AZ-1002: Configure secure access to your workloads using Azure virtual networking

Course Details

Course Code: AZ-1002

Duration: 1 day

Notes:

- This course syllabus should be used to determine whether the course is appropriate for the students, based on their current skills and technical training needs.
- Course content, prices, and availability are subject to change without notice.
- Terms and Conditions apply

Elements of this syllabus are subject to change.

About this course

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

Note

You need an Azure subscription to complete these exercises. If you don't have an Azure subscription, create a free account, and add a subscription before you begin. If you are a student, you can take advantage of the Azure for students offer.

Prerequisites

- None

Configure virtual networks
AI assisted content. This module was partially created with the help of artificial intelligence.

Learn to configure virtual networks and subnets, including IP addressing.

Learning objectives
In this module, you learn how to:

- Describe Azure virtual network features and components.
- Identify features and usage cases for subnets and subnetting.
- Identify usage cases for private and public IP addresses.
- Create a virtual network and assign IP address.

Configure Azure Virtual Network peering
AI assisted content. This module was partially created with the help of artificial intelligence.

Learn to configure an Azure Virtual Network peering connection and address transit and connectivity concerns.

Learning objectives
In this module, you learn how to:

- Identify usage cases and product features of Azure Virtual Network peering.
- Configure your network to implement Azure VPN Gateway for transit connectivity.
- Extend peering by using a hub and spoke network with user-defined routes and service chaining.

Introduction to Azure Firewall
Describe how Azure Firewall protects Azure Virtual Network resources, including the Azure Firewall features, rules, deployment options, and administration with Azure Firewall Manager.

Learning objectives
After completing this module, you'll be able to:

- Explain how Azure Firewall and Azure Firewall Manager work together to protect Azure virtual networks.
- Evaluate whether Azure Firewall is the right solution to protect your Azure

virtual networks from malicious incoming and outgoing traffic.
- Evaluate whether Azure Firewall Premium is the right solution to protect your Azure virtual networks from malicious incoming and outgoing traffic.
- Evaluate whether Azure Firewall Manager is the right solution for deploying policies across multiple firewalls.
- Identify and describe use cases for Azure Firewall and Azure Firewall Manager.

Guided Project - Configure secure access to workloads with Azure virtual networking services
In this module, you practice configuring secure access to workloads using Azure virtual networking. The lab combines both learning and hands-on practice.

Learning objectives
- Create and configure virtual networks
- Create and configure network security groups (NSGs)
- Create and configure Azure Firewall
- Configure network routing
- Create DNS zones and configure DNS settings