



Public Cloud Security

In this advanced, hands-on, two-day class, you will learn about the different components that make up the infrastructures of the top public cloud providers, and the security challenges these environments present, including high availability (HA), auto-scaling, software-defined network (SDN) connectors, and how to manage traffic in the cloud with Fortinet products.

Product Version

FortiGate 6.0

FortiWeb 6.0

Formats

- Instructor-led
- Instructor-led online

Agenda

1. Introduction to the Public Cloud
2. Fortinet Solutions for the Public Cloud
3. Fortinet Solutions for AWS
4. Fortinet Solutions for Azure
5. Fortinet Solutions for Google Cloud Platform
6. FortiCASB

Objectives

After completing this course, you will be able to:

- Deploy a FortiGate VM on Amazon Web Services (AWS) and Azure in single, HA, and auto-scaling modes
- Use Fortinet templates to easily deploy complex environments
- Deploy FortiWeb in AWS and Azure
- Use SDN connectors with cloud vendors
- Integrate other Fortinet services and products with cloud vendors

Who Should Attend

Anyone who is responsible for the deployment or day-to-day management of Fortinet solutions on cloud vendors.

Prerequisites

- General knowledge of IaaS vendors, and experience with the FortiGate and FortiWeb VMs

AWS Prerequisites

In order to run the labs on AWS, *students must have their own AWS accounts* with the following:

- A valid payment method registered on the account
- The ability to subscribe to FortiGate PAYG and FortiWeb PAYG products on the AWS marketplace
- Capacity for at least four elastic IPs and 10 vCPUs in a single region
- Permissions to create the following:
 - VPCs
 - EC2 instances
 - Security groups
 - Lambda functions
 - AIM users
 - Elastic load balancers
 - Auto scaling groups
 - Deploy cloud formation stacks
- Speakers or headphones
- One of the following:
 - HTML5 support
 - An up-to-date Java Runtime Environment (JRE) with Java plugin enabled on your web browser

You should use a wired Ethernet connection, *not* a Wi-Fi connection. Firewalls, including Windows Firewall or FortiClient, must allow connections to the online labs.

Certification

This course and the *Private Cloud Security* course are intended to help you prepare for the NSE 7 Cloud Security certification exam.

Azure Prerequisites

In order to run the labs on Azure, *students must have their own Azure accounts* with the following:

- A pay-as-you-go subscription with a valid payment method. The free trial will not work for some labs.
- The ability to deploy FortiGate and FortiWeb PAYG from the Azure marketplace
- Capacity for at least 10 vCPUs in a single region
- Permissions to create the following:
 - App registrations (service principal) and keys
 - Load balancers
 - VNets
 - Virtual machines with four vCPUs
- The ability to do the following:
 - Run PowerShell scripts
 - Read the Active Directory properties and use Azure functions

The estimated cost per student for running the lab, if done within the specified lab times and everything is deleted at the end, is USD \$10 per cloud vendor per day.

System Requirements

If you take the online format of this class, you must use a computer that has the following:

- A high-speed Internet connection
- An up-to-date web browser
- A PDF viewer