AWS Cloud Security Administrator

In this course, you will learn about the different components that make up the Amazon Web Services (AWS) infrastructure and the security challenges these environments present, including high availability (HA), load balancing, and software-defined networking (SDN) connectors, and how to manage traffic in the cloud with Fortinet products.

Product Version

- FortiOS 7.4

Course Duration

- Lecture time (estimated): 4 hours
- Lab time (estimated): 7 hours
- Total course duration (estimated): 11 hours
  - 2 full days or 3 half days

Who Should Attend

Anyone who is responsible for the deployment or day-to-day management of Fortinet solutions on AWS should attend this course.

Certification

This course is intended to help you prepare for the *FCP - AWS Cloud Security 7.4 Administrator* certification exam. This exam is part of the Fortinet Certified Professional - Public Cloud Security certification track.

Prerequisites

- General knowledge of IaaS vendors and experience with FortiGate VMs.

AWS Prerequisite

No prerequisites required. AWS accounts are provided at the start of the course.

Agenda

1. Introduction to the Public Cloud
2. AWS Components
3. Fortinet Products and Deployments for AWS
4. High Availability in AWS
5. Load Balancers in AWS

Objectives

After completing this course, you should be able to:

- Understand the concept of the public cloud
- Know the various AWS public cloud service terms
- Identify threats and challenges in the public cloud
- Secure the AWS cloud
- Understand various public cloud deployments
- Describe Fortinet licensing models
- Be familiar with Github
- Describe AWS service components
- Identify AWS core networking components
- Identify AWS security components
- Describe AWS network firewall limitations
- Understand traffic flow in a virtual network
- Understand layer 2 traffic flow
- Understand routing and restrictions
- Identify Fortinet products on AWS Marketplace
- Understand Fortinet deployments in AWS
- Understand Fortinet offerings for web application firewall (WAF) in AWS
- Describe FortiWeb Cloud
- Understand different HA architectures in AWS
- Identify FortiGate native active-passive HA
- Understand FortiGate active-passive HA across two AZs
- Be familiar with AWS CloudFormation
- Identify different types of load balancers
- Understand FortiGate active-active HA with AWS ELB
- Understand GWLB
- Understand FortiGate CNF
- Identify the differences between FortiGate CNF and FortiGate VMs

Training Delivery Options and SKUs

Instructor-Led Training

Includes standard NSE training content delivered in person onsite, or live online using a virtual classroom application. Training is delivered within public classes or as a private class. Private requests are scoped, quoted, developed, and delivered by Fortinet Training (minimum quantities apply).

Use the following ILT Training SKU to purchase scheduled public classes of this course through Fortinet Resellers or Authorized Training Partners:

FT-AWS-CDS

Self-Paced Training

Includes online training videos and resources through the Fortinet Training Institute library, free of charge.

See Purchasing Process for more information about purchasing Fortinet training products.

ISC2

- CPE training hours: 4
- CPE lab hours: 7
- CISSP domains: Communication and Network Security

Program Policies and FAQs

For questions about courses, certification, or training products, refer to Program Policy Guidelines or Frequently Asked Questions.