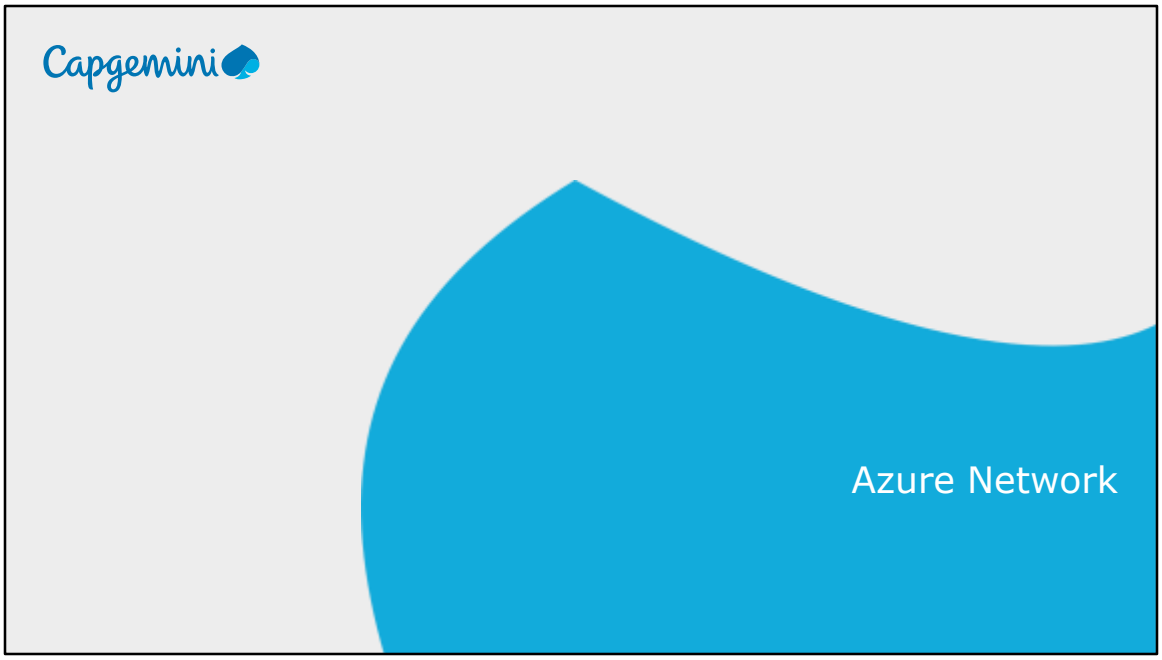

Capgemini
Azure Network

Lesson Objectives

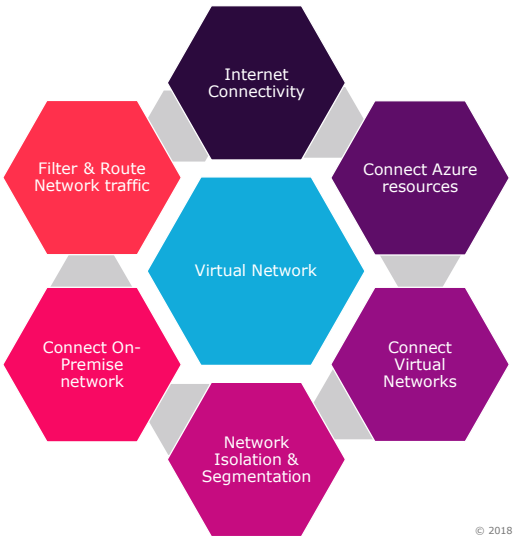
At the end of this module you will be able to:

- ✓ Connect cloud and on-premises infrastructure and services
- ✓ Create Azure virtual networks and subnet in it
- ✓ Create Network security groups with inbound / outbound rules
- ✓ Create Internet load balancing using Azure load balancer
- ✓ Understand the features provided by Application Gateway, Traffic Manager and VPN Gateway

Azure Virtual Network

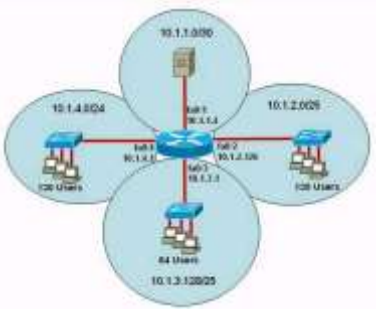
- Azure Virtual Network(VNet) is a private network in the cloud.
- Azure Virtual Network enables many types of Azure resources, such as Azure Virtual Machines (VM), to securely communicate with each other, the internet, and on-premises networks.
- It is a logical isolation of Azure cloud dedicated for your subscription.

