R&D Document

Azure Virtual Network

Ananya Srivastava

Cloud Infra
JIET

Table of Contents

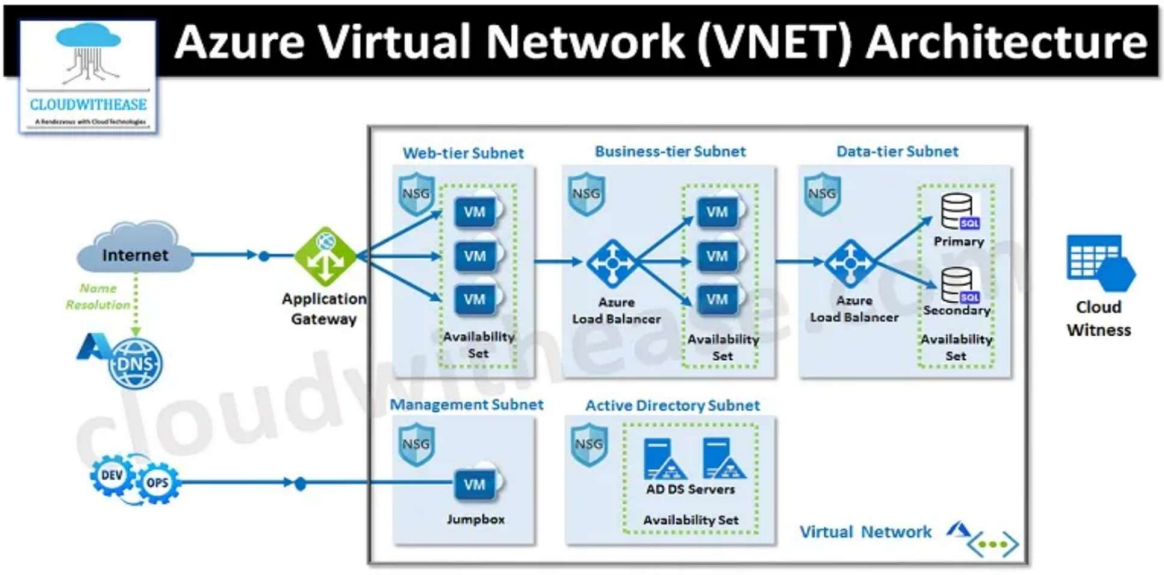
VNet (Virtual Network)

- A Virtual Network (VNet) in Azure is a logically isolated network that securely connects Azure resources and extends on-premises networks.
- It is a network or environment that can be used to run VMs and applications in the cloud.
- When it is created, the services and Virtual Machines within the Azure network interact securely with each other.
- Key features include:

  - **Isolation**: VNets provide isolation at the network level for segmenting resources and controlling traffic.
  - **Subnetting**: Divide a VNet into subnets for resource organization and traffic control.
  - **Address Space**: VNets have an address space defined using CIDR notation, determining the IP address range.

- Azure networking components provide a wide range of functionalities that can help companies build efficient cloud applications that meet their requirements.

- The components of Azure Networking are listed below, and we have explained each of these components in a detailed manner:
  i. Subnets
  ii. Routing
  iii. Network Security Groups



Subnets and Routing

1. Subnets

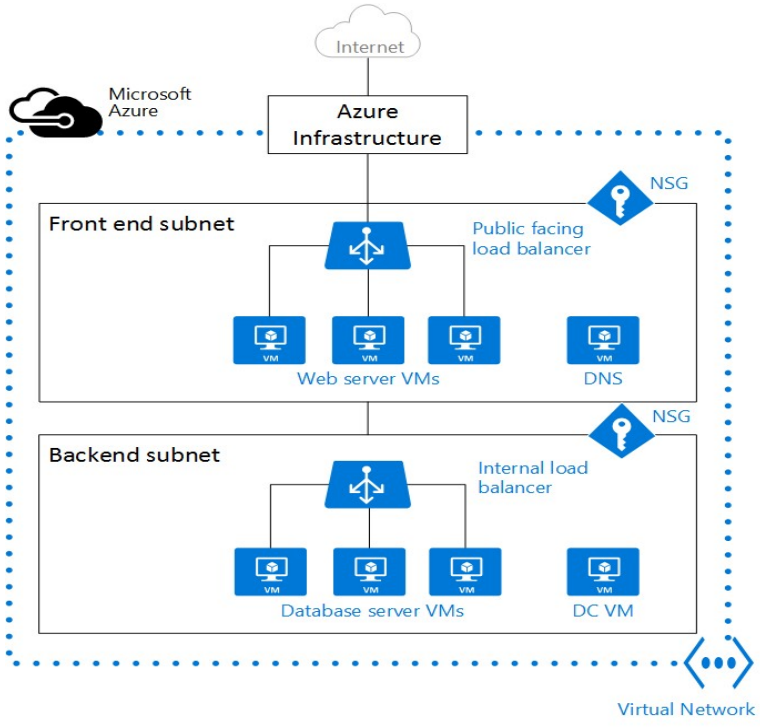
- Subnets are subdivisions of a Virtual Network, allowing for better organization and traffic management.
- These sub-networks can be separated logically, and each subnet consists of a server.
- We can further divide a subnet into two types:

  i. Private
  ii. Public

  - Private - Instances can access the Internet with NAT (Network Address Translation gateway that is present in the public subnet.
  - Public - Instances can directly access the internet.

2. Routes

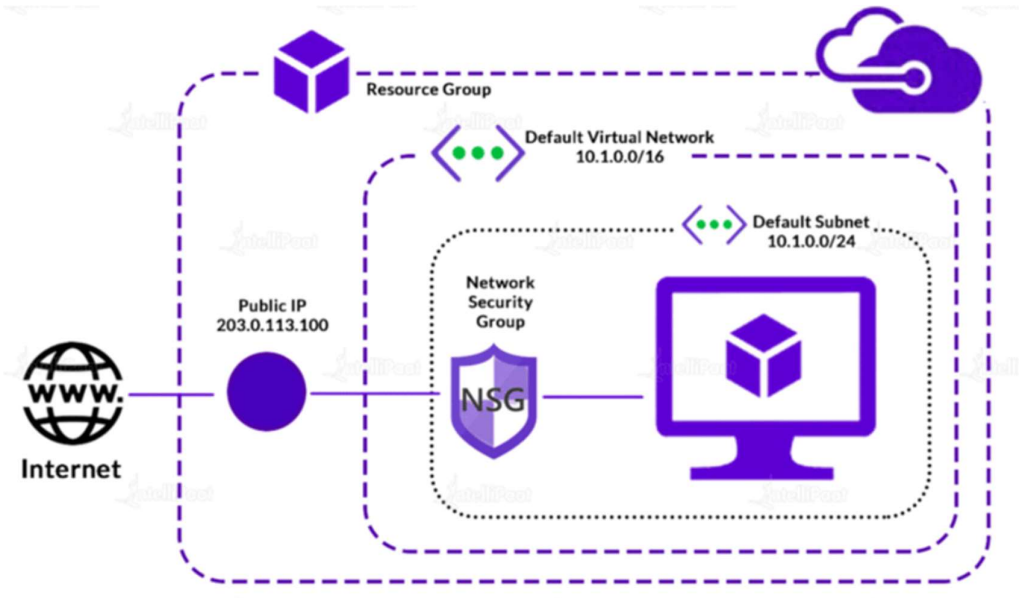
- Routes dictate how network traffic is directed, specifying the destination and next hop.
- Route Tables are collections of routes associated with subnets, enabling custom routing rules.



Network Security Groups (NSGs)

- NSGs are fundamental for Azure's network security, allowing filtering of inbound and outbound traffic.
- Key aspects include:

  - **Rules**: NSGs define allowed or denied traffic based on the five-tuple (source, source port, destination, destination port, and protocol) information.You can't create two security rules with the same priority and direction. A flow record is created for existing connections. Communication is allowed or denied based on the connection state of the flow record. The flow record allows a network security group to be stateful. If you specify an outbound security rule to any address over port 80, for example, it's not necessary to specify an inbound security rule for the response to the outbound traffic. You only need to specify an inbound security rule if communication is initiated externally. The opposite is also true. If inbound traffic is allowed over a port, it's not necessary to specify an outbound security rule to respond to traffic over the port.
  - **Default Rules**: NSGs have default rules for controlling traffic within the Virtual Network and between subnets.
  - **Association**: NSGs can be associated with subnets or individual network interfaces.



Application Security Groups(ASGs)

ASGs group Azure virtual machines based on application requirements, simplifying network security:

- **Simplification**: ASGs allow defining rules based on application roles instead of individual IP addresses.
- **Dynamic Membership**: ASGs support dynamic membership based on tags or other attributes.
- **Rule Association**: Security rules can be associated with ASGs for intuitive and scalable network security management.
- **Subscription Limits:** Each Azure subscription has a limit on the number of ASGs it can contain. The exact limits can be found in the Azure documentation under service limits or quotas.

- **Single Virtual Network Rule:**

  Network Interface Assignment: When you assign a network interface (NIC) to an ASG, all subsequent NICs assigned to that ASG must be in the same virtual network (VNet) as the first NIC.

