Public Cloud Security

Course Description

In this course, you will learn how to deploy FortiGate VMs in the public cloud using various methods. You will learn how to use third-party automation tools to deploy FortiGate VMs and secure your network. You will take a deep dive into AWS SD-WAN Connect deployment and learn how to utilize AWS Transit Gateway to secure east-west and north-south traffic. You will also learn how to effectively troubleshoot FortiGate deployments in Azure and how to use FortiCNP to simplify risk management for your AWS workloads.

Product Version:

- FortiGate 7.2

Course Duration:

3 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 NSE 7 - Public Cloud Security 7.2 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 and Linux VMs
- Completion of the FCP - Cloud Security for AWS and FCP - Cloud Security for Azure courses or a clear understanding
- of network components and how to deploy resources in Azure

AWS Prerequisites

Labs: students must have own account with:

- A valid payment method registered on the account*
- Capacity for at least four elastic IPs and 15 vCPUs in a single region
- Capacity to deploy FortiGate HA with 10 or more network interfaces
- Permissions to create the following:
  - Minimum 6 VPCs and 10 EC2 instances
  - S3 bucket
  - CloudShell
  - Security groups
  - Internet and Transit gateways
  - Lambda functions
  - IAM users with AWSMarketplaceFullAccess, 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 and Terraform
- Capacity for at least 15 vCPUs in a single region
- Capacity to deploy FortiGate HA with 10 or more network interfaces
- Permissions to create the following:
  - App registrations (service principal) and keys
  - Minimum 6 VNets
  - Minimum 7 VMs with 15 vCPUs
  - The ability to do the following:
  - Run Cloud Shell with storage setup
  - Read the Active Directory properties and use Azure functions
  - IAM user with contributor, owner, and user access administrator role permissions

Outlines:

1. FortiGate Deployment
2. Automation
3. Deploying a FortiGate VM Using Terraform
4. Troubleshooting
5. Cloud-Native Protection: FortiCNP

Objectives:

After completing this course, you will be able to:

- Deploy a FortiGate SD-WAN Connect scenario with AWS Transit Gateway
- Deploy a FortiGate VM on AWS/Azure in single, HA modes
- Use Terraform to deploy environments
- Use Ansible to make FortiGate configuration changes
- Troubleshoot Terraform and HA deployment issues
- Use FortiCNP to simplify risk management