Week 3 Lab: Azure Network Policies to Secure traffic between pods

Overview

This lab will build on the discussion from Week 3. Recall we discussed how to manage both East/West traffic, and North/South ingress/egress traffic for your AKS cluster. This lab will focus on using Network Policy to manage East/West traffic, and the Challenge will focus on using the Azure Firewall for governing the required outbound dependency traffic.

This lab will differ from the previous 2 labs in Week 1 and Week 2 because it will describe at a high level what you need to do, but will not specify the exact steps.

Overall

You are expected to create an AKS cluster and enable 3 different network policies to control Pod to Pod traffic. Specifically, once your cluster is created, you will create the following policies:

- Deny all traffic to pod.
- Allow traffic based on pod labels.
- Allow traffic based on namespace.

What's covered in this lab

The following tasks need to be performed:

1. Create a virtual network and subnet to host the AKS cluster.
2. Create an Azure Active Directory (Azure AD) Service Principal for use with the AKS cluster. You can also used Managed Identity instead of the Service Principal if you wish.
3. Assign at least *Contributor* permissions for the AKS cluster Service Principal on the virtual network.
4. Create an AKS cluster in the defined virtual network and enable network policy.
5. Create a network policy to deny all inbound traffic to a pod. This includes:
    a. Create the YAML manifest to implement the policy.
    b. Apply the policy using kubectl.
    c. Test access and demonstrate success of the policy.
6. Repeat step 1. process above to create two more policies that:
    a. Allow inbound traffic based on pod label.
    b. Allow traffic only from within a defined namespace.

7. Delete all your resources (unless you can reapply to the Challenge).

Challenge

Establish a cluster environment that controls outbound egress traffic using the Azure Firewall. You may need to re-create your AKS cluster.