**Handout: Administer Virtual Networking**

**1. Plan Virtual Networks**

* **What is a VNet?**  
  A **Virtual Network (VNet)** is a logical network in Azure that mimics your on-premises network, allowing you to manage, isolate, and secure resources in Azure.
* **Why Use VNets?**  
  VNets support hybrid cloud environments by extending your datacenter to Azure, enabling secure communication between cloud and on-premises resources. You can create a **dedicated private cloud-only virtual network** and securely connect to Azure services.
* **Key Considerations**:
  + Plan the **IP address range** carefully to avoid conflicts with other networks.
  + Use subnets to segment the VNet for different workloads (e.g., web servers, databases).

**2. Create Virtual Networks**

* **Creating VNets Anytime**:  
  You can create VNets during virtual machine (VM) setup or at any point. VNets are necessary for configuring your environment’s network structure in Azure.
* **Address Space and Subnets**:  
  Every VNet needs an **address space**. This defines the range of private IP addresses available within that network. Ensure at least one **subnet** is created within the address space, and be careful not to overlap IP ranges between different VNets or with your on-premises network. Overlapping IP addresses cause routing issues.
* **Example**:  
  For a hybrid cloud solution, if your on-premises network uses the 10.0.0.0/16 range, plan the Azure VNet to use a non-conflicting range, such as 10.1.0.0/16.

**3. Create Subnets**

* **Why Subnets?**  
  Subnets divide the VNet into smaller, logical sections to isolate resources and manage traffic more effectively. Each subnet can have its own security rules and performance settings, optimizing your cloud infrastructure.
* **Benefits of Subnetting**:  
  Subnetting allows better **security** by isolating sensitive workloads (e.g., separating front-end web servers from back-end databases). It also simplifies **network management**, making it easier to monitor and control traffic flows within the VNet.
* **Unique Address Ranges**:  
  Each subnet must have a unique address range. Avoid overlapping IP ranges between subnets within the same VNet to ensure proper routing.

**4. Plan IP Addressing**

* **Private vs Public IP Addresses**:
  + **Private IPs** are used within Azure VNets for internal communication, such as connecting VMs or databases within the VNet. These addresses aren’t accessible from the internet.
  + **Public IPs** are assigned to resources that need to communicate with the public internet, such as web servers or APIs. These IPs allow external users to access your services.
* **IPv4 and IPv6**:  
  Azure supports both **IPv4** and **IPv6** address formats. Public IP addresses can be either dynamic (assigned temporarily) or static (fixed).
* **Choosing Between Dynamic and Static**:
  + **Dynamic IPs** are assigned temporarily and can change when resources are deallocated and reallocated.
  + **Static IPs** ensure a permanent IP address, which is critical for services that require consistent communication, such as DNS servers or web applications.

**5. Create Public IP Addresses**

* **When to Use Public IPs?**  
  Public IP addresses are needed when resources, such as virtual machines, need to be accessible from the internet. You can create and assign these IP addresses through the Azure portal or using PowerShell.
* **Available in Different SKUs**:  
  Azure offers two SKUs for public IP addresses: **Basic** and **Standard**.
  + **Basic SKU**: Designed for non-mission-critical workloads.
  + **Standard SKU**: Provides higher reliability, enhanced features like zone-redundancy, and is used for production workloads that need more stability.

**6. Associate Public IP Addresses**

* **Associating Public IPs with Resources**:  
  Public IPs can be associated with various Azure resources such as VMs, internet-facing load balancers, VPN gateways, and application gateways. Associating these IPs allows external communication with your Azure-hosted services.
* **Best Practices**:  
  Use **static public IPs** for services that need a consistent address over time (e.g., websites or APIs). Dynamic IPs may be suitable for scenarios where the exact IP address is not critical.

**7. Allocate or Assign Private IP Addresses**

* **Dynamic vs. Static Private IP Allocation**:
  + **Dynamic Assignment**: By default, Azure dynamically allocates private IP addresses within a subnet’s IP range. Azure automatically selects the next available IP for your VM or resource.
  + **Static Assignment**: You can assign a **static private IP** manually for resources that require a specific address (e.g., database servers, DNS servers). This ensures that the IP address remains constant throughout the resource’s lifecycle.

**8. Network Security Groups (NSGs)**

* **What Are NSGs?**  
  NSGs are security controls that filter network traffic to and from Azure resources at both the subnet and network interface card (NIC) levels. NSGs allow you to create inbound and outbound rules to control access to your resources.
* **NSG Rules**:  
  NSG rules define which traffic is allowed or denied based on parameters such as source/destination IP addresses, port numbers, and protocols (TCP/UDP). These rules are evaluated by priority, with lower numbers having higher precedence.
* **Best Practices**:
  + Use **least privilege principles**: Only allow necessary traffic (e.g., permit HTTP traffic to web servers while blocking everything else).
  + Apply NSGs at both the subnet and NIC levels for a **layered security** approach.

**9. Implement Application Security Groups (ASGs)**

* **ASG Overview**:  
  Application Security Groups (ASGs) provide another layer of security by grouping virtual machines into logical sets (e.g., group all web servers together). NSGs can then be applied to these groups instead of individual VMs, simplifying security management.
* **Benefits**:
  + Simplifies security management for large applications.
  + Allows dynamic association of resources without needing to rewrite NSG rules.

**10. Azure Firewall**

* **Azure Firewall Overview**:  
  Azure Firewall is a cloud-based, stateful firewall service that provides network and application-level protection across Azure resources. It offers built-in high availability and scalability, integrating seamlessly with Azure’s security ecosystem.
* **Firewall Rules**:  
  Azure Firewall uses three types of rules to filter traffic:
  + **NAT Rules**: Control inbound traffic, allowing you to map public IPs to private IPs.
  + **Network Rules**: Filter traffic based on source/destination IP, protocol, and port.
  + **Application Rules**: Filter outbound traffic using domain names (FQDNs).
* **Threat Intelligence**:  
  Azure Firewall integrates with **Azure Monitor** for logging and offers **threat intelligence-based filtering** to block traffic from known malicious IP addresses.

**11. Azure DNS**

* **Azure DNS Overview**:  
  Azure DNS provides DNS domain hosting as a service, offering high-performance, secure name resolution for Azure resources. You can manage DNS records for custom domains and benefit from automatic name management within your VNets.
* **Private DNS Zones**:  
  Private DNS Zones offer **internal name resolution** between VMs within a VNet and across peered VNets, eliminating the need for custom DNS solutions. Azure automatically manages hostname records for your VMs.
* **Public DNS Zones**:  
  Public DNS Zones allow you to host custom domains and manage DNS records for your public-facing resources. Azure’s global DNS infrastructure ensures high availability and performance.

**12. Lab 04 – Implement Virtual Networking**

* **Objectives**:
  + Create and configure a virtual network.
  + Deploy VMs in different subnets.
  + Assign static and dynamic public/private IP addresses.
  + Configure Network Security Groups to control access.
  + Set up DNS name resolution for internal and external communication.