ADVANCED FIREPOWER R 1.0

5 DAYS

COURSE OUTLINE

- **Day 1:**
  - Lesson 1: Firepower System Overview and Classroom Setup
  - Lesson 2: Hardware Overview and Architecture
  - Lesson 3: Device Management

- **Day 2:**
  - Lesson 4: Firepower Discovery Technology
  - Lesson 5: Object Management
  - Lesson 6: Access Control Policy

- **Day 3:**
  - Lesson 7: Implementing Security Intelligence
  - Lesson 8: File Control and Advanced Malware Protection
  - Lesson 9: Implementing NGIPS
  - Lesson 10: Preprocessor Tuning

- **Day 4:**
  - Lesson 11: Event Analysis
  - Lesson 12: System Administration
  - Lesson 13: Correlation Policies

- **Day 5:**
  - Lesson 14: Remote Access AnyConnect VPN
  - Lesson 15: Site-to-Site VPN
  - Lesson 16: High Availability

- **Labs:**
  - Lab 1: Connecting to the Lab Environment
    > Task 1.1: Connect to the lab
    > Task 1.2: Test Lab Equipment's Connectivity

  - Lab 2: Navigate using the Firepower Management Center (FMC) GUI
    > Task 2.1: Connect to the Firepower Management Center (FMC) GUI changing password and time settings
    > Task 2.2: Getting familiar with the Firepower Management Center (FMC) GUI
    > Task 2.3: Creating a user account and enable evaluation license in the Firepower Management Center (FMC) GUI

  - Lab 3: Manage the virtual Firepower Threat Defense (vFTD) device individually and through the Firepower Management Console (FMC) GUI
    > Task 3.1: Connect to the virtual Firepower Threat Defense (vFTD) device named vFTD1 to manage it using its local GUI
    > Task 3.2: Connect the virtual Firepower Threat Defense (vFTD1) to the Firepower Management Center (FMC) GUI for remote management
    > Task 3.3: Add a Health Policy in the Firepower Management Center (FMC) GUI for the virtual Firepower Threat Defense (vFTD1)
    > Task 3.4: Add a Platform Settings Policy in the Firepower Management Center (FMC) GUI for the virtual Firepower Threat Defense (vFTD1)
    > Task 3.5: Configure interfaces, static routing and add a NAT Policy in the Firepower Management Center (FMC) GUI for the virtual Firepower Threat Defense (vFTD1)

  - Lab 4: Implementing Network Discovery
    > Task 4.1: Create and test a Network Discovery Policy
    > Task 4.2: Configure User Discovery Policy using Active Directory create Host Attributes

  - Lab 5: Implementing Object Management to Prepare for Access Control Policy
    > Task 5.1: Navigating the Objects Section
    > Task 5.2: Creating Objects and Object Groups for Networks, Ports and URLs

- Lab 6: Implementing Access Control Policies
  > Task 6.1: Control Internet Connections to Specific Applications using an Access Control Policy
  > Task 6.2: Controlling In-Between Zones traffic with Layer 7 Filtering
  > Task 6.3: Add a Deny Access Message and IPS Policy to Access Control Policy

- Lab 7: Implementing Security Intelligence
  > Task 7.1: Configuring and Deploying Security Intelligence Feeds
  > Task 7.2: Block a Connection Manually using Whitelisting and Blacklisting

- Lab 8: Implementing file control and Advanced Malware Protection Policies
  > Task 8.1: Create a File Policy to Lookup for Malware and Control access to various File Types

- Lab 9: Implementing NGIPS
  > Task 9.1: Create an Intrusion Prevention policy using Firepower Recommendations

- Lab 10: Implementing Pre-processor Rules
  > Task 10.1: Create a Pre-processor Rule to Insect Traffic

- Lab 11: Detailed Analysis

- Lab 12: System Administration
  > Task 12.1: Schedule a Policy Deployment, Automate Firepower Recommendation Updates, and Backup the FMC
  > Task 12.2: Create External Authentication Object

- Lab 13: Correlation Policies
  > Task 13.1: Create a Correlation Policy Based on Connection Events

- Lab 14: Remote Access AnyConnect VPN
  > Task 14.1: Establish a Remote Access AnyConnect VPN

- Lab 15: Site to Site VPN
  > Task 15.1: Establish a Site to Site VPN

- Lab 16: Implementing High Availability
  > Task 16.1: Create a High Availability Pair