Implementing Cisco Edge Network Security Solutions (SENSS)

**ID** CI-SENSS  **Price** US$ 3,995  **Duration** 5 days

**Who should attend**

The primary audience for this course is as follows:

- Network Security Engineers

**Prerequisites**

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

**Course Objectives**

By the end of this course, you will be able to:

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

**Course Content**

Implementing Cisco Edge Network Security Solutions (SENSS) v1.0 is a comprehensive course that is part of the recommended curriculum for the Cisco Certified Network Professional Security (CCNP® Security) certification. Additionally, it will prepare you with the knowledge and hands-on experience to configure Cisco perimeter edge security solutions utilizing Cisco switches, Cisco routers and Cisco Adaptive Security Appliance (ASA) firewalls.

You will gain the foundational knowledge and the capabilities to implement and manage security on Cisco ASA firewalls, Cisco routers with the firewall feature set, and Cisco switches. You 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, you will be able to reduce the risk to your IT infrastructure and applications.

**Detailed Course Outline**
Module 1: Secure Design Principles

- Network Security Zoning implementation
- Zone interface Points
- Placement of Services
- Cisco Module Network Security Architecture and Principles
- Cisco SecureX Architecture and Components
- Cisco TrustSec Solution Architecture and Components
- Cisco Firewall Threat Controls
- ASA Basic Access Policies
- ASA Application Inspection Policies
- ASA Botnet Traffic Filtering
- ASA Identity Based Firewall

Module 2: Deploying Network Infrastructure Protection

- Cisco Network Infrastructure Architecture
- IOS Control Plane Security Controls
- IOS Management Plane Security Controls
- Configuring Cisco Traffic Telemetry Methods
- ASA Management Plane Security Controls
- Cisco Traffic Telemetry Methods Configuration
- Deploying Cisco IOS Layer 2 and Layer 3 Data Plane Security Controls
- IOS Zone-Based Policy Firewall (ZBFW) Access Policies
- Zones and Zone Pairs configuration and verification
- ZBFW troubleshooting
- IOS Software ZBFW with Application Inspection Policies
- Advanced Access Policies
- Application-Layer Access Policies
- Peer-to-Peer Protocols Inspection
- ZBFW URL Filtering Methods

Labs:

- Configure Control and Management Plane Security Controls
- Configure Traffic Telemetry Methods
- Configure Layer 2 Data Plane Security Controls
- Configure Layer 3 Data Plane Security Controls
- Configure Cisco ASA NAT
- Configure Cisco IOS Software NAT
- Configure Basic Cisco ASA Access Policies
- Configure Advanced Cisco ASA Access Policies

Module 3: Deploying NAT on Cisco IOS and Cisco ASA

- Network Address Translation (NAT)
- ASA NAT configuration
- IOS Software NAT deployment

Module 4: Deploying Threat Controls on Cisco ASA

- IOS Zone-Based Policy Firewall (ZBFW) Access Policies
- Zones and Zone Pairs configuration and verification
- ZBFW troubleshooting
- IOS Software ZBFW with Application Inspection Policies
- Advanced Access Policies
- Application-Layer Access Policies
- Peer-to-Peer Protocols Inspection
- ZBFW URL Filtering Methods

Labs:

- Configure Control and Management Plane Security Controls
- Configure Traffic Telemetry Methods
- Configure Layer 2 Data Plane Security Controls
- Configure Layer 3 Data Plane Security Controls
- Configure Cisco ASA NAT
- Configure Cisco IOS Software NAT
- Configure Basic Cisco ASA Access Policies
- Configure Advanced Cisco ASA Access Policies
• Configure Cisco ASA Botnet Traffic Filter
• Configure Cisco ASA Identity Firewall
• Configure Basic Cisco IOS Zone-Based Policy Firewall Access Policies
• Configure Advanced Cisco IOS Zone-Based Policy Firewall Access Policies