Implementing Cisco Edge Network Security Solutions (SENSS) 1.0 (CS-SENSS-5DAYS)

Modality: Virtual Classroom

Duration: 5 Days

CLC: 38 Units

About this course:

This is a Five-day course. The course will be delivered by an instructor in the form of lectures. Implementing Cisco Edge Network Security Solutions (SENSS) v1.0 is a recently made course which provides the certification of Cisco Certified Network Professional Security (CCNP Security) towards the end of it. The course has a proper curriculum which needs to be completed in order to gain the certification. This training course has been devised and designed for those security engineers who have to configure Cisco perimeter edge security solutions through the usage of Cisco Switches, Cisco Routers, and Cisco Adaptive Security Appliance (ASA) Firewalls. This course is highly suitable for the security engineers to gain the certification because it provides in-depth knowledge and extensive hands-on experience. In this course, students will be taught the foundational techniques with the help of which they will be able to grow and incorporate and regulate the security on Cisco ASA firewalls, Cisco Routers with the firewall feature set, and Cisco Switches. The learners will get the opportunity of gaining hands-on experience in setting up different parameter security solutions for dealing with external threats and protecting network sectors. Towards the end of this course, students will get to train in reducing the risk to their IT infrastructures and applications using Cisco Switches, Cisco ASA, and Router security appliance feature, and subsequently provide in-depth operations support to these products.

On average, a Network Security engineer earns $115,334 per annum.

Learning Objectives:

The course has the following learning objectives:

- Gaining comprehension and practically incorporate Cisco modular Network Security Architectures like SecureX and TrustSec
- Installing the Cisco Infrastructure regulation and control plane security controls
- Setting up the Cisco layer 2 and layer 3 data plane security controls
- Incorporating and regulating Cisco ASA Network Address Translations (NAT)
- Incorporating and regulating Cisco IOS Software Network Address Translations (NAT)
- Designing and installing the Cisco Threat Defense solutions on a Cisco ASA utilizing access policy and application and identity based inspection
- Incorporating Botnet Traffic Filters in the system
- Installing Cisco IOS Zone-Based Policy Firewalls (ZBFW) in the system
- Setting up and validate Cisco IOS ZBFW Application Inspection Policy

Audience:

This course has been designed for channel partners/resellers, customers and employees.

Requirements:

The course requires you to have CCNA Security or valid CCSP prior to the start of the course. Else, any CCIE certification will also work.

Course Outline:

- **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**