Azure Virtual Network

Overview of Azure

Azure is the name of the cloud computing service owned by Microsoft that provides Infrastructure as a Service (IaaS), Platform as a Service (Paas) and Software as a Service (SaaS). Azure's cloud computing services are network, storage, compute, database, analytics, security, and many more. In this blog, we will only focus on the basics of network services.

What Is Azure Virtual Network?

An Azure Virtual Network (VNet) may be a network or environment which will be wont to run VMs and applications within the cloud.
When it's created, the services and Virtual Machines within the Azure network interact securely with one another.

Advantages of Using Azure Virtual Network

Some of the foremost advantages of using Microsoft Azure VNet are as follows:

- It provides an isolated environment for your applications
- A subnet in a very VNet can access the general public internet by default
- We can easily direct traffic from resources
- It is a highly secure network
- It has high network connectivity
- It builds sophisticated network topologies in a very simple manner

Elements of Azure Virtual Network

Azure networking components provide a large range of functionalities that may help companies build efficient cloud applications that meet their requirements.

The components of Azure Networking are listed below, and we have explained each of those components in an exceedingly detailed manner:

1. Subnets
2. Routing
3. Network Security Groups

Subnets

Subnets let users segment the virtual network into one or more sub-networks.
These sub-networks may be separated logically, and every subnet consists of a server.
We can further divide a subnet into two types:

1. **Private –** Instances can access the web with NAT (Network Address Translation) gateway that's present within the public subnet.
2. **Public –** Instances can directly access the net.

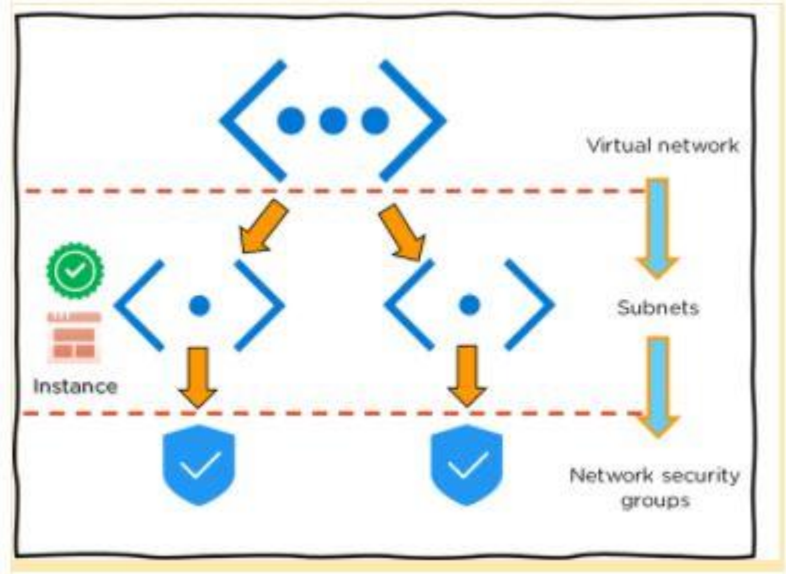
Routing

- It delivers the information by choosing an appropriate path from source to destination.
- For each subnet, the virtual network automatically routes traffic and creates a routing table.

Network Security Groups

- It is a firewall that protects the virtual machine by limiting network traffic.
- It restricts inbound and outbound network traffic depending upon the destination IP addresses, port, and protocol.

How to Launch an Instance using Azure VNet?



- First, create a virtual network within the Azure cloud
- Next, create subnets into each virtual network
- Now, assign each subnet with the respective instance or Virtual Machine
- After which you'll connect the instance to a relevant Network Security Group
- Finally, configure the properties within the network security and set policies
- As a result, you'll be able to launch your instance on Azure

IP Address in Azure

The two different types of IP Address used and allocated in Azure are Public IP and Private IP.

- **Private** – The Private IP address allows communication of resources within the azure resource group. In other words, resources can not access a private IP outside the network. The resources that can be connected using a private address are VM Network Interface, ILB (Internal Load Balancer) and Application Gateway.
- **Public** – The Public IP address allows Azure Resources to communicate with public-facing Azure services via the Internet. In other words, resources can access public IP outside the network. Some resources that can be connected using public address are VM Network Interface, Public Facing ILB, Application Gateway, VPN Gateway and Azure Firewall.

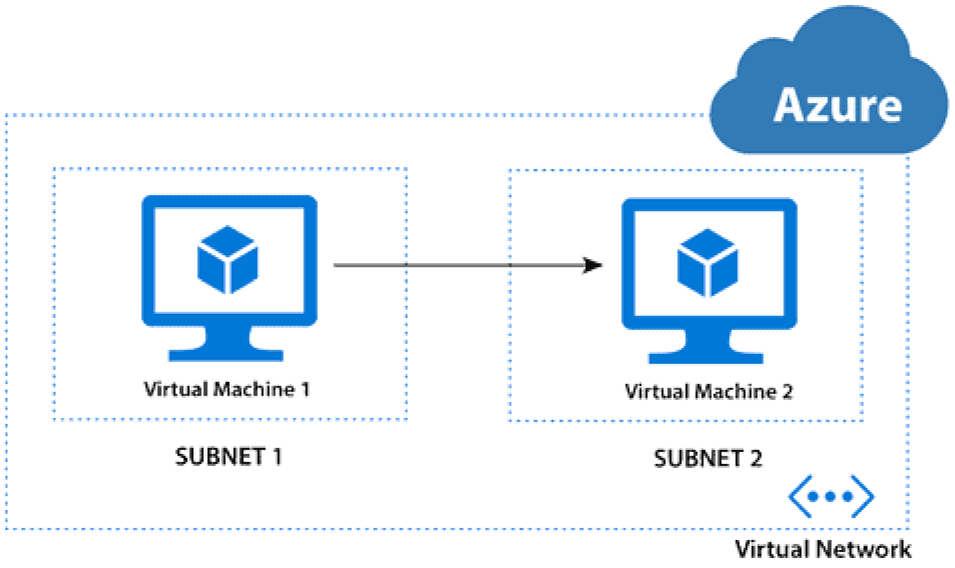
IP Allocation

- **Dynamic IP** – The default allocation method by which Azure can automatically assign the available and unreserved IP address from the subnet's address range. Also, the Dynamic IP is not fixed and changes with time.
- **Static IP** – This is the custom allocation method to assign the available and unreserved IP address from the subnet's address range. The Static IP is fixed and does not vary with time.