Azure Virtual Network Capabilities



Subnets

- A subnet (short for "subnetwork") is an identifiably separate part of an organization's network.
- It is a range of IP Addresses in the VNet.
- VNet can be divided into multiple subnets
- Resources & services deployed to the subnets (same or different) in the same Vnet can communicate with each other without any extra configuration



A subnetwork or subnet is a logical subdivision of an IP network. The practice of dividing a network into two or more networks is called subnetting. For example, 255.255.255.0 is the subnet mask for the 192.168.1.0/24 prefix.

10.0.0.22/24 (or) 10.0.0.22/255.255.255.0

00001010.00000000.00000000.00010110
11111111.11111111.11111111.00000000

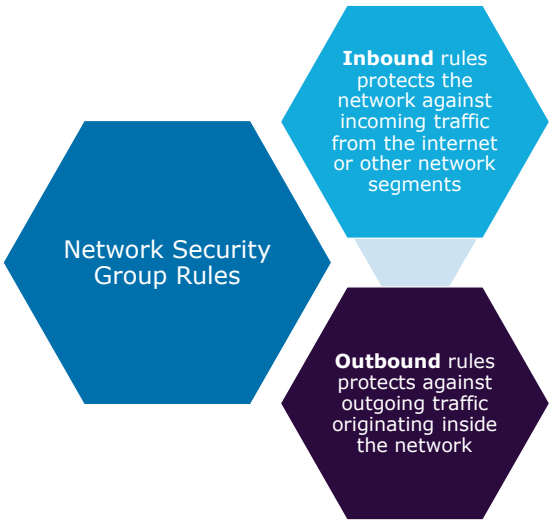
00001010.00000000.00000000.00000000

10.0.0.0 - 10.0.0.255 (256 addresses)

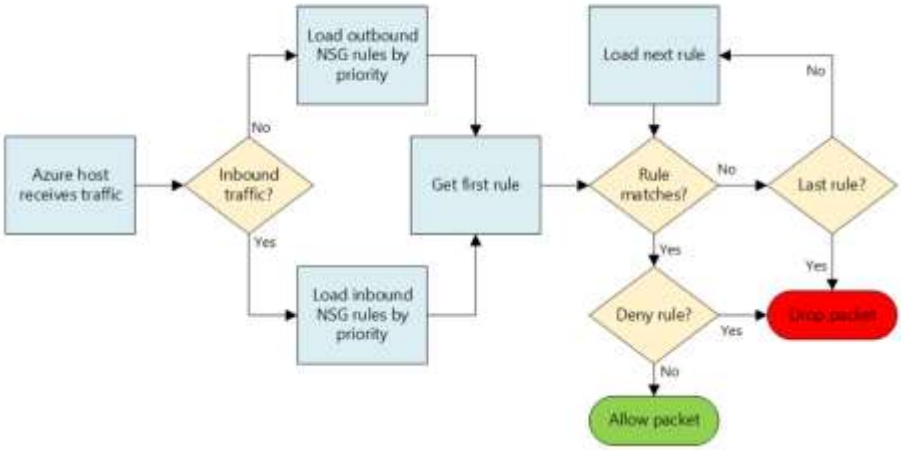
Network Security Groups (NSG)

- A network security group (NSG) contains a list of security rules that allow or deny network traffic to resources connected to Azure Virtual Networks (VNet).
- NSGs can be associated to subnets, individual VMs (classic), or individual network interfaces (NIC) attached to VMs (Resource Manager)
- When an NSG is associated to a subnet, the rules apply to all resources connected to the subnet

