Azure Network

Friday, May 5, 2023 4:19 PM

Azure Virtual Network Equivalent of a local area network

→ Many different customers can create VNets in the same Azure Data Center so these Vnets have to be isolated from one another.

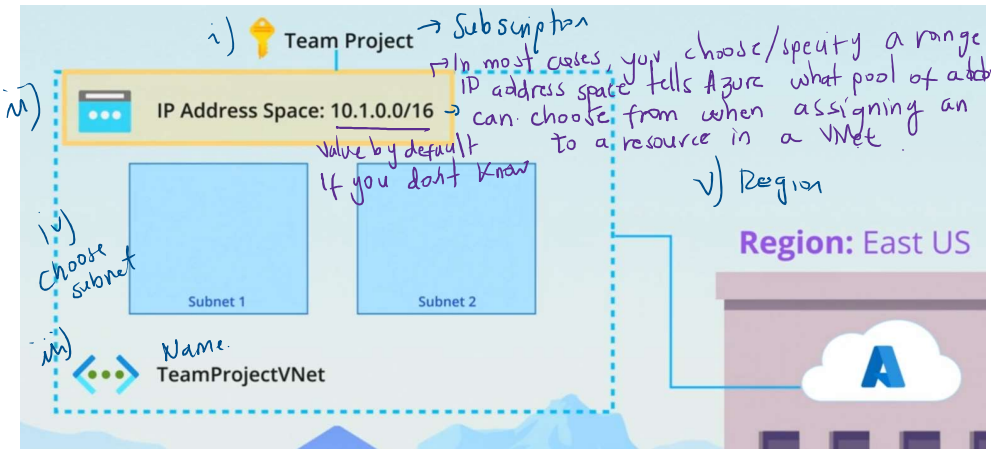
→ You can only put some types of Azure resources in a Vnet.

You can put
- → VM
- → firewalls
- → Azure Kubernetes

You can't put
- → Azure SQL databases instances
- → Azure storage containers
- → Azure Active Directory tenants

→ all of these types of resources can communicate with each other whether they're inside the same Virtual Network or not, the communication is different depending on where they are.

Configuration



→ In most cases, you choose/specify a range of private, non routable IP addresses not used to connect to the internet.

IP address space tells Azure what pool of addresses it can choose from when assigning an IP address to a resource in a VNet.

Screen clipping taken: 5/5/2023 4:28 PM

Choose subnet (subnetwork) in your Vnet.

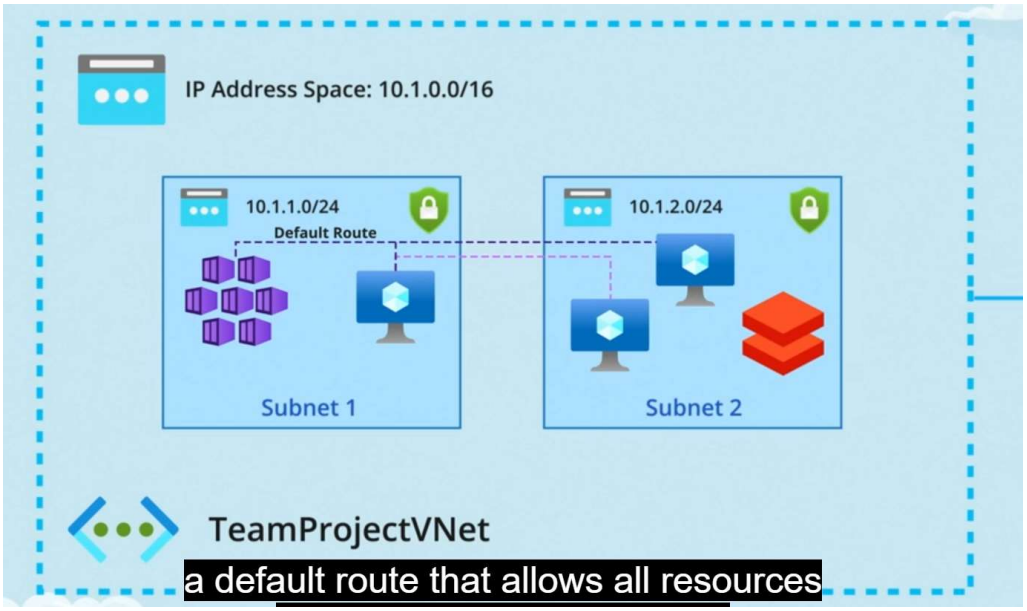
→ use it to divide your resources into logical groupings.

