Advanced Networking

Introduction

In this hack, you will work through an example company, Contoso's architecture requirements for their IaaS workloads. You will put together a network design for Contoso. There are multiple challenges in this hack. Follow these in order to deploy a solution to Azure that is secure, scalable and provides visibility into your environment.

Duration

3 Days

Learning Objectives

This hack introduces you to the core components of IaaS and enables building on these to deploy a scalable architecture. You will start with deploying your private network environment on Azure, deploy virtual machines, add load balancing, and secure with Azure security technologies like Azure Firewall, Web Application firewall, Azure Bastion, network security groups and Private Link. At the end of the hack, the participants will be able to design and deploy a scalable network architecture on Azure and securely connect their Azure workloads to on-premises and external environments.

Challenges

- Challenge 1: Virtual Networks
  - Design and deploy Azure virtual networks.
- Challenge 2: Network Security Groups
  - Secure your workloads using Network Security Groups.
- Challenge 3: Load Balancing
  - Deploy scalable application with Azure Load balancers.
- Challenge 4: Network Connectivity
  - Learn how to connect your Azure virtual network with other environments.
- Challenge 5: Azure Firewall
  - Build secure edge architecture.
- Challenge 6: Azure Bastion
  - Secure management access to your workloads.

- Challenge 7: Azure Private Link
    - Secure access to your Azure services.
- Challenge 8: Azure Private Link Service
    - Enable private access to your services.