E-commerce App Migration

Advisor
Eng. Khaled Mohsen

Project Team

Eng. Fady Nabil

Eng. Mohamed Nabil

Eng. Mohamed Waheed

Eng. Osama Mamdouh

Eng. Sayed Reda

Table of Contents

App Migration

- As an e-commerce platform experiencing frequent downtime and performance issues during high traffic, we faced the challenge of migrating to the cloud to ensure stability, scalability, and reliability.

- Our goal is to seamlessly transition the platform to a cloud environment, ensuring minimal disruption to services while improving performance during peak demand.

- We need a solution that offers dynamic scalability, robust network infrastructure, secure connectivity, and reliable monitoring to prevent future outages and ensure a smooth shopping experience for our customers."

- Migrating the e-commerce application to the cloud is essential for improving scalability, performance, and cost efficiency. Cloud infrastructure dynamically allocates resources, reducing downtime and ensuring reliability. It also supports rapid feature deployment and future growth, while minimizing on-premises maintenance. Below are the key benefits of cloud migration:

- **Scalability**

  The cloud offers dynamic resource allocation, allowing businesses to scale infrastructure up or down based on demand. This flexibility ensures that the platform can handle traffic spikes without compromising performance, which is essential for e-commerce applications with fluctuating user activity.

- **Cost Efficiency**

Cloud services follow a pay-as-you-go model, enabling businesses to pay only for the resources they actually use. This eliminates the need for large upfront investments in physical hardware and reduces ongoing maintenance costs, leading to significant savings over time.

- **Improved Performance**

With global data centers and advanced load-balancing, cloud platforms provide faster data delivery and reduce latency. This results in improved application performance, which is critical for customer satisfaction and business continuity.

- **Security**

Cloud providers implement stringent security measures, including data encryption, secure access controls, and compliance with industry standards. This helps safeguard sensitive business and customer data, reducing the risk of breaches or cyberattacks.

- **Reliability and Availability**

Cloud infrastructure ensures high availability and redundancy, with built-in backup and disaster recovery options. This minimizes downtime and ensures business continuity, providing an uninterrupted experience for users, even in the event of hardware failure or natural disasters.
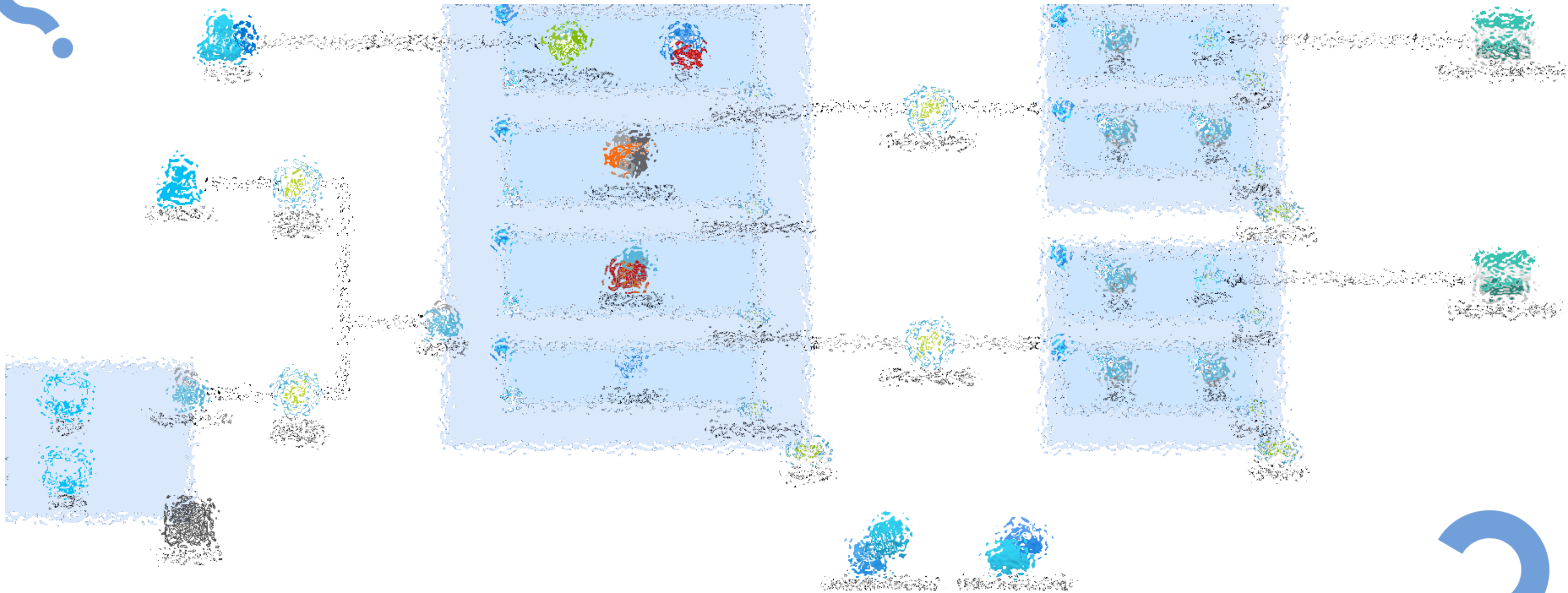
Let's take it step by step

