

CISCO CCNP SECURITY

Securing Networks with Cisco Firepower Next Generation Firewall (SSNGFW)

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

- Five days of instructor-led learning
- 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 five-day training camp for Securing Networks with Cisco Firepower Next Generation Firewall (SSNGFW). As with all of our Cisco Training Experiences – exams are delivered in the classroom.

This 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.

Course Objectives

After taking this course, students should be able to:

- Describe key concepts of NGIPS and NGFW technology and Cisco Firepower Threat Defense system, 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

CISCO CCNP SECURITY

Securing Networks with Cisco Firepower Next Generation Firewall (SSNGFW)

Course Modules

- | | | | |
|----------|---|-----------|---|
| 1 | <ul style="list-style-type: none"> ▪ 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 | 8 | <ul style="list-style-type: none"> ▪ File Control and Advanced Malware Protection ▪ Examining Malware and File Policy ▪ Examining Advanced Malware Protection |
| 2 | <ul style="list-style-type: none"> ▪ 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 | 9 | <ul style="list-style-type: none"> ▪ Next-Generation Intrusion Prevention Systems ▪ Examining Intrusion Prevention and Snort Rules ▪ Examining Variables and Variable Sets |
| 3 | <ul style="list-style-type: none"> ▪ Cisco Firepower NGFW Traffic Control ▪ Firepower Threat Defense Packet Processing ▪ Implementing QoS ▪ Bypassing Traffic | 10 | <ul style="list-style-type: none"> ▪ Site-to-Site VPN ▪ Examining IPsec ▪ Site-to-Site VPN Configuration ▪ Site-to-Site VPN Troubleshooting ▪ Implementing Site-to-Site VPN |
| 4 | <ul style="list-style-type: none"> ▪ Cisco Firepower NGFW Address Translation ▪ NAT Basics ▪ Implementing NAT ▪ NAT Rule Examples ▪ Implementing NAT | 11 | <ul style="list-style-type: none"> ▪ Remote-Access VPN ▪ Examining Remote-Access VPN ▪ Examining Public-Key Cryptography and Certificates ▪ Examining Certificate Enrollment ▪ Remote-Access VPN Configuration ▪ Implementing Remote-Access VPN |
| 5 | <ul style="list-style-type: none"> ▪ Cisco Firepower Discovery ▪ Examining Network Discovery ▪ Configuring Network Discovery | 12 | <ul style="list-style-type: none"> ▪ SSL Decryption ▪ Examining SSL Decryption ▪ Configuring SSL Policies ▪ SSL Decryption Best Practices and Monitoring |
| 6 | <ul style="list-style-type: none"> ▪ 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 | 13 | <ul style="list-style-type: none"> ▪ Detailed Analysis Techniques ▪ Examining Event Analysis ▪ Examining Event Types ▪ Examining Contextual Data ▪ Examining Analysis Tools ▪ Threat Analysis |
| 7 | <ul style="list-style-type: none"> ▪ Security Intelligence ▪ Examining Security Intelligence ▪ Examining Security Intelligence Objects ▪ Security Intelligence Deployment and Logging ▪ Implementing Security Intelligence | 14 | <ul style="list-style-type: none"> ▪ System Administration ▪ Managing Updates ▪ Examining User Account Management Features ▪ Configuring User Accounts ▪ System Administration |
| | | 15 | <ul style="list-style-type: none"> ▪ Cisco Firepower Troubleshooting ▪ Examining Common Misconfigurations ▪ Examining Troubleshooting Commands ▪ Firepower Troubleshooting |

CISCO CCNP SECURITY

Securing Networks with Cisco Firepower Next Generation Firewall (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

CISCO CCNP SECURITY

Securing Networks with Cisco Firepower Next Generation Firewall (SSNGFW)



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

© 2020 thinQtank® Global, Inc. All rights reserved. The product or learning materials are protected by U.S. and intellectual property laws. thinQtank Global, thinQtank Learning and the Q-Man logo are registered trademarks of thinQtank Global, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

thinQtank Global, Inc. warrants that it will perform these training services in a reasonable manner using generally accepted industry standards and practices. THE EXPRESS WARRANTY SET FORTH IS IN LIEU OF ALL OTHER WARRANTIES, EXPRESS, IMPLIED, STATUTORY OR OTHERWISE INCLUDING IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE WITH RESPECT TO THE SERVICES AND DELIVERABLES PROVIDED BY THINQTANK GLOBAL, INC., OR AS TO THE RESULTS WHICH MAY BE OBTAINED THEREFROM. THINQTANK GLOBAL, INC. WILL NOT BE LIABLE FOR ANY THIRD-PARTY SERVICES OR PRODUCTS IDENTIFIED OR REFERRED TO CUSTOMER. All materials provided in this training are copyrighted by thinQtank Global, Inc. ("Learning Materials"). thinQtank Global, Inc. grants the customer of this learning a license to use Learning Materials strictly for the purpose of facilitating such company's internal understanding, utilization and operation of the technology covered herein. Except as set forth expressly in the sentence above, there is no transfer of any intellectual property rights or any other license granted under the terms of this training.