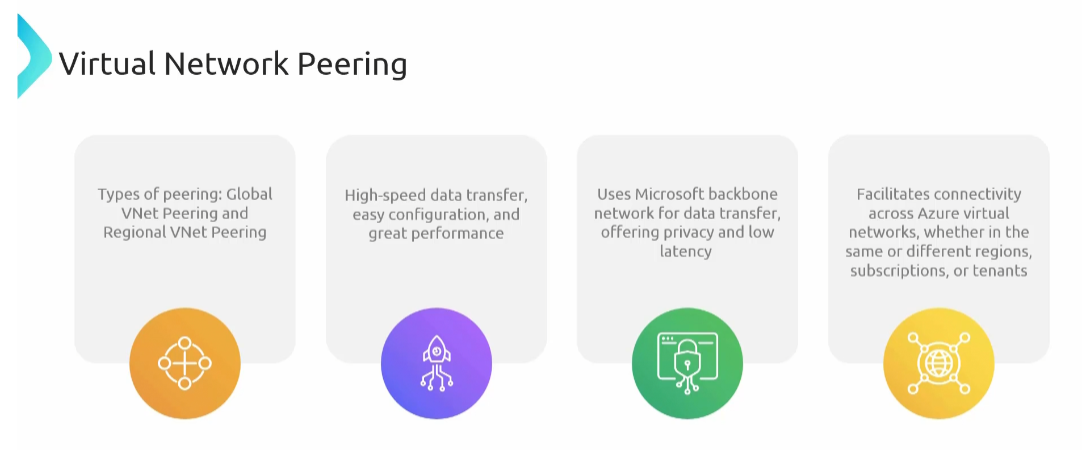
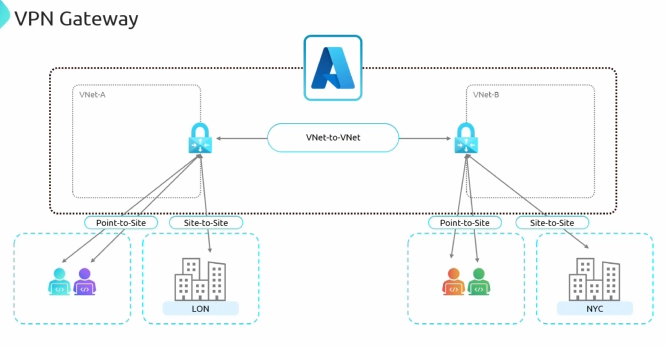
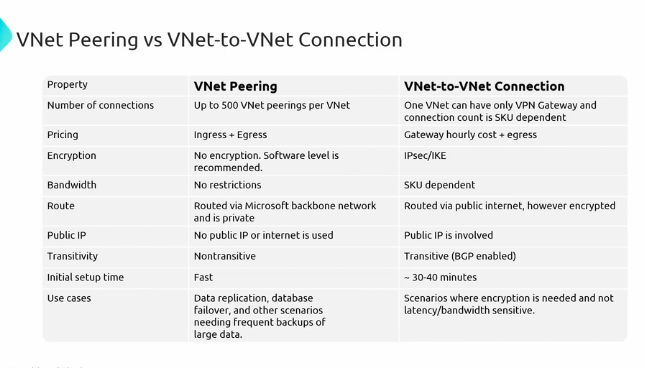
****

**VPN Gateway:**

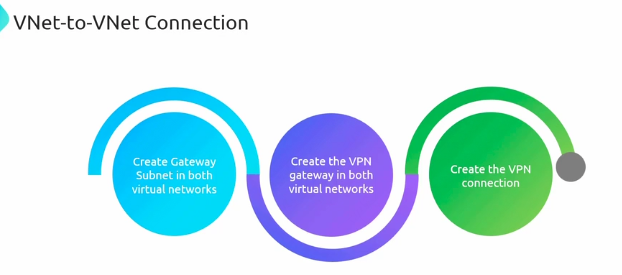
Can establish connections with in VNet connection