NSG Rules



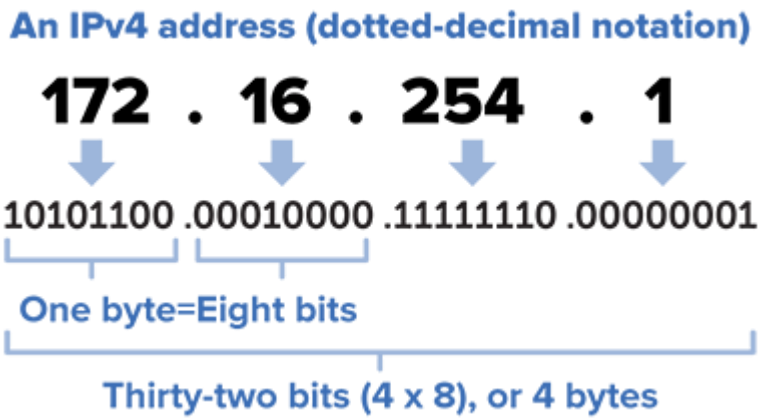
NSG Rules Priority



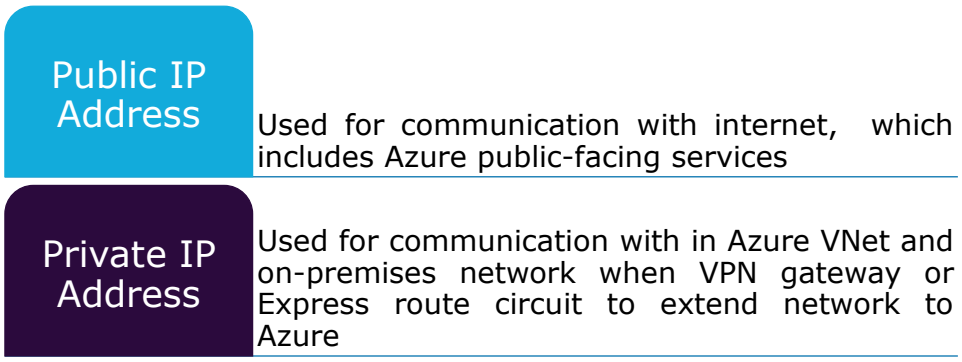
IP address

- An IP address, short for Internet Protocol address, is an identifying number for a piece of network hardware.
- IP address allows a device to communicate with other devices over an IP-based network like the internet.

Any device connected to the IP network must have a unique IP address within the network



Types of IP address



Public IP Address

In Azure resource manager, a public IP address is a resource that has its own properties.

Public IP Address can be associated with Virtual Machines, Internet-facing Load balancers, VPN Gateways and Application Gateways

There are two methods in which an IP address is allocated to a *public* IP resource

• **Dynamic***:* It is the default allocation in which IP address will be allocated when the associated virtual machine is started. IP Address will get changed when VM is stopped and restarted

• **Static** : To ensure the IP address for the associated resource remains the same, the allocation method need to be explicitly set to *static*

Private IP Address

Private IP addresses allows Azure resources to communicate with other resources in a virtual network or an on-premises network through a VPN gateway or ExpressRoute circuit, without using an Internet-reachable IP address

Private IP Address can be associated with Virtual Machines, Internal Load balancers and Application Gateways

Host Name Resolution

DNS hostname resolution

- DNS domain name label can be specified for a public IP resource, which creates a mapping for ***domainnamelabel.location.cloudapp.azure.com*** to the public IP address in the Azure-managed DNS servers

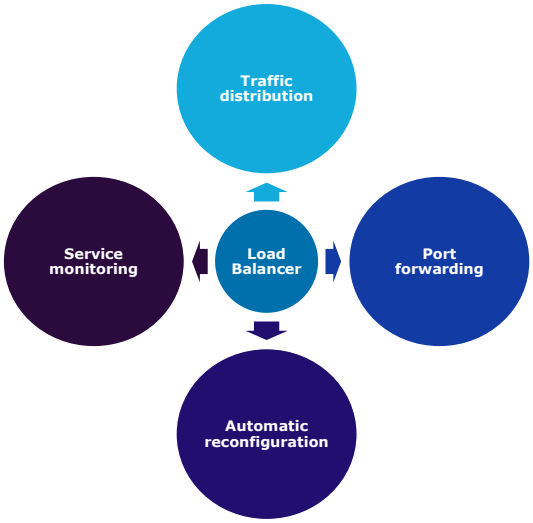
Internal DNS hostname resolution (for VMs)

- All Azure VMs are configured with Azure-managed DNS servers by default, unless it is explicitly configured with custom DNS servers. These DNS servers provide internal name resolution for VMs that reside within the same VNet.

