THINQTANK® LEARNING

CISCO CERTIFIED NETWORK PROFESSIONAL SECURITY CORE

Implementing and Operating Cisco Security Core Technologies (SCOR)
Implementing and Configuring Cisco Identity Services Engine (SISE)

Our Learning Exclusive

- Custom exam prep software and materials
- Exam delivery in classroom with 98% success
- Course specific thinQtank® Learning publications to promote 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

- Nine days of instructor-led learning
- Five days SCOR and four days SISE
- 60% lecture, 40% hands-on labs

Prerequisites

- Skills and knowledge equivalent to CCNA
- Familiarity with Ethernet and TCP/IP networking
- Knowledge of the Windows operating system
- Knowledge of IOS networking and concepts
- Basics of networking security concepts
- Foundation-level wireless knowledge and skills
- Familiarity with 802.1X and Cisco ASA

Target Audience

- Security and Network Engineer
- Network Designer
- Network Administrator
- Systems and Consulting Systems Engineer
- Technical Solutions Architect
- Installers and implementers Cisco ISE
- End users installing, configuring, and deploy Cisco ISE

Exam Information

- 350-701 – Implementing and Operating Cisco Security Core Technologies (SCOR)
- 300-715 – Implementing and Configuring Cisco Identity Services Engine (SISE)

Delivery Methods

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

Exclusive Tools and Learning Package

- Comprehensive video training package
- Virtual builds of all labs and hand-on learning objectives so learners can continue their hands on experience after the completion of the course
- Industry unique training course to achieve multiple certifications in one training camp

Course Overview

thinQtank® Learning is offering a unique nine-day training camp comprised of five days of instructor-led learning for Implementing and Operating Cisco Security Core Technologies (SCOR) and Implementing and Configuring Cisco Identity Service Engine (SISE). As with all of our Cisco Training Experiences – exams are delivered in the classroom.

SCOR

This portion of the course prepares students to master the skills and technologies students need to implement core Cisco security solutions to provide advanced threat protection against cybersecurity attacks. Students will learn security for networks, cloud and content, endpoint protection, secure network access, visibility and enforcements. Students will get extensive hands-on experience deploying Cisco Firepower Next-Generation Firewall and Cisco ASA Firewall; configuring access control policies, mail policies, and 802.1X Authentication; and more. Students will get introductory practice on Cisco Stealthwatch Enterprise and Cisco Stealthwatch Cloud threat detection features.

SISE

This portion of the course is an intensive experience with enhanced hands-on labs that cover all facets of Cisco Identity Services Engine (ISE) version 2.4. The training provides students with the knowledge and skills to enforce security compliance for wired and wireless endpoints and enhance infrastructure security using the Cisco ISE.

In this course, students will learn about the Cisco ISE, a next-generation identity and access control policy platform that provides a single policy plane across the entire organization. The ISE combines multiple services including authentication, authorization, and accounting (AAA) using 802.1x, MAB, web authentication, posture, profiling, device on-boarding, guest services, and VPN access into a single context-aware identity-based platform.

THINQTANK® LEARNING

CISCO CERTIFIED NETWORK PROFESSIONAL SECURITY CORE

Implementing and Operating Cisco Security Core Technologies (SCOR)
Implementing and Configuring Cisco Identity Services Engine (SISE)

Course Objectives SCOR

After taking this course, students should be able to:

- Describe information security concepts and strategies within the network
- Describe common TCP/IP, network application, and endpoint attacks
- Describe how various network security technologies work together to guard against attacks
- Implement access control on Cisco ASA appliance and Cisco Firepower Next-Generation Firewall
- Describe and implement basic email content security features and functions provided by Cisco Email Security Appliance
- Describe and implement web content security features and functions provided by Cisco Web Security Appliance
- Describe Cisco Umbrella security capabilities, deployment models, policy management, and Investigate console
- Introduce VPNs and describe cryptography solutions and algorithms
- Describe Cisco secure site-to-site connectivity solutions and explain how to deploy Cisco IOS VTI-based point-to-point IPsec VPNs, and point-to-point IPsec VPN on the Cisco ASA and Cisco FirePower NGFW
- Describe and deploy Cisco secure remote access connectivity solutions and describe how to configure 802.1X and EAP authentication
- Provide basic understanding of endpoint security and describe AMP for Endpoints architecture and basic features
- Examine various defenses on Cisco devices that protect the control and management plane
- Configure and verify Cisco IOS Software Layer 2 and Layer 3 Data Plane Controls
- Describe Cisco Stealthwatch Enterprise and Stealthwatch Cloud solutions
- Describe basics of cloud computing and common cloud attacks and how to secure cloud environment

Course Objectives SISE

After taking this course, students should be able to:

- ISE deployment options including node types, personas, and licensing
- Install certificates into ISE using a Windows 2012 Certificate Authority (CA)
- Configure the Local and Active Directory Based Identity Store and use of Identity Source Sequences
- Configure AAA clients and network device groups
- Implement Policy Sets to streamline Authentication and Authorization in the organization
- Deploy EasyConnect as an alternative to 802.1X port-based authentication
- Implement 802.1X for wired and wireless networks using the AnyConnect 4.x NAM module, the latest dot1x commands on a catalyst switch, and version 8.4 of the vWLC
- Configure policies to allow MAC Authentication Bypass (MAB) of endpoints
- Use central web authentication (CWA) for redirection of legitimate domain users who need to register devices on the network using MAC addresses (device registration)
- Configure hotspot guest access, self-registration guest access, and sponsored guest access
- Configure profiler services in ISE and use newer probes available in IOS switch code 15.x as well as vWLC 8.4 code
- Work with profiling feeds, logical profiles, and building profiling conditions to match network endpoints
- Configure posture assessments using the new Cisco AnyConnect Secure Mobility 4.x posture module
- Configure Cisco ISE as a TACACS+ Server for Device Administration with Command Authorization
- Configure Cisco ISE to integrate with a 5500-X ASA and a Catalyst Switch for TrustSec and implement end-to-end Security Group Tagging (SGT) and Security Group Access Control (SGACL)
- Maintenance, best practices, and logging

THINQTANK® LEARNING

CISCO CERTIFIED NETWORK PROFESSIONAL SECURITY CORE

Implementing and Operating Cisco Security Core Technologies (SCOR)
Implementing and Configuring Cisco Identity Services Engine (SISE)

SCOR Course Modules

1

- Describing Information Security Concepts (Self-Study)
  - Information Security Overview
  - Managing Risk
  - Vulnerability Assessment
  - Understanding CVSS

2

- Describing Common TCP/IP Attacks (Self-Study)
  - Legacy TCP/IP Vulnerabilities
  - IP Vulnerabilities
  - ICMP Vulnerabilities
  - TCP Vulnerabilities
  - UDP Vulnerabilities
  - Attack Surface and Attack Vectors
  - Reconnaissance Attacks
  - Access Attacks
  - Man-In-The-Middle Attacks
  - Denial of Service and Distributed Denial of Service Attacks
  - Reflection and Amplification Attacks
  - Spoofing Attacks
  - DHCP Attacks

3

- Describing Common Network Application Attacks (Self-Study)
  - Password Attacks
  - DNS-Based Attacks
  - DNS Tunneling
  - Web-Based Attacks
  - HTTP 302 Cushioning
  - Command Injections
  - SQL Injections
  - Cross-Site Scripting and Request Forgery
  - Email-Based Attacks

4

- Describing Common Endpoint Attacks (Self-Study)
  - Buffer Overflow
  - Malware
  - Reconnaissance Attack
  - Gaining Access and Control
  - Gaining Access via Social Engineering
  - Gaining Access via Web-Based Attacks
  - Exploit Kits and Rootkits
  - Privilege Escalation
  - Post-Exploitation Phase
  - Angler Exploit Kit