Step 1: Network Segmentation

We requires a cloud design with centralized management and two workload environments: Production and Testing.

Our Solution:

Created a hub-and-spoke network topology in Azure.
Configured one hub VNet for centralized services and two spoke VNets for hosting both Forntend and Database environments.

Step 2: Workload Hosting Service

We needs a suitable workload hosting service for his web application with greater control and customization.

Our Solution:

Chose Virtual Machines for greater control and customization.
Deployed one VMs in each spoke VNet to host the web application components, ensuring redundancy and high availability.

Step 3: Application Delivery

We requires a scalable load balancing option with applicable security rules to ensure secure and reliable delivery of my web application to end users.

Our Solution:

Configured the Application Gateway, scalable load balancing. Implemented WAF rules to protect the application from common web vulnerabilities.
And we also enabled the DDos Option to protect our network from the Distributed denial-of-service attacks

Step 4: Secure Connectivity

The customer needs secure and efficient connectivity between the VNets ensuring low latency and high bandwidth communication between the web application components in the spokes and the centralized services in the hub.

Our Solution:

Established VNet peering between the hub and spoke VNets. Configured network security groups (NSGs) to control inbound and outbound traffic, and also we have re-route the traffic through the Firewall to make sure that the traffic are inspected and monitored.

Step 5: Centralized Firewall

We wants a centralized cloud native security service to control and log all network traffic flowing between the VNets, providing an additional layer of security for our web application environment..

Our Solution:

Deployed an Azure Firewall in the hub VNet.
Configured the firewall to log and control traffic between the hub and spoke VNets.
Implemented security rules to allow only necessary traffic.
Enable IPDS.

Step 6: Secure Remote Access

To facilitate management and maintenance, the customer needs a secure solution for RDP/SSH connectivity to the virtual machines hosting his web application components without exposing them to the public internet.

Our Solution:

Set up an Azure Bastion host in the hub VNet.
Configured Bastion for secure RDP/SSH connectivity to VMs in the spoke VNets.
Eliminated the need to expose VMs to the public internet, ensuring secure access.

9

Step 7: Monitoring

We needs comprehensive monitoring capabilities to collect and analyze logs and metrics from all components of our web application environment for effective monitoring and troubleshooting...

