THINQTANK® LEARNING

CISCO CERTIFIED NETWORK PROFESSIONAL SECURITY FIREPOWER

Securing Networks with Cisco Firepower Next Generation Firewall (SSNGFW)
Securing Networks with Cisco Firepower Next Generation IPS (SSFIPS)

Our Learning Exclusive

- Custom exam prep software and materials
- Exam delivery in classroom with 98% success
- Course specific thinQtank® Learning publications to promote fun exciting learning
- Extended hours of training including immersive hands-on exercises
- WE DO NOT "TEACH THE TEST" We always deliver valuable hands-on experience
- Receive all reading material and study guides when you register
- All courses taught by CCIE expert instructors

Course Duration

- Nine days of instructor-led learning
- Five days SSNGFW and four days SSFIPS
- 60% lecture, 40% hands-on labs

Prerequisites

- Knowledge of TCP/IP and basic routing protocols
- Familiarity with firewall, VPN, and Intrusion Prevention System (IPS) concepts
- Basic familiarity with the concepts of Intrusion Detection Systems (IDS) and IPS

Target Audience

- Security administrators
- Security consultants
- Network administrators
- System engineers
- Technical support personnel

Exam Information

- 300-710 – Securing Networks with Cisco Firepower (SNCF)

Delivery Methods

- Instructor-Led Training
- Immersive Live-Online Training
- On-Site and Custom Delivery

Exclusive Tools and Learning Package

- Comprehensive video training package
- Virtual builds of all labs and hand-on learning objectives so learners can continue their hands on experience after the completion of the course
- Industry unique training course to achieve multiple certifications in one training camp

Course Overview

thinQtank® Learning is offering a unique nine-day training camp comprised of five days of instructor-led learning for Securing Networks with Cisco Firepower Next Generation Firewall (SSNGFW) and Securing Networks with Cisco Firepower Next Generation IPS (SSFIPS). As with all of our Cisco Training Experiences – exams are delivered in the classroom.

SSNGFW

This portion of the course prepares students with the 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). Students 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. Students 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.

SSFIPS

This portion of the course gives students the knowledge and skills to use the NGIPS 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 students prepare to take the Securing Networks with Cisco Firepower (300-710 SNCF) exam, which leads to CCNP Security and Cisco Certified Specialist - Network Security Firepower certifications.

CISCO CERTIFIED NETWORK PROFESSIONAL SECURITY FIREPOWER

Securing Networks with Cisco Firepower Next Generation Firewall (SSNGFW)
Securing Networks with Cisco Firepower Next Generation IPS (SSFIPS)

Course Objectives SSNGFW

After taking this course, students should be able to:

- 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
- Implement Cisco Firepower NGFW to provide advanced threat protection before, during, and after attacks
- Gain leading-edge skills for high-demand responsibilities focused on security

Course Objectives SSFIPS

After taking this course, students should be able to:

- 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
- 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

THINQTANK® LEARNING

CISCO CERTIFIED NETWORK PROFESSIONAL SECURITY FIREPOWER

Securing Networks with Cisco Firepower Next Generation Firewall (SSNGFW)
Securing Networks with Cisco Firepower Next Generation IPS (SSFIPS)

SSNGFW Course Modules

1
- Cisco Firepower Threat Defense Overview
  - Examining Firewall and IPS Technology
  - Firepower Threat Defense Features and Components
  - Examining Firepower Platforms
  - Examining Firepower Threat Defense Licensing
  - Cisco Firepower Implementation Use Cases

2
- Cisco Firepower NGFW Device Configuration
  - Firepower Threat Defense Device Registration
  - FXOS and Firepower Device Manager
  - Initial Device Setup
  - Managing NGFW Devices
  - Examining Firepower Management Center Policies
  - Examining Objects
  - Examining System Configuration and Health Monitoring
  - Device Management
  - Examining Firepower High Availability
  - Configuring High Availability
  - Cisco ASA to Firepower Migration
  - Migrating from Cisco ASA to Firepower Threat Defense