Azure Virtual Network

Azure Network is the interlinking and communication of all the Azure Resources in an organization. Networking leads to efficient resource work with better consistency and coordination.

Virtual Networking is the communication between devices, servers, virtual machines over the internet. Similarly, Azure Virtual Network (VNet) is a private network with interconnected Azure Resources like Azure Virtual Machines, Infrastructure and Network. It enables communication between various Azure Resources via the Internet. In a Virtual Network, a continuous block of IP Address is used to create multiple subnet networks.



Azure Subnet

As we know, the subnet is a part of a network that covers a range of IP Address. In Azure, VNet can be divided into smaller subnets for organizations. When a VNet is created in Azure, the subnet range and topology needs to be specified. In Subnet, the IP Address range will be a subpart from a big block of IP Address used in Virtual Network (VNet). The Virtual Machines and resources in a network will be assigned the IP Address from these subnets.

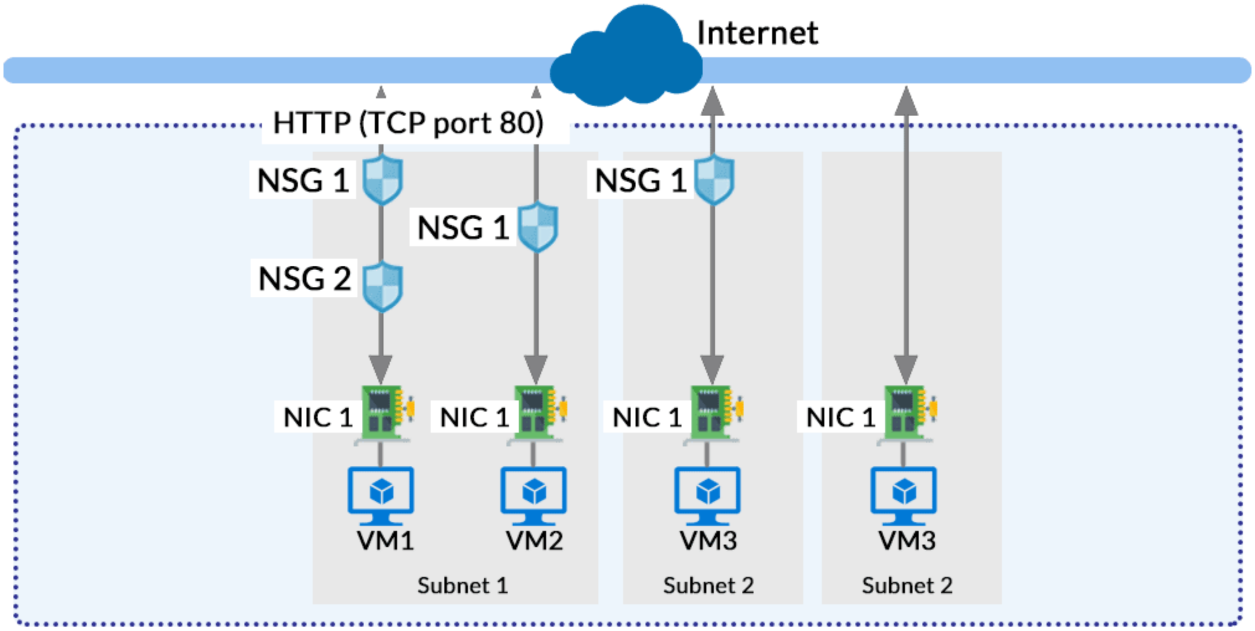
Azure Network Interface

In Azure, NIC is virtual ethernet cards that help communicate the Virtual Machines present in a network. When a Virtual Machine is created in Azure, the NIC with default settings is automatically created. Also, Network Interface settings in Azure can be customized using command tools like Azure CLI and PowerShell.

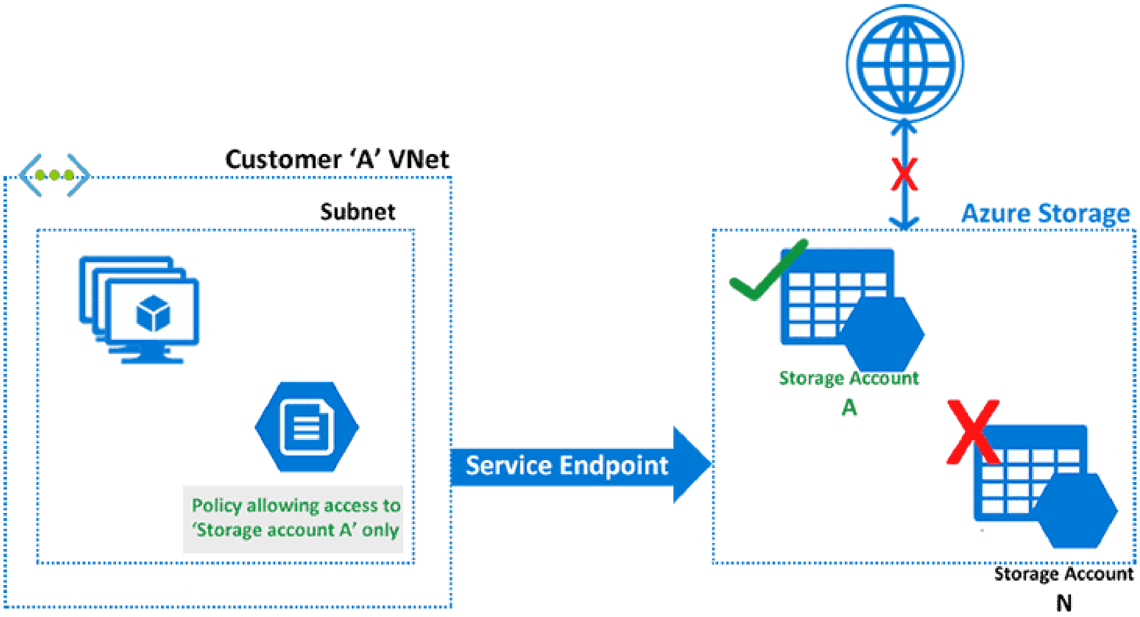
Network Security

Azure provides various protection methods for securing a service in a network. I have listed down some of the basic network security tools with a short description.