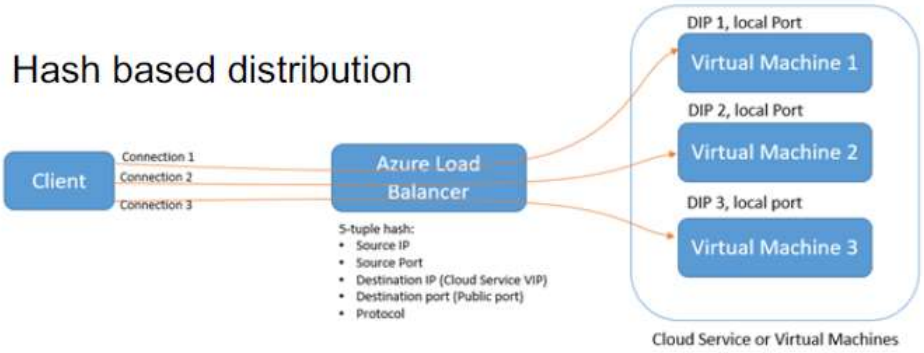
Load Balancer

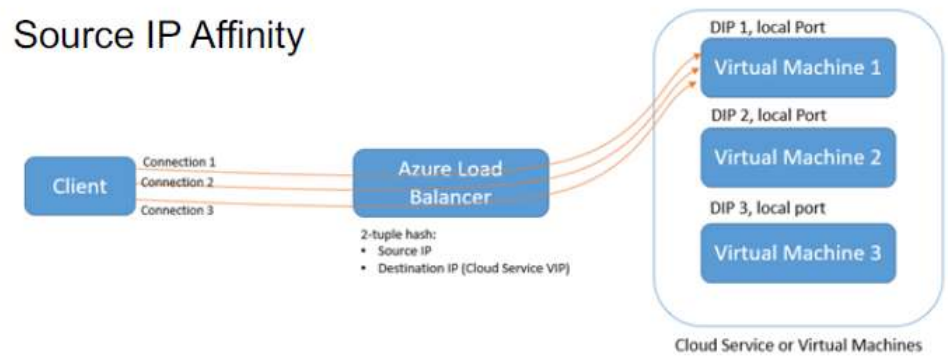
- Load Balancer is used to distribute the traffic evenly among the resources.
- There are 2 types of Load Balancers
  - External Load Balancers(Internet Load Balancers)
    - It receives traffic from internet and sits outside the Virtual network
  - Internal Load Balancers
    - It sits inside the virtual network and wont get the traffic from internet.

