Fundamentals of Cisco Firewall Threat Defense and Intrusion Prevention

Course Description (full version)

The Fundamentals of Cisco Firewall Threat Defense and Intrusion Prevention (SFWIPF) training shows you how to implement and configure Cisco Secure Firewall Threat Defense for deployment as a next generation firewall at the internet edge. You'll gain an understanding of Cisco Secure Firewall architecture and deployment, base configuration, packet processing and advanced options, and conducting Secure Firewall administration troubleshooting.
This training prepares you for the CCNP Security certification, which requires passing the 350-701 Implementing and Operating Cisco Security Core Technologies (SCOR) core exam and one concentration exam such as the 300-710 Securing Networks with Cisco Firepower (SNCF) concentration exam. This training also earns you 40 Continuing Education (CE) credits towards recertification.

How You'll Benefit

This training will teach you how to implement, configure, and manage Cisco Secure Firewall Threat Defense for deployment, including:

- Configure settings and policies on Cisco Secure Firewall Threat Defense
- Gain an understanding of Cisco Secure Firewall Threat Defense policies and explain how different policies influence packet processing through the device
- Perform basic threat analysis and administration tasks using Cisco Secure Firewall Management Center

Who Should Enroll

- Network security engineers
- Administrators

What to Expect in the Exam

350-701 SCOR: Implementing and Operating Cisco Security Core Technologies is a 120-minute exam associated with the CCNP Security certification. The multiple-choice format tests knowledge and skills related to implementing and operating core security technologies, including:

- Network security
- Cloud security
- Content security
- Endpoint protection and detection
- Secure network access
- Visibility and enforcement

300-710 SNCF: Securing Networks with Cisco Firepower is a 90-minute exam associated with the CCNP Security certification. The multiple-choice format tests knowledge of Cisco Firepower® Threat Defense and Firepower® 7000 and 8000 Series virtual appliances, including:

- Policy configurations
- Integrations
- Deployments
- Management and troubleshooting

Course Objectives

- Describe Cisco Secure Firewall Threat Defense
- Describe Cisco Secure Firewall Threat Defense Deployment Options
- Describe management options for Cisco Secure Firewall Threat Defense
- Configure basic initial settings on Cisco Secure Firewall Threat Defense
- Configure high availability on Cisco Secure Firewall Threat Defense

- Configure basic Network Address Translation on Cisco Secure Firewall Threat Defense
- Describe Cisco Secure Firewall Threat Defense policies and explain how different policies influence packet processing through the device
- Configure Discovery Policy on Cisco Secure Firewall Threat Defense
- Configure and explain prefilter and tunnel rules in prefilter policy
- Configure an access control policy on Cisco Secure Firewall Threat Defense
- Configure security intelligence on Cisco Secure Firewall Threat Defense
- Configure file policy on Cisco Secure Firewall Threat Defense
- Configure Intrusion Policy on Cisco Secure Firewall Threat Defense
- Perform basic threat analysis using Cisco Secure Firewall Management Center
- Perform basic management and system administration tasks on Cisco Secure Firewall Threat Defense
- Perform basic traffic flow troubleshooting on Cisco Secure Firewall Threat Defense
- Manage Cisco Secure Firewall Threat Defense with Cisco Secure Firewall Threat Defense Manager

Course Prerequisites

Before taking this offering, you should understand:

- TCP/IP
- Basic routing protocols
- Firewall, VPN, and IPS concepts

Course Outline

1. Introducing Cisco Secure Firewall Threat Defense
2. Describing Cisco Secure Firewall Threat Defense Deployment Options
3. Describing Cisco Secure Firewall Threat Defense Management Options
4. Configuring Basic Network Settings on Cisco Secure Firewall Threat Defense
5. Configuring High Availability on Cisco Secure Firewall Threat Defense
6. Configuring Auto NAT on Cisco Secure Firewall Threat Defense
7. Describing Packet Processing and Policies on Cisco Secure Firewall Threat Defense
8. Configuring Discovery Policy on Cisco Secure Firewall Threat Defense

9. Configuring Prefilter Policy on Cisco Secure Firewall Threat Defense
10. Configuring Access Control Policy on Cisco Secure Firewall Threat Defense
11. Configuring Security Intelligence on Cisco Secure Firewall Threat Defense
12. Configuring File Policy on Cisco Secure Firewall Threat Defense
13. Configuring Intrusion Policy on Cisco Secure Firewall Threat Defense
14. Performing Basic Threat Analysis on Cisco Secure Firewall Management Center
15. Managing Cisco Secure Firewall Threat Defense System
16. Troubleshooting Basic Traffic Flow
17. Cisco Secure Firewall Threat Defense Device Manager

Lab Outline

1. Perform Initial Device Setup
2. Configure High Availability
3. Configure Network Address Translation
4. Configure Network Discovery
5. Configure Prefilter and Access Control Policy
6. Configure Security Intelligence
7. Implement File Control and Advanced Malware Protection
8. Configure Cisco Secure IPS
9. Detailed Analysis Using the Firewall Management Center
10. Manage Cisco Secure Firewall Threat Defense System
11. Secure Firewall Troubleshooting Fundamentals
12. Configure Managed Devices Using Cisco Secure Firewall Device Manager