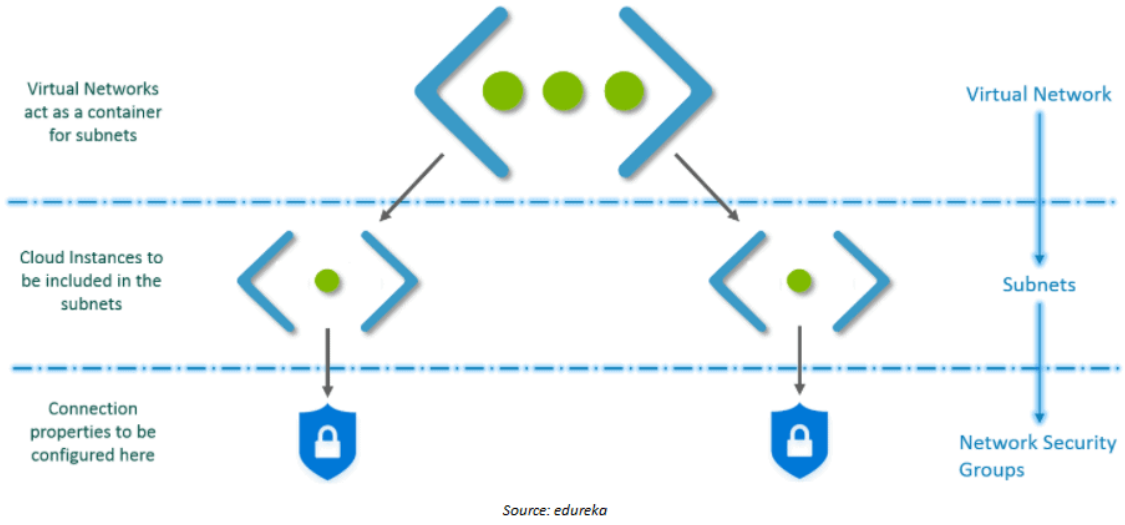
Implement Platform Protection In Cloud

Virtual Network

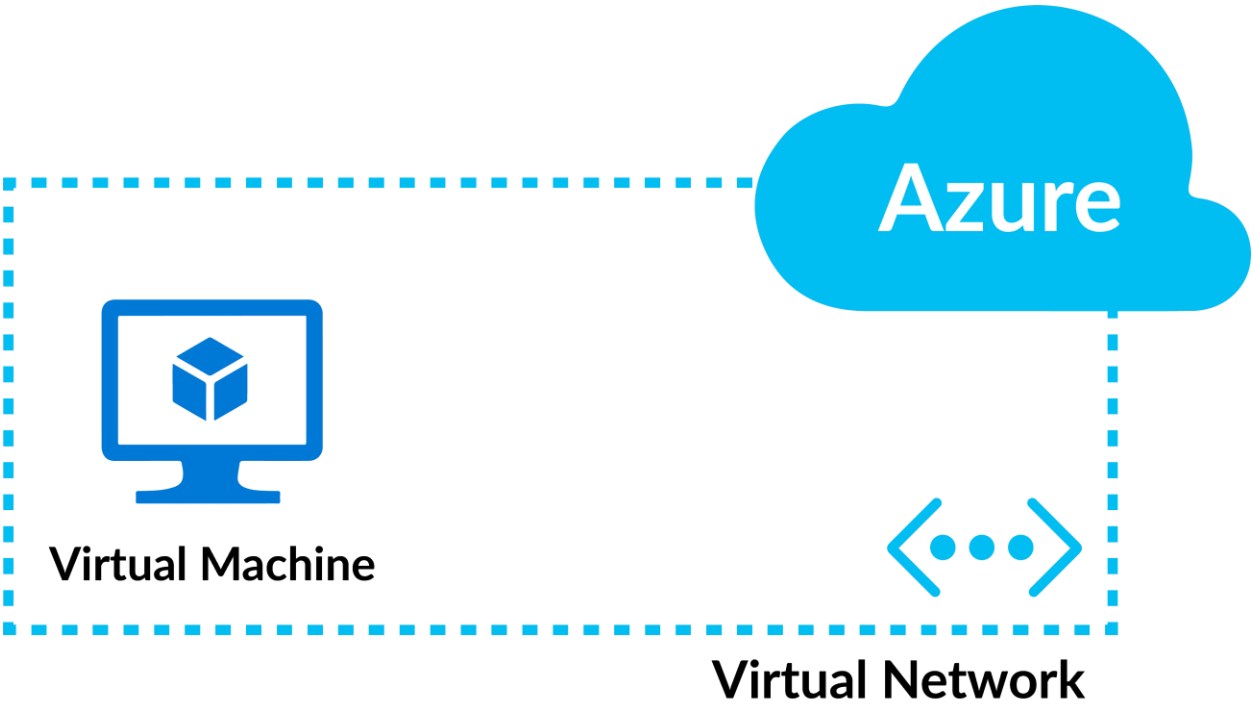
In any cloud, a Virtual Network (VNet) is the basic building component for your private network. Many sorts of resources, such as Virtual Machines (VM), can connect securely with each other, the internet, and on-premises networks, thanks to VNet. VNet is similar to a traditional network that you'd run in your own data centre, but it comes with cloud infrastructure features like scale, availability, and isolation.



