Secure Hybrid Cloud Architecture with Azure Networking

Objective:

Architect and deploy a robust, secure hybrid cloud environment that seamlessly bridges a simulated on-premises network within Azure-to-Azure cloud resources. This setup will leverage powerful Azure networking features, including VPN **gateways** for secure communication between networks, **Azure Firewall** for centralized threat protection, **Azure DNS** for streamlined domain management, and **Network Security Groups (NSGs)** for granular traffic control. The goal is to integrate these components into a cohesive, enterprise-grade solution that demonstrates mastery in building scalable, resilient, and secure network architectures within Azure.

Project Overview

A forward-thinking company is gearing up to migrate its on-premises applications to Azure, aiming to harness the power of the cloud while maintaining a secure and seamless connection to its existing infrastructure. The mission is clear: design and deploy a robust hybrid cloud environment that not only meets but exceeds enterprise-grade standards.

Scenario

Imagine an organization that's ready to elevate its operations by embracing the scalability and innovation of Azure. They want their on-premises network (simulated within Azure) to communicate effortlessly with Azure resources, ensuring business continuity and operational efficiency. The challenge lies in creating a solution that is both secure and cost-effective, leveraging Azure's advanced networking features.

Solution Requirements

1. **Secure Communication Between On-Premises and Azure**
    a. **Implementation**: Establish a **VPN gateway** to enable encrypted connections between the on-premises network and Azure Virtual Networks (VNets).
    b. **Benefit**: Ensures data integrity and confidentiality as it traverses between environments, mitigating potential security risks.
2. **Isolation of Sensitive Workloads**

a. **Implementation**: Segment the network using **subnets** and enforce strict access controls with **Network Security Groups (NSGs)**.
b. **Benefit**: Protects critical assets by limiting exposure and reducing the attack surface within the network.

3. **Centralized DNS Resolution Across Hybrid Environments**
   a. **Implementation**: Utilize **Azure DNS** to manage domain names for resources in both on-premises and Azure environments.
   b. **Benefit**: Streamlines name resolution, simplifies network management, and ensures consistent access to applications and services.
4. **Traffic Inspection via Azure Firewall**
   a. **Implementation**: Deploy **Azure Firewall** as a centralized security solution to monitor and control both inbound and outbound network traffic.
   b. **Benefit**: Provides advanced threat protection, compliance with security policies, and enhanced visibility into network activities.
5. **Cost-Effective Public IPs and Routing**
   a. **Implementation**: Optimize the assignment of **public IP addresses** and configure efficient routing strategies, possibly leveraging **User-Defined Routes (UDRs)**.
   b. **Benefit**: Reduces operational costs while maintaining high network performance and reliability.

Step-by-Step Implementation

1. Simulate On-Premises and Azure Environments

- Create two virtual networks
  I. **OnPremVNet** (simulated on-premises): 10.1.0.0/16.
  This is a simulated on-premises network within Azure that securely connects to Azure cloud resources. The on-premises environment will feature its own local network gateway and VPN devices to enable this secure communication.

  II. **AzureVNet** (cloud): 10.2.0.0/16.

  This is a virtual network created in Azure to secure and enable workload resources to communicate with the simulated on-premises network

