SFWIPA - Advanced Techniques for Cisco Firewall Threat Defense and Intrusion Prevention

Days: *5*

Prerequisites: The learner should possess the following knowledge and skills before attending this course: knowledge of TCP/IP, a basic understanding of routing protocols, and familiarity with the content in the "Securing Internet Edge with Cisco Secure Firewall Threat Defense" training.

Recommended Cisco Learning Offerings:

- Implementing and Administering Cisco Solutions (CCNA)
- Securing Internet Edge with Cisco Secure Firewall Threat Defense

Audience: The primary audience for this course includes System Installers, System Integrators, System Administrators, Network Administrators, and/or Solutions Designers.

Description: The Securing Data Center Networks and VPNs with Cisco Secure Firewall Threat Defense (SFWIPA) training shows you how to deploy and configure the Cisco Secure Firewall Threat Defense system as a data center network firewall or Internet Edge firewall with VPN support. You'll learn how to configure identity-based policies, SSL decryption, remote-access VPN, and site-to-site VPN. The course also covers advanced Intrusion Prevention System (IPS) configuration, event management, integrations with other systems, troubleshooting, and automation using Application Programming Interfaces (APIs). Configuration migration from Cisco ASA is also included. This training prepares you for the 300-710 Securing Networks with Cisco Firepower (SNCF) exam and earns 40 Continuing Education (CE) credits.

Course Objectives: In this course, you will:

- Describe Cisco Secure Firewall Threat Defense
- Describe advanced deployment options and device settings
- Configure dynamic routing and advanced NAT
- Configure SSL decryption policy
- Deploy Remote Access and Site-to-Site VPN
- Deploy identity-based policies and advanced access control settings
- Describe and implement event management and integrations
- Troubleshoot traffic flow using advanced options
- Automate configuration and operations using APIs
- Perform configuration migration from Cisco ASA **OUTLINE:**
- **INTRODUCING CISCO SECURE FIREWALL THREAT DEFENSE** • **INTRODUCING CISCO SECURE FIREWALL THREAT DEFENSE**

SFWIPA - Securing Data Center Networks and VPNs with Cisco Secure Firewall Threat Defense

- DESCRIBING ADVANCED DEPLOYMENT OPTIONS
- CONFIGURING ADVANCED DEVICE SETTINGS
- CONFIGURING DYNAMIC ROUTING
- CONFIGURING ADVANCED NAT
- CONFIGURING SSL POLICY
- DEPLOYING REMOTE ACCESS VPN
- DEPLOYING IDENTITY-BASED POLICIES
- DEPLOYING SITE-TO-SITE VPN
- CONFIGURING SNORT RULES AND NETWORK ANALYSIS POLICIES
- DESCRIBING ADVANCED EVENT MANAGEMENT
- DESCRIBING INTEGRATIONS
- TROUBLESHOOTING ADVANCED TRAFFIC FLOW
- AUTOMATING CISCO SECURE FIREWALL THREAT DEFENSE
- MIGRATING TO CISCO SECURE FIREWALL THREAT DEFENSE

LAB OUTLINE

- DEPLOY ADVANCED CONNECTION SETTINGS
- CONFIGURE DYNAMIC ROUTING
- CONFIGURE SSL POLICY
- CONFIGURE REMOTE ACCESS VPN
- CONFIGURE SITE-TO-SITE VPN
- CUSTOMIZE IPS AND NAP POLICIES
- CONFIGURE CISCO SECURE FIREWALL THREAT DEFENSE INTEGRATIONS
- TROUBLESHOOT CISCO SECURE FIREWALL THREAT DEFENSE
- MIGRATE CONFIGURATION FROM CISCO SECURE FIREWALL ASA