Securing Networks with Cisco Firepower Next-Generation IPS (SSFIPS) v4.0

What you'll learn in this course

The **Securing Networks with Cisco Firepower Next-Generation IPS (SSFIPS)** v4.0 course shows you how to deploy and use Cisco Firepower® Next-Generation Intrusion Prevention System (NGIPS). This hands-on course gives you the knowledge and skills to use the platform features and includes firewall security concepts, platform architecture and key features; in-depth event analysis including detection of network-based malware and file type, NGIPS tuning and configuration including application control, security intelligence, firewall, and network-based malware and file controls; Snort® rules language; file and malware inspection, security intelligence, and network analysis policy configuration designed to detect traffic patterns; configuration and deployment of correlation policies to take action based on events detected; troubleshooting; system and user administration tasks, and more.

This course helps you prepare to take the exam, **Securing Networks with Cisco Firepower (300-710 SNCF)**, which leads to **CCNP Security and Cisco Certified Specialist – Network Security Firepower** certifications. The **300-710 SNCF** exam has a second preparation course as well, **Securing Networks with Cisco Firepower Next Generation Firewall (SSNGFW)**. You can take these courses in any order. This course also earns you 32 Continuing Education (CE) credits towards recertification.

Course duration

- Instructor-led classroom: 5 days in the classroom with hands-on lab practice
- Instructor-led virtual classroom: 5 days of web-based classes with hands-on lab practice
- E-learning: Equivalent of 5 days of instruction with videos, practice, and challenges

How you'll benefit

This course will help you:

- Implement Cisco Firepower Next-Generation IPS to stop threats, address attacks, increase vulnerability prevention against suspicious files, and analyze for not-yet-identified threats
- Gain leading-edge skills focused on security
- Earn 32 CE credits for recertification

Who should enroll

This course is designed for technical professionals who need to know how to deploy and manage a Cisco Firepower NGIPS in their network environment.

- Security administrators
- Security consultants
- Network administrators
- System engineers
- Technical support personnel
- Channel partners and resellers

What to expect in the exam

The **300-SNCF** exam certifies your knowledge of Cisco Firepower® Threat Defense and Firepower®, including policy configurations, integrations, deployments, management, and troubleshooting.

After you pass 300-710 SNCF:

- You earn the **Cisco Certified Specialist - Network Security Firepower** certification.
- You will have satisfied the concentration exam requirement for new **CCNP Security** certification. To complete **CCNP Security**, you also need to pass the **Implementing and Operating Cisco Security Core Technologies (350-701 SCOR)** exam or its equivalent.

Technology areas

- Security

Course details

Objectives

After taking this course, you should be able to:

- Describe the components of Cisco Firepower Threat Defense and the managed device registration process
- Detail Next-Generation Firewalls (NGFW) traffic control and configure the Cisco Firepower system for network discovery
- Implement access control policies and describe access control policy advanced features
- Configure security intelligences features and the Advanced Malware Protection (AMP) for Networks implementation procedure for file control and advanced malware protection
- Implement and manage intrusion and network analysis policies for NGIPS inspection
- Describe and demonstrate the detailed analysis techniques and reporting features provided by the Cisco Firepower Management Center
- Integrate the Cisco Firepower Management Center with an external logging destination
- Describe and demonstrate the external alerting options available to Cisco Firepower Management Center and configure a correlation policy
- Describe key Cisco Firepower Management Center software update and user account management features
- Identify commonly misconfigured settings within the Cisco Firepower Management Center and use basic commands to troubleshoot a Cisco Firepower Threat Defense device

Recommended knowledge and training

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

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

Outline

- Cisco Firepower Threat Defense Overview
- Cisco Firepower NGFW Device Configuration
- Cisco Firepower NGFW Traffic Control
- Cisco Firepower Discovery
- Implementing Access Control Policies
- Security Intelligence
- File Control and Advanced Malware Protection
- Next-Generation Intrusion Prevention Systems
- Network Analysis Policies
- Detailed Analysis Techniques
- Cisco Firepower Platform Integration
- Alerting and Correlation Policies
- Performing System Administration
- Firepower Troubleshooting

How to enroll

To enroll in the SSFIPS course or explore our larger catalog of courses on Cisco Digital Learning, contact us at <training@fastlane-mea.com>

Lab outline

- Perform Initial Device Setup
- Perform Device Management
- Configure Network Discovery
- Implement an Access Control Policy
- Implement Security Intelligence
- Implement Control and Advanced Malware Protection
- Implement NGIPS
- Customize a Network Analysis Policy
- Perform Analysis
- Configure Firepower Platform Integration with Splunk
- Configure Alerting and Event Correlation
- Perform System Administration
- Troubleshoot Firepower

Note: There are some terminology differences between the outlines in the instructor-led and e-learning versions of this course. Both courses cover the same lessons and labs.