Source: edureka

Q1. Why do we use Virtual Networks?

Ans. Isolation is one of the reasons we use the virtual network, but it isn't the sole one. A virtual network is one in which all connected devices, servers, virtual machines, and data centres use software and wireless technology to connect. This allows the network's reach to be extended as far as it needs to be for maximum efficiency, among other advantages



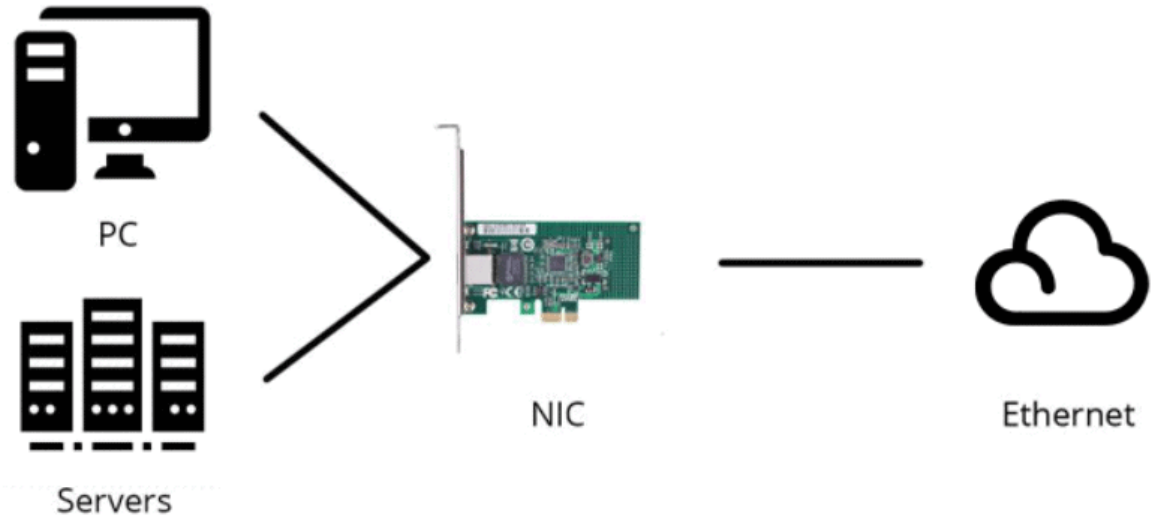
Q2. What do you mean by Subnet and NSG?
Ans. In a virtual network, a subnet is a set of IP addresses. For organization and security, a virtual network might be divided into many subnets. Each NIC (network interface card) in a VM is assigned to a single virtual network subnet.
On Azure, a network security group (NSG) is used to activate a rule or access control list (ACL) that allows or blocks network traffic to virtual machine instances in a virtual network. Subnets or individual virtual machine instances inside a subnet might be connected with NSGs.

Q3. What is the difference between NSG and Firewall?

