300-710 – CCNP Security – SNCF – Course Securing Networks with Cisco Firepower Next Generation Firewall (SSNGFW)

Securing Networks with Cisco Firepower Next Generation Firewall (SSNGFW) v 1.0

for EXAM:

Securing Networks with Cisco Firepower (SNCF 300-710)

About this Course

- The **Securing Networks with Cisco Firepower Next Generation Firewall** (SSNGFW) v1.0 course shows you how to deploy and use Cisco Firepower® Threat Defense system. This hands-on course gives you knowledge and skills to use and configure Cisco® Firepower Threat Defense technology, beginning with initial device setup and configuration and including routing, high availability, Cisco Adaptive Security Appliance (ASA) to Cisco Firepower Threat Defense migration, traffic control, and Network Address Translation (NAT). You will learn how to implement advanced Next-Generation Firewall (NGFW) and Next-Generation Intrusion Prevention System (NGIPS) features, including network intelligence, file type detection, network-based malware detection, and deep packet inspection. You will also learn how to configure site-to-site VPN, remote-access VPN, and SSL decryption before moving on to detailed analysis, system administration, and troubleshooting.

Course Goals

- Describe key concepts of NGIPS and NGFW technology and the Cisco Firepower Threat Defense system, and identify deployment scenarios
- Perform initial Cisco Firepower Threat Defense device configuration and setup tasks
- Describe how to manage traffic and implement Quality of Service (QoS) using Cisco Firepower Threat Defense
- Describe how to implement NAT by using Cisco Firepower Threat Defense
- Perform an initial network discovery, using Cisco

Firepower to identify hosts, applications, and services
- Describe the behavior, usage, and implementation procedure for access control policies
- Describe the concepts and procedures for implementing security intelligence features
- Describe Cisco Advanced Malware Protection (AMP) for Networks and the procedures for implementing file control and advanced malware protection
- Implement and manage intrusion policies
- Describe the components and configuration of site-to-site VPN
- Describe and configure a remote-access SSL VPN that uses Cisco AnyConnect®
- Describe SSL decryption capabilities and usage

Audience

- Security administrators
- Security consultants
- Network administrators
- System engineers
- Technical support personnel
- Cisco integrators and partners

Course Format

Classroom

Online / Virtual

Video Archive (24/7)

Certificate of Course Completion

Course Duration

- 5 working days (monday – friday 09:00 – 17:00)

или

- **40 hours in after hours classes 4 weeks in row**
- sat / sun 10:00 – 14:00, 14:00 – 18:00, 18:00 – 22:00
- mon / wed 19:00 – 23:00
- tue / thu 19:00 – 23:00

Payments

Class Schedules

 Notice
There are no upcoming events.

Prerequisites

- Knowledge of TCP/IP and basic routing protocols
- Familiarity with firewall, VPN, and Intrusion Prevention System (IPS) concepts

This course will prepare you to pass the following exam:

- 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 Intrusion Prevention System** (SSFIPS). You can take these courses in any order.