→ Resources that frequently communicate with each other should usually be put in the same subnet.

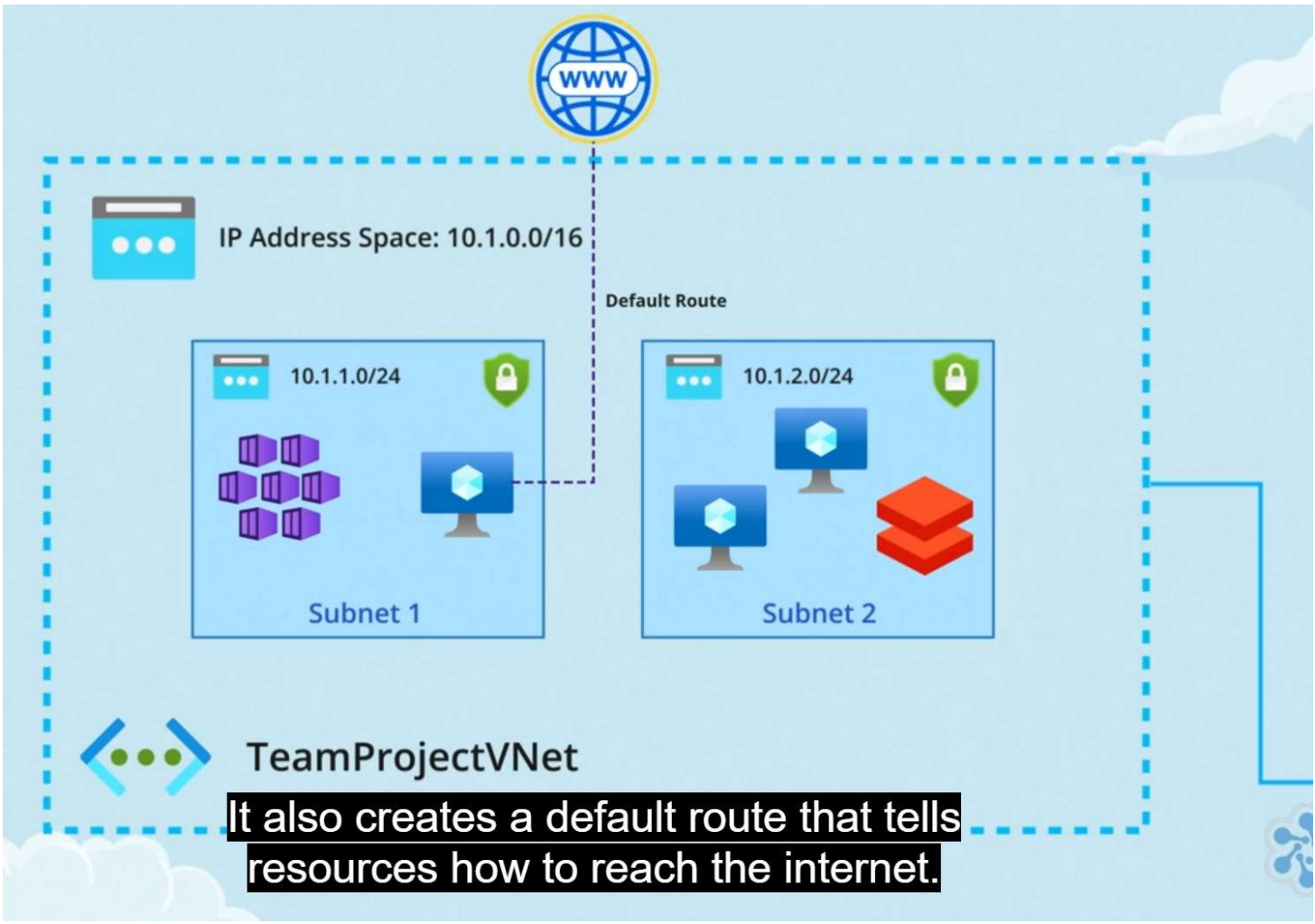
→ different secure rules in different subnets.