Network Security Group (NSG)

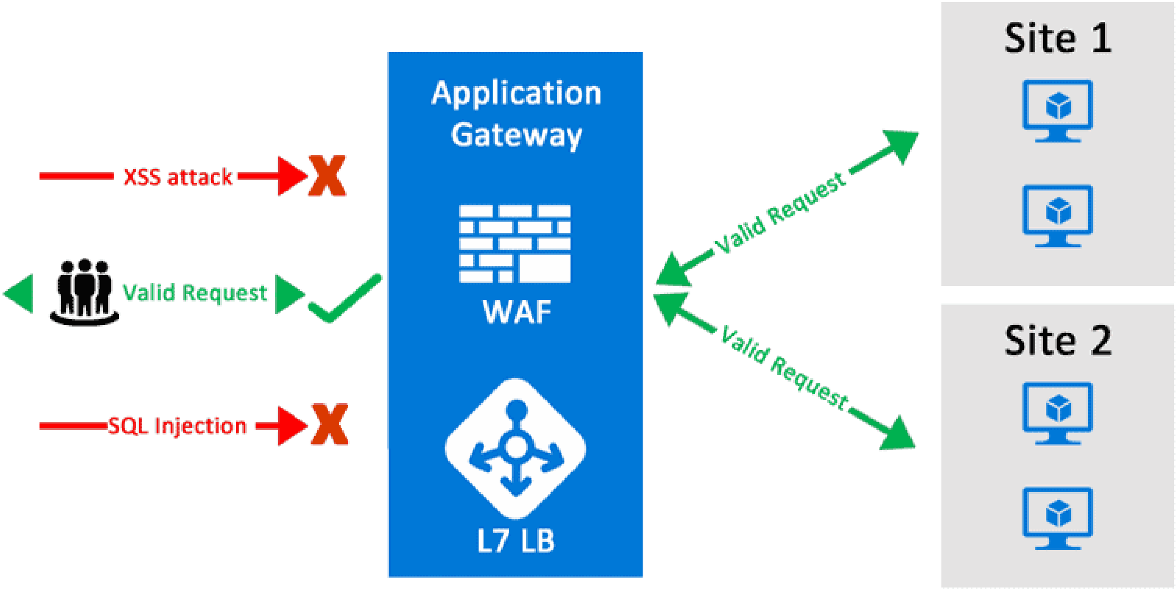


Service Endpoints



Service Endpoints in Azure provides secure connectivity over the optimized route of the Azure Network. Without needing a public IP address, Service Endpoints allows Private IP address in a VNet to reach the endpoint of an Azure Service. It is simple to set up and improves security for the Azure resources in a network. The services here can be Azure Storage, Azure Database, etc.

Web Application Firewall (WAF)

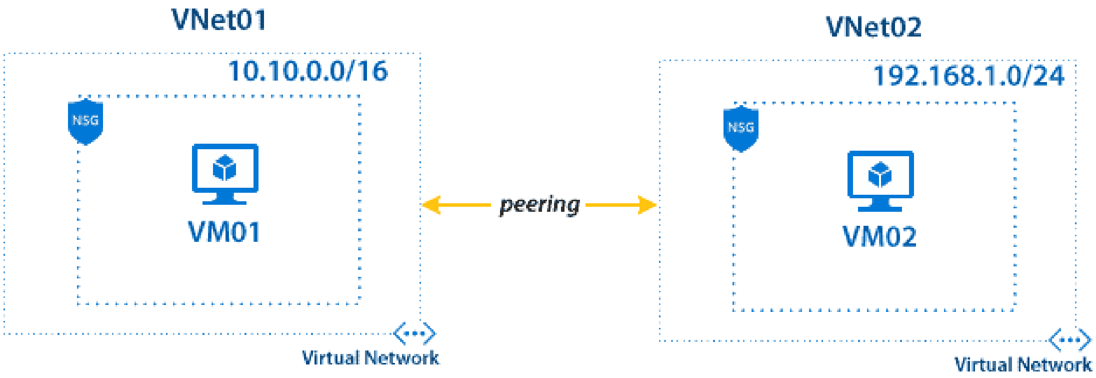


Web applications are a common target for hackers to steal user information. So, protection from the most common attacks like SQL injection, cross-site scripting, etc., is a must. Web Application Firewall by Azure is a firewall for protecting the web application from these common threats. It provides an easy setup for applying various protection of layers that results in better security management. A user can deploy the WAF with other services like Azure Application Gateway, Azure Content Delivery Network (CDN) and Azure Front Door.

Azure Network Models

Network Models are the representation and methods of connecting multiple networks. In Azure also, Microsoft enables some ways to connect multiple networks. I have listed down some of the most used network models.

