Securing Networks with Cisco Firepower Next-Generation IPS

Duration: 4 Days   Course Code: SSFIPS

Overview:

The Securing Networks with Cisco Firepower? Next-Generation Intrusion Prevention System is an instructor-led, lab-based, hands-on course, that is part of a portfolio of security courses designed to enable businesses to support and maintain their Cisco Firepower systems. It 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.
Instructor-led classroom: 4 days
Instructor-led virtual classroom: 5 days

Target Audience:

Technical professionals who need to know how to deploy and manage a Cisco FirePower NGIPS in their network environment.

Objectives:

- **After completing this course, you should be able to:**
- Describe the key features and concepts of NGIPS and firewall security
- Describe the Cisco Firepower system components, features, and high-level implementation steps
- Navigate the Cisco Firepower Management Center GUI and understand the role of policies when configuring the Cisco Firepower system
- Deploy and manage Cisco Firepower managed devices
- Perform an initial Cisco Firepower discovery and basic event analysis to identify hosts, applications and services
- Identify and create the objects required as prerequisites to implementing access control policies
- Identify the features and functionality of access control policies and the implementation procedures
- Describe the concepts and implementation procedures of security intelligence
- Describe the concepts and implementation procedures of file control and advanced malware protection
- Use Cisco Firepower recommendations to implement IPS policies
- 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 features provided by the Cisco Firepower Management Center
- Describe major Cisco Firepower Management Center system administration and user account management features

Prerequisites:

Attendees should meet the following prerequisites:

- Technical understanding of TCP/IP networking and network architecture
- Basic familiarity with the concepts of intrusion detection systems (IDS) and IPS
- CCNA Security (ICND1 and IINS) recommended.

Testing and Certification

Recommended as preparation for exams:

- **500-285** - SSFIPS

Required for those partners looking to achieve the Advanced Security Architecture Specialisation

Content:

Security Technology Overview

Cisco Firepower System Components and Features

Introducing the Cisco Firepower Management Center

Deploying Cisco Firepower Managed Devices

Cisco Firepower Discovery

Access Control Policy Prerequisites

Implementing Access Control Policies

Security Intelligence

File Control and Advanced Malware Protection

Next-Generation Intrusion Prevention Systems

Network Analysis Policies

Detailed Analysis Techniques

System Administration

Labs

- Lab 1: Connect to the Lab Environment
- Lab 2: Navigate the Cisco Firepower Management Center GUI
- Lab 3: Device Management
- Lab 4: Cisco Firepower Discovery
- Lab 5: Access Control Policy Prerequisites
- Lab 6: Implementing an Access Control Policy
- Lab 7: Security Intelligence
- Lab 8: File Control and Advanced Malware Protection
- Lab 9: Implementing NGIPS
- Lab 10: Detailed Analysis
- Lab 11: System Administration

Further Information:

For More information, or to book your course, please call us on 0800/84.009

info@globalknowledge.be

www.globalknowledge.be