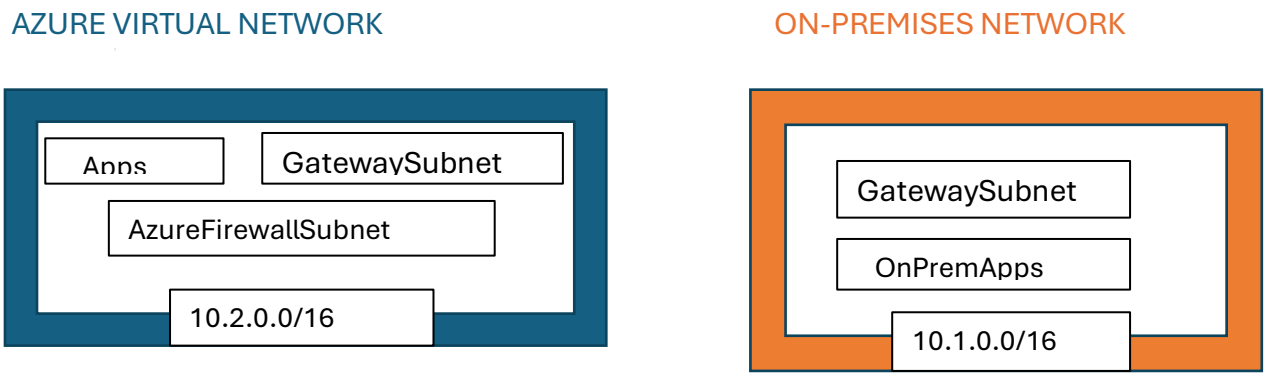
- Create subnets for both networks

OnPremVNet:

- **GatewaySubnet-**a subnet to deploy virtual network gateway of on-premises network
- **OnPremApps**-a subnet to deploy workload resources like virtual machines.

AzureVNet

- **GatewaySubnet**-a subnet to deploy virtual network gateway of virtual network
- **Apps**-a subnet to deploy workload resources like virtual machines.
- **AzureFirewallSubnet**-a subnet to deploy firewall instance to filter inbound and outbound network traffics



2. Set Up VPN Connectivity

Deploy VPN Gateways:

- Set up VPN Gateways in both Virtual Networks (VNets) to enable secure communication.

Configure Local Network Gateway:

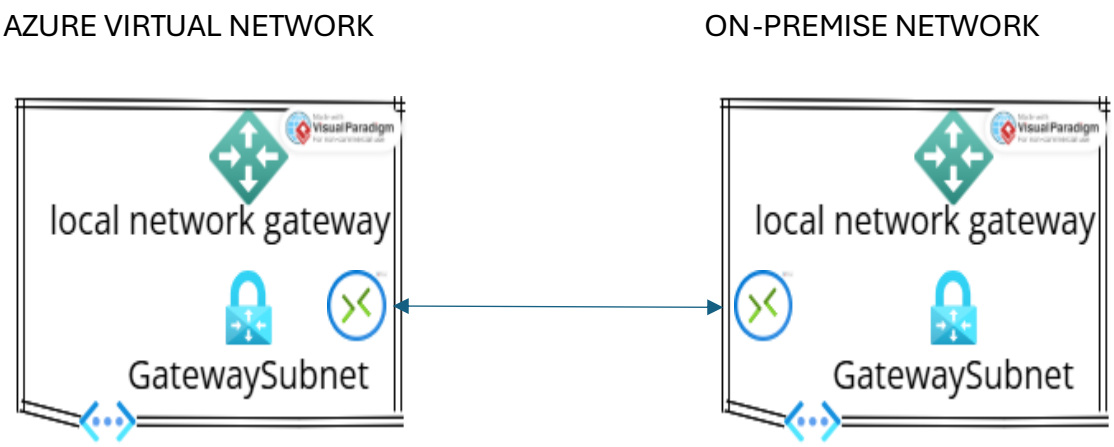
- Create a Local Network Gateway to represent the on-premises network in Azure.
- Define the public IP and address space of the on-premises network.

Configure Site-to-Site VPN:

- Establish a secure IPsec tunnel between `OnPremVNet` and `AzureVNet` to ensure encrypted communication.

Test Connectivity:

- Verify connectivity using tools like `ping` or `traceroute` between virtual machines in both VNets.



3. Implement Azure Firewall

Deploy Azure Firewall:

- Provision Azure Firewall in the `AzureFirewallSubnet` with a dedicated Public IP address.

Create Route Table and Routes:

- Configure a Route Table to direct all outbound traffic from the `Apps` subnet to the Azure Firewall, ensuring centralized traffic management and inspection.