Azure Firewall	Azure Network Security Groups
Azure Firewall is a **robust service** and a fully managed firewall.	Azure Network Security Group is a **basic firewall**.
It is loaded with tons of features to **ensure maximum protection** of your resources.	This solution is used to **filter traffic** at the network layer.
It can **analyze and filter** L3, L4 traffic, and L7 application traffic.	No such facility is available in Azure NSG.
Azure Firewall provides full support to application **FQDN tags**.	This feature is not available in Azure NSG.
It allows you to **mask the source and destination** network addresses	This feature is missing here.
It offers a **threat intelligence-based filtering** option.	This feature is missing in NSG.

NIC

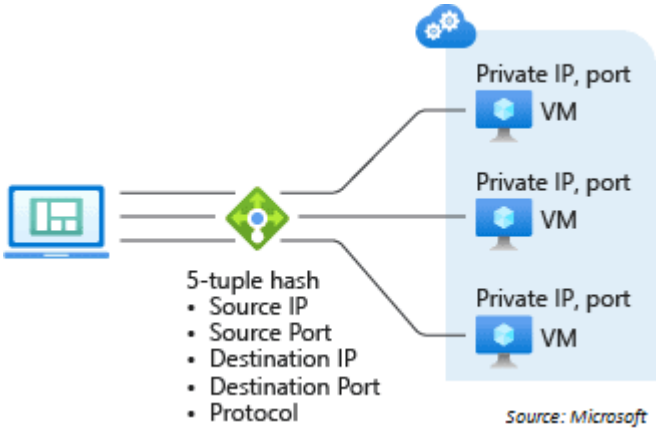
A Network Interface (NIC) is a connection between a Virtual Machine and the software network behind it. One or more network interfaces (NICs) are attached to a Virtual Machine (VM). One or more static or dynamic public and private IP addresses can be assigned to any NIC.



Source: community.fs.com

5-tuple hash

A 5-tuple hash is the default distribution mechanism for Azure Load Balancer. The source IP, source port, destination IP, destination port, and protocol type make up the tuple. The technique only provides stickiness inside a transport session, and the hash is used to map traffic to available servers.

