FORTINET CERTIFIED SOLUTION SPECIALIST Cloud Security

FORTINET Premier Authorized Training Center

fast lane

Public Cloud Security Architect

Course Description

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 FortiCNAPP to simplify risk management for your cloud workloads.

Product Version:

- FortiGate 7.6.4
- FortiWeb 7.6
- FortiCNAPP

Course Duration:

3 days

Certification:

This course is intended to help you prepare for the Fortinet NSE 7 - Public Cloud Security Architect exam. This exam is in the FCSS Cloud Security certification track.

Prerequisites:

- General knowledge of IaaS vendors
- Basic understanding of cloud security concepts
- Experience with FortiGate, FortiWeb, and Linux VMs
- 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 a 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 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 6 VNets
  - Minimum 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

Outlines:

1. Cloud Security Best Practices
2. Infrastructure as Code
3. Securing IaaS Solutions
4. Securing CaaS Solutions
5. Troubleshooting
6. FortiCNAPP Features
7. FortiCNAPP Risk Management and Threat Detection
8. FortiCNAPP Code Security and Vulnerability Management

Objectives:

After completing this course, you will 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 FortiCNAPP to simplify risk management, threat detection, and code security

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.