Data Sheet

Learning Services

Cisco Training on Demand

Implementing Cisco Edge Network Security Solutions (SENSS)

Overview

Implementing Cisco® Edge Network Security Solutions (SENSS) Version 1.0 is a Cisco Training on Demand course. It provides you with foundational knowledge and the capabilities to implement and manage security about Cisco Adaptive Security Appliance (ASA) firewalls, Cisco routers with the firewall feature set, and Cisco switches. You gain hands-on experience with configuring various perimeter security solutions for mitigating outside threats and securing network zones. You also learn how to reduce the risk to your IT infrastructures and applications using Cisco switches, Cisco ASAs and router security appliance features, and provide detailed operations support for these products.

Interested in purchasing this course in volume at discounts for your company? Contact ctod-sales@cisco.com.

Duration

The SENSS Training on Demand course is a self-paced course based on the 5-day instructor-led training version. It consists of 21 sections of instructor video and text totaling more than 8 hours of instruction along with interactive activities, 11 hands-on lab exercises, content review questions, and challenge questions.

Target Audience

The primary audiences for this course are those preparing for the 300-206 SENSS exam and network security engineers

Objectives

After completing this course, you should be able to:

- Describe and implement Cisco modular network security architectures, such as Cisco SecureX Architecture® and TrustSec® products
- 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)
- Implement and maintain Cisco IOS® Software NAT
- Design and deploy Cisco threat defense solutions on a Cisco ASA using access policy and application, and identity-based inspection
- Implementing Cisco Botnet Traffic Filters
- Deploying Cisco IOS zone-based policy firewalls (ZBFW)
- Configure and verify Cisco IOS ZBFW application inspection policy

Course Prerequisites

The knowledge and skills recommended before attending this course are:

- Cisco CCNA® certification
- Cisco CCNA Security certification
- Knowledge of Microsoft Windows operating system

Course Outline

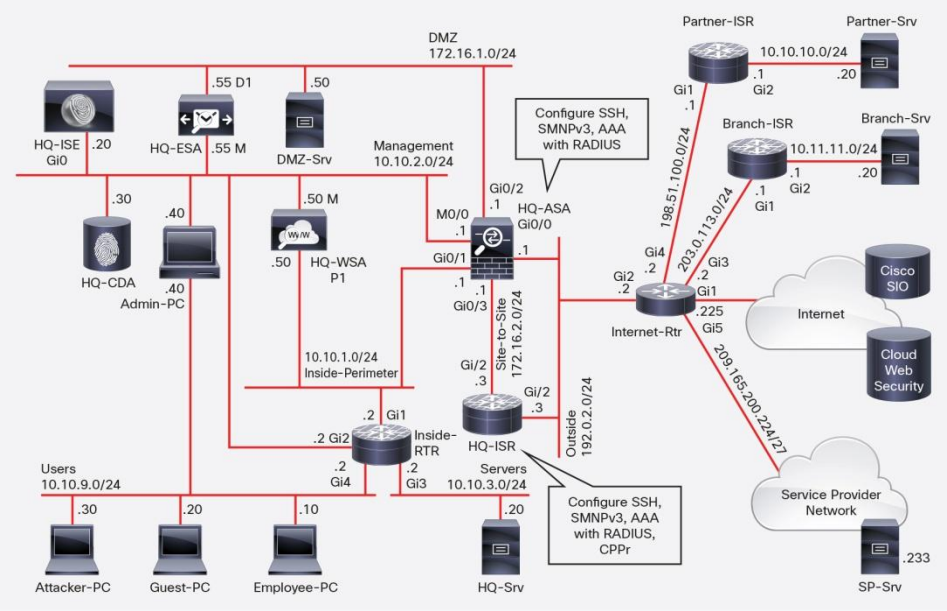
- Course Introduction
- Section 1: Network Security Zoning
- Section 2: Cisco Modular Network Architecture
- Section 3: Cisco SecureX Architecture
- Section 4: Cisco TrustSec Solution
- Section 5: Introducing Cisco Network Infrastructure Protection
- Section 6: Deploying Cisco IOS Control Plane Security Controls
- Section 7: Deploying Cisco IOS Management Plane Security Controls
- Section 8: Deploying Cisco ASA Management Plane Security Controls
- Section 9: Deploying Cisco Traffic Telemetry Methods
- Section 10: Deploying Cisco IOS Layer 2 Data Plane Security Controls
- Section 11: Deploying Cisco Layer 3 Data Plane Security Controls
- Section 12: Introducing Network Address Translation
- Section 13: Deploying Cisco ASA Network Address Translation
- Section 14: Deploying Cisco IOS Software Network Address Translation
- Section 15: Introducing Cisco Firewall Threat Controls
- Section 16: Deploying Basic Cisco ASA Access Policies

- Section 17: Deploying Advanced Cisco ASA Access Policies
- Section 18: Deploying Reputation-Based Cisco ASA Access Policies
- Section 19: Deploying Identity-Based Cisco ASA Access Policies
- Section 20: Deploying Basic Cisco IOS Zone-Based Policy Firewall Access Policies
- Section 21: Deploying Advanced Cisco IOS Zone-Based Policy Firewall Access Policies

Labs Outline

This course contains 11 hands-on lab exercises.

Figure 1. Topology for All Labs in Implementing Cisco Edge Network Security Solutions



The labs included in this course are:

- Discovery Lab 8.8: Configuring Control and Management Plane Security Controls
- Discovery Lab 9.18: Configuring Traffic Telemetry Methods
- Discovery Lab 11.12: Configuring Layer 2 and 3 Data Plane Security Controls
- Discovery Lab 13.12: Configuring Cisco ASA NAT
- Discovery Lab 14.8: Configuring Cisco IOS Router NAT
- Discovery Lab 16.18: Configuring Basic Cisco ASA Access Policies
- Discovery Lab 17.17: Configuring Advanced Cisco ASA Access Policies
- Discovery Lab 18.5: Configuring Cisco ASA Botnet Traffic Filter
- Discovery Lab 19.12: Configure Cisco ASA Identity Firewall
- Discovery Lab 20.12: Configuring Basic Cisco IOS Zone-Based Policy Firewall Access Policies
- Discovery Lab 21.12: Configure Advanced Cisco IOS Zone-Based Policy Firewall Access Policies

Cisco Capital Financing Helps You Achieve Your Objectives

Cisco Capital® financing can help you acquire the technology you need to achieve your objectives and stay competitive. We can help you reduce capital expenditures (CapEx), accelerate your growth, and optimize your investment dollars and ROI. Cisco Capital financing gives you flexibility in acquiring hardware, software, services, and complementary third-party equipment. And there's just one predictable payment. Cisco Capital financing is available in more than 100 countries. Learn more.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C78-737821-00 09/16