SENSS 1.0 – Implementing Cisco Edge Network Security Solutions 1.0

Overview

Course Code		SENSS 1.0	Duration	5.0 days

Implementing Cisco Edge Network Security Solutions (SENSS) v1.0 is a newly created five-day instructor-led training course that 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.

Audience

Channel Partner / Reseller

Customer

Employee

Pre-Requisites

CCNA Security or valid CCSP.

or any CCIE certification can act as a prerequisite

Key Topics

Course Introduction

Cisco Secure Design Principles

Deploying Cisco Network Infrastructure Protection Solutions

Deploying NAT on Cisco IOS and Cisco Adaptive Security Appliance (ASA) Firewalls

Deploying Threat Controls on Cisco ASA Firewalls

Deploying Threat Controls on Cisco IOS Software

Lab Guide

Objectives

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.