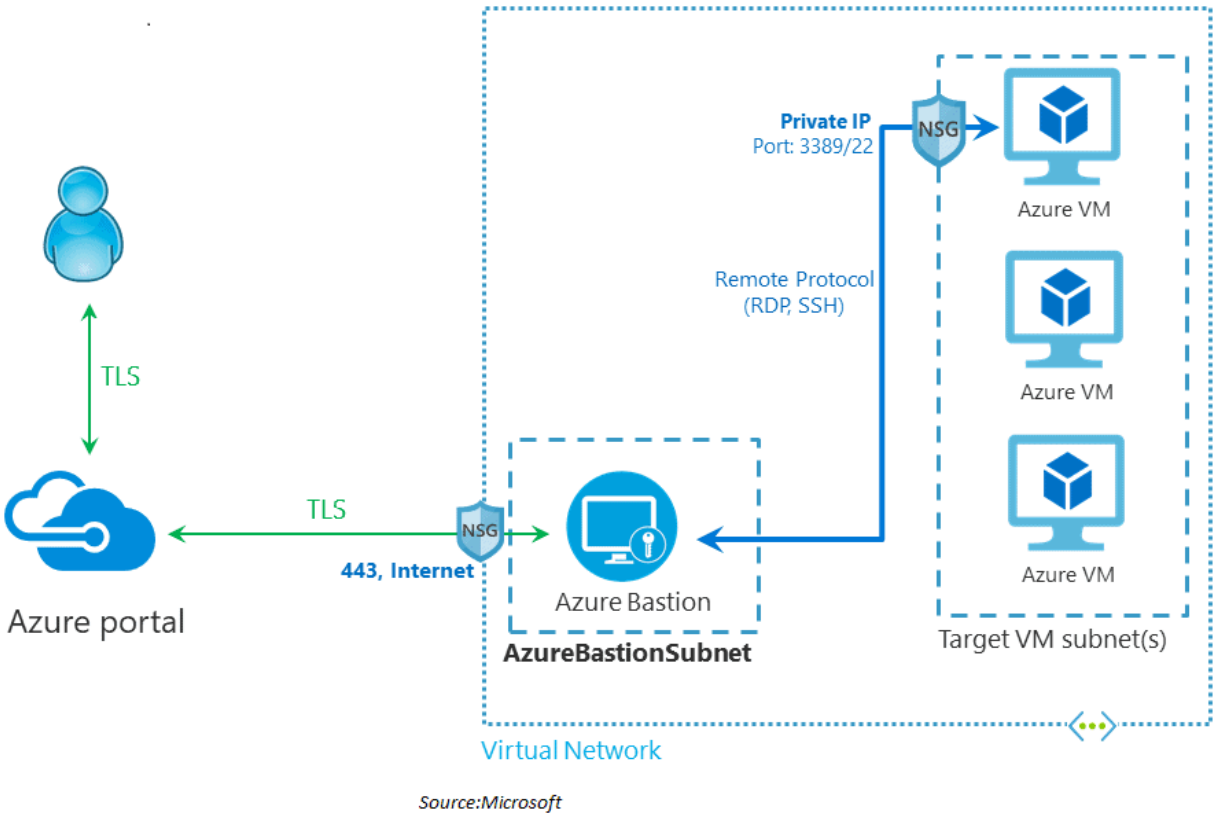


Source: Microsoft

Q4. How to calculate how many IP addresses are there in the range given?
Ans. The formula to calculate the number of assignable IP addresses to CIDR networks is similar to classful networking. Subtract the number of network bits from 32. Raise 2 to that power and subtract 2 for the network and broadcast addresses. For example, a /24 network has 2^32-24 – 2 addresses available for host assignment.

Bastion Host

A bastion host is a server that allows users to connect to a private network from a public network like the Internet. A bastion host must reduce the risks of infiltration due to its vulnerability to attack.



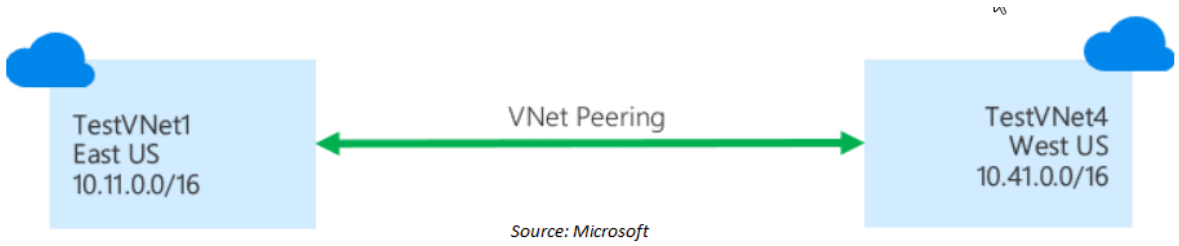
Source:Microsoft

Q5. What is the purpose of Azure Bastian host?
Ans. Azure Bastion is a fully managed service that gives virtual machines (VMs) more secure and smooth Remote Desktop Protocol (RDP) and Secure Shell Protocol (SSH) access without exposing them to public IP addresses.

Q6. Does the Bastion host is like a secured Jump server?
Ans. Yes, it is like a Jump server.

VNet-Peering

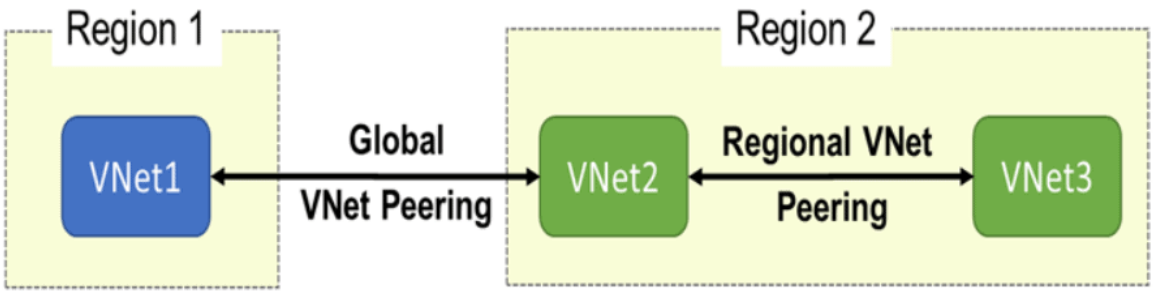
In Azure, virtual network peering allows you to link two or more Virtual Networks seamlessly. For connectivity reasons, the virtual networks appear to be one. The Microsoft backbone technology is used to transport traffic between virtual computers in peer virtual networks. Traffic is routed only through Microsoft's private network, just like traffic between virtual computers on the same network.