- for each subnet, you need to specify which portion of the virtual network's IP address should be reserved for that subnet's resources.
- Resources in different subnets can still communicate with each other, though, because Azure created a default route that allows all resources in a VNet to find each other.
- It also creates a default route that tells resources how to reach the Internet.
- You can create (customized) user-defined routes.

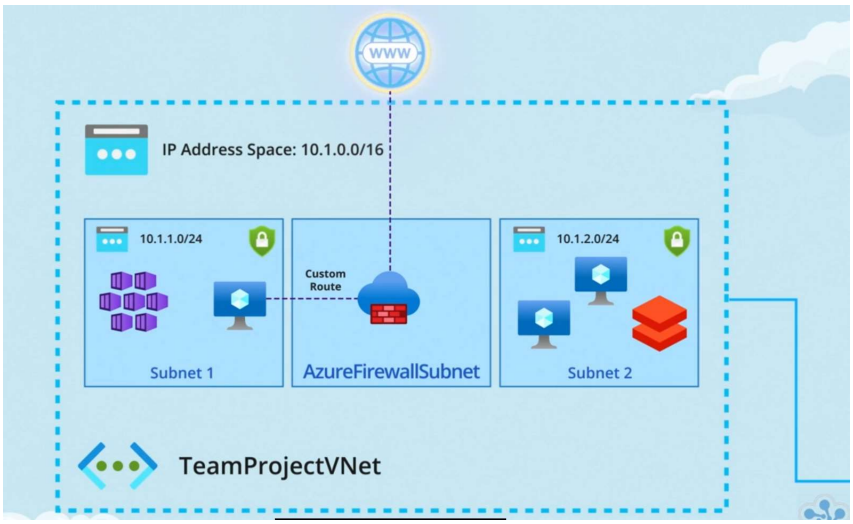
*You can create (customized) user-defined routes.