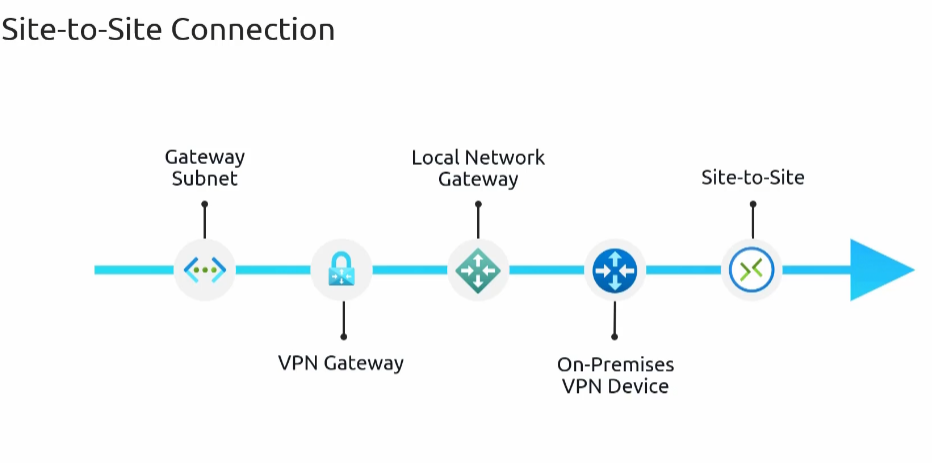


For point-to-site and site-to-site, VNet-to-VNet Connection VPN gateway is essential



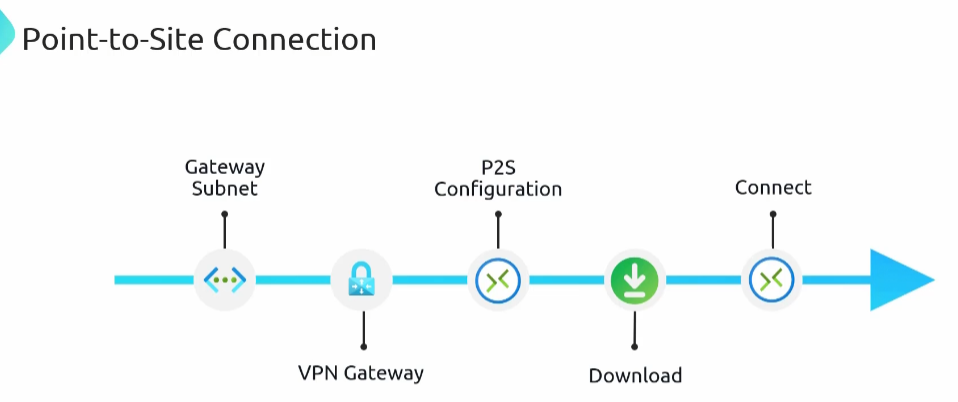
VNet peering is cheap compared to VNet-to-VNet



****

**Site-to-site connection:** secure VPN that spans on-premises vpn device and azure VPN gateway which is located within gateway subject.

Enables your on-premises network to send and receive data from a virtual network as if they were a part of single large local network.