Source: Microsoft

Peering is supported by Azure in the following ways:

- Connect virtual networks within the same Azure region via **virtual network peering.**
- Peering virtual networks across Azure regions is called **global virtual network peering.**



Source: rajanieshkaushikk

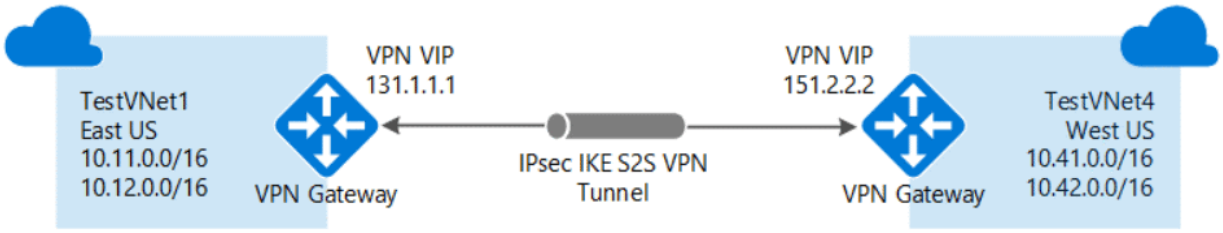
Q7. What is the benefit of using virtual network peering?
Ans. The following are some of the advantages of adopting virtual network peering, whether local or global:

- A connection between resources in various virtual networks that is low-latency and high-bandwidth.
- Data transfer between virtual networks spanning Azure subscriptions, Azure Active Directory tenants, deployment models, and Azure regions is now possible.
- The ability to peer virtual networks that have been formed using Azure Resource Manager.
- There is no downtime in either virtual network when constructing peering or after it has been built.

VPN Gateway

A VPN gateway is a sort of virtual network gateway that is used to transport encrypted traffic across the public Internet between an Azure virtual network and an on-premises location. You can also use a VPN gateway to transport encrypted traffic via the Microsoft network between Azure virtual networks.

Q8. Can we create 2 VPN gateways? One Active and passive if I don't want to do express route?
Ans. In the same network, there can be only one VPN Gateway, so we can not create two VPN gateways in the same network