Screen clipping taken: 5/5/2023 4:49 PM

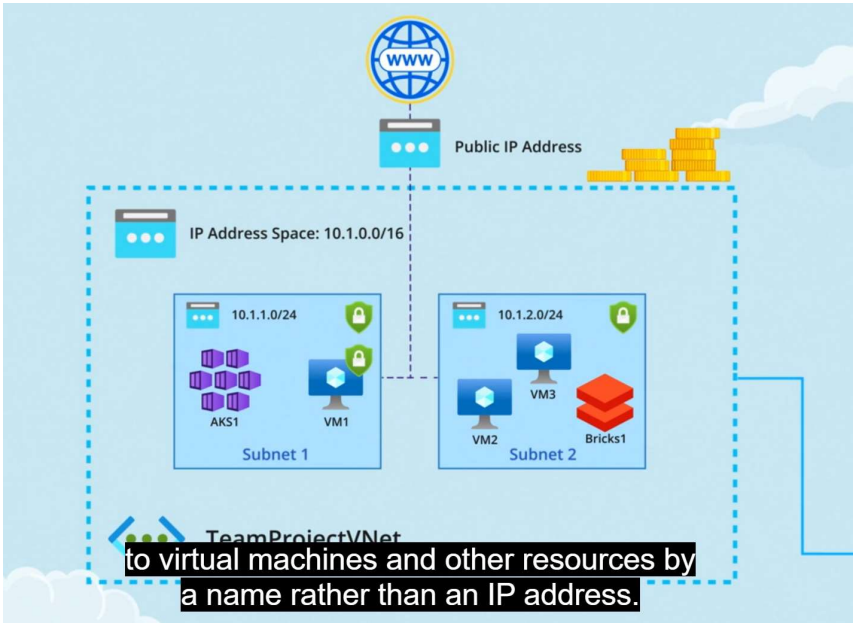


Screen clipping taken: 5/5/2023 4:49 PM

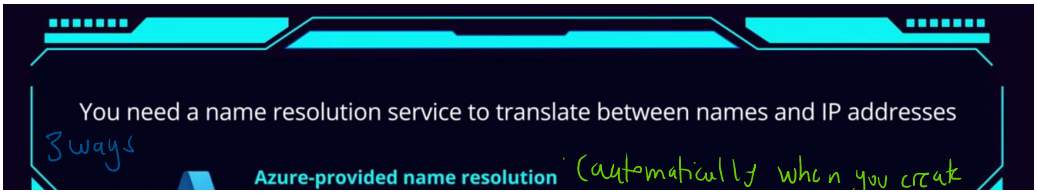


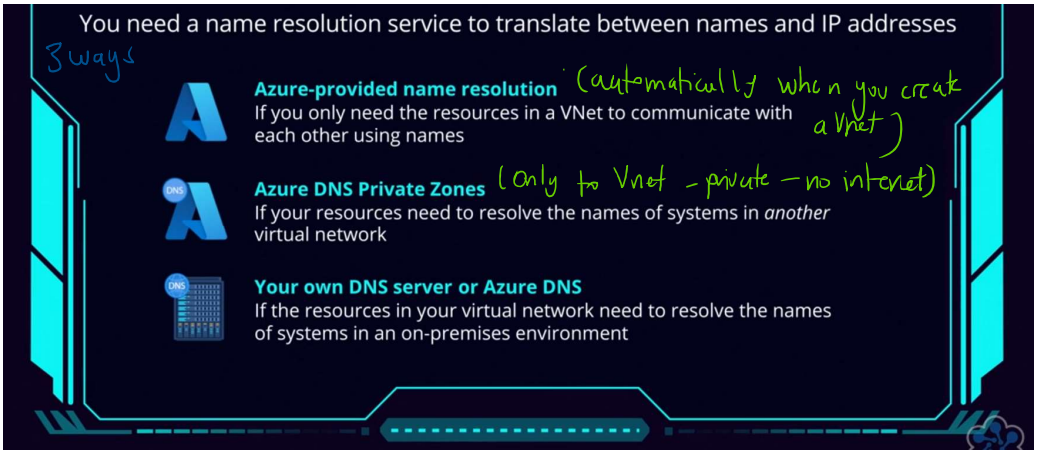
Screen clipping taken: 5/5/2023 4:50 PM

By default, all outbound traffic from a VNet to the internet is allowed.
But, for inbound traffic from the internet, you need to assign a public IP address to it (a specific resource)
↳ you need to pay for them.
→ You have to make sure you have good security on any resource that has a public IP address, because opening it up to the internet makes it more vulnerable.
→ You can refer to resources by a name.