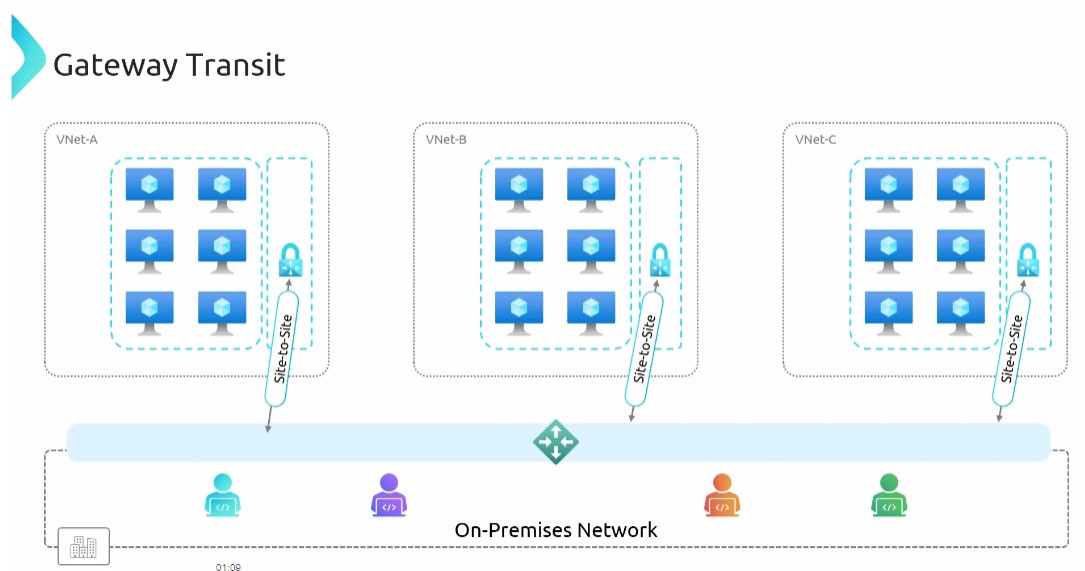


**Point - to -site- connection:** azure users securely can access cloud resources from any location

**Gateway Transit:**

Scenario: Users in On-premises want to access to VNet A and Vnet B and Vnet C

Method -1



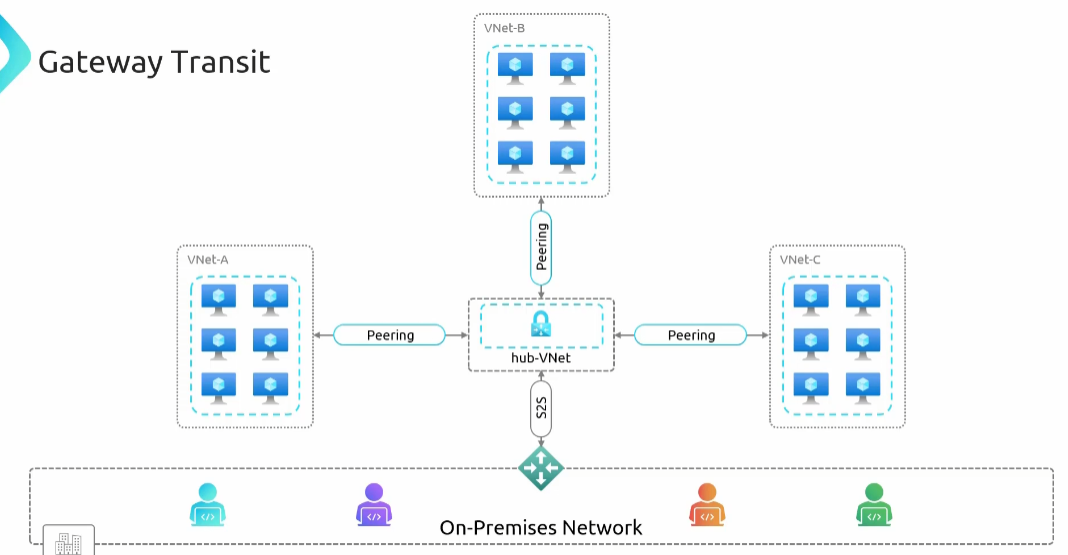
* Create a virtual network gateway in each VNet ( A, B, C)
* And create site-to-site connection to premises
* Multiple VPN gateways means Higher operational cost
* And we need people to work on this
* Managing multiple gateways can become complex and costly.

Method – 2

* Instead of having direct site-to-site connection to on premises network, they are connected to central hub using peering.
* Central hub has a virtual network gate way which is connected to on premises using

Site-to-site connection.

* The Hub Vnet acts as a Central point of control, it makes easier to manage he connections.
* We can place a fire so that all traffic come In and out of Azure network can be inspected.
* The need for multiple gateways is eliminated and cost also reduced.



**User Defined Routes ( UDR )**

By default traffic from the front end subnet to database subnet would flow directly between them with the help of system Routes.

