FIREFLY

CONTACT US

Implementing Cisco Secure Access Solutions

DURATION: 5 DAYS COURSE CODE: SISAS FORMAT: LECTURE/LAB

COURSE DESCRIPTION

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.

WHO SHOULD ATTEND

Network Security Engineers

PREREQUISITES

The knowledge and skills that a learner must have before attending this course are as follows:

- CCNA Security or valid CCSP or any CCIE certification can act as a prerequisite

LEARNING OBJECTIVES

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

COURSE OUTLINE

1. Threat Mitigation Through Identity Services
    - Identity Services
    - 802.1X and EAP
    - Identity System Quick Start
    - Module Summary
    - Module Self-Check
2. Cisco ISE Fundamentals
    - Cisco ISE Overview
    - Cisco ISE PKI
    - Cisco ISE Authentication
    - Cisco ISE External Authentication
    - Module Summary
    - Module Self-Check
3. Advanced Access Control
    - Certificate-Based User Authentication
    - Authorization
    - Cisco TrustSec and MACsec
    - Module Summary
    - Module Self-Check
4. Web Authentication and Guest Access
    - Deploying WebAuth
    - Deploying Guest Service
    - Module Summary
    - Module Self-Check
5. Endpoint Access Control Enhancements
    - Deploying Posture Service
    - Deploying Profiler Service
    - Implementing BYOD
    - Module Summary
    - Module Self-Check
6. Access Control Troubleshooting
    - Troubleshooting Network Access Controls
    - Module Summary
    - Module Self-Check

DISCOVERY LABS

1: Bootstrap Identity System
2: Enroll Cisco ISE in PKI
3: Implement MAB and Internal Authentication
4: Implement External Authentication
5: Implement EAP-TLS
6: Implement Authorization
7: Implement Cisco TrustSec and MACsec
8: Implement WebAuth for Employees
9: Implement Guest Service
10: Implement Posture Service
11: Implement Profiler Service
12: (Optional) Troubleshooting Prep
13: (Optional) Troubleshoot Network Access Controls