FIREFLY

CONTACT US

Implementing Cisco Edge Network Security Solutions

DURATION: 5 DAYS COURSE CODE: SENSS FORMAT: LECTURE/LAB

COURSE DESCRIPTION

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.

WHO SHOULD ATTEND

Network Security Engineers

PREREQUISITES

This sections lists the skills and knowledge that learners must possess to benefit fully from the course. It includes recommended Cisco learning offerings that the learner may complete to benefit fully from this course:

CCNA Security or valid CCSP or any CCIE certification can act as a prerequisite.

LEARNING OBJECTIVES

Understand Cisco modular Network Security Architectures such as SecureX and TrustSec

Implement data, control and management plane security controls

Configure, verify, and troubleshoot NAT features on Cisco ASA and on Cisco IOS Software routers

Configure, verify, and troubleshoot threat controls on Cisco ASA

Configure, verify, and troubleshoot threat controls on Cisco IOS Software routers

COURSE OUTLINE

1. Secure Design Principles
   - Network Security Zoning
   - Cisco Modular Network Architecture
   - Cisco SecureX Architecture
   - Cisco TrustSec Solution
2. Network Infrastructure Protection Deployment
   - Introducing Cisco Network Infrastructure Protection
   - Deploying Cisco IOS Control Plane Security Controls
   - Deploying Cisco IOS Management Plane Security Controls
   - Deploying Cisco ASA Management Plane Security Controls
   - Deploying Cisco Traffic Telemetry Methods
   - Deploying Cisco IOS Layer 2 Data Plane Security Controls
   - Deploying Cisco Layer 3 Data Plane Security Controls
3. NAT Deployment on Cisco IOS Software and Cisco ASA
   - Introducing Network Address Translation
   - Deploying Cisco ASA Network Address Translation
   - Deploying Cisco IOS Software Network Address Translation
4. Threat Controls Deployment on Cisco ASA
   - Introducing Cisco Firewall Threat Controls
   - Deploying Basic Cisco ASA Access Policies
   - Deploying Advanced Cisco ASA Access Policies
   - Deploying Reputation-Based Cisco ASA Access Policies
   - Deploying Identity-Based Cisco ASA Access Policies
5. Threat Controls Deployment on Cisco IOS Software
   - Deploying Basic Cisco IOS Zone-Based Policy Firewall Access Policies
   - Deploying Advanced Cisco IOS Zone-Based Policy Firewall Access Policies

DISCOVERY LABS

1: Configure Control and Management Plane Security Controls
2: Configure Traffic Telemetry Methods
3: Configure Layer 2 Data Plane Security Controls
4: Configure Layer 3 Data Plane Security Controls
5: Configure Cisco ASA NAT
6: Configure Cisco IOS Software NAT
7: Configure Basic Cisco ASA Access Policies
8: Configure Advanced Cisco ASA Access Policies
9: Configure Cisco ASA Botnet Traffic Filter
10: Configure Cisco ASA Identity Firewall
11: Configure Basic Cisco IOS Zone-Based Policy Firewall Access Policies
12: Configure Advanced Cisco IOS Zone-Based Policy Firewall Access Policies