Public Cloud Security

In this course, you will learn how to deploy Fortinet solutions in the public cloud using various methods. You will learn how to use third-party automation tools to deploy and secure your cloud resources. You will also learn how to effectively troubleshoot common connectivity problems in Azure and AWS, and how to use FortiCNP to simplify risk management for your cloud workloads.

Product Version

- FortiGate 7.6
- FortiWeb 7.4

Course Duration

- Lecture time (estimated): 6 hours
- Lab time (estimated): 10 hours
- Total course duration (estimated): 16 hours
  - 3 full days or 4 half days

Who Should Attend

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

Certification

This course is intended to help you prepare for the Fortinet FCSS - *Public Cloud Security 7.6* certification exam. This exam is in the Fortinet Certified Solution Specialist - Public Cloud Security certification track.

Prerequisites

- General knowledge of IaaS vendors
- Experience with FortiGate, FortiWeb, and Linux VMs
- Completion of the FCP - *AWS Cloud Security Administrator* and FCP - *Azure Cloud Security Administrator* courses or a clear understanding of network components and how to deploy resources in Azure and AWS.

AWS Prerequisites

Labs: students must have own account with:

- A valid payment method registered on the account*
- Capacity for min. 4 elastic IPs and 15 vCPUs in single region
- Capacity to deploy FortiGate EC2 instances with a combined total of 10 or more network interfaces
- Capacity to deploy FortiWeb EC2 instances
- Permissions to create the following:
  - Minimum of 6 VPCs and 10 EC2 instances
  - S3 bucket
  - CloudShell
  - Security groups
  - Internet and transit gateways
  - Lambda functions
  - IAM users with AWSMarketplaceFullAccess and AmazonEC2FullAccess permissions

Azure Prerequisites

Labs: students must have own account with:

- Pay-as-you-go subscription with a valid payment method*
- Ability to deploy FortiGate from Azure Marketplace, using Bicep or Terraform
- Capacity for at least 16 vCPUs in a single region
- Capacity to deploy FortiGate VMs with a combined total of 10 or more network interfaces
- Permissions to create the following:
  - App registrations (service principal) and keys
  - Minimum of 6 VNets
  - Minimum of 7 VMs with a combined total of 15 vCPUs
- The ability to do the following:
  - Run Cloud Shell with storage setup
  - Read the AD properties and use Azure functions
  - Create an IAM user with contributor, owner, and user access administrator role permissions

*Estimated lab cost/student, following all instructions, is USD $15/cloud vendor/day. Free trial will not work for some exercises.

Agenda

1. Cloud Security Best Practices
2. Infrastructure as Code
3. Securing IaaS Solutions
4. Securing CaaS Solutions
5. Troubleshooting
6. FortiCNP Features and Use Cases
7. FortiCNP Cloud Protection

Objectives

After completing this course, you should be able to:

- Describe best practices when working with cloud deployments
- Use automation tools to deploy cloud resources in AWS and Azure
- Deploy Fortinet solutions to protect IaaS deployments
- Deploy Fortinet solutions to protect CaaS deployments
- Troubleshoot cloud deployment and network connectivity issues
- Use FortiCNP to simplify risk management

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).

Contact your Fortinet Resellers or Authorized Training Partners to purchase this course.

Self-Paced Training

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

For training and lab SKUs, or additional purchasing information, refer to Purchasing Process.

ISC2

- CPE training hours: 6
- CPE lab hours: 10
- 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.