Virtual Network (VNet):

- VNet enables Azure resources to securely communicate with each other, the internet, and on-premises networks.
- VNet is virtual (like VM)

IP Address ::

- An IP address is a unique numerical identifier for a device or network that connects to the internet.
- IP stands for "Internet Protocol", which is the set of rules that govern how data is sent over the internet or a local network.

Address space::::

- An address space is the range of IP addresses that are available
- Every service or resource that is connected to a VNet will get its own unique address on that VNet within the address space. (that is how services on the same Vnet can find each other and communicate)
- you assign an address space to the Vnet and the serice or resources automatically gets an Ip address in that address space.

Subnet::::

- Subnets enable you to divide VNet into one or more subnetworks and allocate a portion of the VNet address space to each subnet
- by doing thus we can have multiple networks on the same VNet

Uses of subnet::::

- we can group some of resources (may be they are related to a particular project) onto same subnet to mate it easier to keep an overview
- if IP adress range is small, it is easy to allocate address to resources
- we can secure individual subnets using a network secuiry group

Subnet Regions& Subscriptions ::::

- A VNet belongs to a single region. Every resource on the Vnet must be in the same region too.
- A VNet belongs to just one subscription, but a subscription can have multiple VNets.

Advantages of VNet

- Scaling:: If you want to add more address in your address space, you can do it. Vnet will support it. If you want to create a new VNet it is also easy.
- High availability:: by using peering Vnets, load balancer, VPN gateway we can increase the availability of resources
- Isolation :: we can isolate services and products very efficiently and simply with VNets. Using subnets and network security groups you can manage and organize your resources within a VNet

VNet peering::::

That allows you to connect two or more VNets together in the same Azure region or across different Azure regions.

- Traffic between VMs in Peering uses private microsoft network and never passes through the public internet, just like if the VMs were on the same VNet

peering benefits)))

- Low-latency, high bandwidth connection between resources in different virtual networks.
- Resources in separate VNets can communicate
- Transfer data easily between subscriptions and deployment in separate regions

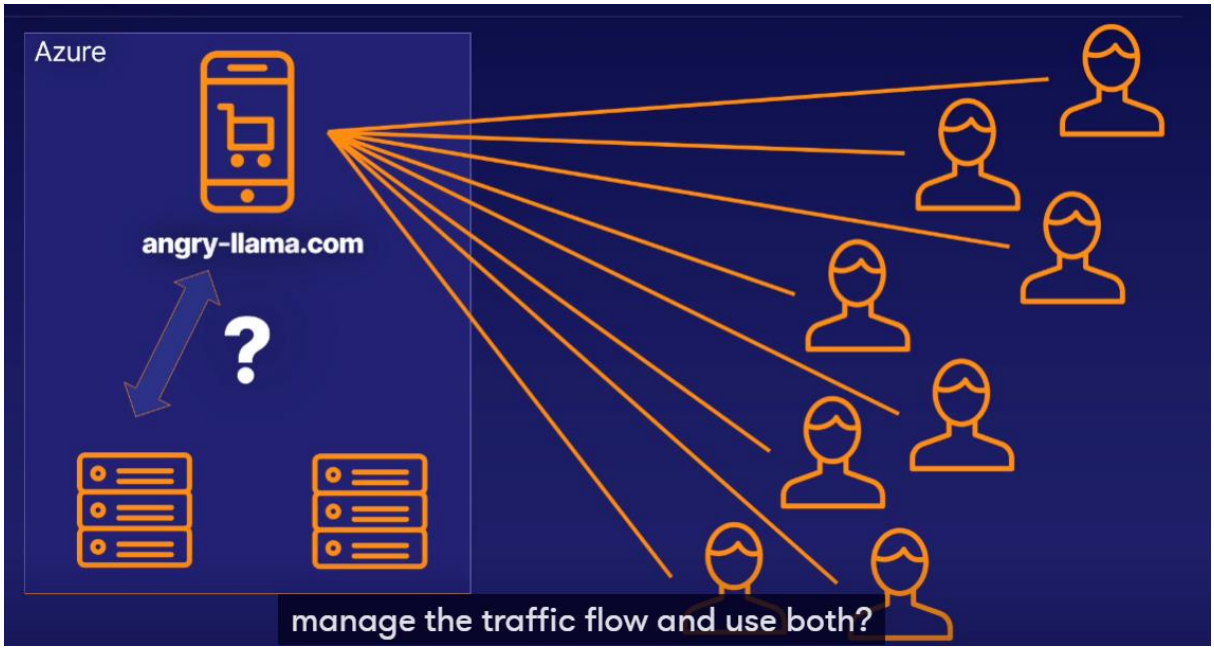
Load Balancer ::