VNet Peering



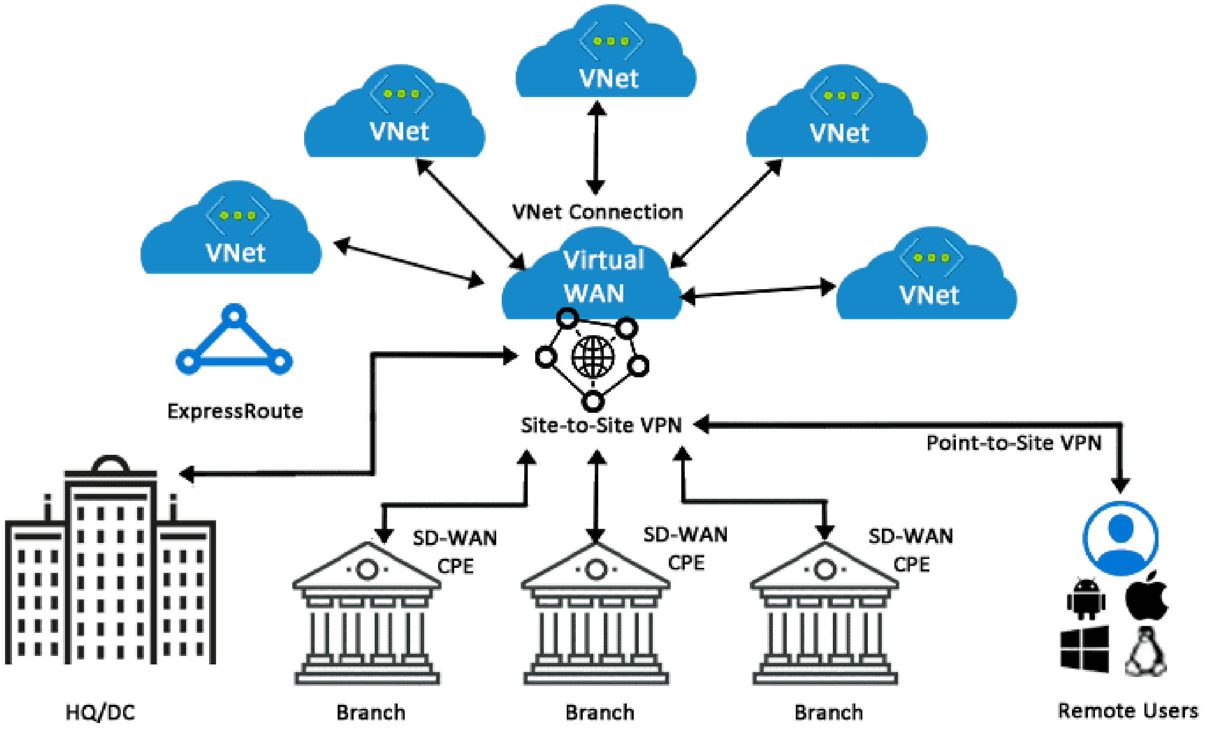
Virtual Network peering enables to connect the two or more Virtual Networks in Azure. It also allows transferring data between deployment models, Azure Subscriptions, Azure Active Directory Tenants and Azure regions without downtime and failure. The traffic between the peered virtual networks use Microsoft's backbone infrastructure and is routed through a private network. Thus, gateways, encryption and public internet are not required.

There are two types of Virtual Network Peering:

1. **Regional VNet Peering** – When the two networks needed to peer are in the same region, the peering is called Regional VNet Peering.
2. **Global VNet Peering** – When the two networks are from different regions, the peering is called Global VNet Peering.

Virtual WAN (Wide Area Network)

Virtual WAN in Azure allows creating a web of multiple networks that are interconnected to each other. It brings multiple networking, security, and routing functionalities together to provide a new single operational interface.

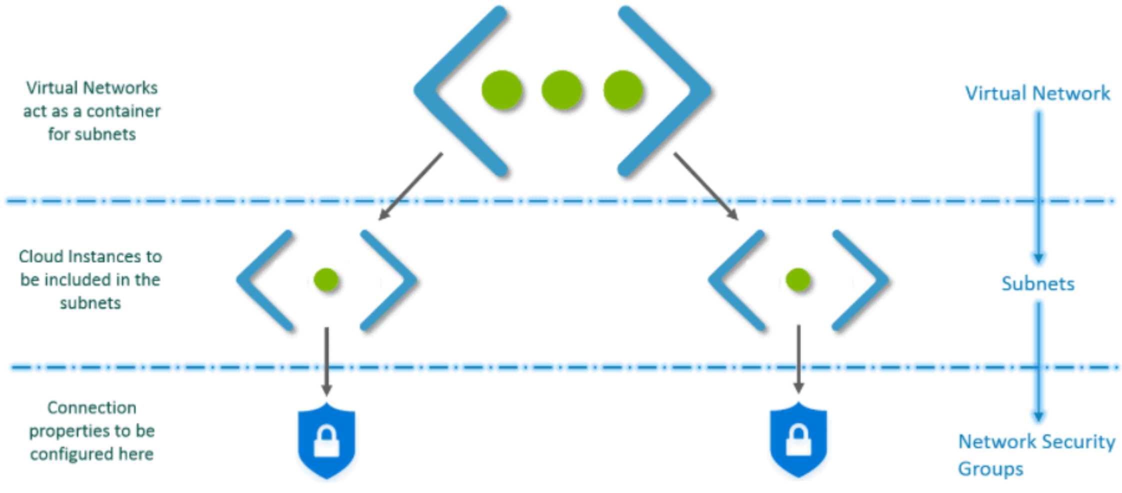


In the above diagram, a Virtual WAN at the centre acts as a single operational hub to manage all the traffic coming from multiple resources in a VNet. Instead of contacting the multiple branches separately, a VNet can contact the central hub to connect with all the branches connected to it.

