Cisco Firepower Next Generation Firewall (SSNGFW v1.0) Training

Course: **00104**
Filter: **Beginner**
Duration: **5 days**
Category:: **Netwoking**
Price: **3895,00 €**

About Course

The Securing Networks with Cisco Firepower Next Generation Firewall (SSNGFW) v1.0 course shows you how to deploy and use Cisco Firepower® Threat Defense system. This hands-on course gives you knowledge and skills to use and configure Cisco® Firepower Threat Defense technology, beginning with initial device setup and configuration and including routing, high availability, Cisco Adaptive Security Appliance (ASA) to Cisco Firepower Threat Defense migration, traffic control, and Network Address Translation (NAT). You will learn how to implement advanced Next-Generation Firewall (NGFW) and Next-Generation Intrusion Prevention System (NGIPS) features, including network intelligence, file type detection, network-based malware detection, and deep packet inspection. You will also learn how to configure site-to-site VPN, remote-access VPN, and SSL decryption before moving on to detailed analysis, system administration, and troubleshooting. This course helps you prepare to take the exam, Securing Networks with Cisco Firepower (300-710 SNCF), which leads to CCNP Security and Cisco Certified Specialist – Network Security Firepower certifications. The 300-710 SNCF exam has a second preparation course as well, Securing Networks with Cisco Firepower Next-Generation Intrusion Prevention System (SSFIPS). You can take these courses in any order.

What you'll learn

- Describe key concepts of NGIPS and NGFW technology and the Cisco Firepower Threat Defense system, and identify deployment scenariosPerform initial Cisco Firepower Threat Defense device configuration and setup tasksDescribe how to manage traffic and implement quality of service (QoS) using Cisco Firepower Threat

DefenseDescribe how to implement NAT by using Cisco Firepower Threat DefensePerform an initial network discovery, using Cisco Firepower to identify hosts, applications, and servicesDescribe the behavior, usage, and implementation procedure for access control policiesDescribe the concepts and procedures for implementing security intelligence features

Targeted audience

- This course is designed for technical professionals who need to know how to deploy and manage a Cisco Firepower NGIPS and NGFW in their network environments. Targeted roles include:
- Security administrators
- Security consultants
- Network administrators
- System engineers
- Technical support personnel
- Channel partners and resellers

Pre-requisites

- Cisco recommends that you have the following knowledge and skills before taking this course:
- Technical understanding of TCP/IP networking and network architecture
- Basic familiarity with firewall and IPS concepts

Curriculum

Module 1: Cisco Firepower Threat Defense Overview

- Examining Firewall and IPS Technology
- Firepower Threat Defense Features and Components
- Examining Firepower Platforms

- Cisco Firepower Implementation Use Cases
- Cisco Firepower NGFW Device Configuration
- Firepower Threat Defense Device Registration
- FXOS and Firepower Device Manager

Module 2: Initial Device Setup

- Managing NGFW Devices
- Examining Firepower Management Center Policies
- Examining Objects
- Examining System Configuration and Health Monitoring
- Device Management
- Examining Firepower High Availability
- Configuring High Availability
- Cisco ASA to Firepower Migration
- Migrating from Cisco ASA to Firepower Threat Defense

Module 3: Cisco Firepower NGFW Traffic Control

- Firepower Threat Defense Packet Processing
- Implementing QoS
- Bypassing Traffic
- Cisco Firepower NGFW Address Translation
- NAT Basics
- Implementing NAT
- NAT Rule Examples
- Implementing NAT

Module 4: Cisco Firepower Discovery

- Examining Network Discovery
- Configuring Network Discovery
- Implementing Access Control Policies
- Examining Access Control Policies
- Examining Access Control Policy Rules and Default Action
- Implementing Further Inspection

- Examining Connection Events
- Access Control Policy Advanced Settings
- Access Control Policy Considerations
- Implementing an Access Control Policy

Module 5: Security Intelligence

- Examining Security Intelligence
- Examining Security Intelligence Objects
- Security Intelligence Deployment and Logging
- Implementing Security Intelligence

Module 6: File Control and Advanced Malware Protection

- Examining Malware and File Policy
- Examining Advanced Malware Protection
- Next-Generation Intrusion Prevention Systems
- Examining Intrusion Prevention and Snort Rules
- Examining Variables and Variable Sets
- Examining Intrusion Policies

Module 7: Site-to-Site VPN

- Examining IPsec
- Site-to-Site VPN Troubleshooting
- Implementing Site-to-Site VPN

Module 8: Remote-Access VPN

- Examining Remote-Access VPN
- Examining Public-Key Cryptography and Certificates
- Examining Certificate Enrollment
- Remote-Access VPN Configuration
- Implementing Remote-Access VPN

Module 9: SSL Decryption

- Examining SSL Decryption
- Configuring SSL Policies
- SSL Decryption Best Practices and Monitoring

Module 10: Detailed Analysis Techniques

- Examining Event Analysis
- Examining Event Types
- Examining Contextual Data
- Examining Analysis Tools
- Threat Analysis

Module 11: System Administration

- Managing Updates
- Examining User Account Management Features
- Configuring User Accounts
- System Administration

Module 12: Cisco Firepower Troubleshooting

- Examining Common Misconfigurations
- Examining Troubleshooting Commands
- Firepower Troubleshooting