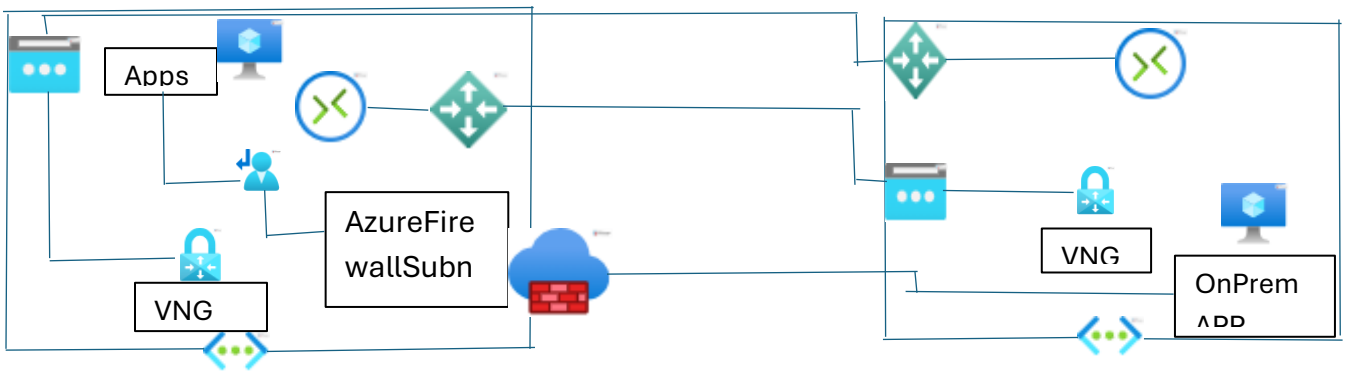
Configure Firewall Rules:

- **Allow Rules:** Permit outbound HTTP/HTTPS traffic to the internet for applications and services.

- **Deny Rules:** Block all unauthorized inbound traffic to protect the Azure Virtual Network from external threats.

This step ensures secure and controlled communication between the on-premises network and Azure Virtual Network, maintaining a strong security posture.

AZURE VIRTUAL NETWORK ON-PREMISE NETWORK



4. Configure DNS Resolution

Create Private DNS Zone:

- Establish a Private DNS Zone (e.g., `contoso.internal`) within the Azure environment for internal name resolution.

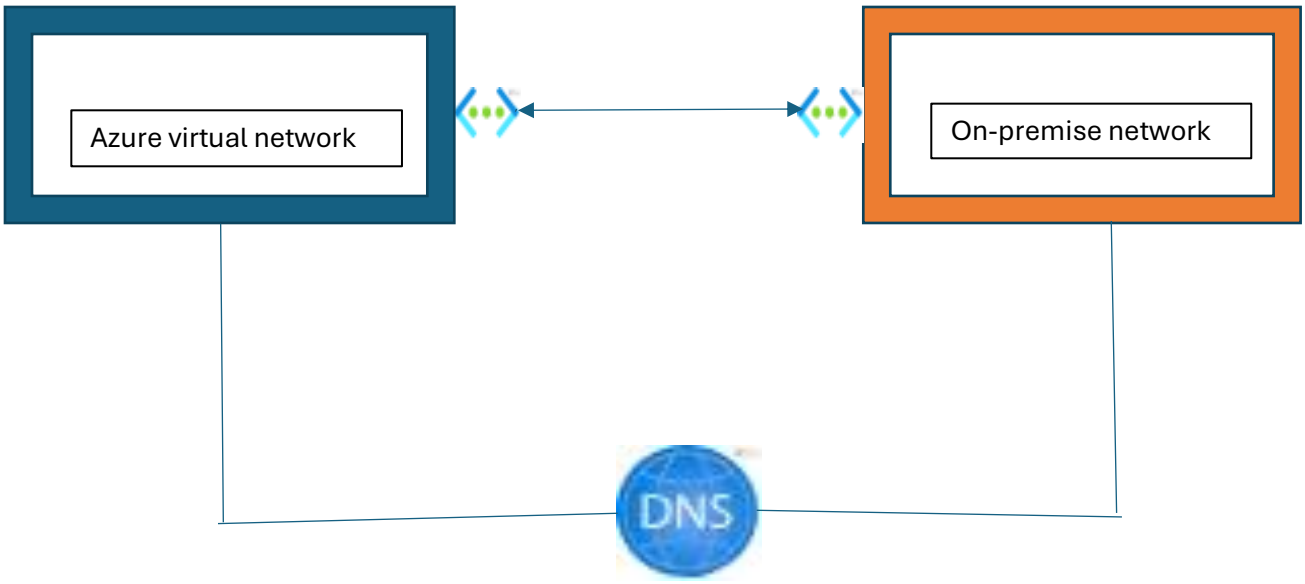
Link Virtual Networks:

- Associate both Azure Virtual Networks (VNets) with the Private DNS Zone to ensure seamless name resolution across the hybrid network.

