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

Modality: Virtual Classroom

Duration: 3 Days

CLC: 28 Units

About this course:

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.

This brand-new instructor led course is a five-day training circling around Implementing Cisco Edge Network Security Solutions Senses V1.0, and it is the section of the curriculum which will lead you to the Cisco Certified Network Professional Security Certifications (CCNP Security). The aim of this course is to provide the students with fundamental knowledge and skills to apply and manage security on Cisco Routers, Cisco Switches, and Cisco Adaptive Security Appliance Firewalls. As students of this course you will be gaining practical experience in setting up several perimeter security solutions to handle external threats as you secure the network zones simultaneously. By the end of the course you will able to successfully reduce the risks posed on their applications and IT infrastructure with the use of Router, Cisco ASA,a nd Cisco Switches security appliance feature and also provide comprehensive functions support for such products.
This course is often taught as part of the 14-Day Official CCNP Security + CCNA Security Dual-Certification Boot Camp. This course also prepares the studens for Cisco: 300-206 SENSS exam.

This course is a part of the 14-Day Offcial CCNP Security + CCNA Security Dual Certification Boot Camp. It will also prepare the students for the Cisco: 300 -206 SENSS exam

This course is part of the following Boot Camps:

- CS-CCNP-Sec - 14-Day Official CCNP Security + CCNA Security Dual-Certification Boot Camp.

The average salary for Cisco Systems Network Security Engineer is **$91,175** per year.

On average a Cisco Systems Network Security Engineer receives $91,175 every year.

Course Objectives:

- Understanding and implementing Cisco modular Network Security Architectures such as SecureX and TrustSec.
- Comprehending and performing the Cisco modular Network Security Architectures such as SecureX and Trustsec
- Deploy Cisco Infrastructure management and control plane security controls.
- Supervise the plane security controls and utilize the Cisco Infrastructure Management
- Configuring Cisco layer 2 and layer 3 data plane security controls.
- Setting up Cisco layer 2 and layer data planesecurity control
- Implement and maintain Cisco ASA Network Address Translations (NAT).
- Enforce and conserve Cisco ASA Network Address Translations (NAT)
- Implement and maintain Cisco IOS Software Network Address Translations (NAT).
- Executing and maintaining the 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.
- Developing and positioning the Cisco Threat Defense solutions on an application and identity-based inspection and Cisco ASA utilizing access policy
- Implementing Botnet Traffic Filters.
- Deploying Cisco IOS Zone-Based Policy Firewalls (ZBFW).
- Configure and verify Cisco IOS ZBFW Application Inspection Policy.

Audience:

- Network security engineers

Prerequisites:

- Cisco Certified Network Associate (CCNA®) certification

- Cisco Certified Network Associate (CCNA®) Security certification
- Knowledge of Microsoft Windows operating system

Suggested prerequisite courses:

- CS-CCNA Cisco Certified Network Associate (CCNA) Routing and Switching Training Boot Camp v3.0 (CS-CCNA)
- CS-CCNA-Wireless Cisco Certified Network Associate (CCNA) Wireless Training Boot Camp (CS-CCNA-Wireless)

Course Outline:

- **Lesson 1: Cisco Secure Design Principles**
- **Lesson 2: Deploying Network Infrastructure Protection**
- **Lesson 3: Deploying NAT on Cisco IOS and Cisco ASA**
- **Lesson 4: Deploying Threat Controls on Cisco ASA**
- **Lesson 5: Deploying Threat Controls on Cisco IOS Software**

Labs

- Lab 1: Configuring Configure Cisco Policy Protection (CPP) and Management Plane Protection (MPP)
- Lab 2: Configure Traffic Telemetry Methods
- Lab 3: Configure Layer 2 Data Plan Security
- Lab 4: Configure Layer 2 Data Plan Security
- Lab 5: Configure NAT on Cisco Adaptive Security Appliance (ASA) Firewall
- Lab 6: Configure NAT on Cisco IOS Software
- Lab 7: Configure Cisco ASA Access Policy
- Lab 8: Configure Cisco ASA Application Inspection Policy
- Lab 9: Configure Cisco ASA Botnet Traffic Filter
- Lab 10: Configure Cisco ASA Identity Based Firewall
- Lab 11: Configure Cisco IOS Software Zone-Based Firewall (ZBFW)
- Lab 12: Configure Cisco IOS Software ZBFW Application Inspection Policy Lab Activity Solutions

Return to Top