Securing Networks with Cisco Firepower Next-Generation IPS (SSFIPS v3.0) Training

Course: **00105**

Filter: **Beginner**

Duration: **20 hours**

Category:: **Systems & Network Security**

Price: **2500,00 €**

About Course

This course is a lab-intensive course which introduces you to the basic next-generation intrusion prevention system (NGIPS) and firewall security concepts, and the Cisco Firepower system components and features. The course then leads you through the powerful features of the Cisco Firepower system, in-depth event analysis, NGIPS tuning and configuration, Snort® rules language overview, and the latest platform features including File & Malware inspection, Security Intelligence, Domain Awareness, and more. The course begins by introducing the system architecture, the latest key features, and the role of policies when implementing the solution. You also learn how to manage deployed devices and perform basic Cisco Firepower discovery before moving on to describe how to use and configure Cisco NGIPS technology, including application control, security intelligence, firewall, and network-based malware and file controls. You also learn to properly tune systems for better performance and greater network intelligence while taking advantage of powerful tools for more efficient event analysis, including file type and network-based malware detection. The course finishes with system and user administration tasks. This course combines lecture materials and hands-on labs throughout to make sure you are able to successfully deploy and manage the Cisco Firepower system. • Technical understanding of TCP/IP networking and network architecture • Basic familiarity with the concepts of intrusion detection systems (IDS) and IPS • This course is designed for technical professionals who need to know how to deploy and manage a Cisco Firepower NGIPS in their network environment. Targeted roles include: • Security administrators • Security consultants • Network administrators • System engineers • Technical support personnel • Channel partners and resellers

What you'll learn

- Describe the key features and concepts of NGIPS and firewall security
- Describe the components, features and high-level implementation steps of the Cisco Firepower systemNavigate the Cisco Firepower Management Center GUI and understand the role of policies when configuring the Cisco Firepower systemDeploy and manage Cisco Firepower-managed devices
- Perform initial Cisco Firepower discovery and basic event analysis to identify hosts, applications and servicesIdentify and create objects required as prerequisites for implementing access control policiesIdentify hosts, applications and servicesIdentify and create objects required as prerequisites for implementing access control policiesIdentify features and functionality of access control policies and implementation procedures
- Describe the concepts and procedures for implementing security intelligence
- Describe the concepts and procedures for implementing file control and advanced malware protection
- Use Cisco Firepower recommendations
- Explain the use of network analysis policies and the role of preprocessor technology in processing network traffic for NGIPS inspection
- Describe and demonstrate the detailed analysis techniques and reporting functions provided by Cisco Firepower Management Center
- Describe the main Cisco Firepower Management Center system administration and user account management functions.
- Identify and create the objects required as prerequisites for implementing access control policies
- Identify features and functionalities of access control policies and implementation procedures

Pre-requisites

- None

Curriculum

Module 1: Security Technology Overview

-

Module 2: Cisco Firepower System Components and Features

-

Module 3: Introducing the Cisco Firepower Management Center

-

Module 4: Deploying Cisco Firepower Managed Devices

-

Module 5: Cisco Firepower Discovery

-

Module 6: Access Control Policy Prerequisites

-

Module 7: Implementing Access Control Policies

-

Module 8: File Control and Advanced Malware Protection

-

Module 9: Next-Generation Intrusion Prevention Systems

-

Module 10: Network Analysis Policies

-

Module 11: Detailed Analysis Techniques

-