

## IMPLEMENTING CISCO EDGE NETWORK SECURITY SOLUTIONS (CI-SENSS)

This subtopic provides an overview of how the course is organized. The course contains these components:

Secure Design Principles

Network Infrastructure Protection Deployment

NAT Deployment on Cisco IOS Software and Cisco ASA

Threat Controls Deployment on Cisco ASA

Threat Controls Deployment on Cisco IOS Software

Lab 2-1: Configure Control and Management Plane Security Controls

Lab 2-2: Configure Traffic Telemetry Methods

Lab 2-3: Configure Layer 2 Data Plane Security Controls

Lab 2-4: Configure Layer 3 Data Plane Security Controls

Lab 3-1: Configure Cisco ASA NAT

Lab 3-2: Configure Cisco IOS Software NAT

Lab 4-1: Configure Basic Cisco ASA Access Policies

Lab 4-2: Configure Advanced Cisco ASA Access Policies

Lab 4-3: Configure Cisco ASA Botnet Traffic Filter

Lab 4-4: Configure Cisco ASA Identity Firewall

Lab 5-1: Configure Basic Cisco IOS Zone-Based Policy Firewall Access Policies

Lab 5-2: Configure Advanced Cisco IOS Zone-Based Policy Firewall Access Policies

### Detailed Course Outline

This in-depth outline of the course structure lists each module, lesson, and topic.

#### Course Introduction

The Course Introduction provides learners with the course objectives and prerequisite learner skills and knowledge. The Course Introduction presents the course flow diagram and the icons that are used in the course illustrations and figures.

This course component also describes the curriculum for this course, providing learners with the information that they need to make decisions regarding their specific learning path.

## Module 1: Secure Design Principles

Module Objective: Understanding Cisco modular Network Security Architectures such as SecureX and TrustSec

### **Lesson 1: Network Security Zoning**

Lesson Objective: Describe the concepts of Network Security Zones

This lesson includes these topics:

Network Security Zones Implementation Model

Zoning

Zone Interface Points

Services

Placement of Services

Summary

### **Lesson 2: Cisco Modular Network Architecture**

Lesson Objective: Provide an overview of the Cisco modular network architecture blueprint

This lesson includes these topics:

Cisco Modular Network Architecture

Cisco Modular Network Architecture Architecture Principles

Cisco Modular Network Architecture Designs

Cisco Modular Network Architecture Example Network

Summary

### **Lesson 3: Cisco SecureX Architecture**

Lesson Objective: Describe the Cisco SecureX architecture as a context-aware security solution

This lesson includes these topics:

Cisco SecureX Architecture and Components

Cisco Security Intelligence Operations Overview

Summary

#### **Lesson 4: Cisco TrustSec Solution**

Lesson Objective: Describe the Cisco TrustSec solution as a part of the Cisco SecureX architecture

This lesson includes these topics:

Cisco TrustSec Solution Overview

Cisco TrustSec Architecture

Cisco TrustSec Solution Components

Summary

#### **Lesson 5: Module Summary**

#### **Lesson 6: Module Self-Check**

### **Module 2: Network Infrastructure Protection Deployment**

Module Objective: Implement data, control and management plane security controls

#### **Lesson 1: Introducing Cisco Network Infrastructure Protection**

Lesson Objective: Provide an overview of network infrastructure protection controls

This lesson includes these topics:

Overview of Cisco Network Infrastructure Protection

Cisco Modular Network Architecture and Network Infrastructure Protection

Identify Network Device Planes

Control Plane Security Controls

Management Plane Security Controls

Network Telemetry

Layer 2 Data Plane Security Controls

Layer 3 Data Plane Security Controls

Summary

#### **Lesson 2: Deploying Cisco IOS Control Plane Security Controls**

Lesson Objective: Examine various defenses in Cisco IOS Software that protect the control plane

This lesson includes these topics:

Overview of Control Plane Security

Infrastructure ACLs

Control Plane Policing Overview

Control Plane Protection Overview

Configure Control Plane Protection

Verify Control Plane Protection

Overview of Routing Protocol Authentication

Overview of Routing Protocol Filtering

Summary

### **Lesson 3: Deploying Cisco IOS Management Plane Security Controls**

Lesson Objective: Describe some strategies to protect the Cisco IOS management plane

This lesson includes these topics:

Overview of Cisco IOS Management Plane Security Controls

Overview of Cisco IOS Secure Management Access

Configure Cisco IOS Secure Management Access

Verify Cisco IOS Secure Management Access

SNMPv3 Overview

Configure Cisco IOS SNMPv3

Verify Cisco IOS SNMPv3

Overview of Management Access AAA

Configure Cisco IOS Management Access AAA

Summary

### **Lesson 4: Deploying Cisco ASA Management Plane Security Controls**

Lesson Objective: Describe some strategies to protect the Cisco ASA management plane

This lesson includes these topics:

Overview of Cisco ASA Management Plane Security Controls

Overview of Cisco ASA Secure Management Access

Configure Cisco ASA Secure Management Access

Overview of Cisco ASA Management Access AAA

Configure Cisco ASA Management Access AAA

Verify Cisco ASA Management Access AAA

Summary

Lab 2-1: Configure Control and Management Plane Security Controls

Lab Objective: Configure network infrastructure protection features on Cisco IOS switches

This lab includes these tasks:

Task 1: Configure Management Plane Security Controls on Cisco IOS Software

Task 2: Configure Management Plane Security Controls on Cisco ASA

Task 3: Configure Management Access AAA on Cisco IOS Software

Task 4: Configure Management Access AAA on Cisco ASA

## **Lesson 5: Deploying Cisco Traffic Telemetry Methods**

Lesson Objective: Describe the baseline forms of telemetry recommended for network infrastructure devices

This lesson includes these topics:

Overview of Cisco Traffic Telemetry Methods

Overview of NTP

Configure NTP on Cisco IOS Software

Verify NTP on Cisco IOS Software

Configure NTP on Cisco ASA

Verify NTP on Cisco ASA

Overview of Device and Network Events Logging

Configure Logging on Cisco IOS Software

Verify Logging on Cisco IOS Software

Configure Logging on Cisco ASA

Verify Logging on Cisco ASA

Overview of Netflow

Configure NetFlow on Cisco IOS Software

Verify NetFlow on Cisco IOS Software

Configure NetFlow on Cisco ASA

Verify NetFlow on Cisco ASA

Summary

Lab 2-2: Configure Traffic Telemetry Methods

Lab Objective: Configure network infrastructure protection features on Cisco IOS switches

This lab includes these tasks:

Task 1: Configure Traffic Telemetry Methods on Cisco IOS Software

Task 2: Configure Traffic Telemetry Methods on Cisco ASA

## **Lesson 6: Deploying Cisco IOS Layer 2 Data Plane Security Controls**

Lesson Objective: Configure and verify Cisco IOS Software Layer 2 Data Plane Controls

This lesson includes these topics:

Overview of Cisco Layer 2 Data Plane Security Controls

PVLAN Overview

Configure PVLANs

Verify PVLANs

DHCP Control Overview

Configure DHCP Snooping

Verify DHCP Snooping

ARP Control Overview

Configure DAI

Verify DAI

Storm Control Overview

Configure Storm Control

Verify Storm Control

MACsec Encryption Overview

Configure MACsec Encryption

Verify MACsec Encryption

Summary

Lab 2-3: Configure Layer 2 Data Plane Security Controls

Lab Objective: Configure network infrastructure protection features on Cisco IOS switches

This lab includes these tasks:

Task 1: Configure DHCP Snooping

Task 2: Configure ARP Inspection

## **Lesson 7: Deploying Cisco Layer 3 Data Plane Security Controls**

Lesson Objective: Configure and verify Cisco IOS Software and Cisco ASA Layer 3 Data Plane Controls

This lesson includes these topics:

Overview of Cisco Layer 3 Data Plane Security Controls

Infrastructure Antispoofing ACLs

uRPF Overview

Configure uRPF on Cisco IOS Software

Verify uRPF on Cisco IOS Software

Configure uRPF on Cisco ASA

Verify uRPF on Cisco ASA

IP Source Guard Overview

Configure IP Source Guard

Verify IP Source Guard

## Summary

Lab 2-4: Configure Layer 3 Data Plane Security Controls

Lab Objective: Configure network infrastructure protection features on Cisco IOS switches

This lab includes these tasks:

Task 1: Configure uRPF on the Cisco IOS Router

Task 2: Configure uRPF on the Cisco ASA

Task 3: Configure IP Source Guard on the Cisco IOS Catalyst Switch

## Lesson 8: Module Summary

## Lesson 9: Module Self-Check

## Module 3: NAT Deployment on Cisco IOS Software and Cisco ASA

Module Objective: Configure, verify, and troubleshoot NAT features on Cisco ASA 5500-X Series Next-Generation Firewalls and on Cisco IOS Software routers