When you have more than one VM serving the application, how do you decide which VM gets a particular user?

A load balancer is the answer.

Imagine this scenario.

Your online business for booking removals of angry llamas is going super well. You're starting to get much more traffic than you originally anticipated. The VM that you use for processing some of the old data is getting overloaded at times. You add a second VM, but how do you now manage the traffic flow and use both?



Adding a load balancer in front of the two VMs to capture the traffic before it reaches them means you can manage where the traffic goes.

Load Balancer distributes traffic from the internet or local network (Inbound Flows) that arrive on the Load Balancer's frontend (The access point for the load balancer. All the traffic goes here first) to backend pool instances (The VM instances receiving traffic), according to rules and health probes (refers to the load balancer rules for directing the traffic. A health probe is a service that makes sure a VM is ready to receive traffic before the load balancer sends any.).

- Balance the load of incoming traffic into a system or application.
- A load balancer works well with internal applications.
- Traffic can be forwarded to a specific machine in the backend pool.
- Allow outbound connectivity for backend pool VMs.

VPN Gateway ::

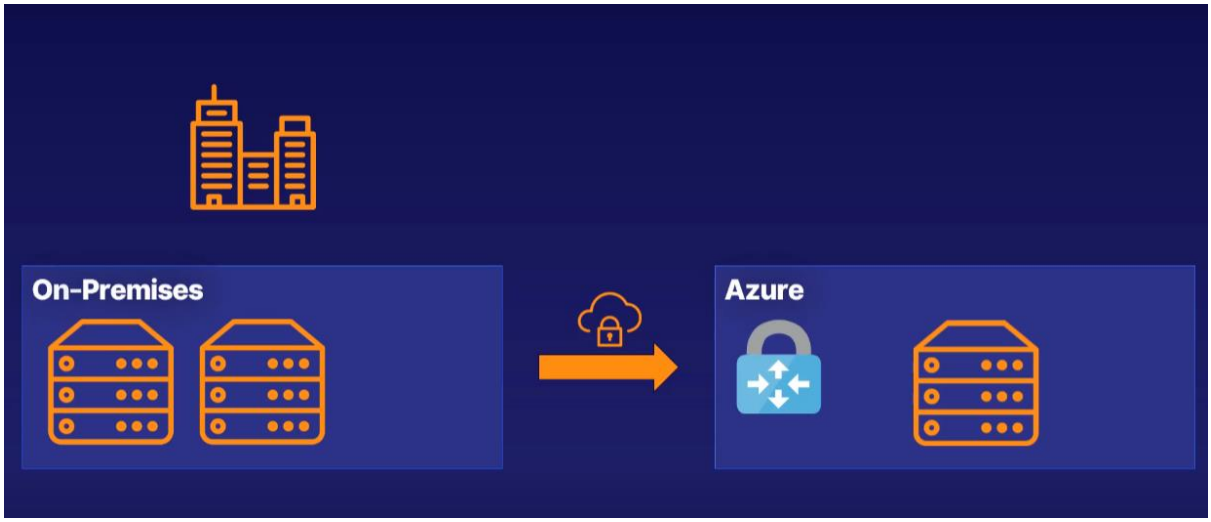
When you want to securely communicate between your Azure resources and your on-premises network, what do you do?

