FUNDAMENTALS OF CISCO FIREWALL THREAT DEFENSE AND INTRUSION PREVENTION 1.0 (SFWIPF)

FUNDAMENTALS OF CISCO FIREWALL THREAT DEFENSE AND INTRUSION PREVENTION 1.0 (SFWIPF)

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.

How you'll benefit

This class will help you:

- Configure settings and policies on Cisco Secure Firewall Threat Defense
- Gain an understanding of Cisco Secure Firewall Threat Defense policies and explain how different policies influence packet processing through the device
- Perform basic threat analysis and administration tasks using Cisco Secure Firewall Management Center

Why Attend with Current Technologies CLC

- Our Instructors are in the top 10% rated by Cisco
- Our Lab has a dedicated 1 Gig Fiber Connection for our Labs
- Our Labs run up to Date Code for all our courses

Who Should Attend

The primary audience for this course is as follows:

- Network Security Engineers
- Administrators

Course Duration
5 days
Course Price
$3,995.00 or 40 CLCs
Methods of Delivery
- Instructor Led
- Virtual ILT
- On-Site

OUTLINE

Module 1: Introducing Cisco Secure Firewall Threat Defense

Module 2: Describing Cisco Secure Firewall Threat Defense Deployment Options

Module 3: Describing Cisco Secure Firewall Threat Defense Management Options

Module 4: Configuring Basic Network Settings on Cisco Secure Firewall Threat Defense

Module 5: Configuring High Availability on Cisco Secure Firewall Threat Defense

Module 6: Configuring Auto NAT on Cisco Secure Firewall Threat Defense

Module 7: Describing Packet Processing and Policies on Cisco Secure Firewall Threat Defense

Module 8: Configuring Discovery Policy on Cisco Secure Firewall Threat Defense

Module 9: Configuring Prefilter Policy on Cisco Secure Firewall Threat Defense

Module 10: Configuring Access Control Policy on Cisco Secure Firewall Threat Defense

Module 11: Configuring Security Intelligence on Cisco Secure Firewall Threat Defense

Module 12: Configuring File Policy on Cisco Secure Firewall Threat Defense

Module 13: Configuring Intrusion Policy on Cisco Secure Firewall Threat Defense

Module 14: Performing Basic Threat Analysis on Cisco Secure Firewall Management Center

Module 15: Managing Cisco Secure Firewall Threat Defense System

Module 16: Troubleshooting Basic Traffic Flow

Module 17: Cisco Secure Firewall Threat Defense Device Manager

LAB OUTLINE

- **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**