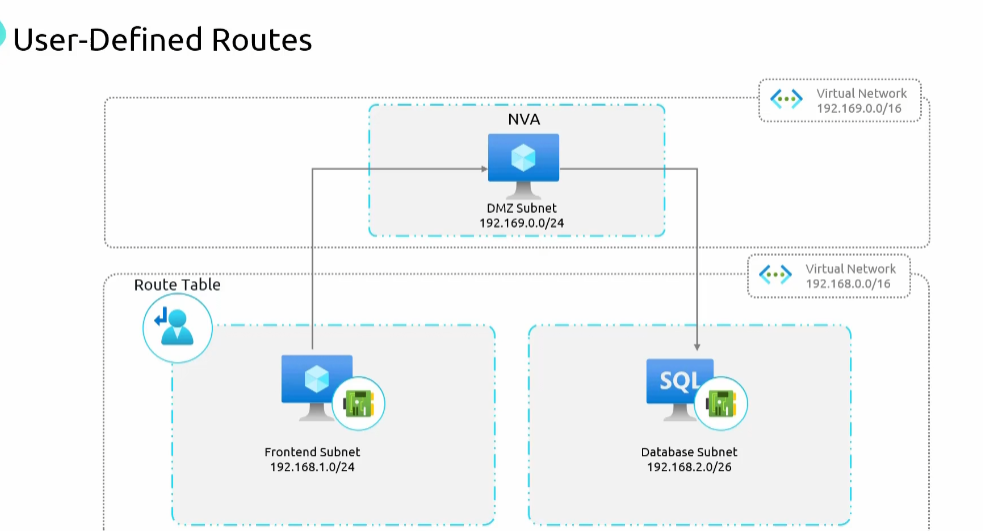
Azure automatically provides set of default routes and those are sufficient for mini networking scenarios. However there are some times when you need to customise the traffic at time UDR comes into picture.

Scenario:

I have a Virtual network with two subnets, front end subnet and database subnet, each having virtual machines. With the help of system routes, systems with in subnets can be able to communicate with each other. And also virtual machines with in Vnet also can able to communicate with each other. What if they want to connect to internet? By default NSG won’t allow traffic from internet. What if VMs needs to connect NTP server (Networking Protocol) or windows update to download the updates? So all these connections to the internet initiated from the VMs is allowed with the help of system routes.

I want to enforce a policy where all the traffic from front end subnet to the database subnet must pass through network subnet appliance. Ex: I have a network appliance on different virtual network, and I want make sure that all traffic goes through that firewall before it reaches database this requirement can’t be fulfilled with by default routes. At that time UDR can be used.

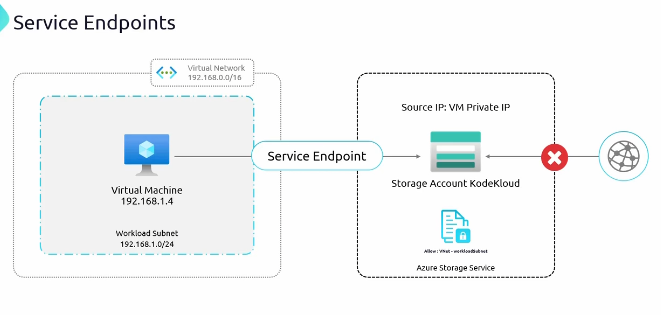
* Create a route table, a user defined route - specifying that traffic from front end subnet going for the database.