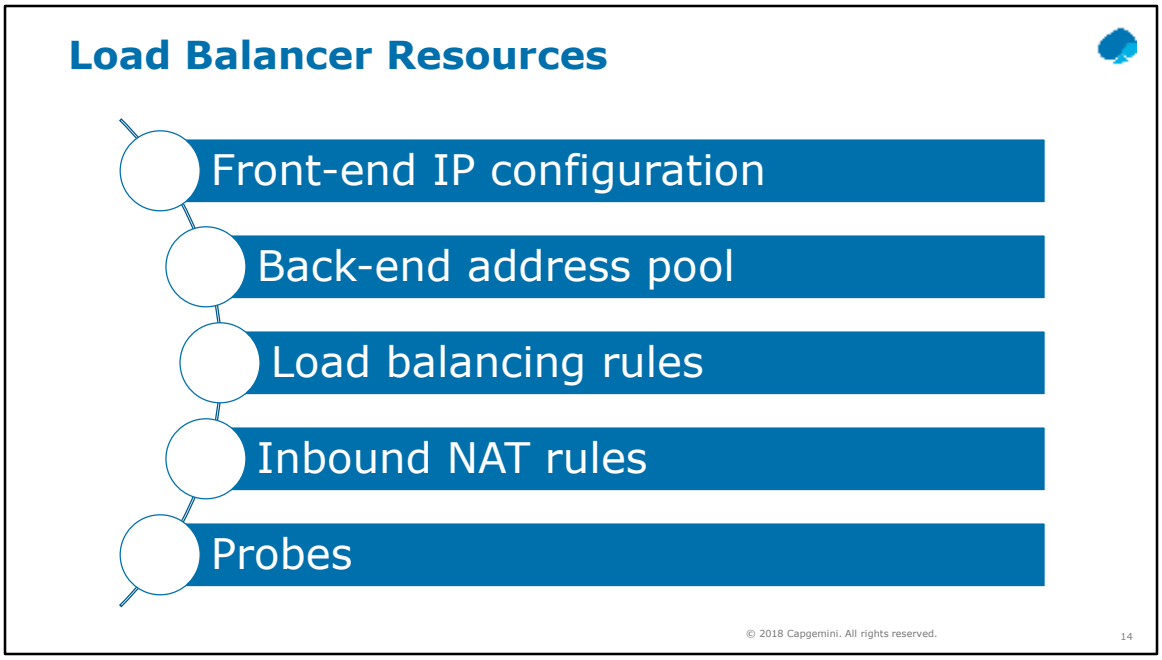
Load Balancer Features



Traffic Distribution







Front-end IP configuration
A Load balancer can include one or more front end IP addresses, otherwise known as a virtual IPs (VIPs). These IP addresses serve as ingress for the traffic.

Back-end address pool
These are IP addresses (DIPs) associated with the virtual machine Network Interface Card (NIC) to which load will be distributed.

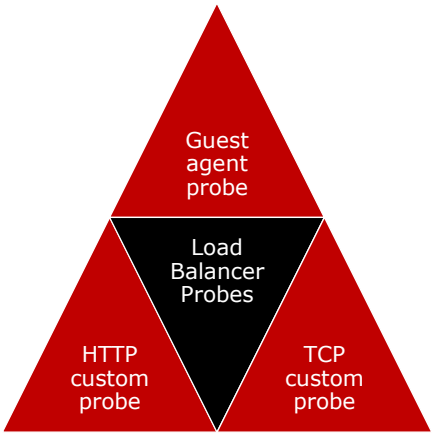
Load balancing rules
A rule property maps a given front end IP and port combination to a set of back end IP addresses and port combination. A single load balancer can have multiple load balancing rules. Each rule is a combination of a front-end IP and port and back-end IP and port associated with VMs.

Inbound NAT rules
NAT rules defining the inbound traffic flowing through the front end IP and distributed to the back end IP.

Probes
probes enable you to keep track of the health of VM instances. If a health probe fails, the VM instance will be taken out of rotation automatically.

Load Balancer Probes

- Azure Load Balancer can probe the health of the various server instances. When a probe fails to respond, the load balancer stops sending new connections to the unhealthy instances.
- Load balancers supports three types of probes
  - Guest Agent Probe, Http Custom Probe & TCP Custom Probe



Azure Available sets

- Azure Availability sets ensures that if a hardware or software failure within Azure happens, only a subset of your VMs are impacted and that your overall solution remains available and operational
- To provide redundancy to the application, it is recommended to add two or more similarly configured virtual machines in an availability set.
- This configuration will meet the SLA of 99.95% Azure SLA
- Combine the Azure load balancer with an availability set to get the most application resiliency

Each virtual machine is assigned an update domain and a fault domain by Azure.

Update domains define the group of virtual machines that can be rebooted at the same time

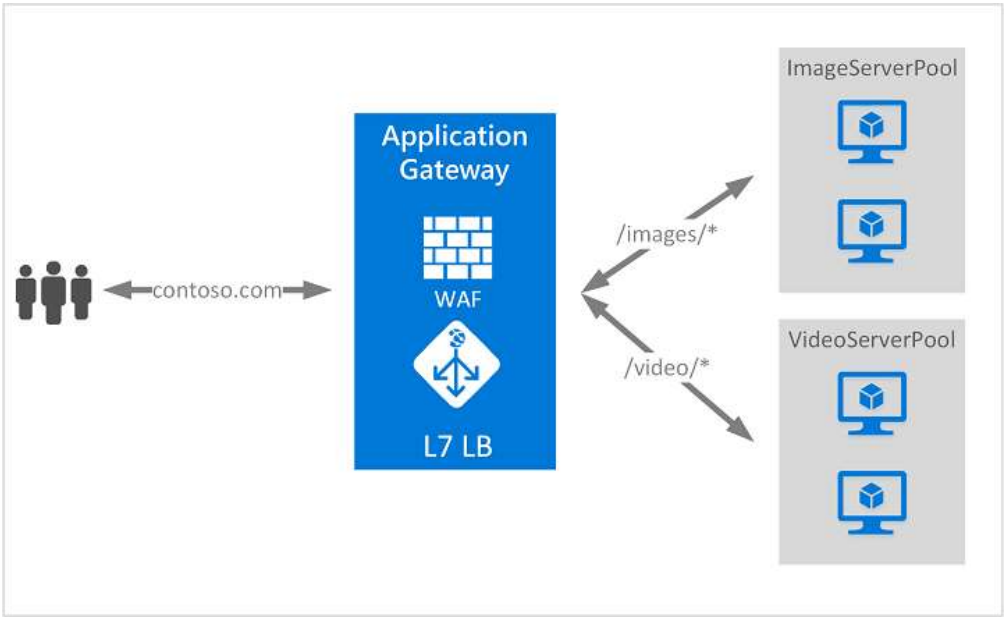
Fault domain define the group of virtual machines that share a common power source and network switch.

