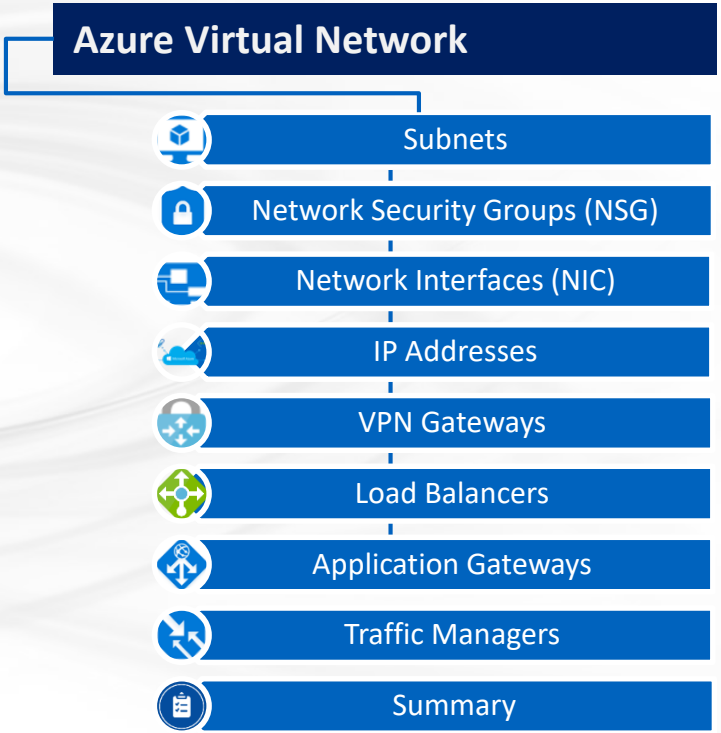
Azure Virtual Networks - Overview

Agenda

Part 01: Azure Virtual Networks – An Overview

AZ-100: Configure and manage virtual networks



Azure Virtual Networks - Overview

Virtual Networks

A virtual network in Azure is similar to the network that we have in our on-premises environment, helping us connect different resources.

Virtual networks -

- Have their own private address space as defined during their creation
- Can have one or more subnets with their own address space allocated, which is one part of the main address space of the vNet

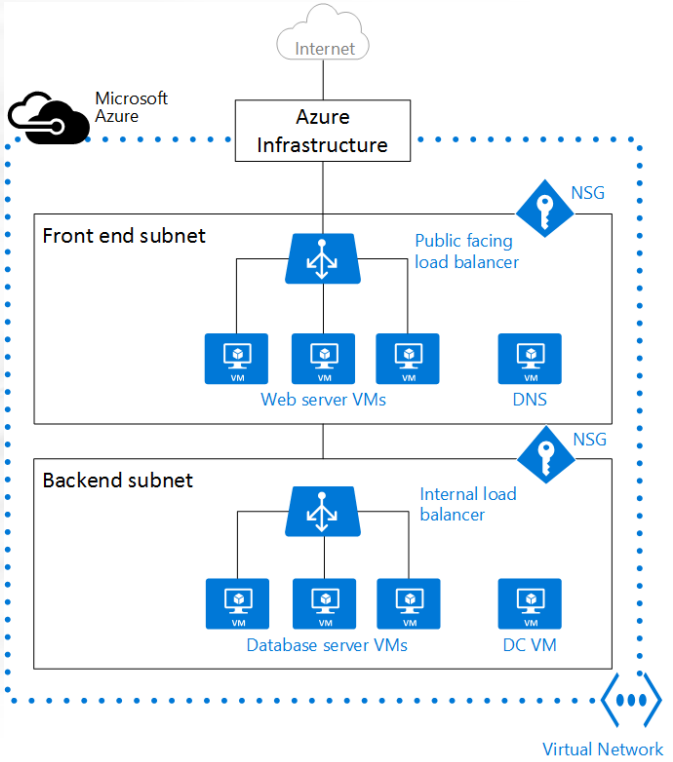
With the provision of the virtual network, Azure provide its own name resolution using the Azure DNS. There is additionally an option to configure our own DNS server

Azure Virtual Networks - Overview

Subnets

Subnets provide separation of concern within virtual networks. A virtual network can be segmented into one or more subnets.