== Use a VPN gateway

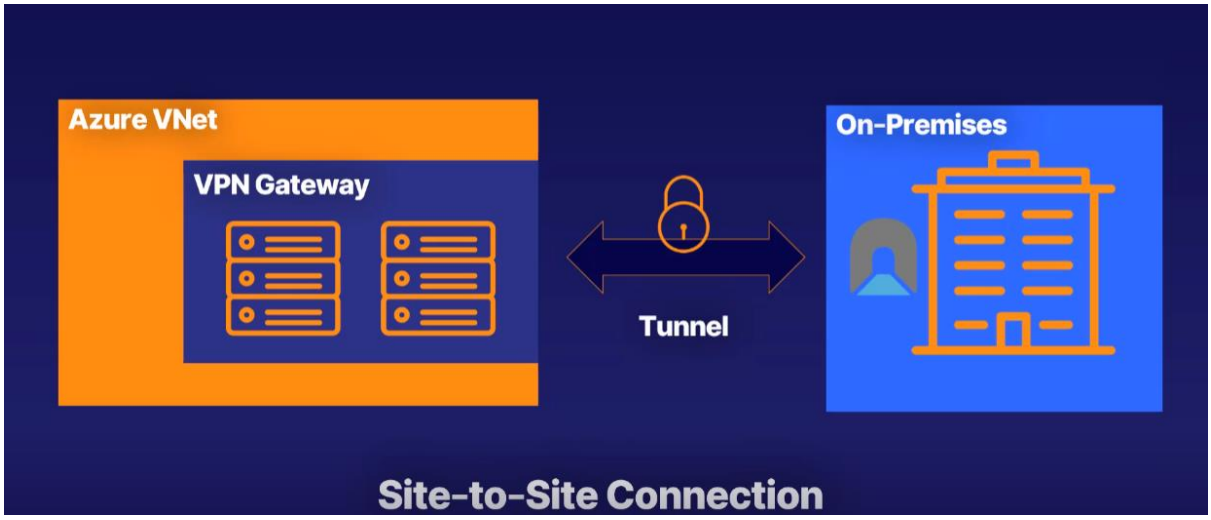
A VPN gateway is a specific type of virtual network gateway that is used to send encrypted traffic between an Azure virtual network and an on-premises location over the public internet.

Let's say you have an established company that has its own on-premises infrastructure. This is working well, but you are wanting to move parts of your system to the cloud to take advantage of the cloud goodness, such as scalability, high availability, and costs reduction. This means you'll have a hybrid solution, with some of your data on-premises and some on Azure.

In order to communicate securely between the two, you create a VPN gateway, which is a specific kind of VNet gateway. A VPN gateway is a key part of having a secure and available hybrid cloud architecture.



An Azure VNet with a VPN gateway attached - this gateway will have its own public IP address - a secure connection called a tunnel, which has one of a number of encryption mechanisms, an on-premises network with a complementary gateway that can accept the encrypted data. And this is called a **site-to-site connection**.