Implement Platform Protection In Cloud

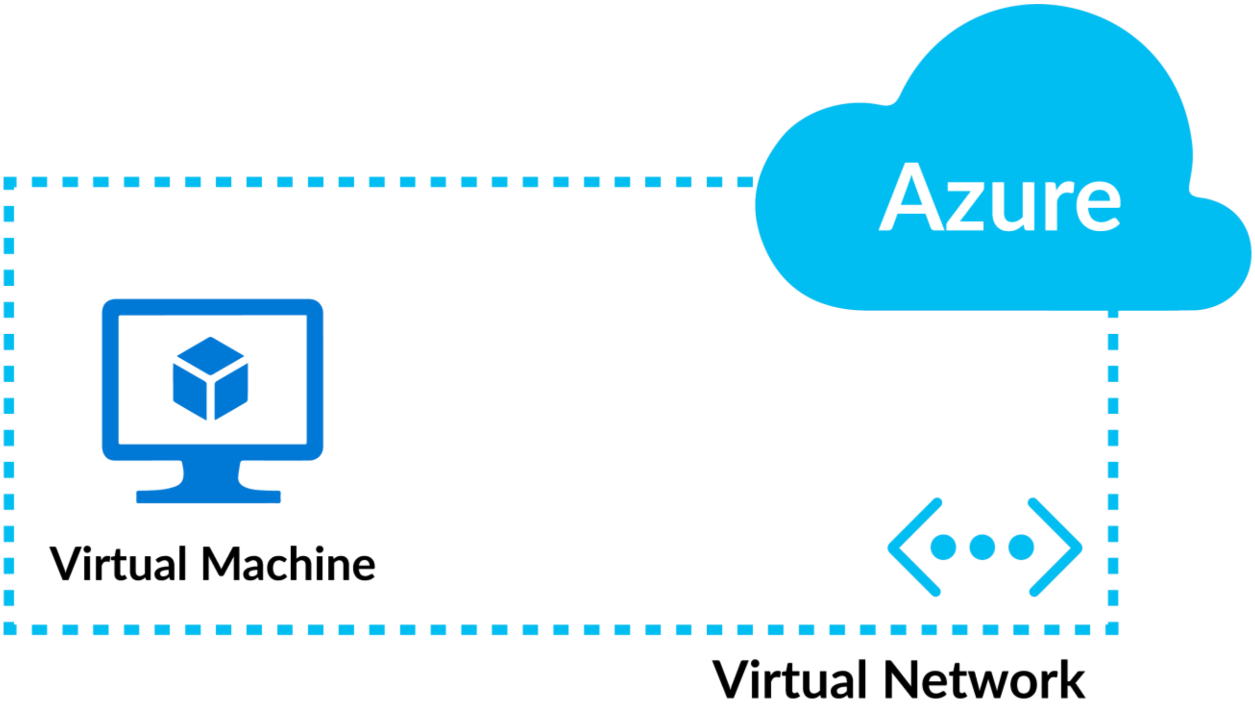
Virtual Network

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.


Virtual Networks act as a container for subnets
Cloud Instances to be included in the subnets
Connection properties to be configured here
Virtual Network
Subnets
Network Security Groups

Source: edureka

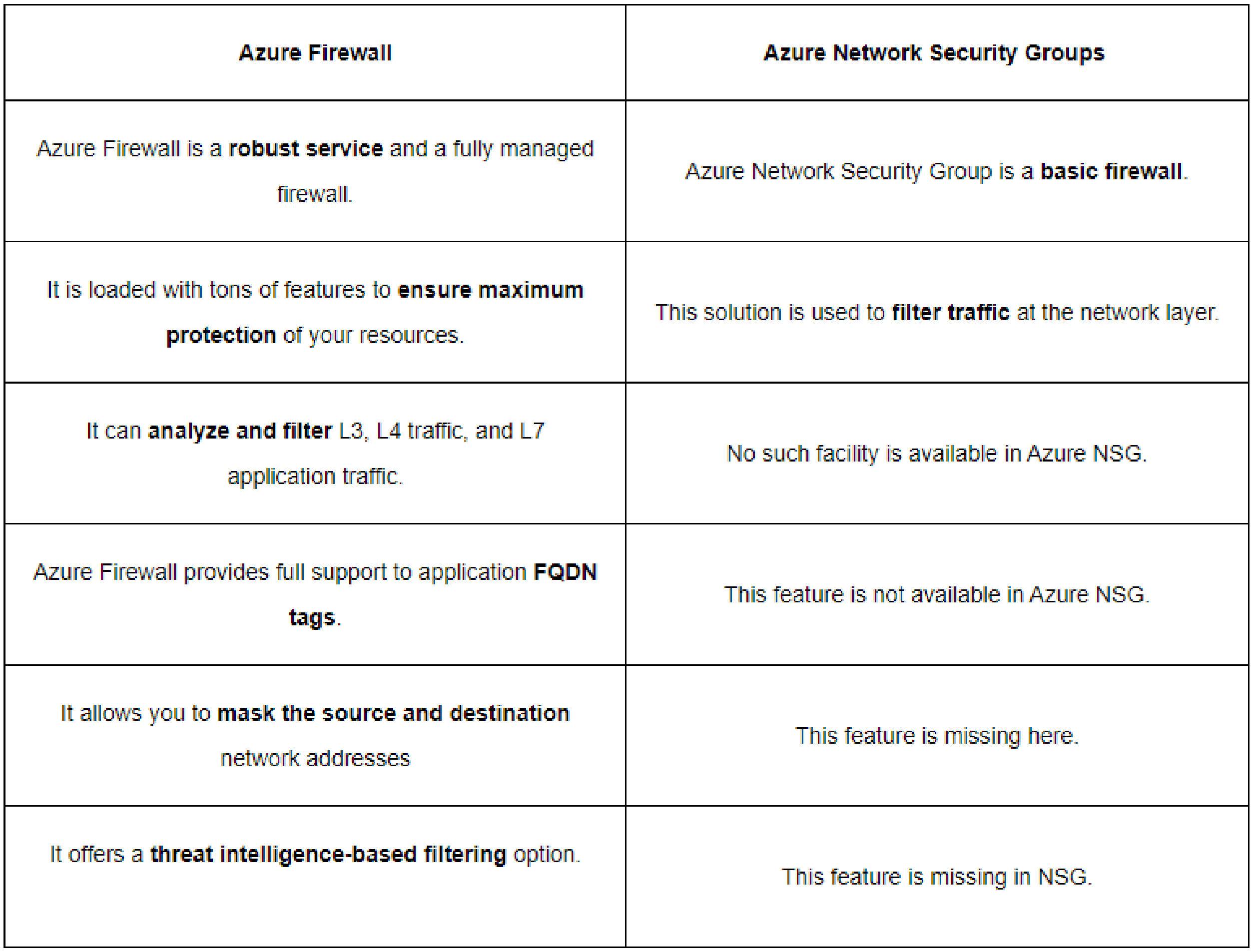
A virtual network is one in which all connected devices, servers, virtual machines, and data centres use software and wireless technology to connect. This allows the network's reach to be extended as far as it needs to be for maximum efficiency, among other advantages.



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.

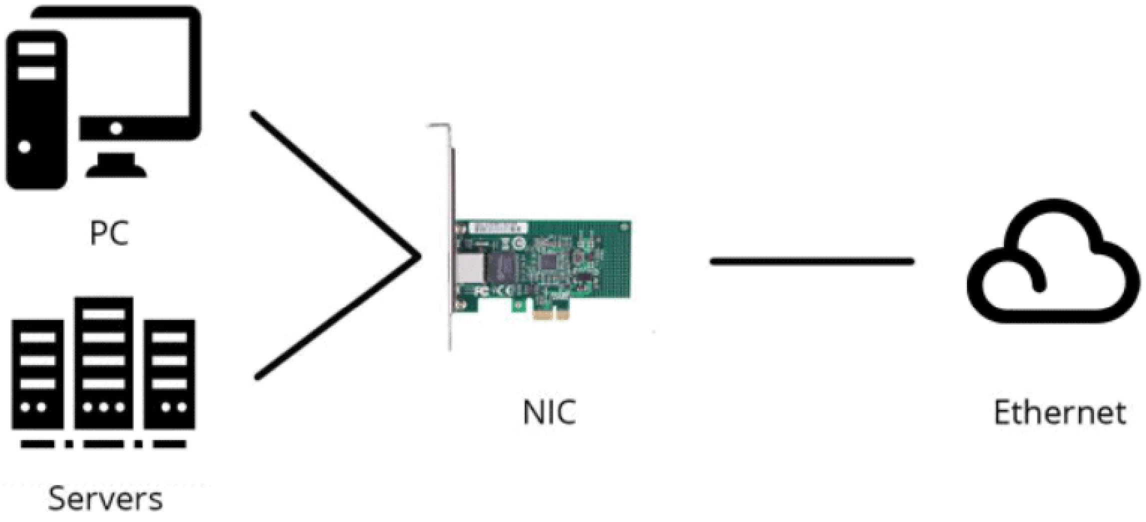
What is the difference between NSG and Firewall?



