Azure Virtual Network

Ranjit Karni

VPark Innovations

Ranjit.balu@gmail.com

Ph.No: 9676976662

Agenda

1. Overview of Azure Networking
2. Virtual Network Benefits
3. Understanding Network Resources
4. Create a Vnet using Azure Portal
5. Create a Subnet
6. Create a Network Security Group
7. Create Network Interface Card (NIC) and PublicIP
8. Understanding and Using Azure DNS

Overview of Azure Networking

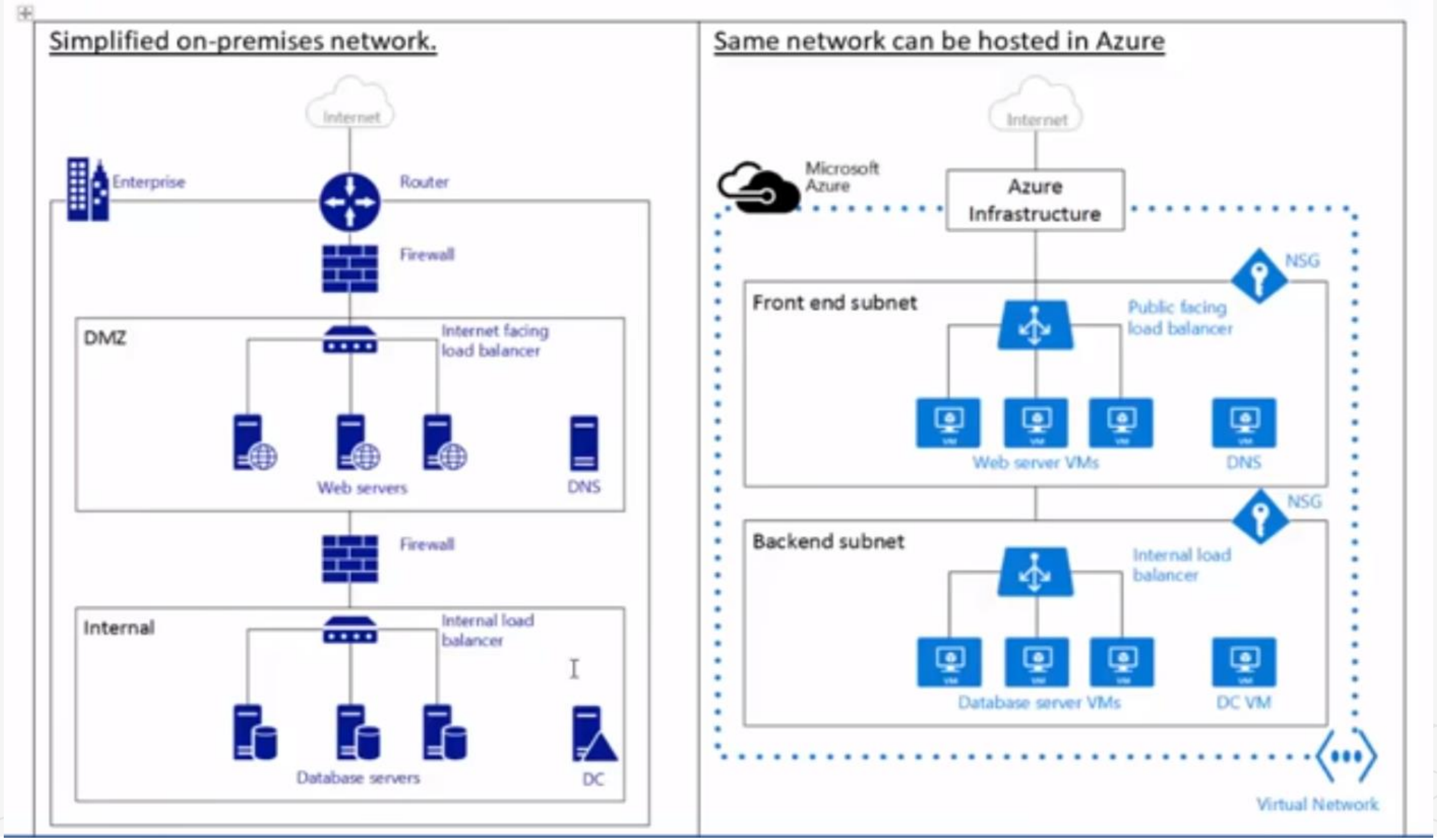
- An Azure Virtual Network (Vnet) is a representation of your own network in the cloud

- It is a logical isolation of the Azure cloud dedicated to your subscription. You can fully control the IP address blocks, DNS Settings, Security Policies and Route Tables within this network

- You can also further segment your Vnet into **subnets** and launch Azure IaaS virtual machines (VMs) and / or Cloud Services (PaaS role instances)

- You can connect the virtual network to your on-premises network using one of the connectivity options available in Azure. In essence, you can expand your network to Azure, with complete control on IP address blocks with the benefit of enterprise scale Azure provides.

Overview of Azure Networking Cont..



Overview of Azure Networking Cont..

- In computer **networks**, a **DMZ (Demilitarized Zone)** is a physical or logical sub-network that separates an internal local area network (LAN) from other untrusted networks, usually the internet

- Notice how the Azure infrastructure takes on the role of the router, allowing access from your Vnet to the public internet without the need of any configuration. Firewalls can be substituted by Network Security Groups(NSGs) applied to each individual subnet. And physical load balancers are substituted by internet facing and internal load balancers in Azure.

