SENSS 1.0 - Implementing Cisco Edge Network Security Solutions 1.0

(5 Days)

Course Overview

Implementing Cisco Edge Network Security Solutions (SENSS) v1.0 is a newly created five-day instructor-led training (vILT) course is part of the curriculum path leading to the Cisco Certified Network Professional Security (CCNP© Security) certification. Additionally, it is designed to prepare security engineers with the knowledge and hands-on experience to prepare them to configure Cisco perimeter edge security solutions utilizing Cisco Switches, Cisco Routers, and Cisco Adaptive Security Appliance (ASA) Firewalls.

The goal of the course is to provide students with foundational knowledge and the capabilities to implement and managed security on Cisco ASA firewalls, Cisco Routers with the firewall feature set, and Cisco Switches.

The student will gain hands-on experience with configuring various perimeter security solutions for mitigating outside threats and securing network zones. At the end of the course, students will be able to reduce the risk to their IT infrastructures and applications using Cisco Switches, Cisco ASA, and Router security appliance feature and provide detailed operations support for these products.

Target Audience

The primary audience for this course is Network Security Engineers

Prerequisites

To fully benefit from this course, students should have the following prerequisite skills and knowledge:

- Cisco Certified Network Associate certification
- Cisco Certified Network Associate Security certification
- Knowledge of Microsoft Windows operating system

Course Objectives

After completing this course the students should be able to:

- Understand current security threat landscape
- Understanding and implementing Cisco modular Network Security Architectures such as
- SecureX and TrustSec
- Deploy Cisco Infrastructure management and control plane security controls
- Configuring Cisco layer 2 and layer 3 data plane security controls
- Implement and maintain Cisco ASA Network Address Translations (NAT)
- Implement and maintain Cisco IOS Software Network Address Translations (NAT)
- Designing and deploying Cisco Threat Defense solutions on a Cisco ASA utilizing access
- policy and application and identity based inspection
- Implementing Botnet Traffic Filters
- Deploying Cisco IOS Zone-Based Policy Firewalls (ZBFW)
- Configure and verify Cisco IOS ZBFW Application Inspection Policy

Course Outline

Module 1: Cisco Secure Design Principles

- Lesson 1: Network Security Zoning
- Lesson 2: Cisco Module Network Architecture
- Lesson 3: Cisco SecureX Architecture
- Lesson 4: Cisco TrustSec Solutions

Module 2: Implement Network Infrastructure Protection

- Lesson 1: Introducing Cisco Network Infrastructure Architecture
- Lesson 2: Deploying Cisco IOS Control Plane Security Controls
- Lesson 3: Deploying Cisco IOS Management Plane Security Controls
- Lesson 4: Deploying Cisco ASA Management Plane Security Controls
- Lesson 5: Deploying Cisco Traffic Telemetry Methods
- Lesson 6: Deploying Cisco IOS Layer 2 Data Plane Security Controls
- Lesson 7: Deploying Cisco IOS Layer 3 Data Plane Security Controls

Module 3: Deploying NAT on Cisco IOS and Cisco Adaptive Security Appliance (ASA)

- Lesson 1: Introducing Network Address Translation
- Lesson 2: Deploying Cisco ASA Network Address Translation
- Lesson 3: Deploying Cisco IOS Software Network Address Translation

Module 4: Deploying Threat Controls on Cisco ASA

- Lesson 1: Introducing Cisco Threat Controls
- Lesson 2: Deploying Cisco ASA Basic Access Controls
- Lesson 3: Deploying Cisco ASA Application Inspection Policies
- Lesson 4: Deploying Cisco ASA Botnet Traffic Filtering
- Lesson 5: Deploying Cisco ASA Identity Based Firewall

Module 5: Deploying Threat Controls on Cisco IOS Software

- Lesson 1: Deploying Cisco IOS Software with Basic Zone-Based Firewall Policies
- Lesson 2: Deploying Cisco IOS Software Zone-Based Firewall with Application Inspection Policies

Labs:

- Lab 2-1: Configuring Cisco Control and Management Plane Security
- Lab 2-2: Configuring Traffic Telemetry Methods
- Lab 2-3: Configuring Layer 2 Data Plane Security Controls
- Lab 2-4: Configuring Layer 3 Data Plane Security Controls
- Lab 3-1: Configure Cisco ASA Network Address Translation
- Lab 3-2: Configure Cisco IOS Software for Network Address Translation
- Lab 4-1: Configuring Cisco ASA Access Control Features
- Lab 4-2: Configuring Cisco Application Inspection Policy
- Lab 4-3: Configuring Cisco Botnet Traffic Filtering
- Lab 4-4: Configuring Cisco Identity Based Firewall
- Lab 5-1: Configuring Cisco IOS Software with Basic Zone-Based Firewall
- Lab 5-2: Configuring Cisco IOS Software with Basic Zone-Based Firewall