kod szkolenia: SSFIPS / PL AA 5d

Securing Networks with Cisco Firepower Next-Generation IPS

Przeznaczenie szkolenia

The 300-710 SNCF exam certifies your knowledge of Cisco Firepower® Threat Defense and Firepower®, including policy configurations, integrations, deployments, management, and troubleshooting.
After you pass 300-710 SNCF:

- You earn the Cisco Certified Specialist – Network Security Firepower certification.
- You will have satisfied the concentration exam requirement for new CCNP Security certification. To complete CCNP Security, you also need to pass the Implementing and Operating Cisco Security Core Technologies (350-701 SCOR) exam or its equivalent.

This course is designed for technical professionals who need to know how to deploy and manage a Cisco Firepower NGIPS in their network environment.

- Security administrators
- Security consultants
- Network administrators
- System engineers
- Technical support personnel
- Channel partners and resellers

Korzyści wynikające z ukończenia szkolenia

This course will help you:

- Implement Cisco Firepower Next-Generation IPS to stop threats, address attacks, increase vulnerability prevention against suspicious files, and analyze for not-yet-identified threats
- Gain leading-edge skills focused on security
- Earn 32 CE credits for recertification

Oczekiwane przygotowanie słuchaczy

To fully benefit from this course, you should have the following knowledge and skills:

- Technical understanding of TCP/IP networking and network architecture
- Basic familiarity with the concepts of Intrusion Detection Systems (IDS) and IPS

Język szkolenia

- Szkolenie: polski
- Materiały: angielski

Czas trwania

5 dni / 35 godzin

Agenda szkolenia

Course outline

- 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
- Performing System Administration
- Troubleshooting Cisco Firepower

Lab outline

- Initial Device Setup
- Device Management
- Implementing Network Discovery
- Implementing an 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
- Performing System Administration
- Troubleshooting Cisco Firepower