5

- Describing Network Security Technologies
  - Defense-in-Depth Strategy
  - Defending Across the Attack Continuum
  - Network Segmentation and Virtualization Overview
  - Stateful Firewall Overview
  - Security Intelligence Overview
  - Threat Information Standardization
  - Network-Based Malware Protection Overview
  - IPS Overview
  - Next Generation Firewall Overview
  - Email Content Security Overview
  - Web Content Security Overview
  - Threat Analytic Systems Overview
  - DNS Security Overview
  - Authentication, Authorization, and Accounting Overview
  - Identity and Access Management Overview
  - Virtual Private Network Technology Overview
  - Network Security Device Form Factors Overview

6

- Deploying Cisco ASA Firewall
  - Cisco ASA Deployment Types
  - Cisco ASA Interface Security Levels
  - Cisco ASA Objects and Object Groups
  - Network Address Translation
  - Cisco ASA Interface ACLs
  - Cisco ASA Global ACLs
  - Cisco ASA Advanced Access Policies
  - Cisco ASA High Availability Overview

7

- Deploying Cisco Firepower Next-Generation Firewall
  - Cisco Firepower NGFW Deployments
  - Cisco Firepower NGFW Packet Processing and Policies
  - Cisco Firepower NGFW Objects
  - Cisco Firepower NGFW NAT
  - Cisco Firepower NGFW Prefilter Policies
  - Cisco Firepower NGFW Access Control Policies
  - Cisco Firepower NGFW Security Intelligence
  - Cisco Firepower NGFW Discovery Policies
  - Cisco Firepower NGFW IPS Policies
  - Cisco Firepower NGFW Malware and File Policies

8

- Deploying Email Content Security
  - Cisco Email Content Security Overview
  - SMTP Overview
  - Email Pipeline Overview
  - Public and Private Listeners
  - Host Access Table Overview
  - Recipient Access Table Overview
  - Mail Policies Overview
  - Protection Against Spam and Graymail
  - Anti-virus and Anti-malware Protection
  - Outbreak Filters
  - Content Filters
  - Data Loss Prevention
  - Email Encryption

CISCO CERTIFIED NETWORK PROFESSIONAL SECURITY CORE

Implementing and Operating Cisco Security Core Technologies (SCOR)
Implementing and Configuring Cisco Identity Services Engine (SISE)

SCOR Course Modules Continued

9
- Deploying Web Content Security
  - Cisco WSA Overview
  - Deployment Options
  - Network Users Authentication
  - HTTPS Traffic Decryption
  - Access Policies and Identification Profiles
  - Acceptable Use Controls Settings
  - Anti-Malware Protection

10
- Deploying Cisco Umbrella (Self-Study)
  - Cisco Umbrella Architecture
  - Deploying Cisco Umbrella
  - Cisco Umbrella Roaming Client
  - Managing Cisco Umbrella
  - Cisco Umbrella Investigate Overview

11
- Explaining VPN Technologies and Cryptography
  - VPN Definition
  - VPN Types
  - Secure Communication and Cryptographic Services
  - Keys in Cryptography
  - Public Key Infrastructure

12
- Introducing Cisco Secure Site-to-Site VPN Solutions
  - Site-to-Site VPN Topologies
  - IPsec VPN Overview
  - IPsec Static Crypto Maps
  - IPsec Static Virtual Tunnel Interface
  - Dynamic Multipoint VPN
  - Cisco IOS FlexVPN

13
- Deploying Cisco IOS VTI-Based Point-to-Point
  - Cisco IOS VTIs
  - Static VTI Point-to-Point IPsec IKEv2 VPN Configuration

