REAL WORLD
TECHNOLOGY TRAINING & SOLUTIONS
"Training You Can Really Use"

Implementing Cisco® Edge Network Security Solutions (SENSS) v1.0

Duration: 5 Days

Method: Instructor-Led Training (ILT) | Live Online Training

Course Description

This course provides participants with the foundational knowledge and the capabilities to implement and manage security on Cisco Adaptive Security Appliance (ASA) firewalls, Cisco Routers with the firewall feature set, and Cisco Switches. Participants 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, they 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.

Target Audience

This course is intended for:

- Network Security Engineers

Prerequisites

To attend this course, candidates must have:

- Completed the *Implementing and Administering Cisco Solutions (CCNA)* course or have the equivalent skills and knowledge.
- Knowledge of Microsoft Windows® operating system

Course Objectives

Upon successful completion of this course, attendees will be able to:

- 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).

REAL WORLD
TECHNOLOGY TRAINING & SOLUTIONS
"Training You Can Really Use"

Course Objectives

- Implement and maintain Cisco IOS Software Network Address Translations (NAT).
- Designing and deploying Cisco Threat Defence 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.

Course Topics

Module 1: Cisco Secure Design Principles

- Network Security Zoning
- Cisco Module Network Architecture
- Cisco SecureX Architecture
- Cisco TrustSec Solutions

Module 2: Implement Network Infrastructure Protection

- Introducing Cisco Network Infrastructure Architecture
- 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 IOS Layer 3 Data Plane Security Controls

Module 3: Deploying NAT on Cisco IOS and Cisco Adaptive Security Appliance (ASA)

- Introducing Network Address Translation
- Deploying Cisco ASA Network Address Translation
- Deploying Cisco IOS Software Network Address Translation

Module 4: Deploying Threat Controls on Cisco ASA

- Introducing Cisco Threat Controls
- Deploying Cisco ASA Basic Access Controls
- Deploying Cisco ASA Application Inspection Policies
- Deploying Cisco ASA Botnet Traffic Filtering
- Deploying Cisco ASA Identity Based Firewall

Module 5: Deploying Threat Controls on Cisco IOS Software

- Deploying Cisco IOS Software with Basic Zone-Based Firewall Policies
- Deploying Cisco IOS Software Zone-Based Firewall with Application Inspection Policies

LABS INCLUDED

Microsoft Partner

Tri7 Business Centre, Unit 7, 7 Ivy Green Crescent, Kingston 5
Tel: 876-978-1107 / 876-978-1486 / 876-927-9455
WhatsApp: 876-978-9353
E-Mail: training@RWTTS.com | **Website:** www.RWTTS.com

Accredited Training Center EC-Council