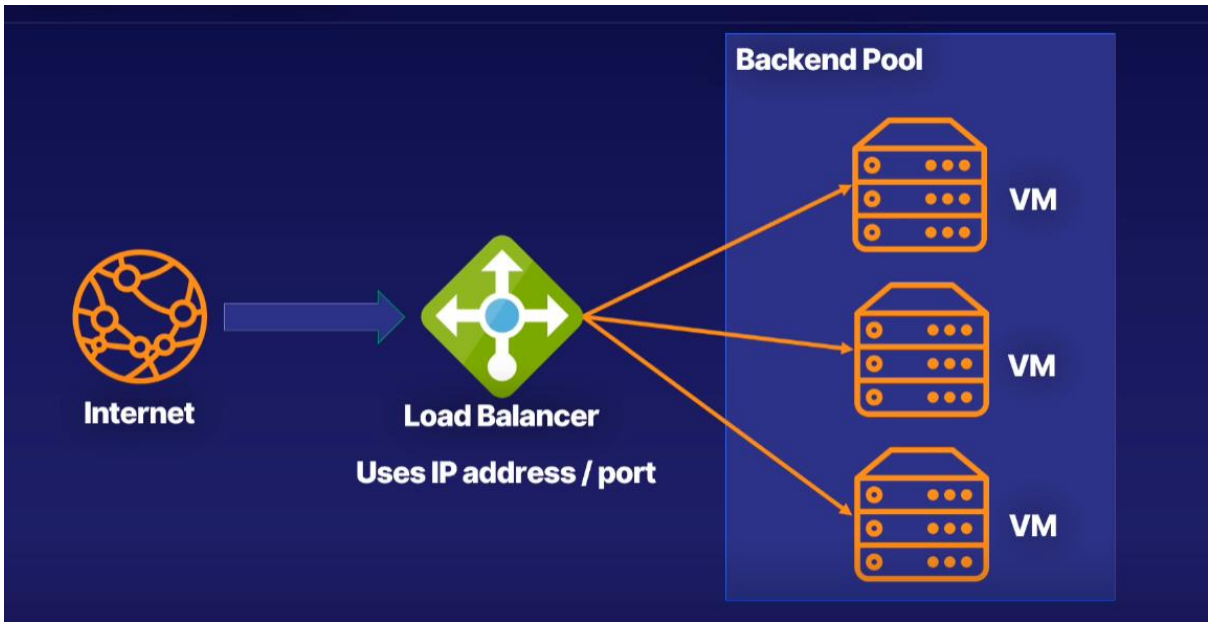
You can also have one VPN gateway with more than one on-premises network connecting to it. This is called a **multi-site connection**.

Summary

- A VPN gateway is a specific kind of VNet gateway, which is two or more virtual machines deployed to a specific subnet.
- A VNet gateway of type VPN becomes a VPN gateway.
- VPN gateway is used to send encrypted data from Azure to on-premises.

There are three parts to a VPN gateway use case scenario.

- Azure gateway subnet of two or more machines,
- a secure tunnel for data to be transmitted, and
- an on-premises gateway to connect to as well.



A load balancer receives your internet and network traffic and, based on an IP address and a port, it will send that data to one of the VMs in the backend pool.

Application Gateway ::

What do you get if you take a load balancer and sprinkle a little cloud on it?

== An application gateway

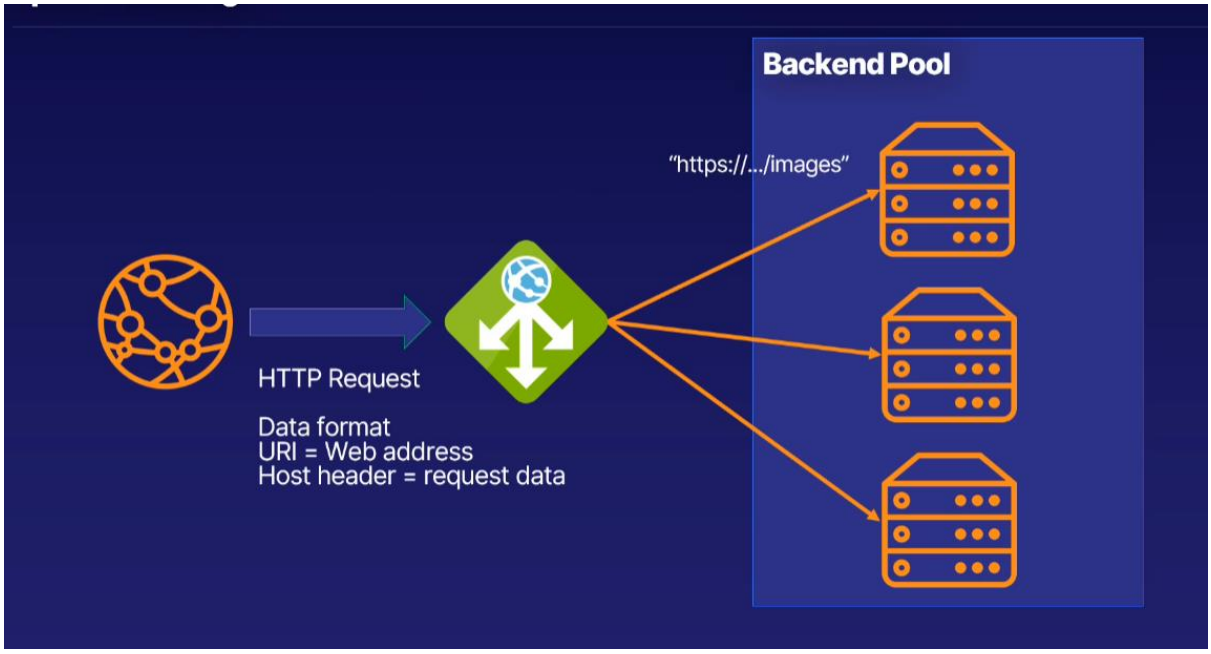
A load balancer receives your internet and network traffic and, based on an IP address and a port, it will send that data to one of the VMs in the backend pool.

