Data Sheet

Learning@Cisco

Securing Networks with Cisco Firepower Next Generation IPS (SSFIPS) v3.1

Overview

The Securing Networks with Cisco Firepower Next-Generation IPS (SSFIPS) version 3.1 Cisco® Training on Demand course provides you with technical training to deploy the Cisco Firepower® system. Among other powerful features, you learn in-depth event analysis, Next-Generation Intrusion Prevention System (NGIPS) tuning and configuration, and the Snort rules language. You also become familiar with the concepts and practices of file and malware inspection, domain awareness, and security management, and learn to describe the difference between firewall and NGIPS technologies.

In addition, you learn the relationship between Cisco, Sourcefire®, and Snort. You're able to detail a Cisco Firepower system and describe the role and relationships of policies in configuring the system. You also learn how to perform the device setup tasks for the Cisco Firepower architecture and configure both passive and advanced deployment options. You gain knowledge of how to interpret host profiles and create fingerprints along with managing user identities, and how to configure and access control policies and object types within the Cisco Firepower system, together with security intelligence, whitelists, blacklists, and logging. Finally, you learn how to examine malware and file dispositions, examine Snort rules and variable sets, create intrusion sets, and understand the role of Snort in the administrative flow, together with detailed analysis techniques.

Duration

The SSFIPS Training on Demand course consists of 13 modules, totaling more than 9 hours of video instruction along with 11 hands-on lab exercises.

Target Audience

This course is designed for security administrators and consultants, network administrators, systems engineers, and technical support personnel who need to know how to deploy and manage a Cisco Firepower NGIPS in their network environment and how to write Snort rules.

Objectives

After completing this course, you should be able to:

- Describe the key features and concepts of next-generation IPS and firewall security
- Identify the components of the Cisco Firepower system
- Communicate the role and relationships of policies in the Cisco Firepower system
- Identify the various Cisco Firepower system deployment architectures
- Interpret host profile information
- Explain the object types, their uses within the Cisco Firepower system, and implementation procedures for security intelligence
- Describe and identify considerations for access control policy rules
- Understand file visibility and control, malware and file policies, and the principles of AMP for Firepower
- Implement and manage intrusion policies and variables
- Understand Cisco Firepower management system administration and user account management

Course Prerequisites

The knowledge and skills necessary before attending this course is:

- Technical understanding of TCP/IP networking and network architecture
- Basic familiarity with the concepts of Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS)

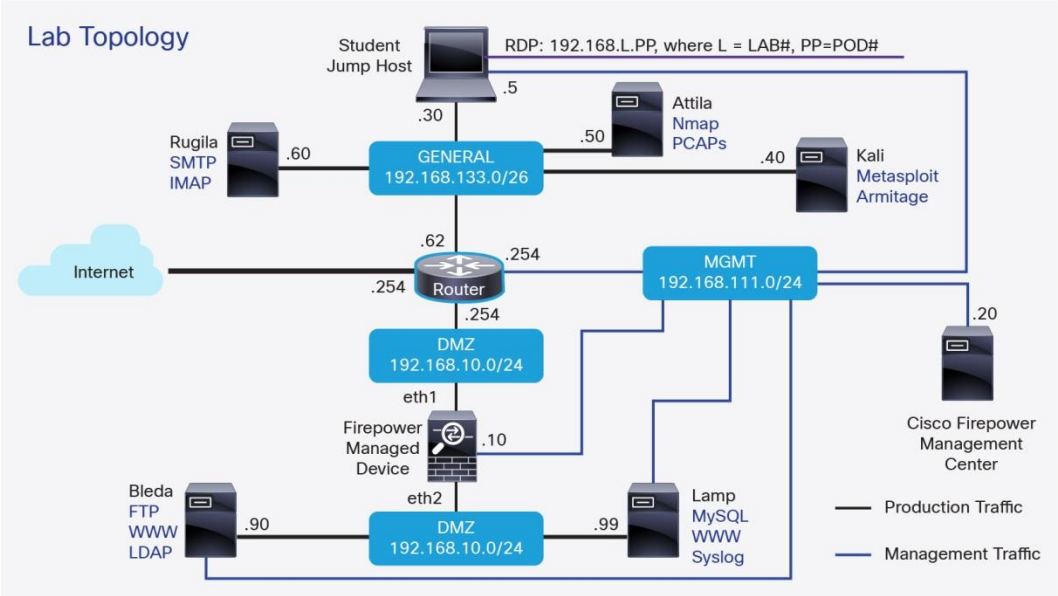
Course Outline

- Module 1: Security Technology Overview
- Module 2: Cisco Firepower NGIPS Components and Features
- Module 3: Cisco Firepower Management Center Introduction
- Module 4: Deploying Cisco Firepower Managed Devices
- Module 5: Firepower Discovery
- Module 6: Access Control Policy Prerequisites
- Module 7: Implementing Access Control Policies
- Module 8: Security Intelligence
- Module 9: Fire Control and Advanced Malware Protection
- Module 10: Next-Generation Intrusion Prevention Systems
- Module 11: Network Analysis Policies
- Module 12: Detailed Analysis Techniques
- Module 13: System Administration

Labs Outline

This course contains 11 hands-on virtual lab exercises.

Topology for All Labs in the course:



The labs included in this course are:

- SSFIPS3.1 Lab 1: Connecting to the Lab Environment
- SSFIPS3.1 Lab 2: Navigating the Firepower Management Center GUI
- SSFIPS3.1 Lab 3: Device Management
- SSFIPS3.1 Lab 4: Implementing Network Discovery
- SSFIPS3.1 Lab 5: Access Control Policy Prerequisites
- SSFIPS3.1 Lab 6: Implementing an Access Control Policy
- SSFIPS3.1 Lab 7: Implementing Security Intelligence
- SSFIPS3.1 Lab 8: File Control and Advanced Malware Protection
- SSFIPS3.1 Lab 9: Implementing NGIPS
- SSFIPS3.1 Lab 10: Detailed Analysis
- SSFIPS3.1 Lab 11: System Administration

Instructor Bio

Mark Brereton has 20 years of experience as an instructor in IT and IT security. In addition to providing training for Cisco's customers, partners, and employees, Mark assists with the maintenance and development of several security-oriented classes. Before working for Cisco, Mark worked as an instructor for Sourcefire, where he developed his knowledge of Snort and commercial IPS products, and prior to that, he worked for RSA Security, where he developed his knowledge of authentication, PKI, and other security products. Mark is also a qualified teacher.

Cisco Capital

Financing to Help You Achieve Your Objectives

Cisco Capital can help you acquire the technology you need to achieve your objectives and stay competitive. We can help you reduce CapEx. Accelerate your growth. 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 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 **https://www.cisco.com/go/offices**.

Printed in USA C78-738836-01 07/18