



**Document Generated: 11/21/2024**

**Learning Style: Virtual Classroom**

**Provider: Cisco**

**Difficulty: Intermediate**

**Course Duration: 5 Days**

## **Securing Networks with Cisco Firepower Next-Generation IPS (SSFIPS4) 4.0 (SSFIPS4)**

### **About this course:**

Securing Networks with Cisco Firepower Next-Generation IPS (SSFIPS) v4.0 is a 5-day course which 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 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 for high-demand responsibilities focused on security

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.

## **Course Objective:**

Upon completing this course, the learner will be able to meet these overall objectives:

- 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

## **Audience:**

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

## **Prerequisite:**

The knowledge and skills that a learner should have before attending this course are as follows:

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

## **Course 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**

**System Administration**

**Cisco Firepower Troubleshooting**

## **Lab Outline:**

- Initial Device Setup
- Device Management
- Configuring Network Discovery
- Implementing and Access Control Policy
- Implementing Security Intelligence
- File Control and Advanced Malware Protection
- Implementing NGIPS

- Customizing a Network Analysis Policy
- Detailed Analysis
- Configuring Cisco Firepower Platform Integration with Splunk
- Configuring Alerting and Event Correlation
- System Administration
- Cisco Firepower Troubleshooting

## Credly Badge:



### **Display your Completion Badge And Get The Recognition You Deserve.**

Add a completion and readiness badge to your LinkedIn profile, Facebook page, or Twitter account to validate your professional and technical expertise. With badges issued and validated by Credly, you can:

- Let anyone verify your completion and achievement by clicking on the badge
- Display your hard work and validate your expertise
- Display each badge's details about specific skills you developed.

Badges are issued by QuickStart and verified through Credly.

[Find Out More](#) or [See List Of Badges](#)