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

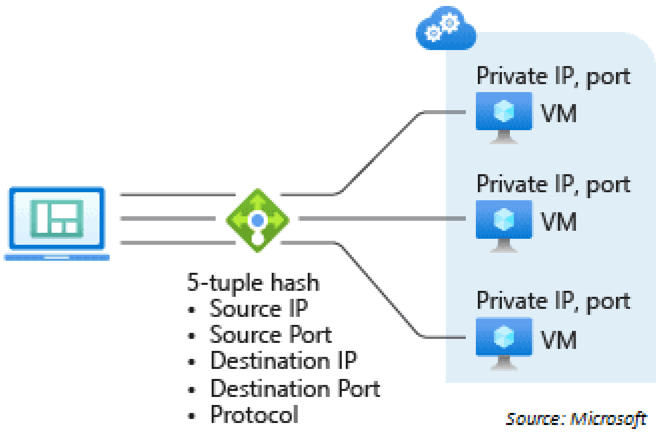
A Network Interface (NIC) is a connection between a Virtual Machine and the software network behind it. One or more network interfaces (NICs) are attached to a Virtual Machine (VM). One or more static or dynamic public and private IP addresses can be assigned to any NIC.



Source: community.fs.com

5-tuple hash

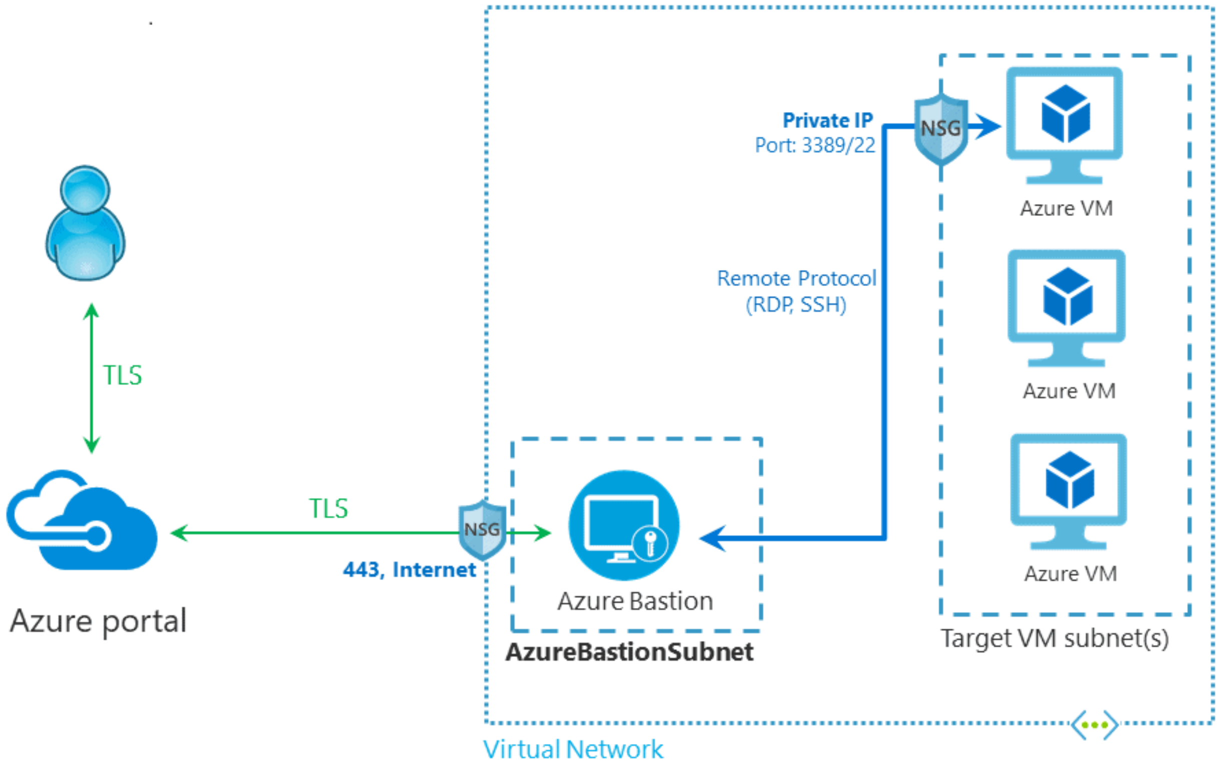
A 5-tuple hash is the default distribution mechanism for Azure Load Balancer. The source IP, source port, destination IP, destination port, and protocol type make up the tuple. The technique only provides stickiness inside a transport session, and the hash is used to map traffic to available servers.



Source: Microsoft

Bastion Host

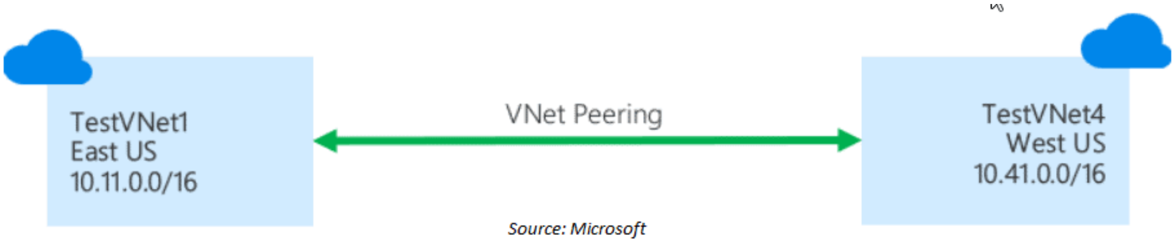
A bastion host is a server that allows users to connect to a private network from a public network like the Internet. A bastion host must reduce the risks of infiltration due to its vulnerability to attack.