Screen clipping taken: 5/5/2023 4:55 PM





Screen clipping taken: 5/5/2023 4:58 PM

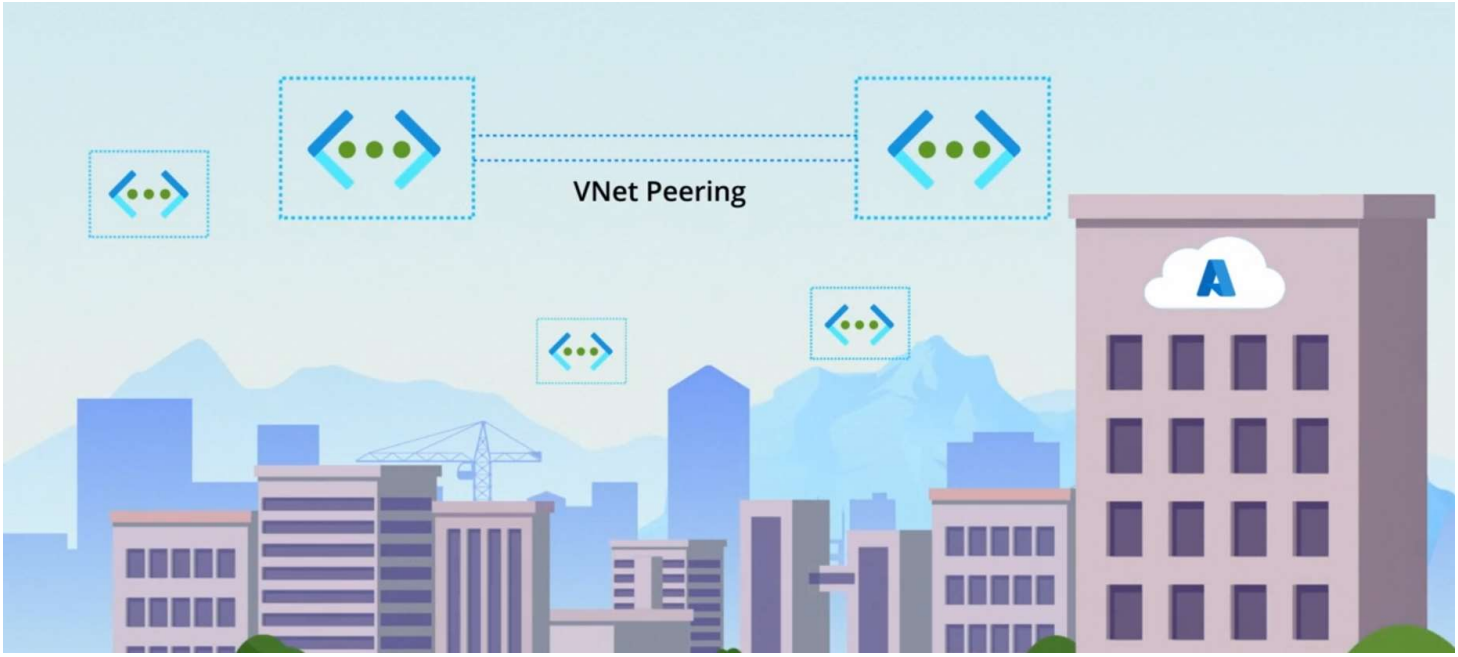
Connecting to other networks

Once you created your VNet, you want to connect with resources that are outside of it.

→ You could set up an internet connection between the 2, but a much faster and secure way to do it is to use VNet peering

→ You just need to configure one peering connection in each direction between the 2 VNets, and then resources will be able to communicate with each other, as if they're on the same network.

→ If the 2 Vnets are in different regions, then you can use global VNet peering.

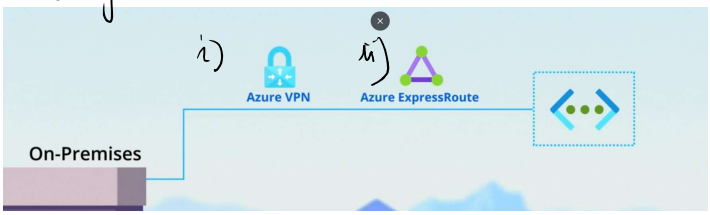


Screen clipping taken: 5/5/2023 7:41 PM

Regardless of wether the VNets are in the same region or not, the peering connection goes over the Microsoft backbone

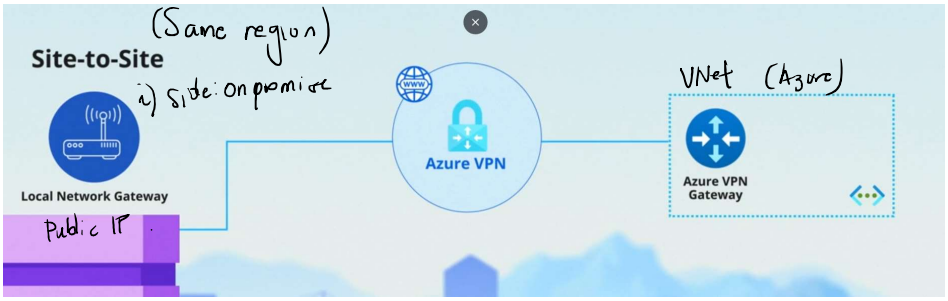
Regardless of wether the VNets are in the same region or not, the peering connection goes over the Microsoft backbone network rather than over the internet, which is why it's faster and more secure.