## Lesson 1: Introducing Network Address Translation

Lesson Objective: Describe network address translation

This lesson includes these topics:

Overview of Network Address Translation

Cisco Modular Network Architecture and Network Address Translation

Inside and Outside NAT

Static and Dynamic NAT

NAT and NAT with PAT

Policy-based NAT

NAT and Cisco Products and Features

## Summary

## Lesson 2: Deploying Cisco ASA Network Address Translation

Lesson Objective: Configure, verify, and troubleshoot network address translation on Cisco ASA

This lesson includes these topics:



Overview of Cisco ASA NAT

Configure Network Object NAT

Configure Static NAT Using Network Object NAT

Configure Dynamic NAT with PAT Using Network Object NAT

Verify Network Object NAT

Configure Manual NAT

Configure Dynamic NAT Using Manual NAT

Configure Twice NAT Using Manual NAT

Verify Manual NAT

Troubleshoot NAT

Summary

Lab 3-1: Configure Cisco ASA NAT

Lab Objective: Configure static NAT

This lab includes these tasks:

Task 1: Configure Static NAT

Task 2: Configure Dynamic NAT

Task 3: (Optional) Configure Twice NAT

### **Lesson 3: Deploying Cisco IOS Software Network Address Translation**

Lesson Objective: Configure, verify, and troubleshoot network address translation on Cisco IOS Software routers

This lesson includes these topics:

Configure Static NAT and PAT

Verify Static NAT and PAT

Configure Dynamic NAT and PAT

Configure Policy-Based Dynamic NAT with PAT

Verify Dynamic NAT and PAT

Troubleshoot NAT

Summary

Lab 3-2: Configure Cisco IOS Software NAT

Lab Objective: Implement static NAT on a Cisco IOS router

This lab includes these tasks:

Task 1: Configure Static NAT

Task 2: Configure Dynamic NAT

## **Lesson 4: Module Summary**

## **Lesson 5: Module Self-Check**

## **Module 4: Threat Controls Deployment on Cisco ASA**

Module Objective: Configure, verify, and troubleshoot threat controls on Cisco ASA

## **Lesson 1: Introducing Cisco Firewall Threat Controls**

Lesson Objective: Provide an overview of Cisco firewall threat controls

This lesson includes these topics:

Overview of Firewall Threat Controls

Cisco Modular Network Architecture and Firewall Threat Controls

Firewall Filtering Layers

Firewall Filtering Approaches

Firewall Filtering Technologies

Combining Firewall Filtering Technologies

Firewall Threat Controls and Cisco Products and Features

Summary

## **Lesson 2: Deploying Basic Cisco ASA Access Policies**

This lesson includes these topics:

Overview of Cisco ASA Access Control Features

Connection Table

Examining the Connection Table

Local Host Table

Examining the Local Host Table

Connection Table Logging

Interface ACLs

Configure Interface ACLs

Verify Interface ACLs

Global ACLs

Configure Global ACLs

Verify Global ACLs

Object Groups

Configure Object Groups

Verify Object Groups

Troubleshoot ACLs

Summary

Lab 4-1: Configure Basic Cisco ASA Access Policies

Lab Objective: Configure object groups

This lab includes these tasks:

Task 1: Configure Object Groups

Task 2: Configure Interface ACLs

Task 3: Configure Global ACL

Task 4: Verify Connectivity Across the ASA

### **Lesson 3: Deploying Advanced Cisco ASA Access Policies**

Lesson Objective: Describe and configure advanced Cisco ASA access policies

This lesson includes these topics:

Advanced Cisco ASA Access Policies Overview

Cisco MPF Overview

OSI Layer 3–4 Policies Overview

Default OSI Layer 3–4 Stateful Tracking  
Tune OSI Layer 3–4 Stateful Tracking  
Verify OSI Layer 3–4 Stateful Tracking  
Support for Dynamic Protocols  
Configure Support for Dynamic Protocols  
Verify Support for Dynamic Protocols  
Application Layer (OSI Layer 5–7) Policies Overview  
HTTP Inspector Overview  
Configure HTTP Inspection  
Verify HTTP Inspection  
FTP Inspector Overview  
Evaluate Application Inspection of Other Protocols  
Summary  
Lab 4-2: Configure Advanced Cisco ASA Access Policies  
Lab Objective: Implement HTTP inspection  
This lab includes these tasks:  
Task 1: Tune OSI Layer 3-4 Stateful Inspection  
Task 2: Examine Support for Dynamic Protocols  
Task 3: Configure Application Inspection for HTTP Traffic  
Task 4: Configure Application Inspection for FTP Traffic