Our Solution:

Integrated Azure Monitor.
Configured monitoring for the critical components such as "App GW, Firewall" of the infrastructure.
We also enforced Tagging Policy for all azure resources to be able to track the cost.
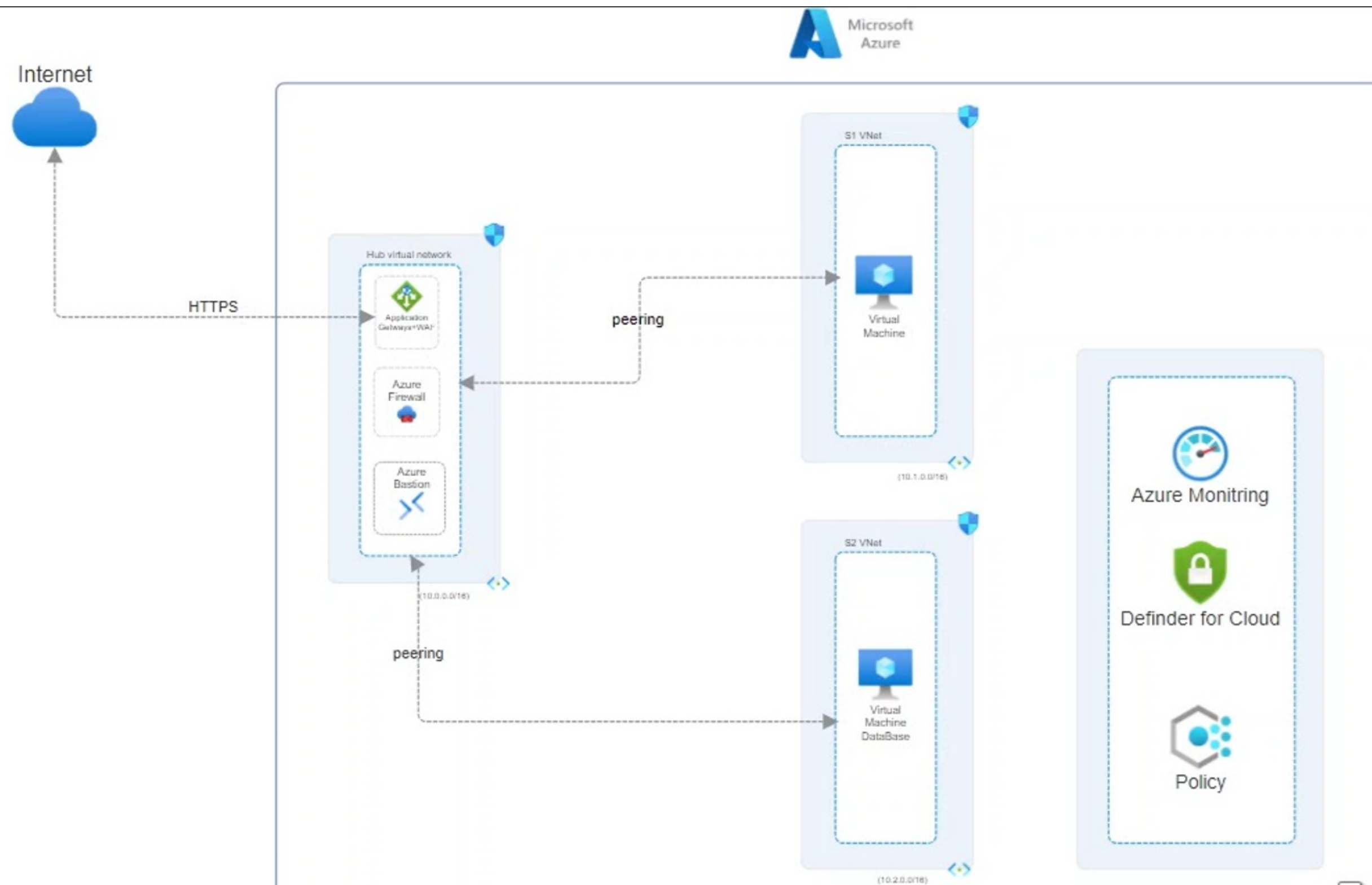
Step 8: Backup and Disaster Recovery

We want regular backups and quick recovery of the virtual machines hosting his web application components to protect against data loss and ensure business continuity

Our Solution:

Implemented Azure Backup and Recovery Services Vault.
Configured regular backups for all VMs hosting the web application components.
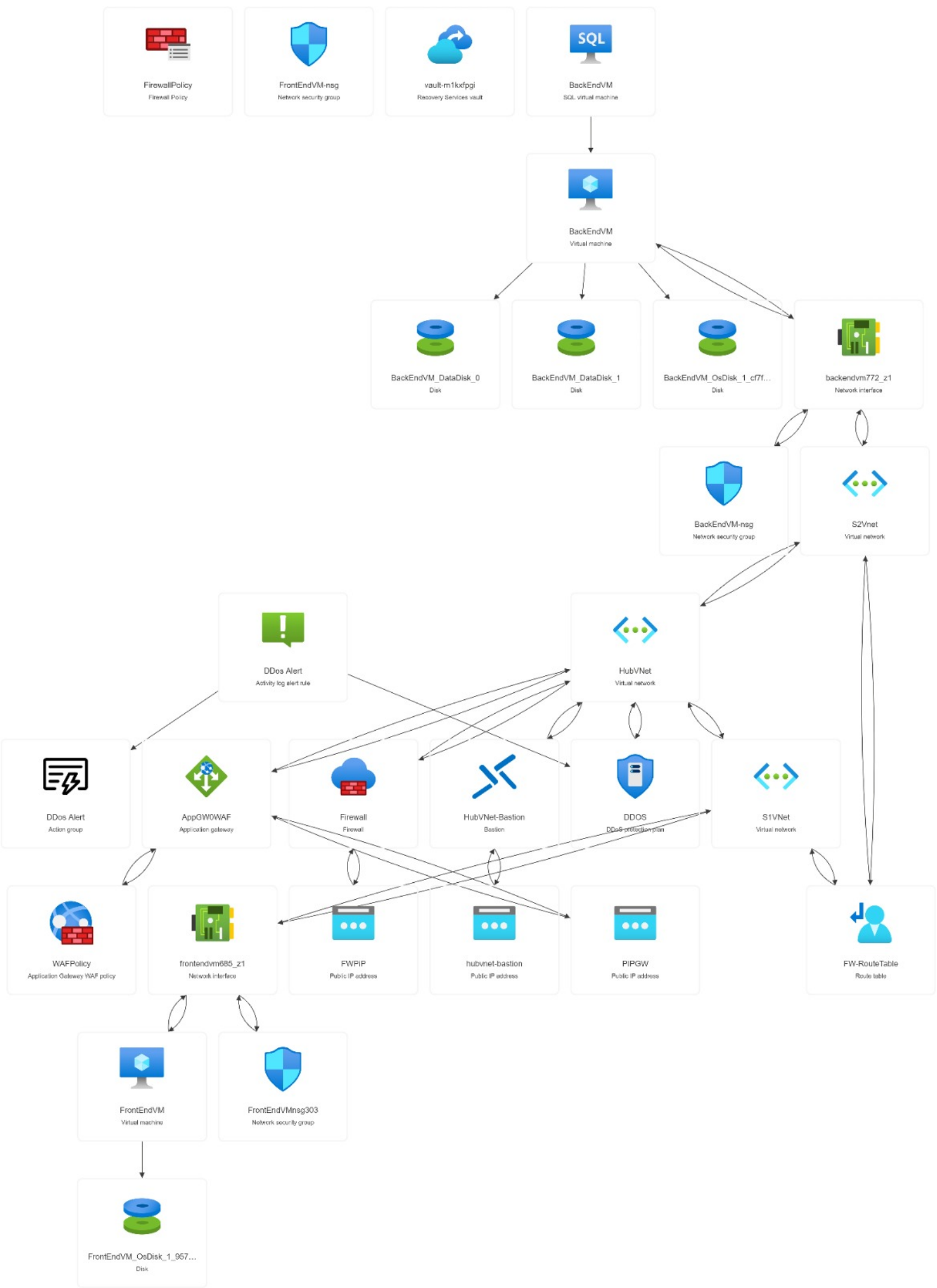
Implementation on Azure

Demo

Any Questions ?

Thank you
for listening!