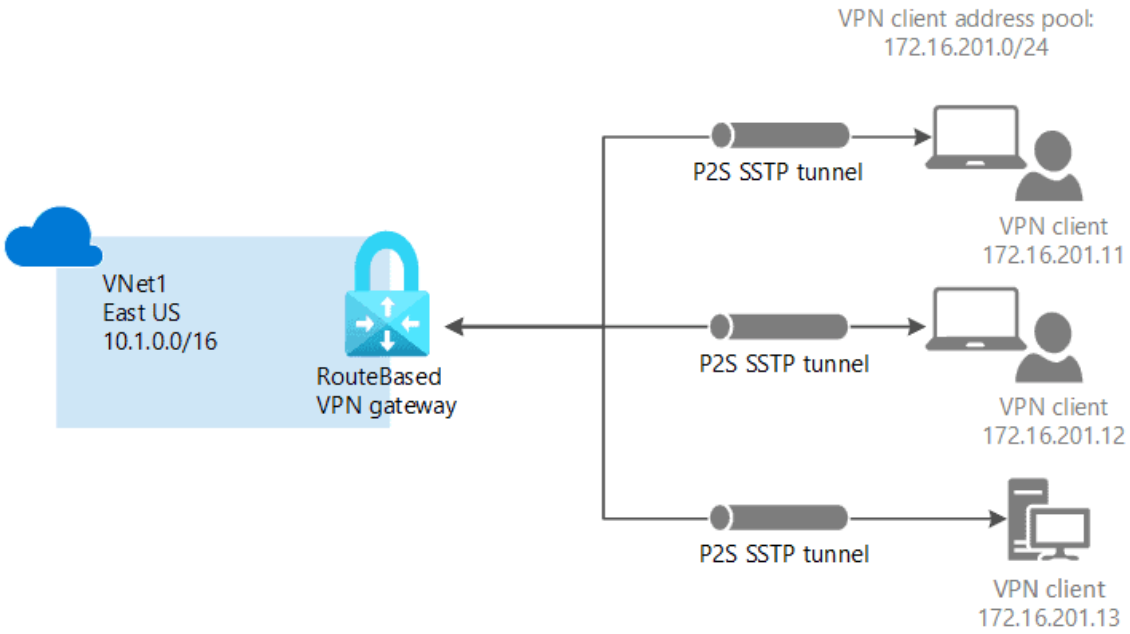
Source: Microsoft

Q9. Which is best VNet peering or VPN Gateway?
Ans. We provide two methods for connecting VNet, depending on your scenario and needs, you may prefer one over the other.

- **VNet Peering:** Provides a low-latency, high-bandwidth connection that can be used for cross-region data replication and database failover. Customers with tight data policies choose VNet Peering over public internet because traffic is totally private and stays on the Microsoft backbone. There are no extra hops because there is no gateway in the path, ensuring low latency communications.
- **VPN Gateways:** Provide a low-bandwidth connection and are beneficial in situations where encryption is required but bandwidth constraints are acceptable. Customers are also less latency-sensitive in these instances.

Point-to-Site Connection

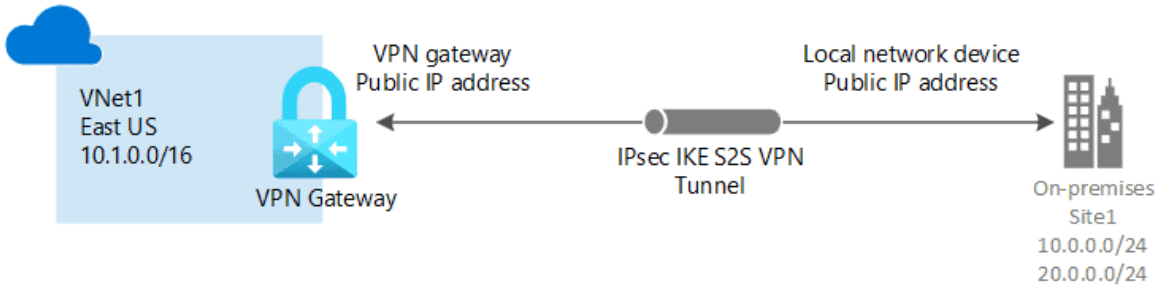
A Point-to-Site (P2S) VPN gateway connection lets you create a secure connection to your virtual network from an individual client computer. A P2S connection is established by starting it from the client's computer.