On premise case.
2 ways



Screen clipping taken: 5/5/2023 7:46 PM

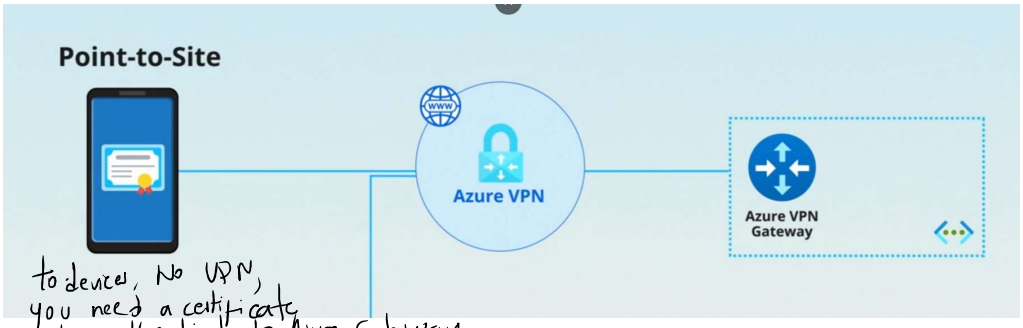
the main difference between the 2 is that a VPN (Virtual Private Network) traverses the internet, while Express Route is a direct connection between your on-promise network and Azure. Since traffic on a VPN goes over the internet, it's encrypted to prevent other parties from viewing it.



Screen clipping taken: 5/5/2023 7:50 PM

Only one Azure VPN Gateway by VNet, it can support site-to site and point to site,

- the only situation where you can't support both site-to-site and point-to-site connections from the same gateway is when you need to configure a different type of routing for each



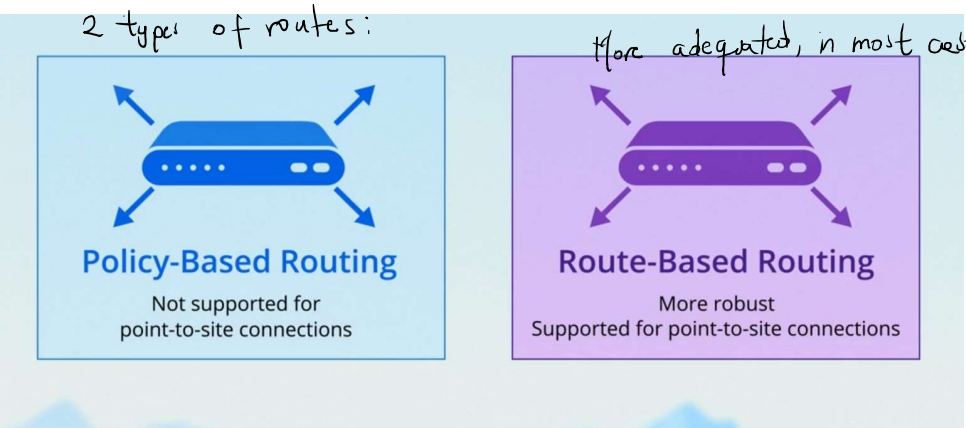
Screen clipping taken: 5/5/2023 7:54 PM

to authenticate to Azure Gateway

Screen clipping taken: 5/5/2023 7:54 PM

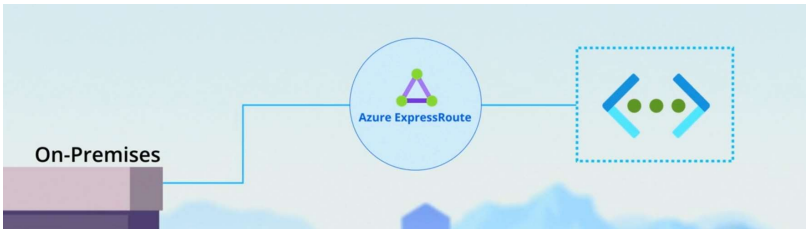
2 types of routes:

More adequated, in most cases



Screen clipping taken: 5/5/2023 7:56 PM

Another sln:

