SCOR + SISE

OUR LEARNING EXCLUSIVE

- Custom exam prep software and materials
- Exam delivery in the classroom, with a **98% success rate**
- Course-specific thinQtank® Learning publications to make the learning fun and engaging
- Extended hours of training, including immersive hands-on exercises
- **We do not teach the test.** We always deliver valuable hands-on experience
- All reading material and study guides sent to you when you register
- Every course taught by CCIE expert instructors

TRAINING CAMP FORMAT

thinQtank® Learning delivers **both courses in a single instructor-led training camp**, with both exams sat in the classroom. Camps are scheduled by cohort rather than to a fixed calendar, and the balance of lecture and hands-on lab work is set to suit the group and the delivery method. Contact us for the schedule covering your dates.

Modules marked **Self-Study** come with the courseware and form part of your exam preparation.

PREREQUISITES

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

TARGET AUDIENCE

- Security and network engineers
- Network designers and network administrators
- Systems engineers and consulting systems engineers
- Technical solutions architects
- Those who install, configure and deploy Cisco ISE

DELIVERY METHODS

- Instructor-led training
- Immersive live-online training
- On-site and custom delivery

COURSE OVERVIEW

thinQtank® Learning offers a training camp combining **Implementing and Operating Cisco Security Core Technologies (SCOR)** and **Implementing and Configuring Cisco Identity Services Engine (SISE)**. As with all our Cisco training experiences, the exams are delivered in the classroom.

SCOR

The course prepares you to master the skills and technologies needed to implement core Cisco security solutions and provide advanced threat protection against cybersecurity attacks. You learn security for networks, cloud and content, endpoint protection and detection, secure network access, visibility and enforcement.

You get extensive hands-on experience deploying **Cisco Secure Firewall ASA** and **Threat Defense**, configuring access control and mail policies and 802.1X authentication, and working with **Umbrella**, **Secure Endpoint** and **Secure Network and Cloud Analytics**.

SISE

The course teaches the deployment, configuration and operation of **Cisco ISE** as the central platform for identity-based access control. It works from core architecture through network access control, identity stores, policy design and day-to-day operations.

You cover authentication and authorization policies, guest onboarding, network device integration, endpoint profiling, posture assessment, **TACACS+** device administration, **TrustSec** segmentation and certificate management — across both wired and wireless environments.

EXAMS — TWO IN ONE CAMP

350-701 SCOR — Implementing and Operating Cisco Security Core Technologies

The CCNP Security **core** exam. This outline follows course version 2.0.

300-715 SISE — Implementing and Configuring Cisco Identity Services Engine

A CCNP Security **concentration** exam, and on its own it earns Cisco Certified Specialist – Security Identity Management Implementation. This outline follows course version 5.0.

Core plus one concentration is the whole of CCNP Security. This camp covers both, so you leave with the professional certification rather than half of it.

EXCLUSIVE TOOLS AND LEARNING PACKAGE

- Comprehensive video training package
- Virtual builds of all labs and hands-on learning objectives, so you can keep practising after the course ends
- An industry-unique training course achieving multiple certifications in one camp

COURSE OBJECTIVES — SCOR

After taking this course you should be able to:

- Describe information security concepts and strategies within the network
- Explain TCP/IP security flaws and how attacks are mounted
- Identify network application-based attacks, and describe endpoint attack techniques
- Explain how network security technologies work together against attacks
- Implement access control on Cisco Secure Firewall ASA
- Deploy Cisco Secure Firewall Threat Defense basic configurations
- Deploy Cisco Secure Firewall Threat Defense IPS, malware and file policies
- Deploy Cisco Secure Email Gateway basic and policy configurations, and implement Cisco Secure Web Appliance content security
- Describe Cisco Umbrella capabilities, deployment models and policy management
- Understand endpoint security technologies, and the Cisco Secure Endpoint architecture
- Describe Cisco Secure Network Access solutions, and configure 802.1X and EAP authentication
- Introduce VPNs, and describe cryptography solutions and algorithms
- Describe Cisco site-to-site connectivity, and deploy IOS VTI-based point-to-point IPsec VPNs
- Configure point-to-point IPsec VPNs on Secure Firewall ASA and Threat Defense
- Describe and deploy Cisco secure remote access connectivity solutions
- Examine network infrastructure protection, and the control and management plane defences
- Configure and verify Cisco IOS Layer 2 and Layer 3 data plane controls
- Describe baseline telemetry, and Cisco Secure Network Analytics deployment
- Describe cloud computing basics, common cloud attacks and cloud environment security
- Describe Cisco Secure Cloud Analytics deployment
- Describe software-defined networking and network programmability basics