Site-to-Site Connection

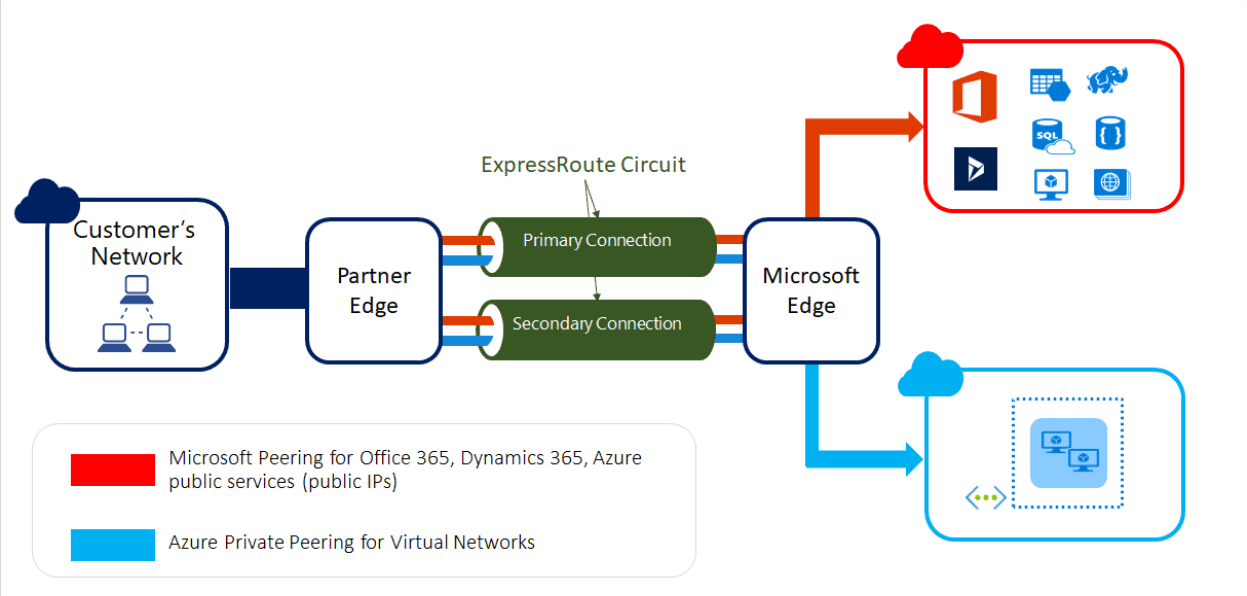
If we have an on-premises virtual network, and we may have other virtual networks existing in other cloud providers. To connect to our virtual network in Azure with the network that is an on-premises data centre, we can use a Site-to-site VPN.

A Site-to-Site VPN gateway connection is used to connect your on-premises network to an Azure virtual network over an IPsec/IKE (IKEv1 or IKEv2) VPN tunnel. This type of connection requires a VPN device located on-premises that has an externally facing public IP address assigned to it.



Express Route

ExpressRoute, with the help of a connectivity provider, enables you to extend your on-premises networks into the Microsoft cloud over a secure connection. You can connect to Microsoft cloud services such as Microsoft Azure and Microsoft 365 using ExpressRoute.

