Fundamentals of Cisco Firewall Threat Defense and Intrusion Prevention

Duration: 5 Days **Course Code: SFWIPF** **Version: 1.0** **Delivery Method: Company Event**

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.

Company Events

These events can be delivered exclusively for your company at our locations or yours, specifically for your delegates and your needs. The Company Events can be tailored or standard course deliveries.

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 Technologies

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

Describing Cisco Secure Firewall Threat Defense Deployment Options

Describing Cisco Secure Firewall Threat Defense Management Options

Configuring Basic Network Settings on Cisco Secure Firewall Threat Defense

Configuring High Availability on Cisco Secure Firewall Threat Defense

Configuring Auto NAT on Cisco Secure Firewall Threat Defense

Describing Packet Processing and Policies on Cisco Secure Firewall Threat Defense

Configuring Discovery Policy on Cisco Secure Firewall Threat Defense

Configuring Prefilter Policy on Cisco Secure Firewall Threat Defense

Configuring Access Control Policy on Cisco Secure Firewall Threat Defense

Configuring Security Intelligence on Cisco Secure Firewall Threat Defense

Configuring File Policy on Cisco Secure Firewall Threat Defense

Configuring Intrusion Policy on Cisco Secure Firewall Threat Defense

Performing Basic Threat Analysis on Cisco Secure Firewall Management Center

Managing Cisco Secure Firewall Threat Defense System

Troubleshooting Basic Traffic Flow

Cisco Secure Firewall Threat Defense Device Manager

Labs:

Lab 1: Perform Initial Device Setup

Lab 2: Configure High Availability

Lab 3: Configure Network Address Translation

Lab 4: Configure Network Discovery

Lab 5: Configure Prefilter and Access Control Policy

Lab 6: Configure Security Intelligence

Lab 7: Implement File Control and Advanced Malware Protection

Lab 8: Configure Cisco Secure IPS

Lab 9: Detailed Analysis Using the Firewall Management Center

Lab 10: Manage Cisco Secure Firewall Threat Defense System

Lab 11: Secure Firewall Troubleshooting Fundamentals

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 00 971 4 446 4987

training@globalknowledge.ae

www.globalknowledge.com/en-ae/

Global Knowledge, Dubai Knowledge Village, Block 2A,First Floor, Office F68, Dubai, UAE