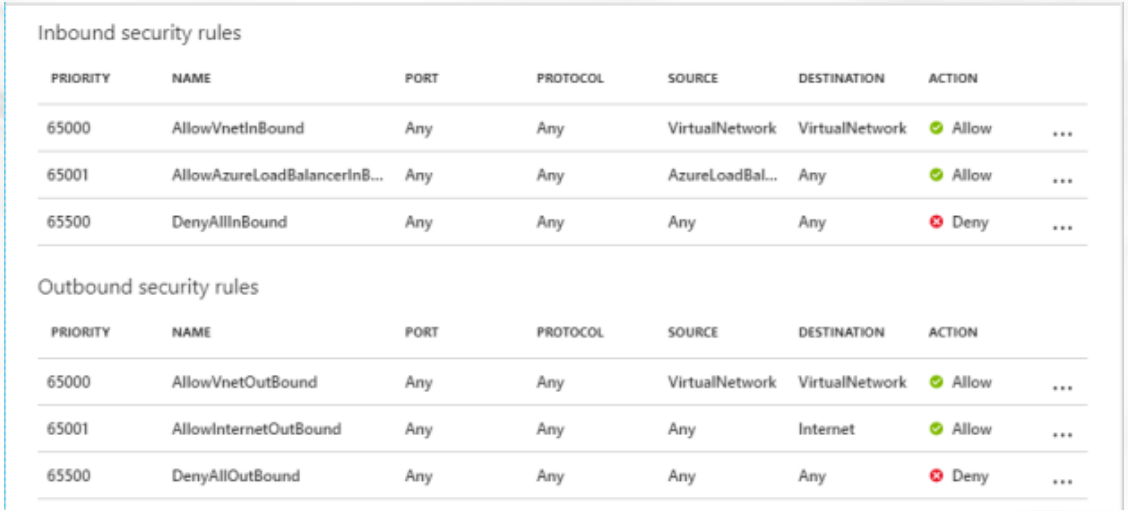
- Each subnet must have a unique IP address range, within the address space of the virtual network
- Address range for the Subnets cannot overlap
- Resources within subnets can communicate with each other
- Certain resources needs to have their own dedicated subnets



Azure Virtual Networks - Overview

Network Security Group

You can filter the incoming and outgoing traffic to and from Azure resources using Network Security Groups. A network security group contains a set of rules that allow or deny network traffic



Inbound security rules

PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInB...	Any	Any	AzureLoadBal...	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

Outbound security rules

PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow
65500	DenyAllOutBound	Any	Any	Any	Any	Deny

Azure Virtual Networks - Overview

Network Interfaces (NICs)

It allows the connectivity between Azure Virtual Machine and the vNet, enabling the VM to communicate with internal and external resources over the network.

One virtual machine can have more than one network interface depending upon the size of the VM opted for.

Azure Virtual Networks - Overview

IP Addresses (IPs)

IP addresses are assigned to resources to communicate with each other within and outside Azure. There are two types of IP addresses in Azure:

1. Public IP addresses: These IP addresses can be assigned to-
   - Virtual Machines
   - External/Internet facing Load Balancers (Layer 3 Load Balancing)
   - VPN Gateways (P2S and S2S Connectivity)
   - Application Gateways (Layer 7 Load Balancing)

2. Private IP addresses: These IP addresses can be assigned to -
   - Virtual Machines
   - Internal Load Balancers (Layer 3 LBs)
   - Application Gateways (Layer 7 LBs)

Azure Virtual Networks - Overview

VPN Gateways

The VPN Gateway helps connecting networks within Azure, such as –

1. Azure vNet to vNet.

It also helps in connecting Azure vNet to on-premises network, such as –

1. Point to Site Connectivity (P2S)
2. Site to Site Connectivity (S2S)

Azure Virtual Networks - Overview

Azure Load Balancers

Azure LBs are layer 4 load balancers operating at TCP and UDP levels and deliver high availability. They –

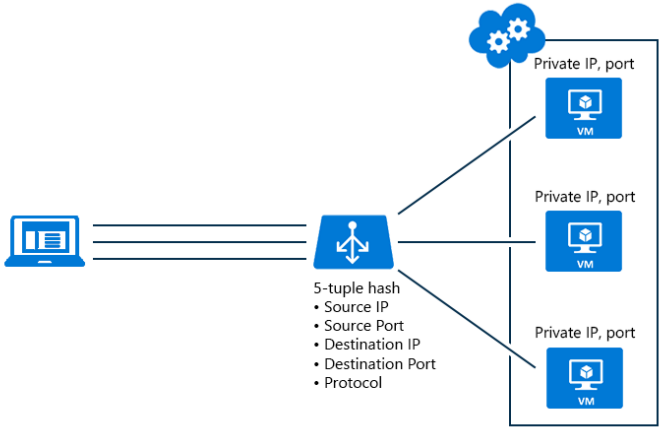
1. Load-balance incoming internet traffic to your VMs
2. Load-balance traffic across VMs inside a virtual network
3. Help in forwarding traffic to a specific port on a particular VM with the defined inbound network address translation (NAT) rules.
4. Provide outbound connectivity for VMs in the VNet using a public Load Balancer

Azure Virtual Networks - Overview

Azure Load Balancers Contd.