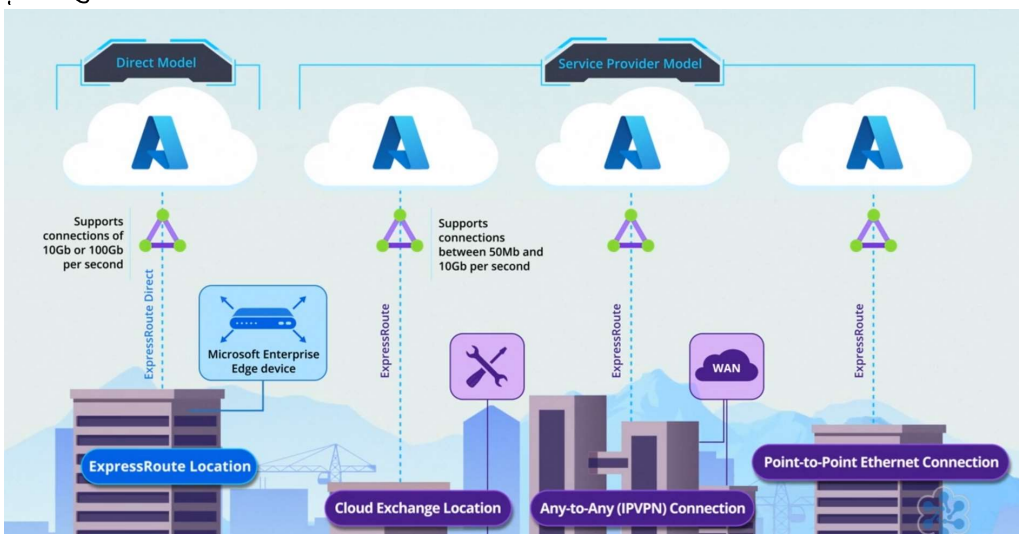


Screen clipping taken: 5/5/2023 7:57 PM

→ If you don't want your connection to go over the internet, or you need more band width, you can setup a direct connect with Express Route.

→ Much more expensive solution.

Ways to connect Express Route.

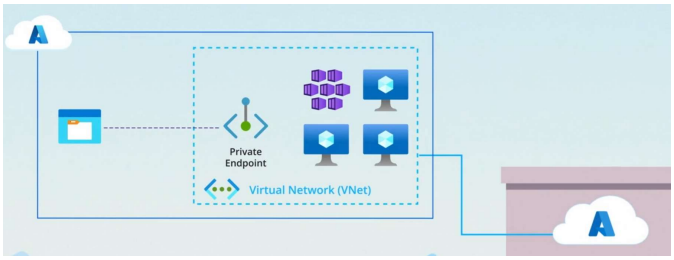


Screen clipping taken: 5/5/2023 8:02 PM

Private endpoints

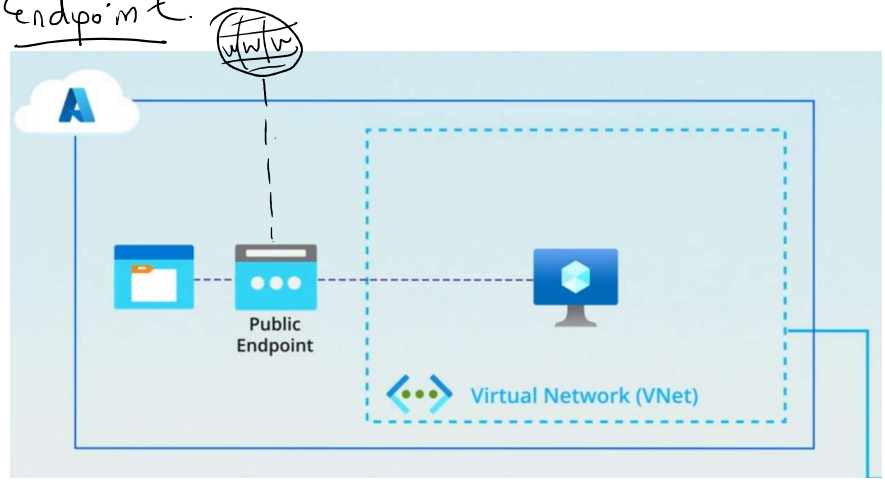
Some Azure resources, (SQL database instances and Azure Storage Containers, can't be put in a Virtual Network directly, but there is an indirect way to bring them into a VNet.

Storage Containers, can't be put in a Virtual Network directly, but there is an indirect way to bring them into a VNet.
→ Sln is Private Endpoint: it's simply a private IP address in a virtual network that's connected to an Azure resource that's outside of the VNet.



