IMPLEMENTING CISCO SECURE ACCESS SOLUTIONS (CI-SISAS)

Temario

The Implementing Cisco Security Access Solutions (SISAS) course describes an access control solution that centers on the Cisco Identity Services Engine (ISE). The learners build the solution by implementing basic authentication and then extending the system with the authorization, guest services, Cisco TrustSec, posture, and profiling components. The most fundamental concepts include the authentication methods, such as 802.1X, MAC Authentication Bypass (MAB), and Web authentication (WebAuth). The learners implement various types of the Extensible Authentication Protocol (EAP) using two different 802.1X supplicants: the native Windows OS supplicant and the Cisco AnyConnect supplicant. The Cisco AnyConnect supplicant is used for a range of scenarios, including EAP chaining. Although the Web Authentication and the guest services are often deployed together, the learners first implement the WebAuth feature for employee access and then enable the guest feature to allow guest access. The posture service on the ISE is used to determine the security posture status of the endpoints. The learners use the built-in posture elements pre-configured in the ISE, and also implement a custom remediation to automatically install antivirus software. The ISE offers a wide range of profiling capabilities. The learners test the default functionality with the common probes enabled, and extend the profiling granularity by defining custom policies. The course ends with a troubleshooting lesson and an optional troubleshooting lab exercise.

Pre-requisitos

This subtopic lists the skills and knowledge that learners must possess to benefit fully from the course. The subtopic also includes recommended Cisco learning offerings that learners should first complete to benefit fully from this course.

- Familiarity with basic Cisco access control solutions and 802.1X
- Familiarity with general networking principles equivalent to the CCNA level
- Familiarity with basic network security concepts equivalent to the CCNA Security level

Dirigido a

This course is aimed at engineers looking to deploy or support a Cisco's Identity Services Engine solution and individuals looking to achieve the Cisco Certified Network Professional Certification for Security.

Objetivos del curso

Upon completing this course, you will be able to meet these objectives:

- Deploy Cisco ISE
- Implement 802.1X and MAB
- Deploy Security Group Access and MAC Security
- Implement WebAuth and guest service
- Deploy posture
- Implement profiling
- Understand Cisco Identity Services Engine architecture and access control capabilities
- Understand 802.1X architecture, implementation and operation

- Understand commonly implemented Extensible Authentication Protocols (EAP)
- Implement Public-Key Infrastructure with ISE
- Understand the implement Internal and External authentication databases
- Implement MAC Authentication Bypass
- Implement identity based authorization policies
- Understand Cisco TrustSec features
- Implement Web Authentication and Guest Access
- Implement ISE Posture service
- Implement ISE Profiling
- Understand Bring Your Own Device (BYOD) with ISE
- Troubleshoot ISE
-

Contenido

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