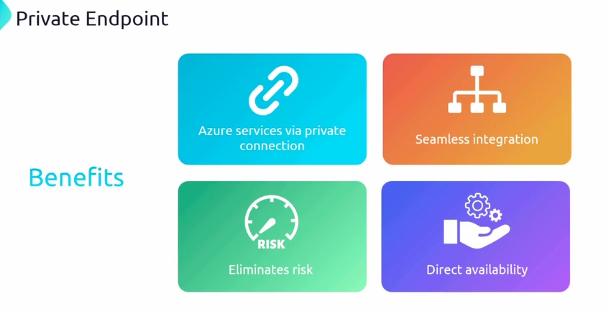


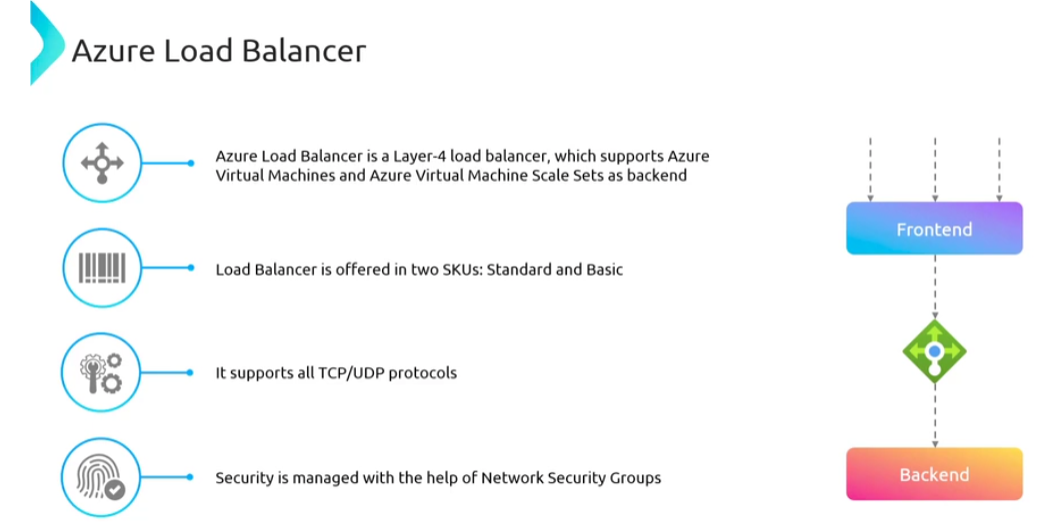
**Service End Points:**

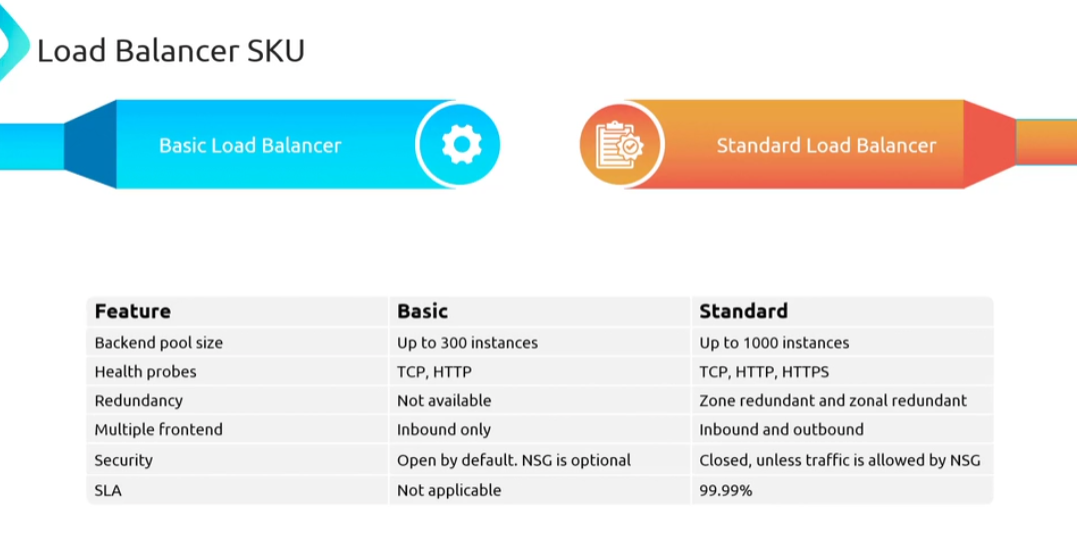
Scenario: I have a virtual machine inside virtual network and I want to access storage account outside VNet. Previously I can able access through public IP and storage account also can connect to internet with public IP. After that storage account set up the firewall and blocked all the public IP addresses. I can’t access storage account through public IP here service end points comes into picture. Storage account is not private now the connection became secured.

With In storage account network settings we will configure VMs private IP address to make connection.









If your load balancer doesn’t have public IP then it is an internal load balancer.