Azure Vnet Pricing:

- There is no extra cost for using Virtual Networks in Azure

- The compute instances launched within the Vnet will be charged the standard rates as described in Azure VM Pricing

- The VPN Gateways and Public IP Addresses used in the Vnet will also be charged standard rates

Virtual Network Benefits

Isolation: Vnets are completely isolated from one another. That allows you to create disjoint networks for development, testing and production that use the same CIDR address blocks

Access to the public internet: All IaaS VMs and PaaS role instances in a Vnet can access the public Internet by default. You can control access by using Network Security Groups (NSGs).

Access to VMs within the Vnet: PaaS role instances and IaaS VMs can be launched in the same virtual network and they can connect to each other using private IP addresses even if they are in different subnets without the need to configure a gateway or use public IP addresses.

Name resolution: Azure provides internal name resolution for IaaS VMs and PaaS role instances deployed in your Vnet. You can also deploy your own DNS servers and configure the Vnet to use them

Security: Traffic entering and exiting the virtual machines and PaaS role instances in a Vnet can be controlled using Network Security Groups

Connectivity: Vnets can be connected to each other, and even to your on-premises datacenter, by using a site-to-site VPN connection, or ExpressRoute connection.

Note: The most important and misunderstood thing about windows Azure Virtual Networks is that you cannot add an existing virtual machine to a newly created virtual network. It is important that if you want to leverage Virtual Networking in windows Azure that you must create the virtual networks **BEFORE** creating your virtual machines. Don’t miss the this important step. You’ll be disappointed if you’ve spent a lot of time setting up a virtual machine and later find that you can’t move it to a virtual network.

Understanding Network Resources

IP addresses: There are two types of IP addresses assigned to resources in Azure: **Public** and **Private**

- Public IP Addresses allow Azure resources to communicate with Internet and other Azure public-facing services like Azure Redis Cache, Azure Storage, Azure SQL, Azure KeyVault. It can be either static or dynamic and are assigned to VM, Internet facing load balancers, VPN Gateways and Application Gateways. Static IP cost more where as dynamic IP is cheaper and the IP changes if you decommission the VM.

- Private IP Addresses allows communication between resources in a virtual network, along with those connected through a VPN, without using an internet routable IP addresses. It can be set dynamic (DHCP lease) or static (DHCP reservation).

Preferred IP for Intranets:

Small Network1: 192.168.0.X – for 2 power 8 Systems – IP Address Range = 198.168.0.0/24 (Only last byte changes)

Small Network2: 192.168.1.X – for 2 power 8 Systems – IP Address Range = 198.168.1.0/24 (Only last byte changes)

Large Network: 172.16.X.X – for 2 power 8 Systems – IP Address Range = 172.16.0.0/16 (last 2 bytes change)

Very Large Network: 10.X.X.X - for 2 power 8 Systems – IP Address Range = 10.0.0.0/8 (last 3 bytes change)

Classless Inter-Domain Routing (CIDR) notation is a compact representation of an IP address and its associated routing prefix. The **notation** is constructed from an IP address, a slash ('/') character and a decimal number. The number is the count of leading 1 bits in the routing mask, traditionally called the network mask.

Network Block & Host Block in CIDR Range:

Ex: In 128.42.0.0/21 address space, 128.42.0.0 is network address and 0.0.0.0 is host address, you can create 2 power 10 host addresses from this address space.

Subnets

- Subnet is a **range of IP addresses** in a Vnet, you can divide a Vnet into multiple subnets for organization and security.

- VMs and PaaS role instances deployed to subnets (same or different) within a Vnet can communicate with each other without any extra configuration.

- You can also configure route tables and NSGs to a subnet.

- Based on number of system in a network, Subnet Mask is set.

255.255.255.0 – 2 power 8 Systems

255.255.0.0 – 2 power 16 Systems

255.0.0.0 – 2 power 24 systems

- Within each subnet, you cannot use 5 IP Addresses. The first three IP addresses and the last IP address are reserved and cannot be used for VMs. The first IP Address is subnet address and the last IP Address is subnet broadcast address.

- The smallest subnets that are supported use a **29** bit subnet mask.

Network Security Group (NSG)

- **Network Security Group** provides advanced security protection for the VMs that you create in Azure.

- It controls **inbound** and **outbound** traffic passing through a **Network Interface Card (NIC)** (Resource Manage Deployment Model), a VM (classic deployment), or a subnet (both deployment models).

- **Network Security Group rules** specify whether the traffic is approved or denied. Each rule consists of the following properties:

  - **Name:** A unique identifier for the rule.

  - **Direction:** Traffic is inbound or bound

  - **Priority:** Rules with higher priority apply.

  - **Access:** Specifies whether the traffic is allowed or denied.

  - **Source Port range:** This specifies source ports

  - **Source IP Address Prefix:** This identifies from where traffic originates

  - **Destination IP Address Prefix:** This identifies the traffic destination

  - **Destination Port Range:** This specifies destination ports

  - **Protocol:** Protocol specifies a protocol that matches the rule. It can be UDP, TCP or the asterisk (*) wildcard character *.

NIC and Load Balancers

Network Interface Card (NIC): VMs can communicate with other VMs and other resources on the network by using virtual network interface card (NIC). Virtual NICs configure VMs with private and optional public IP address. VMs can have more than once NIC for different configurations.

Azure Load Balancers: Virtual machines and cloud services in a virtual network can be exposed to internet using Azure load balancers.

> **External Load Balancer**: You can use an external load balancer to provide high availability for IaaS VMs and PaaS role instances accessed **from the public internet**.
>
> **Internal Load Balancer**: You can use an internal load balancer to provide high availability for IaaS VMs and PaaS role instances accessed **from other services** in your Vnet.

Questions?

Ranjit Karni

Vpark Innovations

Ranjit.balu@gmail.com

Ph No: +91-9676976662