Fundamentals of Cisco Firewall Threat Defense and Intrusion Prevention (CPLL-SFWIPF)

Duration: 180 days

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.

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 training also earns you 40 Continuing Education (CE) credits towards recertification.

Skills You'll Learn

- Understand how to deploy and manage Cisco Secure Firewall Threat Defense system
- Learn to configure network settings on Cisco Secure Firewall
- Understand the packet processing flow and policy types used in Cisco Secure Firewall for traffic control and inspection
- Learn to configure policies within Cisco Secure Firewall Threat Defense
- Identify and troubleshoot common issues related to traffic flow, connectivity, packet drops, and performance bottlenecks on the Cisco Secure Firewall
- Learn to use the Cisco Secure Firewall Threat Defense Manager to streamline deployment and simplify policy management

Learning Path Objectives

- 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