14
- Deploying Point-to-Point IPsec VPNs on the Cisco ASA and Cisco Firepower NGFW
  - Point-to-Point VPNs on the Cisco ASA and Cisco Firepower NGFW
  - Cisco ASA Point-to-Point VPN Configuration
  - Cisco Firepower NGFW Point-to-Point VPN Configuration

15
- Introducing Cisco Secure Remote Access VPN Solutions
  - Remote Access VPN Components
  - Remote Access VPN Technologies
  - SSL Overview

16
- Deploying Remote Access SSL VPNs on the Cisco ASA and Cisco Firepower NGFW
  - Remote Access Configuration Concepts
  - Connection Profiles
  - Group Policies
  - Cisco ASA Remote Access VPN Configuration
  - Cisco Firepower NGFW Remote Access VPN Configuration

17
- Explaining Cisco Secure Network Access Solutions
  - Cisco Secure Network Access
  - Cisco Secure Network Access Components
  - AAA Role in Cisco Secure Network Access Solution
  - Cisco Identity Services Engine
  - Cisco TrustSec

18
- Describing 802.1X Authentication
  - 802.1X and EAP
  - EAP Methods
  - Role of RADIUS in 802.1X Communications
  - RADIUS Change of Authorization

19
- Configuring 802.1X Authentication
  - Cisco Catalyst Switch 802.1X Configuration
  - Cisco WLC 802.1X Configuration
  - Cisco ISE 802.1X Configuration
  - Supplicant 802.1x Configuration
  - Cisco Central Web Authentication

20
- Describing Endpoint Security Technologies (Self-Study)
  - Host-Based Personal Firewall
  - Host-Based Anti-Virus
  - Host-Based Intrusion Prevention System
  - Application Whitelists and Blacklists
  - Host-Based Malware Protection
  - Sandboxing Overview
  - File Integrity Checking

21
- Deploying Cisco AMP for Endpoints*
  - Cisco AMP for Endpoints Architecture
  - Cisco AMP for Endpoints Engines
  - Retrospective Security with Cisco AMP
  - Cisco AMP Device and File Trajectory
  - Managing Cisco AMP for Endpoints

22
- Introducing Network Infrastructure Protection (Self-Study)
  - Identifying Network Device Planes
  - Control Plane Security Controls
  - Management Plane Security Controls
  - Network Telemetry
  - Layer 2 Data Plane Security Controls
  - Layer 3 Data Plane Security Controls

CISCO CERTIFIED NETWORK PROFESSIONAL SECURITY CORE

Implementing and Operating Cisco Security Core Technologies (SCOR)
Implementing and Configuring Cisco Identity Services Engine (SISE)

SCOR Course Modules Continued

23

- Deploying Control Plane Security Controls (Self-Study)
  - Infrastructure ACLs
  - Control Plane Policing
  - Control Plane Protection
  - Routing Protocol Security

24

- Deploying Layer 2 Data Plane Security Controls (Self-Study)
  - Overview of Layer 2 Data Plane Security Controls
  - VLAN-Based Attacks Mitigation
  - STP Attacks Mitigation
  - Port Security
  - Private VLANs
  - DHCP Snooping
  - ARP Inspection
  - Storm Control
  - MACsec Encryption

25

- Deploying Layer 3 Data Plane Security Controls (Self-Study)
  - Infrastructure Antispoofing ACLs
  - Unicast Reverse Path Forwarding
  - IP Source Guard

