our Cisco Training Experiences – exams are delivered in the classroom.

Cisco Certified Network Professional Security (CCNP Security) certification 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.

Course Objectives

The SENSS portion of the course 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 this portion of our 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. The student will gain hands-on experience with configuring various perimeter security solutions for mitigating outside threats and securing network zones. At the end of the course, students will be able to reduce the risk to their IT infrastructures and applications using Cisco Switches, Cisco ASA, and Router security appliance feature and provide detailed operations support for these products.

The SIMOS portion of the 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. Students of this course 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.

CISCO CCNP SECURITY
Cisco Certified Network Professional Security Part 1 (SENSS and SIMOS)

Course Objectives Cont.

SENSS - Implementing Cisco Edge Network Security Solutions

- 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

SIMOS - Implementing Cisco Secure Mobility Solutions

- 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, hub-and-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)

THINQTANK® LEARNING

CISCO CCNP SECURITY
Cisco Certified Network Professional Security Part 1 (SENSS and SIMOS)

Course Modules (SENSS - Implementing Cisco Edge Network Security Solutions)

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

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

3 Deploying NAT on Cisco IOS and Cisco ASA
- Network Address Translation (NAT)
- ASA NAT configuration
- IOS Software NAT deployment

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

5 Deploying Threat Control on Cisco IOS
- 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

SENSS Course 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

THINQTANK® LEARNING

CISCO CCNP SECURITY
Cisco Certified Network Professional Security Part 1 (SENSS and SIMOS)

Course Modules (SIMOS - Implementing Cisco Secure Mobility Solutions)

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

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
- Point-to-Point IPsec VPNs on the Cisco ASA
- Basic Point-to-Point Tunnels on the Cisco ASA
- Enable IKE on an Interface and Configuring IKE Policy
- Configure PSKs, choosing Transform Set and VPN Peer
- Site-to-Site VPN with Connection Profiles Menu
- Verify/Troubleshoot Point-to-Point Tunnels (Cisco ASA)
- Overview of Cisco IOS VTIs
- Configure/Verify Static VTI Point-to-Point Tunnels
- Configure/Verify Dynamic VTI Point-to-Point Tunnels
- Verify Dynamic VTI Point-to-Point Tunnels
- Overview of Cisco IOS DMVPN
- DMVPN Solution Components
- GRE, NHRP, DMVPN
- Configure DMVPN on Hub, Spoke and Routing

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

3

- 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)

4 SSL VPNs

- Components of SSL/TLS
- Overview of group policies and connection profiles
- Basic Cisco Clientless SSL VPN
- Configure ASA gateway
- Configure basic authentication
- Access control (including URL entry and bookmarks)
- Verify basic clientless SSL VPN
- Troubleshoot basic clientless SSL VPN
- Deploying Application Access (plug-ins, smart tunnels)
- Configure and verify plugins and smart tunnels
- Advanced Authentication in Clientless SSL VPN
- Configure and verify Certificate based Authentication
- Configure and Verify External Authentication
- Troubleshoot Authentication in Clientless SSL VPN

CISCO CCNP SECURITY
Cisco Certified Network Professional Security Part 1 (SENSS and SIMOS)

Course Modules (SIMOS - Implementing Cisco Secure Mobility Solutions) Continued

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 Cisco AnyConnect SSL VPN
- DTLS Overview
- Parallel DTLS and TLS Tunnels
- Configure and Verify DTLS
- Cisco AnyConnect Client Configuration Management
- Cisco AnyConnect Client Operating System Integration Options
- Cisco AnyConnect Trusted Network Detection
- Configure, Verify and Troubleshoot Cisco AnyConnect Start Before Logon
- 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

5 Endpoint Security and Dynamic Access Policies

- Site to Site Secure Connectivity on Cisco ASA
- Implement a Cisco IOS static VTI point-to-point 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

SIMOS Course Labs

- Site to Site Secure Connectivity on Cisco ASA
- Implement a Cisco IOS static VTI point-to-point 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

CISCO CCNP SECURITY
Cisco Certified Network Professional Security Part 1 (SENSS and SIMOS)

thinQtank® Global, Inc. dba thinQtank® Learning P.O. Box 803215, Valencia, CA 91380 USA
Tel 855-TO-THINQ Fax 208-979-0668 www.thinqtanklearning.com