For example, when you add two virtual machines into a availability set, Azure automatically assigns different fault & update domain to each virtual machine.

Azure Application Gateway

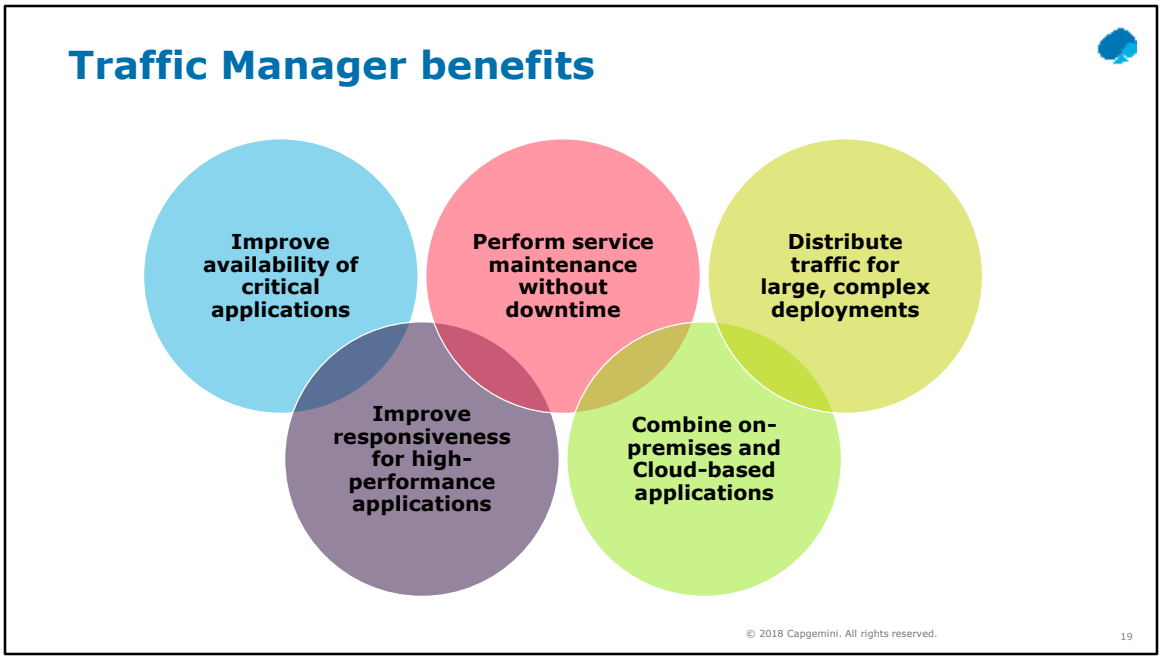
- Azure Application Gateway is a web traffic load balancer that enables us to manage traffic to web applications.
- Traditional load balancers operate at the transport layer and route traffic based on source IP address and port, to a destination IP address and port. But with the Application Gateway you can be even more specific. For example, you can route traffic based on the incoming URL
- This type of routing is known as application layer (OSI layer 7) load balancing

If /images is in the incoming URL, we can route traffic to a specific set of servers (known as a pool) configured for images. If /video is in the URL, that traffic is routed to another pool optimized for videos.