Azure LBs uses a 5-tuple hash composed of –

1. Source IP address
2. Source port
3. Destination IP address
4. Destination port
5. Protocol



https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-overview

Azure Virtual Networks - Overview

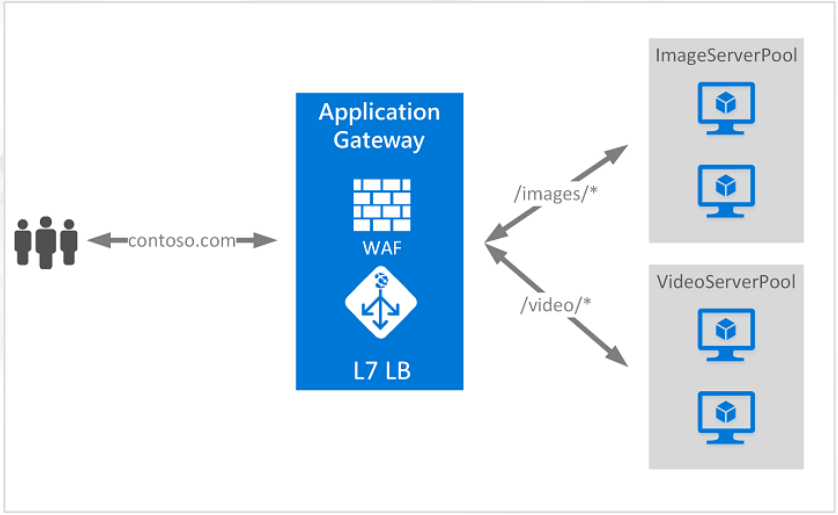
Application Gateways

They are the layer 7 load balancers and provide load balancing of the web applications. They can also work as a Web Application Firewall (WAF) providing security to the applications. They provide –

1. SSL termination with certificate offloading
2. Connection Draining
3. Create custom error pages with your own branding
4. URL based routing
5. Multiple Site hosting
6. Session Affinity
7. Websocket and HTTP/2 traffic

There are two SKUs for application gateway, which are:

1. Standard
2. Web Application Firewall (WAF)



Azure Virtual Networks - Overview

Application Gateways Contd.

Application Gateway	Load Balancers
Application Gateway can distribute HTTP and HTTPs traffic	LB can distribute different types of traffic
Application Gateways are defined inside the virtual network	Load Balancers can be defined inside or outside of virtual network
Application Gateways have both Frontend IP configuration and Backend Pools	Load Balancers have the Frontend IP configuration
Has HTTPs settings to define the cookie based session affinity	No HTTPs setting
Has Listeners, which listen to the incoming HTTP/HTTPs traffic from different source	There are no HTTP/HTTPs listeners as they distribute different types of traffic

Azure Virtual Networks - Overview

Traffic Manager

Traffic Managers are the DNS-based load balancer. They help in –

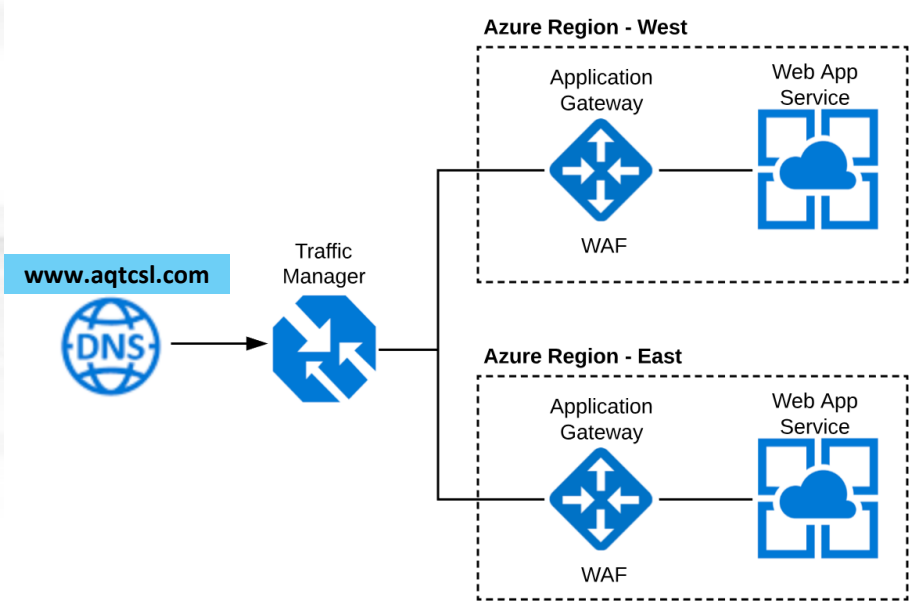
1. The distribution of traffic optimally to services across different Azure regions
2. Providing high availability and performance.
3. Providing service maintenance without downtime
4. Proving hybrid application experience
5. Distributing traffic for complex deployments

Azure Virtual Networks - Overview

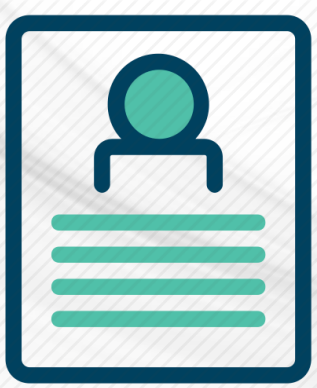
Traffic Manager contd.

The below routing methods are available in Traffic Manager -

1. Priority
2. Weighted
3. Performance
4. Geographic
5. Multivalue
6. Subnet



Summary



- ✓ Azure Virtual Network
  - ❑ Subnets
  - ❑ Network Security Groups
  - ❑ NICs
  - ❑ IP addresses
  - ❑ VPN gateways
  - ❑ Load Balancers
  - ❑ Application Gateways
  - ❑ Traffic Managers

Download the training material from – Azure Training