Source:Microsoft

VNet-Peering

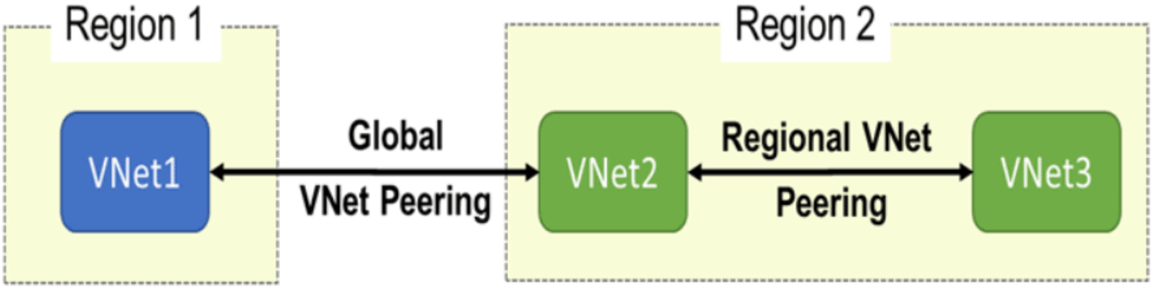
In Azure, virtual network peering allows you to link two or more Virtual Networks seamlessly. For connectivity reasons, the virtual networks appear to be one. The Microsoft backbone technology is used to transport traffic between virtual computers in peer virtual networks. Traffic is routed only through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

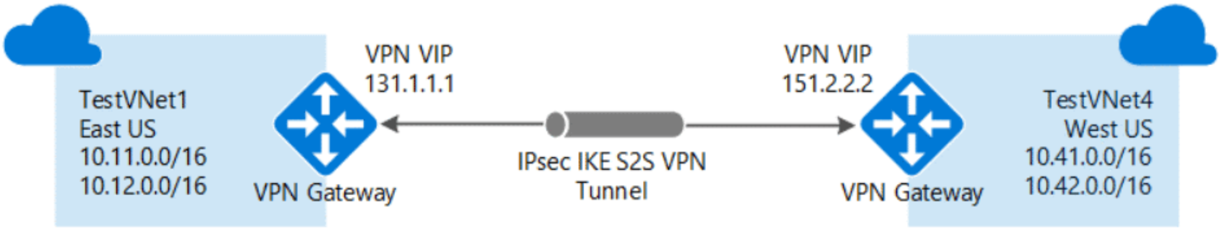


Source: rajanieshkaushikk

- 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.



Source: Microsoft

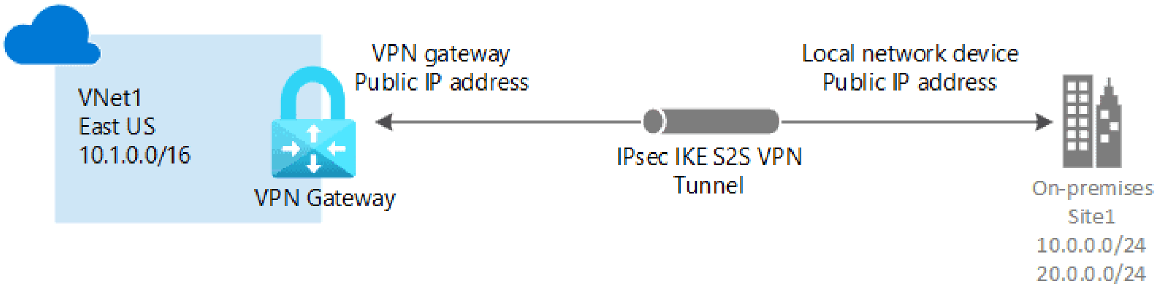
Which is best VNet peering or VPN Gateway?

- **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.

Site-to-Site Connection

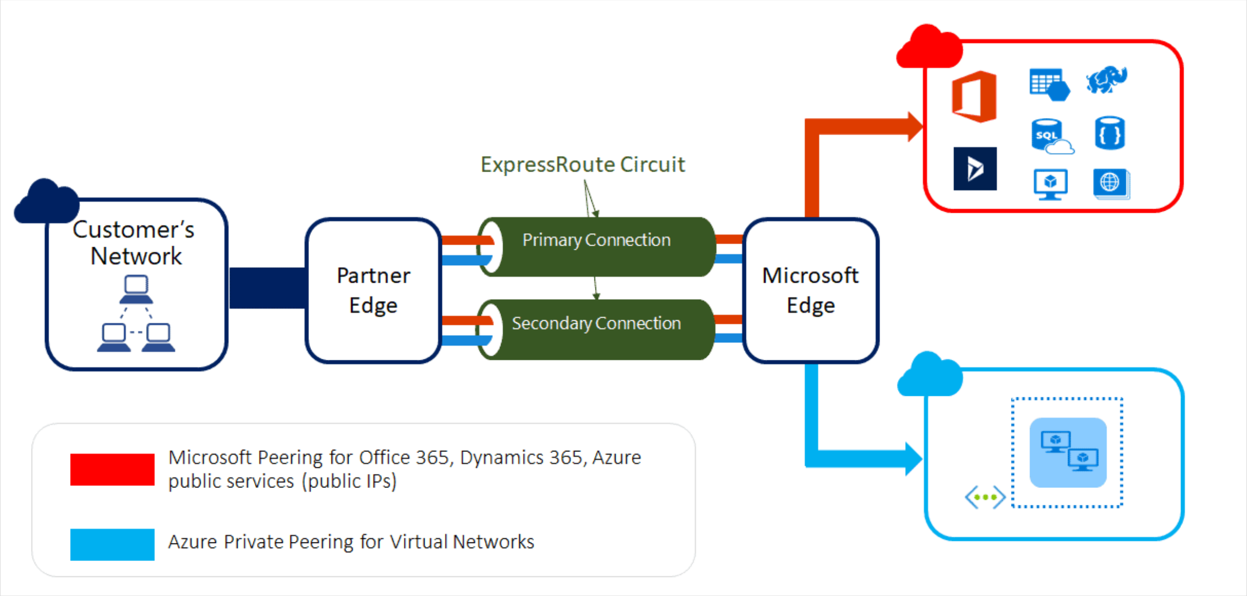
If we have an on-premises virtual network, and we may have other virtual networks existing in other cloud providers. To connect to our virtual network in Azure with the network that is an on-premises data centre, we can use a Site-to-site VPN.

