Implementing Cisco Secure Access Solutions (CS-SISAS) 1.0

Modality: Virtual Classroom

Duration: 2 Days

CLC: 25 Units

About this course:

The course educates the learners on the process of implementing the fundamental authentication and then facilitating the system with the authorization, guest services, Cisco TrustSec, posture, and profiling parts. The basic topics cover the authentication procedures including 802.1X, MAC Authentication Bypass (MAB), and Web authentication (WebAuth).

Students incorporate the different kinds of Extensible Authentication Protocol (EAP) through two different 802.1X supplicants, i.e., the native Windows OS supplicant and the Cisco AnyConnect supplicant. The Cisco AnyConnect supplicant is utilized for a wide array of situations like EAP chaining.

Even though the Web Authentication and guest services are frequently utilized together, the user first incorporates the WebAuth trait for employee access and then proceed to regulate the guest feature for permitting the guest access. The ISE's posture service is acquired to discover the status of security posture of the endpoints.

The learner will employ the default posture elements pre-installed in the ISE, additionally, incorporate a custom remediation for automatically installing the antivirus software. The ISE provides many kinds of profiling capabilities. Learners will inquire the default operability with the help of functioning common probes, and stretch the profiling granularity after explaining the custom policies.

The course will conclude after completing a troubleshooting lesson and an optional troubleshooting lab activity. Furthermore, the course will also make the student prepare for the Cisco: 300-208 SISAS exam.

This course is also a component of the below stated Boot Camps:

- CS-CCNP-Sec - 14-Day Official CCNP Security + CCNA Security Dual-Certification Boot Camp.

A professional Cisco Network Architect earns an average salary of **$137,000** per year.

Course Objectives:

- How to deploy Cisco ISE
- How to use 802.1X and MAB
- How to deploy Security Group Access and MAC Security

- How to incorporate WebAuth and guest service
- How to deploy posture
- Understand how to implement profiling

Audience:

- Network security engineers

Prerequisites:

- Acquaintance with fundamental Cisco access control solutions and 802.1X
- Understanding of general networking principles similar to those used at the CCNA level
- Familiarity with essential network security concepts similar to those used at the CCNA Security level

Recommended Prerequisite Course:

- Cisco 640-554 CCNA Security - Implementing Cisco IOS Network Security - IINS
- CS-CCNA-Sec CCNA Security Boot Camp: Implementing Cisco IOS Network Security (IINS) (CS-CCNA-Sec)

Course Outline:

Lesson 1: Threat Mitigation Through Identity Services

- Topic 1A: Identity Services
- Topic 1B: 802.1X and EAP
- Topic 1C: Identity System Quick Start

Lesson 2: Cisco ISE Fundamentals

- Topic 2A: Cisco ISE Overview
- Topic 2B: Cisco ISE PKIPKI
- Topic 2C: Cisco ISE Authentication
- Topic 2D: Cisco ISE External Authentication

Lesson 3: Advanced Access Control

- Topic 3A: Certificate-Based User Authentication
- Topic 3B: Authorization
- Topic 3C: Cisco TrustSec and MACsec

Lesson 4: Web Authentication and Guest Access

- Topic 4A: Deploying WebAuth
- Topic 4B: Deploying Guest Service

Lesson 5: Endpoint Access Control Enhancements

- Topic 5A: Deploying Posture Service
- Topic 5B: Deploying Profiler Service
- Topic 5C: Implementing BYOD

Lesson 6: Access Control Troubleshooting

- Topic 6A: Troubleshooting Network Access Controls

Hands On Labs

- Lab 1: Bootstrap Identity System
- Lab 2: Enroll Cisco ISE in PKI
- Lab 3: Implement MAB and Internal Authentication
- Lab 4: Implement External Authentication
- Lab 5: Implement EAP-TLS
- Lab 6: Implement Authorization
- Lab 7: Implement Central WebAuth and Guest Services
- Lab 8: Implement Posture Service
- Lab 9: Implement the Profile Service
- Lab 10: Troubleshooting Network Access Control