SFWIPF - Fundamentals of Cisco Firewall Threat Defense and Intrusion Prevention

Days: 5

Prerequisites: Before taking this offering, you should understand: TCP/IP, basic routing protocols, Firewall, VPN, and IPS concepts.

Audience: This class is recommended for network security engineers and administrators.

Description: 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.

Course Objectives: In this course, you will:

- Cisco Secure Firewall Threat Defense Overview: Description, deployment options, and management choices.
- Basic Configuration: Initial settings, high availability, and Network Address Translation (NAT) setup.
- Policies & Rules: Overview of policies, packet processing, Discovery Policy, prefilter, tunnel, and access control rules.
- Advanced Security: Configure security intelligence, file policy, and Intrusion Policy.
- Threat Management: Perform basic threat analysis and traffic troubleshooting.
- Administration: Manage system tasks and traffic with Cisco Secure Firewall Management Center and Threat Defense Manager.

OUTLINE:

- **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**

SFWIPF - Fundamentals of Cisco Firewall Threat Defense and Intrusion Prevention

- 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

LAB OUTLINE:

- PERFORM INITIAL DEVICE SETUP
- CONFIGURE HIGH AVAILABILITY
- CONFIGURE NETWORK ADDRESS TRANSLATION
- CONFIGURE NETWORK DISCOVERY
- CONFIGURE PREFILTER AND ACCESS CONTROL POLICY
- CONFIGURE SECURITY INTELLIGENCE
- IMPLEMENT FILE CONTROL AND ADVANCED MALWARE PROTECTION
- CONFIGURE CISCO SECURE IPS
- DETAILED ANALYSIS USING THE FIREWALL MANAGEMENT CENTER
- MANAGE CISCO SECURE FIREWALL THREAT DEFENSE SYSTEM
- SECURE FIREWALL TROUBLESHOOTING FUNDAMENTALS
- CONFIGURE MANAGED DEVICES USING CISCO SECURE FIREWALL DEVICE MANAGER