  ASG Boundaries: You cannot have an ASG span across multiple VNets. Each ASG is confined to a single VNet.

- **Security Rule Constraints:**

  Source and Destination ASGs: When creating security rules where ASGs are used as source and destination, both ASGs must have their NICs in the same VNet.

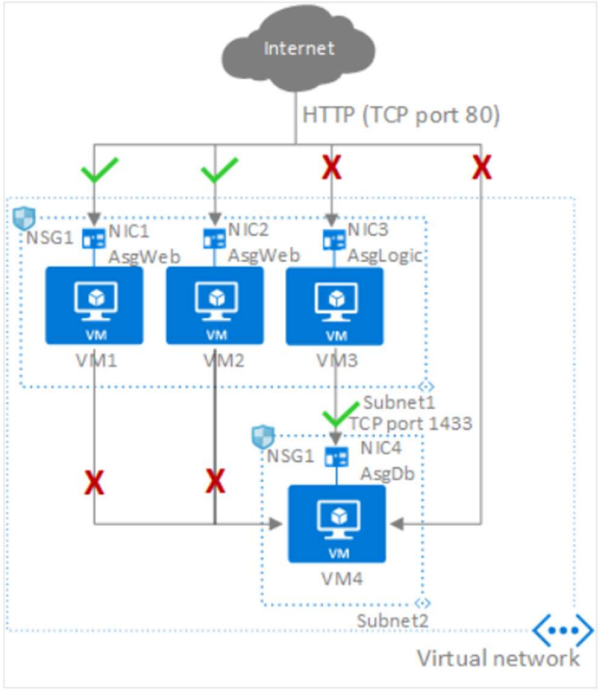
Example Scenario

Imagine you have two application security groups:

- AsgWeb with NICs in VNet1
- AsgDb with NICs in VNet2

Valid Configuration: Both AsgWeb and AsgDb must be in the same VNet to create a rule involving both as source and destination.

Invalid Configuration: AsgWeb in VNet1 and AsgDb in VNet2 cannot be used together in a single security rule because they are in different VNets.



Virtual Network Peering & VNet Gateway

Virtual Network Peering allows connecting Azure Virtual Networks directly, enabling resources in one VNet to communicate with resources in another.

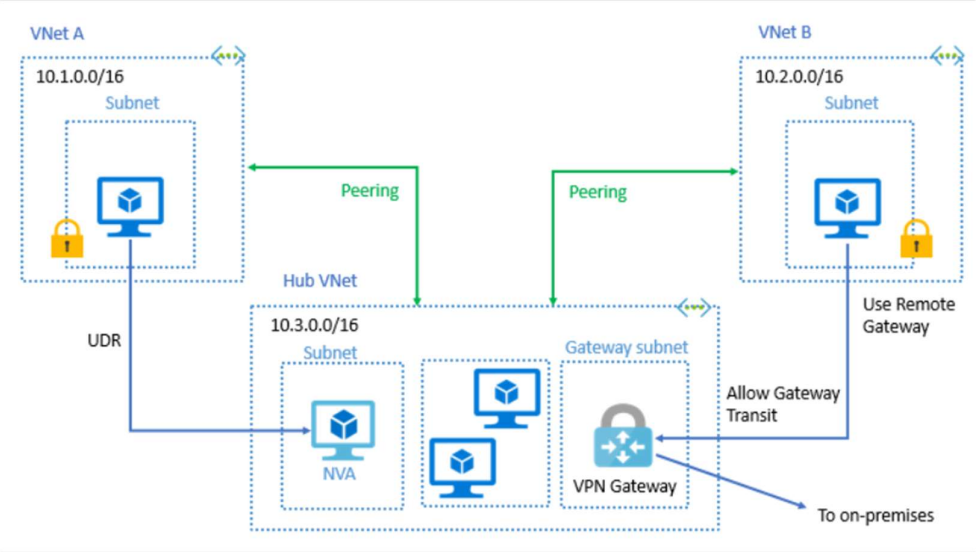
Key features include:

- Global VNet Peering: Peering can be established across regions.
- Transitive Routing: Traffic between peered VNets flows directly, improving performance.

VNet Gateway enables secure communication between on-premises networks and Azure Virtual Networks.

Key features include:

- Site-to-Site VPN: Connects on-premises networks to Azure over an encrypted VPN tunnel.
- Point-to-Site VPN: Enables secure remote access to Azure resources



References

- Microsoft Azure Official Documentation
- “Azure Networking Cookbook" by Mustapha Kebbe
- “Exam Ref AZ-700 Designing and Implementing Microsoft Azure Networking Solutions" by James Fogerson