Securing Networks with Cisco Firepower Next-Generation IPS

Course Code	SSFIPS
Duration	5 days

Overview

The Securing Networks with Cisco Firepower Next-Generation IPS course shows you how to deploy and use Cisco Firepower Next-Generation Intrusion Prevention System (NGIPS). This hands-on course gives you the knowledge and skills required to use the platform features and includes firewall security concepts, platform architecture and key features; in-depth event analysis including detection of network-based malware and file type, NGIPS tuning and configuration including application control, security intelligence, firewall, and network-based malware and file controls; Snort® rules language; file and malware inspection, security intelligence, and network analysis policy configuration designed to detect traffic patterns; configuration and deployment of correlation policies to take action based on events detected; troubleshooting; system and user administration tasks, and more.

Audience

Technical professionals who need to know how to deploy and manage a Cisco FirePower NGIPS in their network environment.

Learning Objectives

By actively participating in this course, you will learn about the following:

- Describing the components of Cisco Firepower Threat Defense and the managed device registration process.
- Detailing Next-Generation Firewalls (NGFW) traffic control and configuring the Cisco Firepower system for network discovery.
- Implementing access control policies and describing access control policy advanced features.
- Configuring security intelligences features and the Advanced Malware Protection (AMP) for Networks implementation procedure for file control and advanced malware protection.
- Implementing and managing intrusion and network analysis policies for NGIPS inspection.
- Describing and demonstrating the detailed analysis techniques and reporting features provided by the Cisco Firepower Management Center.
- Integrating the Cisco Firepower Management Center with an external logging destination.
- Describing and demonstrating the external alerting options available to Cisco Firepower Management Center and configuring a correlation policy.
- Describing key Cisco Firepower Management Center software update and user account management features.
- Identifying commonly misconfigured settings within the Cisco Firepower Management Center and using basic commands to troubleshoot a Cisco Firepower Threat Defense device.

Pre-Requisites

- Technical understanding of TCP/IP networking and network architecture
- Basic familiarity with the concepts of intrusion detection systems (IDS) and IPS
- CCNA Security (ICND1 and IINS) recommended.

Recommended courses:
- SCOR - Implementing and Operating Cisco Security Core Technologies

Course Contents

- ▶▶ Cisco Firepower Threat Defense Overview
- ▶▶ Cisco Firepower NGFW Device Configuration
- ▶▶ Cisco Firepower NGFW Traffic Control
- ▶▶ Cisco Firepower Discovery
- ▶▶ Implementing Access Control Policies
- ▶▶ Security Intelligence
- ▶▶ File Control and Advanced Malware Protection
- ▶▶ Next-Generation Intrusion Prevention Systems
- ▶▶ Network Analysis Policies
- ▶▶ Detailed Analysis Techniques
- ▶▶ Cisco Firepower Platform Integration
- ▶▶ Alerting and Correlation Policies
- ▶▶ System Administration
- ▶▶ Cisco Firepower Troubleshooting

Labs
- ▶▶ Initial Device Setup
- ▶▶ Device Management
- ▶▶ Configuring Network Discovery
- ▶▶ Implementing and Access Control Policy
- ▶▶ Implementing Security Intelligence
- ▶▶ File Control and Advanced Malware Protection
- ▶▶ Implementing NGIPS
- ▶▶ Customizing a Network Analysis Policy
- ▶▶ Detailed Analysis
- ▶▶ Configuring Cisco Firepower Platform Integration with Splunk
- ▶▶ Configuring Alerting and Event Correlation
- ▶▶ System Administration
- ▶▶ Cisco Firepower Troubleshooting

Exam Details
This course is currently not aligned to an exam.

Further Information
For more information or to book this course, please contact our Course Enquiries Team on
01752 227330 (Option 2) or email us at **enquiries@skilltec.co.uk**.