Securing Networks with Cisco Firepower Next Generation Firewall

Varighed: 5 Days   Kursus Kode: SSNGFW   Version: 1.0

Beskrivelse:

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.

Målgruppe:

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.

Agenda:

- **After completing this course, you should be able to:**
- Describe key concepts of NGIPS and NGFW technology and the Cisco Firepower Threat Defense system and identify deployment scenarios
- Perform initial Firepower Threat Defense device configuration and setup tasks
- Describe how to manage traffic and implement Quality of Service (QoS) using Cisco Firepower Threat Defense
- Describe how to implement NAT by using Cisco Firepower Threat Defense
- Perform an initial network discovery, using Cisco Firepower to identify hosts, applications and services
- Describe the behavior, usage and implementation procedure for access control policies
- Describe the concepts and procedures for implementing security Intelligence features
- Describe Cisco AMP for Networks and the procedures for implementing file control and Advanced Malware Protection
- Implement and manage intrusion policies
- Describe the components and configuration of site-to-site VPN
- Describe and configure a remote-access SSL VPN that uses Cisco AnyConnect
- Describe SSL decryption capabilities and usage

Forudsætninger:

Attendees should meet the following prerequisites:

- Knowledge of TCP/IP and basic routing protocols - **ICND1** or **CCNA** Recommended
- Familiarity with firewall, vpn and IPS concepts - **IINS or SFNDU** Recommended
- CCNABC - Cisco CCNA Bootcamp
- ICND1 - Interconnecting Cisco Networking Devices - Part 1
- IINS - Implementing Cisco Network Security

Test og certificering

Recommended as preparation for the following exams:

- **300-710 SNCF** - Securing Networks with Cisco Firepower

Please note you should also attend the Securing Networks with Cisco Firepower Next-Generation Intrusion Prevention System (SSFIPS) in preparation for this exam.

- SCOR - Implementing and Operating Cisco Security Core Technologies
- SFNDU - Understanding Cisco Security Foundations

Yderligere Kurser:

The following courses is recommeneded for further study:

- **SSFIPS** - Securing Networks with Cisco Firepower Next-Generation Intrusion Prevention System
- SSFIPS - Securing Networks with Cisco Firepower Next-Generation IPS

Indhold:

Cisco Firepower Threat Defense Overview

- Examining Firewall and IPS Technology
- Firepower Threat Defense Features and Components
- Examining Firepower Platforms
- Examining Firepower Threat Defense Licensing
- Cisco Firepower Implementation Use Cases

Cisco Firepower NGFW Device Configuration

- Firepower Threat Defense Device Registration
- FXOS and Firepower Device Manager
- 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

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

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

Security Intelligence

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

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

Site-to-Site VPN

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

Remote-Access VPN

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

SSL Decryption

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

Detailed Analysis Techniques

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

System Administration

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

Cisco Firepower Troubleshooting

- Examining Common Misconfigurations
- Examining Troubleshooting Commands
- Firepower Troubleshooting

Labs

- Lab 1: Initial Device Setup
- Lab 2: Device Management
- Lab 3: Configuring High Availability
- Lab 4: Migrating from Cisco ASA to Firepower Threat Defense
- Lab 5: Implementing QoS
- Lab 6: Implementing NAT
- Lab 7: Configuring Network Discovery
- Lab 8: Implementing an Access Control Policy
- Lab 9: Implementing Security Intelligence
- Lab 10: Implementing Site-to-Site VPN
- Lab 11: Implementing Remote Access VPN
- Lab 12: Threat Analysis
- Lab 13: System Administration
- Lab 14: Firepower Troubleshooting

Flere Informationer:

For yderligere informationer eller booking af kursus, kontakt os på tlf.nr.: 44 88 18 00

training@globalknowledge.dk

www.globalknowledge.com/da-dk/

Global Knowledge, Stamholmen 110, 2650 Hvidovre