But what if you want to route the traffic based on other parameters than simply IP address and port number?

With Application Gateway, you can make routing decisions based on additional attributes of an HTTP request.

For example, if you have a request for a URL that is images, you could send that to a specific pool of machines that are better at handling images. The same can be done for videos.

You can send traffic from a specific web address to a specific machine.



Benefits:

! An application gateway can scale up or down based on the traffic that comes to it.

! An application gateway has end-to-end encryption for all traffic, meaning you can comply with any requirements about securing the traffic. If not needed, you can disable secure transfer to the backend pool to improve processing times too.

! Span multiple availability zones and improve fault resiliency

! Use the same application gateway for more than one website (like 100 websites)

Summary

- An application gateway is another type of load balancer that works on a higher level.
- It works on the HTTP request of the traffic instead of the IP address and port.
- Traffic from a specific web address, such as an image or video URL, can go to a specific machine in the backend pool.

- It works well with all the Azure services and can share the same cloud benefits like high availability and pricing. And this supports auto scaling, end-to-end encryption, zone redundancy, and multi-site hosting.

Content Delivery Network ::

You want your users to load your site and resources as fast as possible, and if your application is hosted in Australia, and you have users from Paris, then they will wait a while to get that information.

== The fix is using a content delivery network.

A content delivery network, or CDN, stores a cached version of your application on edge nodes, which are servers close to the user. Your application will load faster, and less traffic will hit your main server. When content changes, caches are invalidated and updated.

A content delivery network is most often called a CDN. It's a distributed network of servers that can deliver web content close to users. CDNs store cached content on what is called edge servers in locations that are close to end users to minimize latency.

EX:

You have customers from here, all over the world, but you have just the one location for your online resources this data center here. So what happens when your customers from far away, like up here, wants to load your website?

Well, it takes longer.

Instead, what if they only had to request the data from the closest Azure datacentre to them?

== That is what the CDN does.

It places copies of the data of your application on what is known as edge nodes. So now your users only have to go and get the data from close by, and everyone's happy.

What if my website changes?????????? (Like any updates in websites like price, content…)

The data in the edge node will be deleted. Usually it is some hours, depending on how often the data might change.

Data has expired, meaning they have to get a fresh set of data, then they can request it from the master copy. And then they get a new cached version, like that. They take that back, that goes on the edge node

Cache::

Collection of temporary copies of original files. The primary purpose is to optimize speed for an application. When a copy expires, a new copy is needed.

Origin Server::

The original location of the files, such as web application. It is the master copy of your application

Benefits::

@ improve the user experience and the performance of your application.

@ Scale to suit any spikes in traffic, and also protect your main backend server instance from high loads.

@ Edge servers will serve requests closet to the user. Less traffic is then sent to server hosting your application.

Express Routes::

If you require a super-fast connection, right into the bowels of Azure, that is completely private?

== ExpressRoute is for you.

For example,

If a company need their data to be both on-premises on Azure, it has to be highly available, and it needs to be periodically migrated, then ExpressRoute is the must-have connection from the company to Azure.

- ExpressRoutes don't go over the public internet, which means the security of your data and infrastructure is better.

- You get a more reliable and faster connection that has lower latency than any standard internet connection.

If you need a private, secure, high-bandwidth, low-latency connection, directly from your data center or infrastructure to Azure, ExpressRoute is the service you want.