COURSE OBJECTIVES — SISE

After taking this course you should be able to:

- Describe the role of Cisco ISE in modern network security, and its main use cases
- Examine node personas, deployment models and the licensing implications of each
- Install Cisco ISE and work through the initial setup
- Evaluate 802.1X principles and the authorization outcomes they produce
- Describe MAC Authentication Bypass and its fallback behaviour
- Configure network access devices and device groups within Cisco ISE
- Discuss identity sources and certificate-based authentication
- Configure Active Directory and LDAP integration, and interpret identity selection logic
- Discuss policy set structure and how policy sets are evaluated
- Build authentication and authorization policies, and interpret how they apply
- Analyse policies using logs and live session data
- Analyse guest access via Cisco web authentication, and configure guest settings and account lifecycle
- Set up guest portals for different flows, and sponsor-driven guest access
- Understand BYOD architecture and policy strategy, configure supplicant delivery and certificate provisioning, and operate post-onboarding workflows
- Explain endpoint profiling and classification logic, analyse data collection methods, and design profiling that scales
- Apply posture services — agent delivery, policies and compliance-based access
- Examine TACACS+ for administrative access, configure device administration, and operate advanced authorization logic
- Compare TrustSec architecture and configure TrustSec segmentation
- Operationalise Cisco ISE through maintenance, monitoring and upgrades

SCOR COURSE MODULES INSTRUCTOR-LED

01 Network Security Technologies
- Defense-in-Depth Strategy
- Defending Across the Attack Continuum
- Network Segmentation and Virtualization Overview
- Stateful Firewall Overview
- Cisco IOS Zone-Based Policy 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

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

03 Cisco Secure Firewall Threat Defense Basics
- Threat Defense Deployments
- Threat Defense Packet Processing and Policies
- Threat Defense Objects
- Threat Defense NAT
- Threat Defense Prefilter Policies
- Threat Defense Access Control Policies
- Threat Defense Security Intelligence
- Threat Defense Discovery Policies

04 Threat Defense IPS, Malware and File Policies
- Cisco Secure Firewall Threat Defense IPS Policies
- Cisco Secure Firewall Threat Defense Malware and File Policies

05 Cisco Secure Email Gateway Basics
- Cisco Secure Email Overview
- SMTP Overview
- Email Pipeline Overview
- Public and Private Listeners
- Host Access Table Overview
- Recipient Access Table Overview

06 Cisco Secure Email Policy Configuration
- Mail Policies Overview
- Protection Against Spam and Graymail
- Anti-virus and Anti-malware Protection
- Outbreak Filters
- Content Filters
- Data Loss Prevention
- Email Encryption

07 Cisco Secure Web Appliance Deployment
- Cisco Secure Web Appliance Overview
- Deployment Options
- Network Users Authentication
- HTTPS Traffic Decryption
- Access Policies and Identification Profiles
- Acceptable Use Controls Settings
- Anti-Malware Protection

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

09 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

10 Cisco IOS VTI-Based Point-to-Point IPsec VPNs
- Cisco IOS VTIs
- Static VTI Point-to-Point IPsec IKEv2 VPN Configuration

11 Point-to-Point IPsec VPNs on Secure Firewall ASA and Threat Defense
- Point-to-Point VPNs on the Cisco Secure Firewall ASA and Threat Defense
- Cisco Secure Firewall ASA Point-to-Point VPN Configuration
- Cisco Secure Firewall Threat Defense Point-to-Point VPN Configuration

12 Cisco Secure Remote Access VPN Solutions
- Remote Access VPN Components
- Remote Access VPN Technologies
- SSL Overview

13 Remote Access SSL VPNs on Secure Firewall ASA and Threat Defense
- Remote Access Configuration Concepts
- Connection Profiles
- Group Policies
- Cisco Secure Firewall ASA Remote Access VPN Configuration
- Cisco Secure Firewall Threat Defense Remote Access VPN Configuration

SCOR COURSE MODULES SELF-STUDY

14 Describing Information Security Concepts SELF-STUDY
- Information Security Overview
- Assets, Vulnerabilities and Countermeasures
- Managing Risk
- Vulnerability Assessment
- Understanding CVSS