SCOR Labs and Demonstrations

L

- Configure Network Settings And NAT On Cisco ASA
- Configure Cisco ASA Access Control Policies
- Configure Cisco Firepower NGFW NAT
- Configure Cisco Firepower NGFW Access Control Policy
- Configure Cisco Firepower NGFW Discovery and IPS Policy
- Configure Cisco NGFW Malware and File Policy
- Configure Listener, HAT, and RAT on Cisco ESA
- Configure Mail Policies
- Configure Proxy Services, Authentication, and HTTPS Decryption
- Enforce Acceptable Use Control and Malware Protection
- Examine the Umbrella Dashboard
- Examine Cisco Umbrella Investigate
- Explore DNS Ransomware Protection by Cisco Umbrella
- Configure Static VTI Point-to-Point IPsec IKEv2 Tunnel
- Configure Point-to-Point VPN between the Cisco ASA and Cisco Firepower NGFW
- Configure Remote Access VPN on the Cisco Firepower NGFW
- Explore Cisco AMP for Endpoints
- Perform Endpoint Analysis Using AMP for Endpoints Console
- Explore File Ransomware Protection by Cisco AMP for Endpoints Console
- Explore Cisco Stealthwatch Enterprise v6.9.3
- Explore CTA in Stealthwatch Enterprise v7.0
- Explore the Cisco Cloudlock Dashboard and User Security
- Explore Cisco Cloudlock Application and Data Security
- Explore Cisco Stealthwatch Cloud
- Explore Stealthwatch Cloud Alert Settings, Watchlists, and Sensors

THINQTANK® LEARNING

CISCO CERTIFIED NETWORK PROFESSIONAL SECURITY CORE

Implementing and Operating Cisco Security Core Technologies (SCOR)
Implementing and Configuring Cisco Identity Services Engine (SISE)

SISE Course Topics

1
- Introducing Cisco ISE Architecture and Deployment
  - Cisco ISE Features and Services
  - Cisco ISE Deployment Models

2
- Cisco ISE Policy Enforcement
  - Introducing 802.1X and MAB Access: Wired and Wireless
  - Introducing Cisco ISE Identity Management
  - Configuring Cisco ISE Certificate Services
  - Introducing Cisco ISE Policy Sets
  - Configuring Cisco ISE Authentication and Authorization Policy
  - Implementing Third-Party Network Access Device Support
  - Overview of Cisco TrustSec using Cisco ISE
  - Introducing Cisco ISE EasyConnect

3
- Web Auth and Guest Services
  - Introducing Web Access with Cisco ISE
  - Introducing Cisco ISE Guest Access Components
  - Configuring Guest Access Settings
  - Configuring Portals: Sponsors and Guests

4
- Cisco ISE Profiler
  - Introducing Cisco ISE Profiler
  - Configuring Cisco ISE Profiling

5
- Cisco ISE BYOD
  - Introducing the Cisco ISE BYOD Process
  - Describing BYOD Flow
  - Configuring My Devices Portal Settings
  - Configuring Certificates in BYOD Scenarios

6
- Cisco ISE Endpoint Compliance
  - Introducing Cisco ISE Endpoint Compliance
  - Configuring Client Posture Services and Provisioning in Cisco ISE

7
- Working with Network Access Devices
  - Configuring TACACS+ for Cisco ISE Device Administration

SISE Labs and Demonstrations

L
- ISE Familiarization and Certificate Usage
- Active Directory and Identity Source Sequences
- Policy Sets, Conditions Studio, and Network Devices
- Passive Identity
- 802.1X-Wired Networks - PEAP
- 802.1X-Wired Networks - EAP-FAST
- 802.1X-Wireless Networks
- 802.1X-MAC Authentication Bypass (MAB)
- Centralized Web Authentication (CWA)
- Guest Access and Reports
- Endpoint Profiling and Reports
- BYOD and My Devices Portal
- Posture Compliance and Reports
- Compliance Based VPN Access
- TACACS+ Device Administration
- Additional Guest Scenarios
- Posture Compliance Using the Temporal Agent
- pxGrid Integration with Firepower
- TrustSec Security Group Access
- ISE Distributed Deployment
- pxGrid Integration with Stealthwatch

CISCO CERTIFIED NETWORK PROFESSIONAL SECURITY CORE

Implementing and Operating Cisco Security Core Technologies (SCOR)
Implementing and Configuring Cisco Identity Services Engine (SISE)

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