Traffic Manager

- Microsoft Azure Traffic Manager allows us to control the distribution of user traffic for service endpoints in different datacenters.
  - Service endpoints supported by Traffic Manager include Azure VMs, Web Apps, and cloud services.
  - Traffic Manager can be used with external, non-Azure endpoints also.



Improve availability of critical applications : Traffic Manager delivers high availability for your applications by monitoring your endpoints and providing automatic failover when an endpoint goes down.

Improve responsiveness for high-performance applications : Azure allows you to run cloud services or websites in datacenters located around the world. Traffic Manager improves application responsiveness by directing traffic to the endpoint with the lowest network latency for the client.

Perform service maintenance without downtime : You can perform planned maintenance operations on your applications without downtime. Traffic Manager directs traffic to alternative endpoints while the maintenance is in progress.

Combine on-premises and Cloud-based applications : Traffic Manager supports external, non-Azure endpoints enabling it to be used with hybrid cloud and on-premises deployments, including the "burst-to-cloud," "migrate-to-cloud," and "failover-to-cloud" scenarios.

Distribute traffic for large, complex deployments : Using nested Traffic Manager profiles, traffic-routing methods can be combined to create sophisticated and flexible rules to support the needs of larger, more complex deployments.

Azure VPN Gateway

- A VPN gateway is a specific type of virtual network gateway that is used to send encrypted traffic between an Azure virtual network and an on-premises location over the public Internet.
- Gateways can be of two types:
  - **VPN**: Network traffic is sent encrypted over internet
  - **Express**: Network traffic is sent on a dedicated private connection

Express Route enables to connect Azure with on-premises network over a dedicated private connection facilitated by connectivity provider. They do not go over public internet. You can establish the same in three different ways.

Co-located at a cloud exchange: If you are co-located in a facility with cloud exchange, you can order virtual cross-connections to the Microsoft cloud through the co-location provider's Ethernet exchange. It can offer layer 2 cross connections or managed layer 3 cross connections.

Point to Point Ethernet connections: You can connect your on-premises datacenters/offices to the Microsoft cloud through point-to-point Ethernet links. It can offer layer 2 cross-connections or managed layer 3 cross connections.

Any to any networks: You can integrate your WAN with the Microsoft cloud. WAN providers typically offer managed Layer 3 connectivity.

Once connected to one region it will provide access to all regions within the geopolitical region.

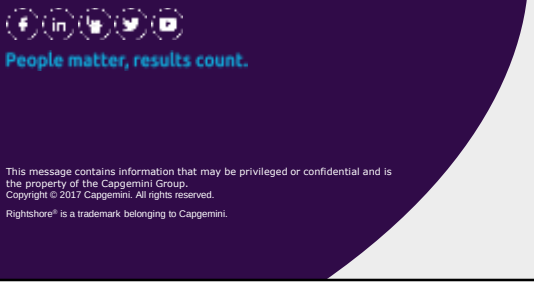
Use ExpressRoute premium add-on to extend the connectivity across geopolitical boundaries.

Summary

- Virtual Network provision us to connect everything from virtual machines to incoming VPN connections.
- Network security group (NSG) allow or deny network traffic to resources connected to Azure Virtual Networks
- Load Balancer delivers high availability and network performance to the applications. It balances inbound and outbound connections and requests to your applications or service endpoints

Summary

- Application Gateway builds secure, scalable, and highly available web front ends in Azure. It optimizes delivery from application server farms while increasing application security with a web application firewall
- Traffic Manager distributes traffic optimally to services across global Azure regions, while providing high availability and responsiveness
- VPN Gateway establish secure, cross-premises connectivity
  - ExpressRoute provides a dedicated private network fiber connections to Azure



People matter, results count.

About Capgemini

With more than 190,000 people, Capgemini is present in over 40 countries and celebrates its 50th Anniversary year in 2017. A global leader in consulting, technology and outsourcing services, the Group reported 2016 global revenues of EUR 12.5 billion. Together with its clients, Capgemini creates and delivers business, technology and digital solutions that fit their needs, enabling them to achieve innovation and competitiveness. A deeply multicultural organization, Capgemini has developed its own way of working, the Collaborative Business Experience™, and draws on Rightshore®, its worldwide delivery model.

Learn more about us at

www.capgemini.com