

# AZ 1002- Configure Secure Access To Your Workloads Using Networking with Azure Virtual Network



**Days:** 1

**Prerequisites:** Basic knowledge of virtual networking in cloud environments. Familiarity with IP address formats and subnetting. Familiarity with Azure services, the Azure portal, and basic networking, DNS, and Azure Firewall concepts.

**Description:** In this learning path, you practice configuring secure access to workloads using Azure networking.

## **OUTLINE:**

### **LESSON 1 - CONFIGURE VIRTUAL NETWORKS**

- Plan virtual networks
- Create subnets
- Create virtual networks
- Plan IP addressing
- Create public IP addressing
- Associate public IP addresses
- Allocate or assign private IP addresses
- Module assessment

### **LESSON 2 - CONFIGURE AZURE VIRTUAL NETWORK PEERING**

- Determine Azure Virtual Network peering uses
- Determine gateway transit and connectivity
- Create virtual network peering
- Extend peering with user-defined routes and service chaining
- Module assessment

### **LESSON 3 - MANAGE AND CONTROL TRAFFIC FLOW IN YOUR AZURE DEPLOYMENT WITH ROUTES**

- Identify routing capabilities of an Azure virtual network
- What is an NVA?

### **LESSON 4 - HOST YOUR DOMAIN ON AZURE DNS**

- What is Azure DNS?
- Configure Azure DNS to host your domain
- Dynamically resolve resource name by using alias record

### **LESSON 5 - CONFIGURE NETWORK SECURITY GROUPS**

- Implement network security groups
- Determine network security group rules
- Determine network security group effective rules
- Create network security group rules
- Implement application security groups
- Module assessment

### **LESSON 6 - INTRODUCTION TO AZURE FIREWALL**

- What is Azure Firewall?
- How Azure Firewall works
- When to use Azure Firewall
- When to use Azure Firewall Premium
- Module assessment

### **LESSON 7 - GUIDED PROJECT - CONFIGURE SECURE ACCESS TO WORKLOADS WITH AZURE VIRTUAL NETWORKING SERVICES**

- Module assessment