SSNGFW

Securing Networks with Cisco Firepower Next Generation Firewall

40 horas | Security | Cisco

INTRODUÇÃO

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.

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 the new CCNP Security certification. To complete your CCNP Security, you also need to pass the Implementing and Operating Cisco Security Core Technologies (350-701 SCOR) exam or its equivalent.

OBJETIVO DO CURSO

This course will help you:

• Implement Cisco Firepower NGFW to provide advanced threat protection before, during, and after attacks;

• Gain leading-edge skills for high-demand responsibilities focused on Firepower NGFW security solutions.

• Prepare student to take 300-710 SNCF exam.

After taking 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 Cisco 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 Advanced Malware Protection (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

PÚBLICO-ALVO

• Security or network professionals seeking knowledge to design, install, configure, operate, and support the Cisco Firepower NGFW Security solution;

• Professionals who need to prepare for the Cisco 300-710 certification exam.

PRÉ-REQUISITOS

To fully benefit from this course, you should have:

• Knowledge of TCP/IP and basic routing protocols;

• Desirable familiarity with firewall, VPN, and Intrusion Prevention System (IPS) security concepts.

CONTEÚDO PROGRAMÁTICO

Course Introduction

Course Outline

Course Goals & Objectives

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

Lab outline

Lab 1: Initial Device Setup

Lab 2: Device Management

Lab 3: Configuring High Availability

Lab 4: Migrating from Cisco ASA to Cisco 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