Add DNS Records:

- Define A Records for essential resources (e.g., `app.contoso.internal` mapped to `10.2.0.4`) to enable reliable access and communication within the network.

This configuration facilitates efficient DNS resolution across the hybrid connectivity infrastructure, enhancing resource accessibility and network performance.



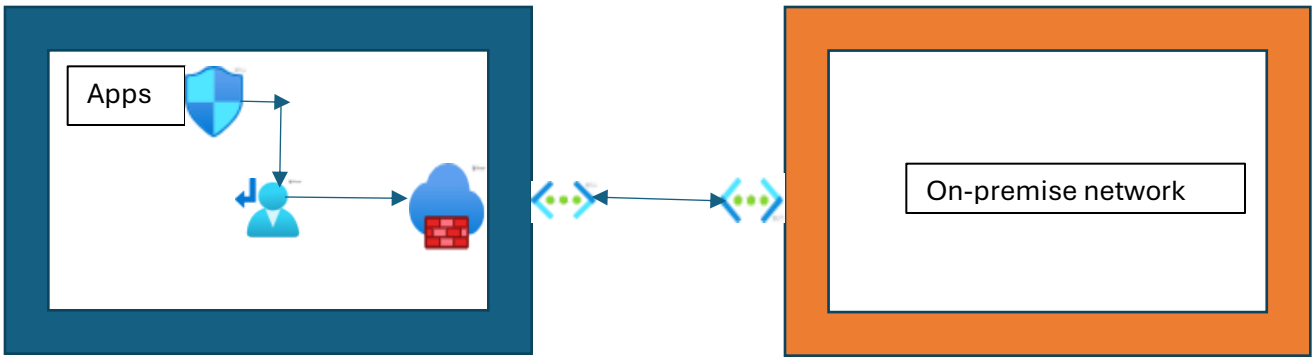
5. Apply Network Security Groups (NSGs)

Isolate Subnets:

- **Allow Rules:** Permit specific protocols access only from the `on-premises` subnet to enhance secure remote management (Inbound security rule). The default inbound security rule is “DenyAllInbound”.
- **Deny Rules:** Restrict direct internet access from the `Apps` subnet, enforcing all outbound traffic to route through the Azure Firewall for inspection and security (Outbound security rule). The default outbound security rule is “AllowInternetOutBound”.

Implementing NSGs ensures granular control over inbound and outbound traffic within subnets, enhancing the overall security posture of the hybrid connectivity setup.

We can apply network security rule at subnet level and resource level, it is also managed by users.



6. Validate the Solution

- **Test Hybrid Connectivity**:
  - From `onprem-vm`, access `azure-vm` via its private IP or DNS name.
- **Test Firewall Rules**:
  - From `azure-vm`, verify HTTP traffic to the internet is allowed, but other ports are blocked.

Conclusion

The **Secure Hybrid Cloud Architecture with Azure Networking** project effectively demonstrates a comprehensive understanding of Azure's core networking services and their integration into a real-world, enterprise-grade solution. By leveraging **virtual networks**, **subnets**, **VPN gateways**, **Azure Firewall**, **DNS zones**, **NSGs**, and **route tables**, this project showcases the ability to design and deploy a secure, scalable, and well-connected hybrid environment.
Key accomplishments include:

1. **Hybrid Connectivity**: Establishing secure site-to-site VPN connectivity between an on-premises network (simulated in Azure) and Azure VNets, enabling seamless cross-environment communication.
2. **Security Best Practices**: Enforcing traffic inspection and filtering using Azure Firewall, isolating workloads with NSGs, and implementing least-privilege access controls.
3. **Centralized DNS Management**: Configuring Azure Private DNS zones for consistent name resolution across hybrid resources.
4. **Cost-Effective Design**: Utilizing public IPs and route tables to optimize traffic flow while minimizing expenses.

Contributor: Abinet Degefa