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

Course Code: AZ-1002
Duration: 1 day
Instructor-led Training (ILT) | Virtual Instructor-led Training (VILT)

OVERVIEW

Configure secure access to your workloads using Azure virtual networking

To earn this Microsoft Applied Skills credential, learners demonstrate the ability to secure resources by using Azure virtual networking solutions.

Candidates for this credential should be familiar with Azure services, the Azure portal, and basic networking, DNS, and Azure Firewall concepts.

SKILLS COVERED

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

WHO SHOULD ATTEND?

- Administrator

PREREQUISITES

There are no prerequisites required to attend this course.

MODULES

Module 1: Configure virtual networks

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.

Prerequisites

- Basic knowledge of virtual networking in cloud environments.
- Familiarity with IP address formats and subnetting.

Module 2: Configure Azure Virtual Network peering

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.

Prerequisites

- Basic understanding of cloud networking including virtual networks and virtual machines.
- Familiarity with the command line connectivity testing tools.

Module 3: Manage and control traffic flow in your Azure deployment with routes

Learn how to control Azure virtual network traffic by implementing custom routes.

Learning objectives

In this module, you will:

- Identify the routing capabilities of an Azure virtual network
- Configure routing within a virtual network
- Deploy a basic network virtual appliance
- Configure routing to send traffic through a network virtual appliance

Prerequisites

- Knowledge of basic networking concepts
- Familiarity with Azure virtual networking

Module 4: Host your domain on Azure DNS

Create a DNS zone for your domain name. Create DNS records to map the domain to an IP address. Test that the domain name resolves to your web server.

Learning objectives

In this module, you will:

- Configure Azure DNS to host your domain.

Prerequisites

- Knowledge of networking concepts like name resolution and IP addresses

Module 5: Configure network security groups

Learn how to implement network security groups, and ensure network security group rules are correctly applied.

Learning objectives

In this module, you learn how to:

- Determine when to use network security groups.
- Create network security groups.
- Implement and evaluate network security group rules.
- Describe the function of application security groups.

Prerequisites

- Familiarity with Azure virtual networks and resources such as virtual machines.
- Working knowledge of the Azure portal so you can configure the network security groups.
- Basic understanding of traffic routing and traffic control strategies.

Module 6: 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.

Prerequisites

To get the best learning experience from this module, you should have:

- Beginner-level knowledge of Azure, including Availability Zones, Azure virtual networks, and ExpressRoute.
- Beginner-level knowledge of networking, including IP addresses, public versus private IP addresses, hub and spoke network topology, subnets, and network packets.
- Beginner-level knowledge of cloud computing, including scalability and availability.

Module 7: 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

Prerequisites

- Experience using the Azure portal to create resources.
- Experience with cloud networking.
- The prerequisites can be obtained by completing the other modules in this learning path.

END OF PAGE