

Fundamentals of Cisco Firewall Threat Defense and Intrusion Prevention

Duration: 5 Days Course Code: SFWIPF Version: 1.0

Overview:

This Fundamentals of Cisco Firewall Threat Defense and Intrusion Prevention (SFWIPF) course 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 course is worth 40 Continuing Education (CE) credits towards recertification.

Virtual Learning

This interactive training can be taken from any location, your office or home and is delivered by a trainer. This training does not have any delegates in the class with the instructor, since all delegates are virtually connected. Virtual delegates do not travel to this course, Global Knowledge will send you all the information needed before the start of the course and you can test the logins.

Objectives:

■ After completing this course you should be able to:

- 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

Prerequisites:

Attendees should meet the following prerequisites:

- TCP/IP
- Basic routing protocols
- Firewall, VPN, and IPS concepts
- CCNA - Implementing and Administering Cisco Solutions
- SCOR - Implementing and Operating Cisco Security Core

Testing and Certification

Recommended as preparation for the following exam:

- 300-710 - Securing Networks with Cisco Firewall Exam
- Exam topics are current spread over two courses SSNGFW and SSFIPS, these are being replaced with SFWIPF and SFWIPA

Content:

| | | |
|---|---|--|
| Introducing Cisco Secure Firewall Threat Defense | Configuring Security Intelligence on Cisco Secure Firewall Threat Defense | Lab 3: Configure Network Address Translation |
| Describing Cisco Secure Firewall Threat Defense Deployment Options | Configuring File Policy on Cisco Secure Firewall Threat Defense | Lab 4: Configure Network Discovery |
| Describing Cisco Secure Firewall Threat Defense Management Options | Configuring Intrusion Policy on Cisco Secure Firewall Threat Defense | Lab 5: Configure Prefilter and Access Control Policy |
| Configuring Basic Network Settings on Cisco Secure Firewall Threat Defense | Performing Basic Threat Analysis on Cisco Secure Firewall Management Center | Lab 6: Configure Security Intelligence |
| Configuring High Availability on Cisco Secure Firewall Threat Defense | Managing Cisco Secure Firewall Threat Defense System | Lab 7: Implement File Control and Advanced Malware Protection |
| Configuring Auto NAT on Cisco Secure Firewall Threat Defense | Troubleshooting Basic Traffic Flow | Lab 8: Configure Cisco Secure IPS |
| Describing Packet Processing and Policies on Cisco Secure Firewall Threat Defense | Cisco Secure Firewall Threat Defense Device Manager | Lab 9: Detailed Analysis Using the Firewall Management Center |
| Configuring Discovery Policy on Cisco Secure Firewall Threat Defense | Labs: | Lab 10: Manage Cisco Secure Firewall Threat Defense System |
| Configuring Prefilter Policy on Cisco Secure Firewall Threat Defense | Lab 1: Perform Initial Device Setup | Lab 11: Secure Firewall Troubleshooting Fundamentals |
| Configuring Access Control Policy on Cisco Secure Firewall Threat Defense | Lab 2: Configure High Availability | Lab 12: Configure Managed Devices Using Cisco Secure Firewall Device Manager |

Further Information:

For More information, or to book your course, please call us on Head Office Tel.: +974 40316639

training@globalknowledge.qa

www.globalknowledge.com/en-qa/

Global Knowledge, Qatar Financial Center, Burj Doha, Level 21, P.O.Box 27110, West Bay, Doha, Qatar