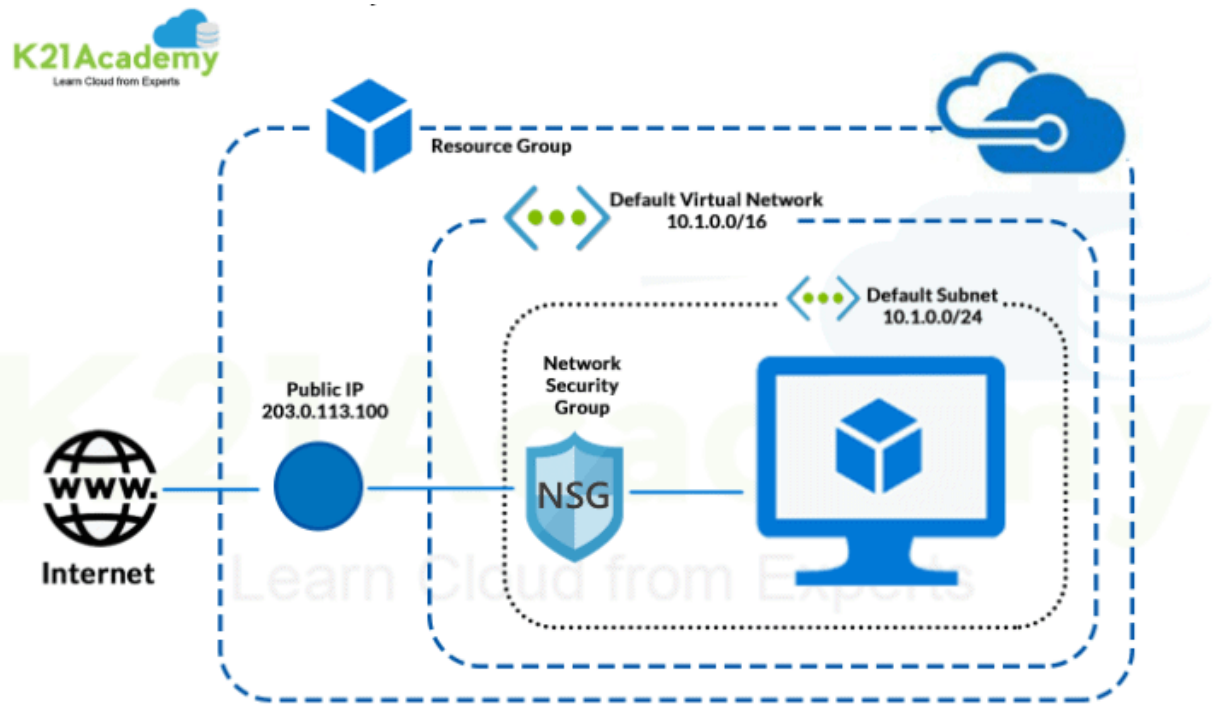


Source: Microsoft

NSG

Azure Network Security Groups is a fully managed offering from Microsoft that helps refine traffic from and to Azure VNet. The Azure NSG consists of certain security rules that users can allow or deny at their convenience. Evaluation of these rules is done through a 5-tuple hash.

The 5-tuple hash takes values from the Source port number, IP Addresses, Destination IP address and port number, etc. It allows to associate Network Security Groups with a VNet or a VM network interface very easily, and it works on layers 3 and 4 of the OSI model.

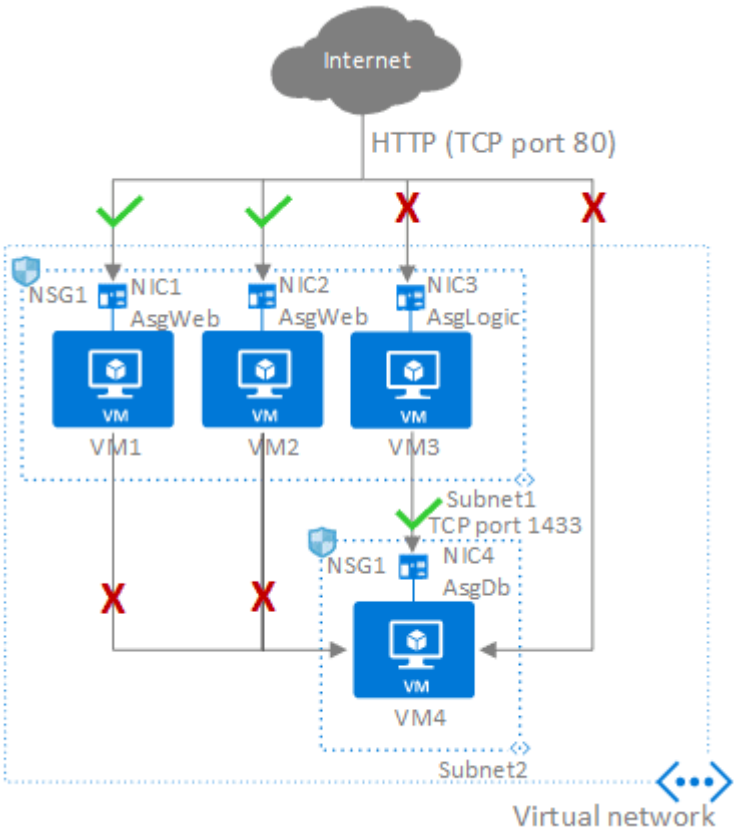


Q10. If priority is from 100-4096, why is NSG priority is 65000-65500?
Ans. The default rules will be the last to run and will fall within an unspecified range. Users are allowed to have a priority range of 100 to 4096. (with the lowest value being the rule that runs first).

ASG

Application Security Groups allow you to set network security as a natural extension of the structure of an application, allowing you to organize virtual machines and define network security policies based on those groups.

Your security strategy can be reused at scale without the need for manual IP address maintenance. The platform takes care of the complexities of explicit IP addresses and various rule sets, so you can concentrate on your business logic.



Q11. Why do we need ASG?
Ans. ASGs are used within an NSG to apply a network security rule to a specific workload or set of VMs, described as the “network object” by the ASG and to which explicit IP addresses are added. This allows you to arrange VMs into related groups or workloads, making the NSG rule creation process easier.