ProTech
protechtraining.com

"Charting the Course ...

... to Your Success!"

Implementing Cisco Edge Network Security Solutions (SENSS)

Course Summary

Description

Implementing Cisco Edge Network Security Solutions (SENSS) is a newly created five-day instructor-led training (vILT) course 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.

Objectives

At the end of this course, students will be able to:

- Understand current security threat landscape
- 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)
- Implement and maintain Cisco IOS Software Network Address Translations (NAT)
- Designing and deploying Cisco Threat Defense 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

Topics

- Cisco Secure Design Principles
- Implement Network Infrastructure Protection
- Deploying NAT on Cisco IOS and Cisco Adaptive Security Appliance (ASA)
- Deploying Threat Controls on Cisco ASA
- Deploying Threat Controls on Cisco IOS Software

Audience

The primary audience for this course is as follows: Network Security Engineers

Prerequisites

To fully benefit from this course, students should have the following prerequisite skills and knowledge:

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

Duration

Five days

ProTech
protechtraining.com

"Charting the Course ...

... to Your Success!"

Implementing Cisco Edge Network Security Solutions (SENSS)

Course Outline

I. Cisco Secure Design Principles

A. Lesson 1: Network Security Zoning
   1. This lesson defines how to identify the benefits of implementing a Cisco Zone based security architecture solution. Upon completing this lesson, the learner will be able to meet these objectives:
   2. Describe the principles behind zone based security architecture

B. Lesson 2: Cisco Module Network Architecture
   1. This lesson defines how why it is important to develop a modular security architecture. Upon completing this lesson, the learner will be able to meet these objectives:
   2. Describe the various approaches to architecting a security solution based on access areas

C. Lesson 3: Cisco SecureX Architecture
   1. This lesson defines how to identify the components and functions of a Cisco SecureX solution. Upon completing this lesson, the learner will be able to meet these objectives:
   2. Describe Cisco SecureX network-centric approach
   3. Understand the enforcement model
   4. Align corporate business needs to network security policies
   5. Integrate global intelligence with context-aware networking

D. Lesson 4: Cisco TrustSec Solutions
   1. This lesson defines how to identify the components and functions of a Cisco TrustSec solution. Upon completing this lesson, the learner will be able to meet these objectives:
   2. Describe the architecture and deployment options for a TrustSec solution
   3. Understand the basics to identify based security control
   4. Basics of Profiling and devices assessment
   5. How Security Group Tagging (SGA) is integrated into the network

II. Implement Network Infrastructure Protection

A. Lesson 1: Introducing Cisco Network Infrastructure Architecture
   1. This lesson defines how to describe the basic concepts of why network infrastructure equipment should be protected. Upon completing this lesson, the learner will be able to meet these objectives:
   2. Understand the threats and risks facing the network infrastructure

B. Lesson 2: Deploying Cisco IOS Control Plane Security Controls
   1. This lesson defines how and why to configuring Cisco IOS security to limit access to the IOS control plane. Upon completing this lesson, the learner will be able to meet these objectives:
   2. Describe how to implement Cisco IOS control plane security

C. Lesson 3: Deploying Cisco IOS Management Plane Security Controls
   1. Upon completing this lesson, the learner will be able to meet these objectives:
   2. Describe how to implement Cisco IOS management plane security

D. Lesson 4: Deploying Cisco ASA Management Plane Security Controls
   1. Upon completing this lesson, the learner will be able to meet these objectives:
   2. Describe how to implement Cisco ASA management plane security

E. Lesson 5: Deploying Cisco Traffic Telemetry Methods
   1. Upon completing this lesson, the learner will be able to meet these objectives:
   2. Understand how telemetry data such as NTP, logging, and NetFlow can improve network security posture

F. Lesson 6: Deploying Cisco IOS Layer 2 Data Plane Security Controls
   1. Upon completing this lesson, the learner will be able to meet these objectives:
   2. Describe

G. Lesson 7: Deploying Cisco IOS Layer 3 Data Plane Security Controls
   1. Upon completing this lesson, the learner will be able to meet these objectives:
   2. Describe Cisco IOS Layer 3 Data Plane Security controls such as antispoofing ACLs, uRPF, and IP Source Guard.

Implementing Cisco Edge Network Security Solutions (SENSS)

Course Summary (cont'd)

III. Deploying NAT on Cisco IOS and Cisco Adaptive Security Appliance (ASA)

A. Lesson 1: Introducing Network Address Translation
   1. Understand the basics need for Network Address translation. Upon completing this lesson, the learner will be able to meet these objectives:
   2. Review the fundamentals of Network Address Translation
   3. Learn the different between PAT, Dynamic NAT, and Static NAT

B. Lesson 2: Deploying Cisco ASA Network Address Translation
   1. Understand the requirements for setting up Network Address Translation on a Cisco ASA firewall. Upon completing this lesson, the learner will be able to meet these objectives:
   2. Learn to configure NAT to support many use cases

C. Lesson 3: Deploying Cisco IOS Software Network Address Translation
   1. Understand how to implement NAT on an IOS software device. Upon completing this lesson, the learner will be able to meet these objectives:
   2. Learn how NAT functions on an IOS Software device
   3. Configure both Static NAT and dynamic NAT

IV. Deploying Threat Controls on Cisco ASA

A. Lesson 1: Introducing Cisco Threat Controls
   1. This lesson defines how to identify what features are available on the ASA to support threat control. Upon completing this lesson, the learner will be able to meet these objectives:
   2. Understand the features and solutions for configuring ASA threat control

B. Lesson 2: Deploying Cisco ASA Basic Access Controls
   1. This lesson defines how to configure Cisco ASA basic access policies. Upon completing this lesson, the learner will be able to meet these objectives:
   2. Understand the configuration requirements and functionality of Cisco ASA access controls

C. Lesson 3: Deploying Cisco ASA Application Inspection Policies
   1. Upon completing this lesson, the learner will be able to meet these objectives:
   2. Setup and configure ASA with Application Inspections policies

D. Lesson 4: Deploying Cisco ASA Botnet Traffic Filtering
   1. Upon completing this lesson, the learner will be able to meet these objectives:
   2. Overview and Configuration of Cisco ASA Botnet Traffic Filter

E. Lesson 5: Deploying Cisco ASA Identity Based Firewall
   1. Upon completing this lesson, the learner will be able to meet these objectives:
   2. Overview and Configuration of Cisco Identity Based Firewall

V. Deploying Threat Controls on Cisco IOS Software

A. Lesson 1: Deploying Cisco IOS Software with Basic Zone-Based Firewall Policies
   1. This lesson provides an overview and configuration tasks of Cisco IOS Zone-Based Policy Firewall:
   2. Overview and configuration of ZBPF Access Control Policies.

B. Lesson 2: Deploying Cisco IOS Software Zone-Based Firewall with Application Inspection Policies
   1. Upon completing this lesson, the learner will be able to meet these objectives.
   2. Describe how to implement ZBFW policy for certain application inspection rules