

Securing Networks with Cisco Firepower Next - Generation IPS

Duration: 5 Days **Course Code: SSFIPS** **Version: 4.0**

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.

Target Audience:

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

Objectives:

- **After completing this course, you should be able to:**
- Describe the components of Cisco Firepower Threat Defense and the managed device registration process
- Detail Next-Generation Firewalls (NGFW) traffic control and configure the Cisco Firepower system for network discovery
- Implement access control policies and describe access control policy advanced features
- Configure security intelligences features and the Advanced Malware Protection (AMP) for Networks implementation procedure for file control and advanced malware protection
- Implement and manage intrusion and network analysis policies for NGIPS inspection
- Describe and demonstrate the detailed analysis techniques and reporting features provided by the Cisco Firepower Management Center
- Integrate the Cisco Firepower Management Center with an external logging destination
- Describe and demonstrate the external alerting options available to Cisco Firepower Management Center and configure a correlation policy
- Describe key Cisco Firepower Management Center software update and user account management features
- Identify commonly misconfigured settings within the Cisco Firepower Management Center and use basic commands to troubleshoot a Cisco Firepower Threat Defense device

Prerequisites:

Attendees should meet the following prerequisites:

- 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.
- CCNABC - Cisco Certified Network Associate Fast Track
- ICND1 - Interconnecting Cisco Networking Devices Part 1
- IINS - Implementing Cisco Network Security V3.0
- SCOR - Implementing and Operating Cisco Security Core Technologies
- SFNDU - Understanding Cisco Security Foundations

Testing and Certification

Recommended as preparation for exams:

- This course is currently not aligned to an exam.

Follow-on-Courses:

■ SSNGFW - Securing Networks with Cisco Firepower Next Generation Firewall

Content:

Cisco Firepower Threat Defense Overview	Security Intelligence	Cisco Firepower Platform Integration
Cisco Firepower NGFW Device Configuration	File Control and Advanced Malware Protection	Alerting and Correlation Policies
Cisco Firepower NGFW Traffic Control	Next-Generation Intrusion Prevention Systems	System Administration
Cisco Firepower Discovery	Network Analysis Policies	Cisco Firepower Troubleshooting
Implementing Access Control Policies	Detailed Analysis Techniques	Labs: <ul style="list-style-type: none">■ Lab1: Initial Device Setup■ Lab 2: Device Management■ Lab 3: Configuring Network Discovery■ Lab 4: Implementing and Access Control Policy■ Lab 5: Implementing Security Intelligence■ Lab 6: File Control and Advanced Malware Protection■ Lab 7: Implementing NGIPS■ Lab 8: Customizing a Network Analysis Policy■ Lab 9: Detailed Analysis■ Lab 10: Configuring Cisco Firepower Platform Integration with Splunk■ Lab 11: Configuring Alerting and Event Correlation■ Lab 12: System Administration■ Lab 13: Cisco Firepower Troubleshooting

Further Information:

For More information, or to book your course, please call us on 00 971 4 446 4987

training@globalknowledge.ae

www.globalknowledge.com/en-ae/

Global Knowledge, Dubai Knowledge Village, Block 2A, First Floor, Office F68, Dubai, UAE