TRENDS® | Academy
Learning | Evolving | Empowering

Azure Cloud Security Administrator

Duration: 2 Days

Course Description:

In this course, you will learn about the different components that make up the Microsoft Azure infrastructure and the security challenges these environments present, including high availability (HA), autoscaling, Azure Virtual WAN, and software-defined networking (SDN) connectors, and how to manage traffic in the cloud with Fortinet products.

Target Audience:

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

Prerequisites:

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

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 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
  - Up to two virtual networks
  - FortiGate VM as a single VM, in HA, and as a scale
  - unit
  - Azure Virtual WAN and Azure Route Server

The ability to do the following:
- Read the Active Directory properties and use Azure functions

Course Objectives:

- Deploy a FortiGate VM in Azure in single and HA modes
- Use Fortinet templates to easily deploy complex environments
- Deploy FortiWeb in Azure
- Use SDN connectors with Azure
- Integrate FortiGate VMs with Azure Virtual WAN
- Integrate other Fortinet services and products with Azure

Course Outlines:

- Introduction to Public Cloud Azure
- Azure Components, Networking, and Security Services
- Fortinet Solutions and Deployment in Azure
- Deploying Dependable Fortinet Solutions in Azure
- Deployment of VPN Fortinet Solutions in Azure