

Securing Networks with Cisco Firepower Threat Defense NGFW (FIREPOWER200) v2.0

What you'll learn in this course

The **Securing Networks with Cisco Firepower Threat Defense NGFW (FIREPOWER200) v2.0** course shows you how to deploy and use Cisco® Firepower® Threat Defense system. This hands-on course gives you the 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.

Course duration

- Instructor-led training: 5 days in the classroom with hands-on lab practice
- Virtual instructor-led training: 5 days of web-based classes with hands-on lab practice
- E-learning: 14 hours of video plus hands-on lab practice

How you'll benefit

This class 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 security

Who should enroll

The primary audience for this course is technical professionals who need to know how to deploy and manage a Cisco Firepower Threat Defense NGFW in their network environments. This class would be suitable for anyone who is replacing Cisco ASA devices with Cisco Firepower Threat Defense.

- System administrators
- Network administrators
- Solution designers
- System installers
- Cisco integrators and partners

How to enroll

- For instructor-led training, visit the [Cisco Learning Locator](#).
- For private group training, visit [Cisco Private Group Training](#).
- For e-learning volume discounts, email ask_cpl@cisco.com.
- For digital library access, visit [Cisco Platinum Learning Library](#).

Technology areas

- Security

Course details

Objectives

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

Prerequisites

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

- Knowledge of TCP/IP and basic routing protocols, and familiarity with firewall, VPN, and Intrusion Prevention System (IPS) concepts

Outline

- Cisco Firepower Threat Defense Overview
- Cisco Firepower NGFW Device Configuration
- Cisco Firepower NGFW Traffic Control
- Cisco Firepower NGFW Address Translation
- Cisco Firepower Discovery
- Implementing Access Control Policies
- Security Intelligence

- File Control and Advanced Malware Protection
- Next-Generation Intrusion Prevention Systems
- Site-to-Site VPN
- Remote-Access VPN
- SSL Decryption
- Detailed Analysis Techniques
- System Administration
- Cisco Firepower Troubleshooting

Lab outline

- Initial Device Setup
- Device Management
- Configuring High Availability
- Migrating from Cisco ASA to Cisco Firepower Threat Defense
- Implementing QoS
- Implementing NAT
- Configuring Network Discovery
- Implementing an Access Control Policy
- Implementing Security Intelligence
- Implementing Site-to-Site VPN
- Implementing Remote Access VPN
- Threat Analysis
- System Administration
- Firepower Troubleshooting



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

 Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Course content is dynamic and subject to change without notice.

© 2019 Cisco and/or its affiliates. All rights reserved.

FIREPOWER200_2-0 C22-741782-01 02/19