15 Describing Common TCP/IP Attacks SELF-STUDY
- Legacy TCP/IP Vulnerabilities
- IP Vulnerabilities
- ICMP 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

16 Describing Common Network Application Attacks SELF-STUDY
- Password Attacks
- DNS Tunneling
- Web-Based Attacks
- HTTP 302 Cushioning
- Command Injections
- SQL Injections
- Cross-Site Scripting and Request Forgery
- Email-Based Attacks

17 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

18 Cisco Umbrella Deployment SELF-STUDY
- Cisco Umbrella Capabilities
- Cisco Umbrella Identities and Policies Overview
- Cisco Umbrella DNS Security
- Cisco Umbrella Investigate Overview
- Cisco Umbrella Secure Web Gateway
- Cisco Umbrella CASB Functionalities

19 Endpoint Security Technologies SELF-STUDY
- Host-Based Personal Firewall
- Host-Based Anti-Virus
- Host-Based Intrusion Prevention System
- Application Allowed Lists and Blocked Lists
- Host-Based Malware Protection
- Sandboxing Overview
- File Integrity Checking

20 Cisco Secure Endpoint SELF-STUDY
- Cisco Secure Endpoint Architecture
- Cisco Secure Endpoint Engines
- Retrospective Security with Cisco Secure Endpoint
- Cisco Secure Endpoint Device and File Trajectory
- Managing Cisco Secure Endpoint

21 Cisco Secure Network Access Solutions SELF-STUDY
- Cisco Secure Network Access
- Cisco Secure Network Access Components
- AAA Role in Cisco Secure Network Access Solution
- Cisco ISE
- Cisco TrustSec

22 Describing 802.1X Authentication SELF-STUDY
- 802.1X and EAP
- EAP Methods
- Role of RADIUS in 802.1X Communications
- RADIUS Change of Authorization

23 Configuring 802.1X Authentication SELF-STUDY
- Cisco Catalyst Switch 802.1X Configuration
- Cisco IBNS 2.0 Configuration on Cisco Catalyst Switch
- Cisco WLC 802.1X Configuration
- Cisco ISE 802.1X Configuration
- Supplicant 802.1X Configuration
- Cisco Central Web Authentication

24 Network Infrastructure Protection SELF-STUDY
- 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

25 Control Plane Security Controls SELF-STUDY
- Infrastructure ACLs
- Control Plane Policing
- Control Plane Protection
- Routing Protocol Security

26 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

SCOR COURSE MODULES SELF-STUDY, CONTINUED

27 Layer 3 Data Plane Security Controls SELF-STUDY
- Infrastructure Antispoofing ACLs
- Unicast Reverse Path Forwarding
- IP Source Guard

28 Management Plane Security Controls SELF-STUDY
- Cisco Secure Management Access
- Simple Network Management Protocol Version 3
- Secure Access to Cisco Devices
- AAA for Management Access

29 Traffic Telemetry Methods SELF-STUDY
- Network Time Protocol
- Device and Network Events Logging and Export
- Network Traffic Monitoring Using NetFlow

30 Cisco Secure Network Analytics Deployment SELF-STUDY
- Cisco Secure Network Analytics Overview
- Required Components
- Flow Stitching and Deduplication
- Optional Components
- Integration with Cisco ISE
- Global Threat Alerts
- Cisco Encrypted Traffic Analytics
- Host Groups
- Security Events and Alarms
- Host, Role and Default Policies

31 Cloud Computing and Cloud Security SELF-STUDY
- Evolution of Cloud Computing
- Cloud Service Models
- Security Responsibilities in the Cloud
- Cloud Deployment Models
- Patch Management in the Cloud
- Security Assessment in the Cloud

32 Cloud Security SELF-STUDY
- Cisco Threat-Centric Approach to Network Security
- Cloud Physical Environment Security
- Application and Workload Security
- Cloud Management and API Security
- Network Functions Virtualization and VNF
- Cisco NFV Examples
- Reporting and Threat Visibility in Cloud
- Cloud Access Security Broker
- Cisco Cloudlock
- OAuth and OAuth Attacks

33 Cisco Secure Cloud Analytics Deployment SELF-STUDY
- Cisco Secure Cloud Analytics for Public Cloud Monitoring
- Cisco Secure Cloud Analytics for Private Network Monitoring
- Cisco Secure Cloud Analytics Operations

