

Fundamental of Cisco Firewall Threat Defense & Intrus. Prev.

Course code: SFWIPF

The goal of this course is to provide you with a solid foundation in Firepower Threat defense NGFW technology. You will gain the competency and skills required to implement and manage a Firepower system regardless of platform. Through detailed information on policy management, traffic flow through the system, and the system architecture you will be enabled with the skills necessary to deploy and manage many of the advanced features available in the Firepower system.

Required skills

Knowledge of TCP/IP, Basic routing protocols, Familiar with a concept of Firewall, VPN and IPS concepts.

Teaching materials

Participants will receive access to an electronic version of the study materials.

Instructor

The instructors have hands-on experience, and their expertise is validated by a range of top-level international certifications. For specialized topics, we collaborate with external trainers and experts — the best in their respective fields.

Course outline

- Describe Cisco FTD
- Perform preliminary NGFW configuration tasks
- Implement NGFW traffic control
- Implementing NAT in the Cisco Firepower Management Centre
- Configure Network Discovery
- Implement an Access Control Policy
- Implement Security Intelligence
- Describe file control and advanced malware protection
- Describe next-generation IPS
- Configure and troubleshoot site-to-site VPN
- Implement Remote VPN
- Configure SSL policies
- Analyze common events in the Firepower
- Perform Firepower administration tasks
- Troubleshoot common Firepower issues

GOPAS Praha

Kodaňská 1441/46
101 00 Praha 10
Tel.: +420 234 064 900-3
info@gopas.cz

GOPAS Brno

Nové sady 996/25
602 00 Brno
Tel.: +420 542 422 111
info@gopas.cz

GOPAS Bratislava

Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 248 282 701-2
info@gopas.sk



Copyright © 2020 GOPAS, a.s.,
All rights reserved