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.

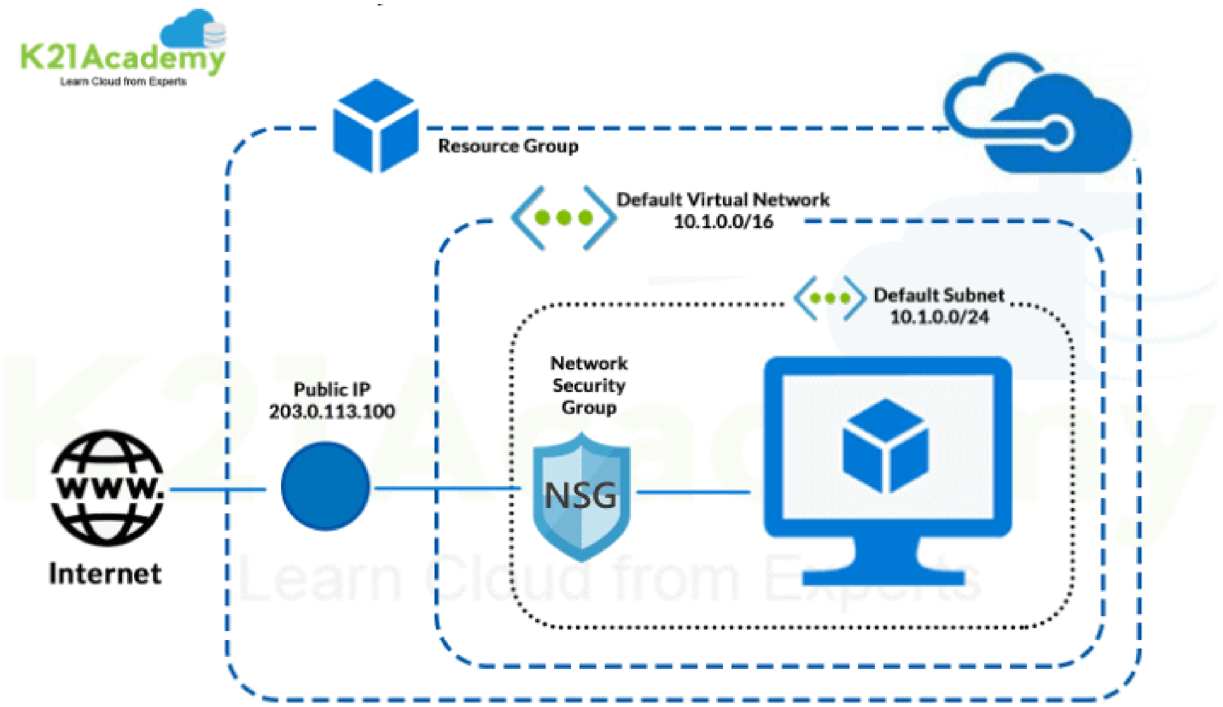

ExpressRoute Circuit
Customer's Network
Partner Edge
Primary Connection
Secondary Connection
Microsoft Edge
SQL
Microsoft Peering for Office 365, Dynamics 365, Azure public services (public IPs)
Azure Private Peering for Virtual Networks

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.

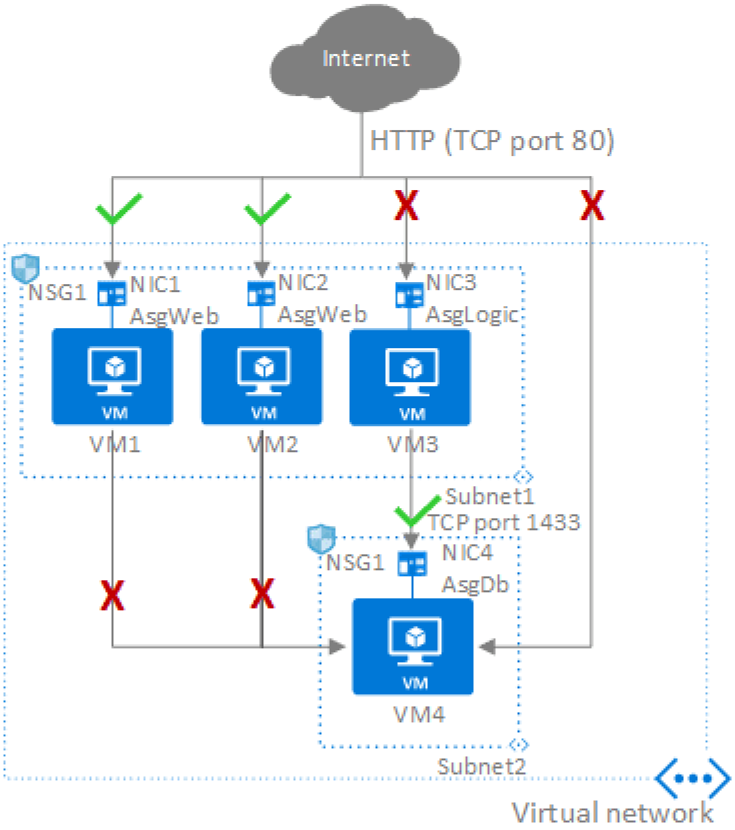
The 5-tuple hash takes values from the Source port number, IP Addresses, Destination IP address and port number, etc. It allows to associate Network Security Groups with a VNet or a VM network interface very easily, and it works on layers 3 and 4 of the OSI model.



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.


Internet
HTTP (TCP port 80)
NSG1
NIC1
AsgWeb
NIC2
AsgWeb
NIC3
AsgLogic
VM
VM
VM
VM1
VM2
VM3
Subnet1
TCP port 1433
NSG1
NIC4
AsgDb
VM
VM4
Subnet2
Virtual network