#### **Lesson 4: Deploying Reputation-Based Cisco ASA Access Policies**

Lesson Objective: Describe and configure reputation-based Cisco ASA access policies

This lesson includes these topics:

Overview of the Cisco Botnet Traffic Filter  
Configure the Cisco Botnet Traffic Filter  
Verify the Cisco Botnet Traffic Filter

## Summary

Lab 4-3: Configure Cisco ASA Botnet Traffic Filter

Lab Objective: Implement the Botnet Traffic Filter on the Cisco ASA

This lab includes these tasks:

Task 1: Configure the Botnet Traffic Filter using Dynamic Database

Task 2: Configure the Botnet Traffic Filter using Static Database

## **Lesson 5: Deploying Identity-Based Cisco ASA Access Policies**

Lesson Objective: Describe and configure identity-based Cisco ASA access policies

This lesson includes these topics:

Overview of the Identity Firewall

Identity Firewall Flow

Cisco CDA Overview

Integrate Cisco CDA with AD and Cisco ASA

Verify Cisco CDA Integration with AD

Integrate Cisco ASA with AD and Cisco CDA

Verify Cisco ASA Integration with AD and Cisco CDA

Configure Identity-Based Access Rules

Verify the Identity-Based Firewall

Troubleshoot Identity-Based Firewall

## Summary

Lab 4-4: Configure Cisco ASA Identity Firewall

Lab Objective: Configure identity-based firewall features

This lab includes these tasks:

Task 1: Configure Cisco CDA

Task 2: Configure the Cisco ASA for Active Directory Integration

Task 3: Configure the Cisco ASA with Identity Options

Task 4: Configure the Cisco ASA Identity-Based Access Rules

## Lesson 6: Module Summary

## Lesson 7: Module Self-Check

### Module 5: Threat Controls Deployment on Cisco IOS Software

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

#### **Lesson 1: Deploying Basic Cisco IOS Zone-Based Policy Firewall Access Policies**

This lesson includes these topics:

Overview of the Cisco IOS Zone-Based Policy Firewall

Configure Zones and Zone Pairs

Verify Zones and Zone Pairs

Configure a Basic OSI Layer 3 and 4 Interzone Access Policy

Verify a Basic OSI Layer 3 and 4 Interzone Access Policy

Configure a Basic OSI Layer 3 and 4 Intrazone Access Policy

Configure Inspection of Control Plane and Management Plane Traffic

Tune Stateful Engine and Connection Settings

Configure Support for NAT

Troubleshoot the Zone-Based Policy Firewall

Summary

Lab 5-1: Configure Basic Cisco IOS Zone-Based Policy Firewall Access Policies

Lab Objective: Implement Cisco IOS Zone-Based Policy Firewall

This lab includes these tasks:

Task 1: Configure Security Zones

Task 2: Configure Access Control Between the INSIDE and OUTSIDE Zones

Task 3: Configure Access Control Between the VPN and INSIDE Zones

Task 4: Configure Access Control for Management Traffic Between the SELF and OUTSIDE Zones

#### **Lesson 2: Deploying Advanced Cisco IOS Zone-Based Policy Firewall Access Policies**

Lesson Objective: Describe and configure application inspection policies on Cisco IOS Zone-Based Policy Firewall

This lesson includes these topics:

Overview of Advanced Access Policies

Overview of Application-Layer Access Policies

HTTP Inspector Overview

Configure HTTP Inspection

Verify HTTP Inspection

Inspection of Instant Messaging

Inspection of Peer-to-Peer Protocols

Additional Application Inspection

URL Filtering Methods in Cisco IOS Zone-Based Policy Firewall

Configure Local List-Based URL Filtering

Summary

Lab 5-2: Configure Advanced Cisco IOS Zone-Based Policy Firewall Access Policies

Lab Objective: Configure and verify sHTTP inspection

This lab includes these tasks:

Task 1: Configure HTTP Application-Layer Inspection

**Lesson 3: Module Summary**

**Lesson 4: Module Self-Check**