3
- Cisco Firepower NGFW Traffic Control
  - Firepower Threat Defense Packet Processing
  - Implementing QoS
  - Bypassing Traffic

4
- Cisco Firepower NGFW Address Translation
  - NAT Basics
  - Implementing NAT
  - NAT Rule Examples
  - Implementing NAT

5
- Cisco Firepower Discovery
  - Examining Network Discovery
  - Configuring Network Discovery

6
- Implementing Access Control Policies
  - Examining Access Control Policies
  - Examining Access Control Policy Rules and Default Action
  - Implementing Further Inspection
  - Examining Connection Events
  - Access Control Policy Advanced Settings
  - Access Control Policy Considerations
  - Implementing an Access Control Policy

7
- Security Intelligence
  - Examining Security Intelligence
  - Examining Security Intelligence Objects
  - Security Intelligence Deployment and Logging
  - Implementing Security Intelligence

8
- File Control and Advanced Malware Protection
  - Examining Malware and File Policy
  - Examining Advanced Malware Protection

9
- Next-Generation Intrusion Prevention Systems
  - Examining Intrusion Prevention and Snort Rules
  - Examining Variables and Variable Sets

10
- Site-to-Site VPN
  - Examining IPsec
  - Site-to-Site VPN Configuration
  - Site-to-Site VPN Troubleshooting
  - Implementing Site-to-Site VPN

11
- Remote-Access VPN
  - Examining Remote-Access VPN
  - Examining Public-Key Cryptography and Certificates
  - Examining Certificate Enrollment
  - Remote-Access VPN Configuration
  - Implementing Remote-Access VPN

12
- SSL Decryption
  - Examining SSL Decryption
  - Configuring SSL Policies
  - SSL Decryption Best Practices and Monitoring

13
- Detailed Analysis Techniques
  - Examining Event Analysis
  - Examining Event Types
  - Examining Contextual Data
  - Examining Analysis Tools
  - Threat Analysis

14
- System Administration
  - Managing Updates
  - Examining User Account Management Features
  - Configuring User Accounts
  - System Administration

15
- Cisco Firepower Troubleshooting
  - Examining Common Misconfigurations
  - Examining Troubleshooting Commands
  - Firepower Troubleshooting

THINQTANK® LEARNING

CISCO CERTIFIED NETWORK PROFESSIONAL SECURITY FIREPOWER

Securing Networks with Cisco Firepower Next Generation Firewall (SSNGFW)
Securing Networks with Cisco Firepower Next Generation IPS (SSFIPS)

SSNGFW Labs and Demonstrations

L

- Initial Device Setup
- Device Management
- Configuring High Availability
- Migrating from Cisco ASA to Cisco Firepower Threat Defense
- Implementing QoS
- Implementing NAT
- Configuring Network Discovery
- Implementing an Access Control Policy
- Implementing Security Intelligence
- Implementing Site-to-Site VPN
- Implementing Remote Access VPN
- Threat Analysis
- System Administration
- Firepower Troubleshooting

SSFIPS Course Topics

- Initial Device Setup
- Device Management
- Configuring High Availability
- Migrating from Cisco ASA to Cisco Firepower Threat Defense
- Implementing QoS
- Implementing NAT
- Configuring Network Discovery
- Implementing an Access Control Policy
- Implementing Security Intelligence
- Implementing Site-to-Site VPN
- Implementing Remote Access VPN
- Threat Analysis
- System Administration
- Firepower Troubleshooting

SSFIPS Labs and Demonstrations

L

- Initial Device Setup
- Device Management
- Implementing Network Discovery
- Implementing an 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
- Performing System Administration
- Troubleshooting Cisco Firepower

CISCO CERTIFIED NETWORK PROFESSIONAL SECURITY FIREPOWER

Securing Networks with Cisco Firepower Next Generation Firewall (SSNGFW)
Securing Networks with Cisco Firepower Next Generation IPS (SSFIPS)

thinQtank® Global, Inc. dba thinQtank® Learning P.O. Box 803215, Valencia, CA 91380 USA
Tel 855-TO-THINQ Fax 208-979-0668 www.thinqtanklearning.com