

Learning Services

Securing Networks with Cisco Firepower Threat Defense NGFW



The Securing Networks with Cisco Firepower Threat Defense NGFW (FIREPOWER200) course is an instructor-led, lab-based, hands-on course offered by Cisco® Learning Services. It demonstrates the powerful features of Cisco Firepower® Threat Defense, including VPN configuration, traffic control, NAT configuration, SSL decryption, advanced NGFW and NGIPS tuning and configuration, analysis, and troubleshooting.

This course will show students how to use and configure Cisco Firepower Threat Defense technology, beginning with initial device setup and configuration and including routing, high availability, Cisco ASA to Firepower Threat Defense migration, traffic control, and Network Address Translation (NAT).

The course will then explore 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.

Students 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 combines lecture materials and hands-on labs throughout to make sure that students are able to successfully deploy and manage the Cisco Firepower system.

Duration

Instructor-Led Training (ILT): 5 days.

Virtual Instructor-Led Training (VILT): 5 days.

Target audience

The primary audience for this course is system installers, system integrators, system administrators, network administrators, and solutions designers who need to know how to deploy and manage a Cisco Firepower Threat Defense NGFW in their network environments. This course focuses on the features of Firepower Threat Defense that relate to the network edge use case, where the Firepower system functions primarily as a VPN headend and security gateway. This class would be suitable for customers that are replacing Cisco ASA devices with Firepower Threat Defense.

Course objectives

Upon completion of 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

Course prerequisites

- Knowledge of TCP/IP and basic routing protocols, and familiarity with firewall, VPN, and IPS concepts

Course outline

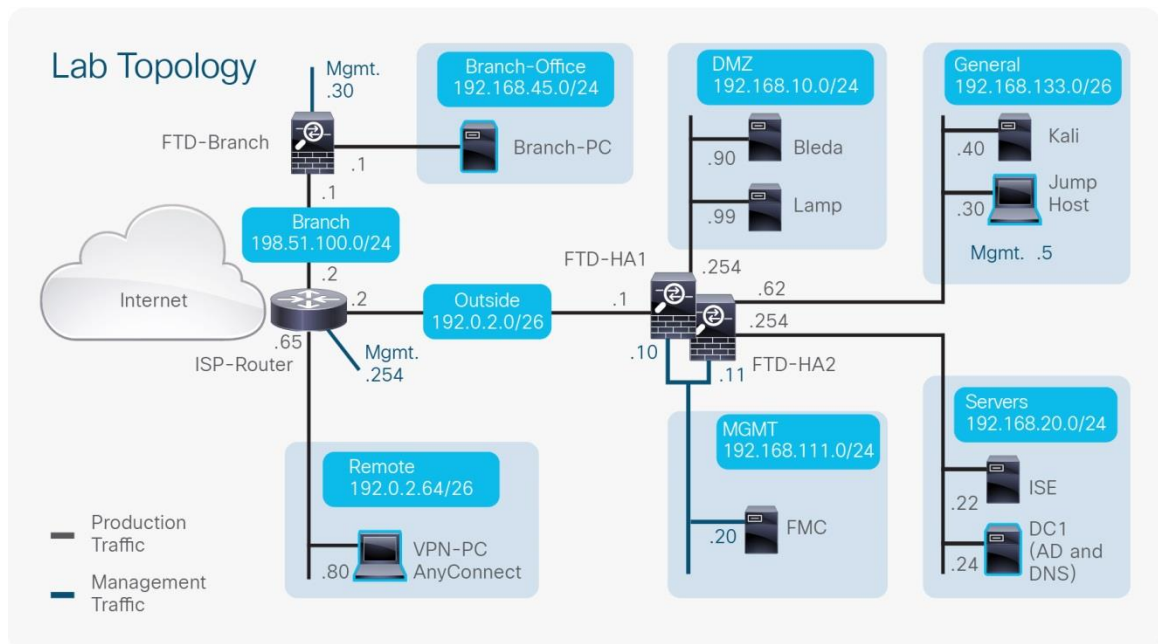
- Module 1: Cisco Firepower Threat Defense Overview
- Module 2: Firepower NGFW Device Configuration
- Module 3: Firepower NGFW Traffic Control
- Module 4: Firepower NGFW Address Translation
- Module 5: Firepower Discovery
- Module 6: Implementing Access Control Policies
- Module 7: Security Intelligence
- Module 8: File Control and Advanced Malware Protection
- Module 9: Next-Generation Intrusion Prevention Systems
- Module 10: Site-to-Site VPN

- Module 11: Remote-Access VPN
- Module 12: SSL Decryption
- Module 13: Detailed Analysis Techniques
- Module 14: System Administration
- Module 15: 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 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

Lab topology



Registration email

For more information about schedules and registration for this course, contact aeskt_registration@cisco.com.

Cisco Capital financing helps you achieve your objectives

Cisco Capital[®] financing can help you acquire the technology you need to achieve your objectives and stay competitive. We can help you reduce Capital Expenditures (CapEx), accelerate your growth, and optimize your investment dollars and ROI. Cisco Capital financing gives you flexibility in acquiring hardware, software, services, and complementary third-party equipment. And there's just one predictable payment. Cisco Capital financing is available in more than 100 countries. [Learn more](#).

Websites for more information

For more information, visit the following websites:

- Cisco Learning Services for Cisco products and technologies: <https://www.cisco.com/go/cls>
- Security training: <https://www.cisco.com/c/en/us/training-events/resources/learning-services/technology/security.html>
- Data center training: <https://www.cisco.com/c/en/us/training-events/resources/learning-services/technology/data-center.html>
- Network management training: <https://www.cisco.com/c/en/us/training-events/resources/learning-services/technology/network-management.html>
- Optical networking training: <https://www.cisco.com/c/en/us/training-events/resources/learning-services/technology/optical.html>
- Service provider mobility training: <https://www.cisco.com/c/en/us/training-events/resources/learning-services/technology/mobile.html>
- Routing training for service providers: <https://www.cisco.com/c/en/us/training-events/resources/learning-services/technology/service-provider-routing.html>
- Broadband video training for service providers: <https://www.cisco.com/c/en/us/training-events/resources/learning-services/technology/service-provider-video.html>




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 <https://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)