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.

Target Audience:

Anyone deploying a Cisco Secure Firewall Threat Defense soloution.

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 currently spread over two courses SSNGFW and SSFIPS, these are being replaced with SFWIPF and SFWIPA

Content:

Introducing Cisco Secure Firewall Threat Defense

- Need for a Firewall
- Traditional Network Security and the New Reality
- Cisco Secure Portfolio
- Cisco Secure Firewall Threat Defense Features Overview
- Cisco Secure Firewall Threat Defense Platform Overview
- Cisco Secure Firewall Use Cases
- Cisco Secure Firewall Smart Licensing

Describing Cisco Secure Firewall Threat Defense Deployment Options

- Deployment Modes Overview
- Firewall Deployment Mode
- Configuring Global Interfaces
- Configuring IPS Interfaces
- Resilient and Scalable Design

Describing Cisco Secure Firewall Threat Defense Management Options

- Cisco Secure Firewall Threat Defense Management Overview
- Cisco Secure Firewall Management Center
- Cisco Secure Firewall Threat Defense Device Manager
- Cisco Defense Orchestrator

Configuring Basic Network Settings on Cisco Secure Firewall Threat Defense

- Initial Cisco Secure Firewall Threat Defense Setup
- Cisco Secure Firewall Management Center Initial Setup
- Cisco Secure Firewall Threat Defense Registration with Cisco Secure Firewall Management Center
- Cisco Secure Firewall Threat Defense Device Management
- Interfaces and Security Zones Configuration
- Static Routing Configuration
- Platform Settings Configuration
- Health Policy

Configuring High Availability on Cisco Secure Firewall Threat Defense

- Active/Standby Failover Overview
- Stateless and Stateful Failover
- Health Monitor Initiated Failover
- Active/Standby Failover Configuration
- Verify and Troubleshoot Active/Standby High Availability

Configuring Auto NAT on Cisco Secure Firewall Threat Defense

Describing Packet Processing and Policies on Cisco Secure Firewall Threat Defense

- Objects Overview
- Policies Overview
- Cisco Secure Firewall Engines and Detailed Packet Processing

Configuring Discovery Policy on Cisco Secure Firewall Threat Defense

- Discovery Policy Overview
- Network Discovery Policy Configuration
- Discovery Events and Host Profile Analysis

Configuring Prefilter Policy on Cisco Secure Firewall Threat Defense

- Prefilter Policy Overview
- Prefilter Policy Configuration
- Connection Events Analysis

Configuring Access Control Policy on Cisco Secure Firewall Threat Defense

- Access Control Policy Overview
- Access Control Policy Rules and Rule Actions
- Access Control Policy Deployment
- Access Control Policy Best Practices

Configuring Security Intelligence on Cisco Secure Firewall Threat Defense

- Security Intelligence Overview
- Security Intelligence Objects
- IP and URL Security Intelligence Configuration and Verification
- DNS Security Intelligence Configuration and Verification

Configuring File Policy on Cisco Secure Firewall Threat Defense

- File Policy Overview
- Network Malware Protection and File Type Detection Architecture
- File Policy Configuration
- Malware and File Events Analysis

Configuring Intrusion Policy on Cisco Secure Firewall Threat Defense

- IPS and Snort Introduction
- Intrusion (Snort) Rule Introduction
- Intrusion Policy Fundamentals
- Creating Customizable (User Created) IPS Policies
- Intrusion Event Overview

Performing Basic Threat Analysis on Cisco Secure Firewall Management Center

- Events Overview
- Indications of Compromise
- Content Explorer
- Dahsboards
- Reports
- Using the Unified Event Viewer
- Threat Analysis Example

Managing Cisco Secure Firewall Threat Defense System

- Update management
- User Account Management
- Backup of the System
- Configuration Export and Import
- Configuration Rollback

Troubleshooting Basic Traffic Flow

- Cisco Secure Firewall Threat Defense CLI
- Traffic Flow Troubleshooting Process and Tools
- Traffic Flow Troubleshooting Examples

Cisco Secure Firewall Threat Defense Device Manager

- Cisco Secure Firewall Threat Defense Device Manager Initial Configuration
- Cisco Secure Firewall Threat Defense Device Manager Policies Overview

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

- NAT Overview
- AutoNAT Configuration

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 0800/84.009

info@globalknowledge.be

www.globalknowledge.com/en-be/