34 Software-Defined Networking SELF-STUDY
- Software-Defined Networking Concepts
- Network Programmability and Automation
- Cisco Platforms and APIs
- Basic Python Scripts for Automation

SCOR LABS AND DEMONSTRATIONS

01 Configure Network Settings and NAT on Cisco Secure Firewall ASA
02 Configure Cisco Secure Firewall ASA Access Control Policies
03 Configure Cisco Secure Firewall Threat Defense NAT
04 Configure Cisco Secure Firewall Threat Defense Access Control Policy
05 Configure Cisco Secure Firewall Threat Defense Discovery and IPS Policy
06 Configure Cisco Secure Firewall Threat Defense Malware and File Policy
07 Configure Listener, HAT, and RAT on Cisco Secure Email Gateway
08 Configure Cisco Secure Email Policies
09 Configure Proxy Services, Authentication, and HTTPS Decryption
10 Enforce Acceptable Use Control and Malware Protection
11 Configure Static VTI Point-to-Point IPsec IKEv2 Tunnel
12 Configure Point-to-Point VPN between Cisco Secure Firewall Threat Defense Devices
13 Configure Remote Access VPN on Cisco Secure Firewall Threat Defense
14 Examine Cisco Umbrella Dashboard and DNS Security
15 Explore Cisco Umbrella Secure Web Gateway and Cloud-Delivered Firewall
16 Explore Cisco Umbrella CASB Functionalities
17 Explore Cisco Secure Endpoint
18 Perform Endpoint Analysis Using Cisco Secure Endpoint Console
19 Explore File Ransomware Protection by Cisco Secure Endpoint Console
20 Explore Cisco Secure Network Analytics
21 Explore Global Threat Alerts Integration and ETA Cryptographic Audit
22 Explore Cloud Analytics Dashboard and Operations
23 Explore Secure Cloud Private and Public Cloud Monitoring

SISE COURSE MODULES

01 Cisco ISE Evolution, Foundation, and Role
02 Architecture and Design
03 Cisco ISE Installation and Initial Configuration
04 802.1X in Cisco ISE
05 MAB in Cisco ISE
06 Network Device Integration with Cisco ISE
07 Identity Sources and Authentication Types
08 Active Directory and LDAP Integration
09 Identity Selection and Resolution Logic
10 Cisco ISE Policy Framework
11 Authentication Policies
12 Authorization Policies
13 Troubleshoot Policies and Sessions
14 Guest Access Overview
15 Guest Access Policies and Settings
16 Guest Portals and Lifecycle Operations
17 Sponsor Portals
18 BYOD Architecture and Use Cases
19 BYOD Onboarding with Native Supplicant Provisioning
20 BYOD Lifecycle Operations
21 Profiling Architecture and Capabilities
22 Probes and Data Collection
23 Profile Policies and Authorization
24 Profile Monitoring and Design
25 Posture Service Flow and Agents
26 Posture Updates and Client Provisioning
27 Posture Policies and Compliance-Based Access
28 Posture Testing and Monitoring
29 AAA and TACACS+
30 TACACS+ Device Administration
31 TACACS+ Command Authorization
32 Cisco TrustSec Overview
33 Cisco TrustSec in Cisco ISE
34 Cisco ISE Administration

SISE LABS AND DEMONSTRATIONS

01 Explore Initial Cisco ISE Configuration, GUI, and System Certificate
02 Configure Network Device Groups and Network Devices
03 Integrate Cisco ISE with Active Directory
04 Configure MAB
05 Configure Wired 802.1X
06 Configure Wireless 802.1X, Optional Wired EAP-TLS, and TEAP
07 Troubleshoot Cisco ISE 802.1X Configuration Errors
08 Configure Hotspot Guest Access
09 Configure Sponsored Guest Access
10 Configure BYOD
11 Manage BYOD Devices
12 Configure Profiling
13 Configure Authorization Policy Rules and Run Profiler Reports
14 Configure Posture Preparations and Client Provisioning
15 Configure Posturing and Reporting
16 Configure TACACS+ Basic Device Administration
17 Configure TACACS+ Command Authorization
18 Configure Cisco TrustSec
19 Configure Secure Syslog with TLS v1.3 and Install Cisco ISE Patch