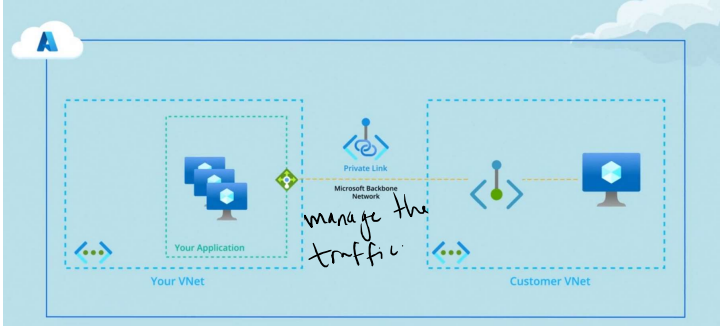
Screen clipping taken: 5/5/2023 8:09 PM

If you don't use Private Endpoint, then you need to use Public Endpoint.

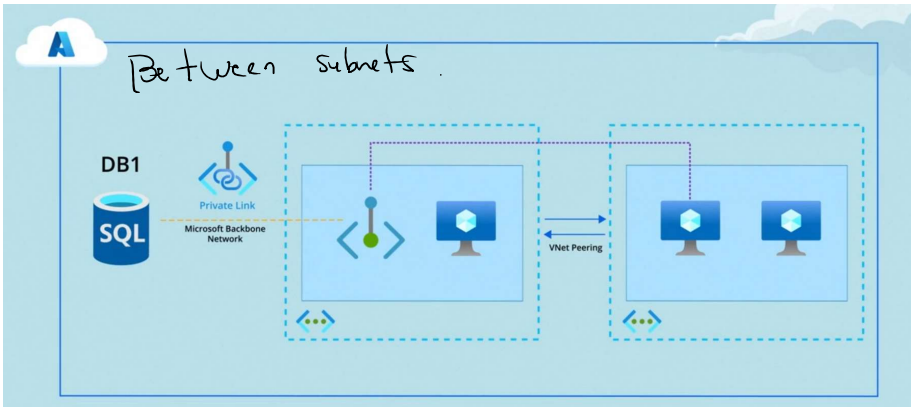


Screen clipping taken: 5/5/2023 8:12 PM

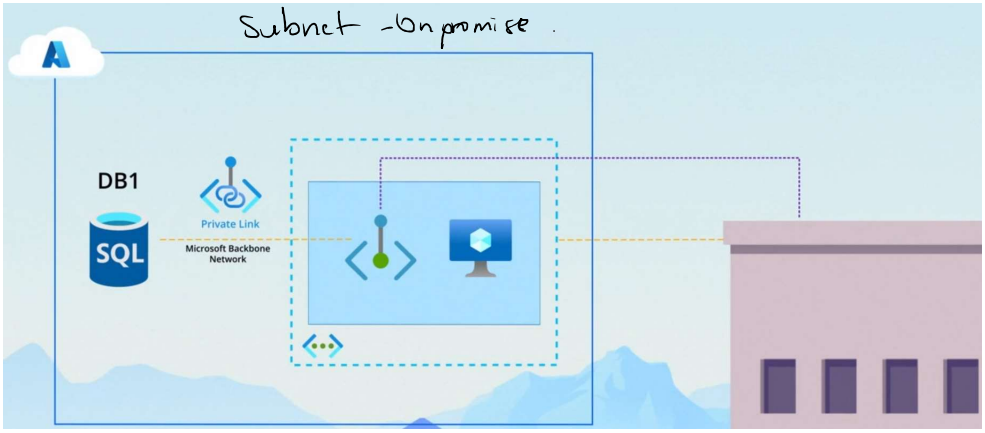
the problem with public Endpoints is that they're exposed to the internet, which is a security risk.
→ Not all resources can be connected to a private endpoint, a resource has to be hosted by a service that supports Private Link this is what is actually used to connect your private endpoint to the service.



Screen clipping taken: 5/5/2023 8:20 PM



Screen clipping taken: 5/5/2023 8:21 PM



Screen clipping taken: 5/5/2023 8:22 PM