Azure Networking

Azure Networking is a communication protocol for connecting multiple resources via the Internet. Microsoft provides various services and tools under Azure that make your network strong and easy to manage. This blog will cover the basics of networking concepts 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.

Getting Familiar with IP Addressing

Before understanding IP Address, we need to learn the binary numbers. If you are not familiar with binary and decimal conversion, look at the brief explanation below.

In the decimal number system, the combinations are made using only the numbers from 0 to 9. In other words, it is the number system with a base of 10 (0 to 9). Similarly, in the Binary Number System base of 2 (0 and 1) is used. Each value in a binary number is made with 2^N ('N' is the place value that increases from right to left). The below table shows the basic conversion between binary and decimal.

Binary	Conversion	Decimal
000	$0 \times 2^2 + 0 \times 2^1 + 0 \times 2^0$	0
001	$0 \times 2^2 + 0 \times 2^1 + 1 \times 2^0$	1
010	$0 \times 2^2 + 1 \times 2^1 + 0 \times 2^0$	2
011	$0 \times 2^2 + 1 \times 2^1 + 1 \times 2^0$	3
100	$1 \times 2^2 + 0 \times 2^1 + 0 \times 2^0$	4
101	$1 \times 2^2 + 0 \times 2^1 + 1 \times 2^0$	5

Azure Networking : Brief Introduction of Azure Virtual Network

Azure Networking is a communication protocol for connecting multiple resources via the Internet. Microsoft provides various services and tools under Azure that make your network strong and easy to manage. This blog will cover the basics of networking concepts and an overview of Azure networking architecture with the following topics.

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.

Getting Familiar with IP Addressing

Before understanding IP Address, we need to learn the binary numbers. If you are not familiar with binary and decimal conversion, look at the brief explanation below.

In the decimal number system, the combinations are made using only the numbers from

0 to 9. In other words, it is the number system with a base of 10 (0 to 9). Similarly, in the Binary Number System base of 2 (0 and 1) is used. Each value in a binary number is made with 2^N ('N' is the place value that increases from right to left). The below table shows the basic conversion between binary and decimal.

What is IP Address?

IANA is the Internet Assigned Numbers Authority that manages and assigns the IP address in the world. IP Address identifies each device on a network uniquely. There are currently two IP Adress that is IPv4 and IPv6. An **IPv4** address contains a total of 32 binary bits divided into 4 equal octets (8-bit block), whereas **IPv6** is written in hexadecimal notation, separated into 8 groups of 16 **bits** by the colons, thus (8 x 16 = 128) bits in total. We will focus on IPv4 as it is the most used. Each octet of an IP

Binary	Conversion	Decimal
000	$0 \times 2^2 + 0 \times 2^1 + 0 \times 2^0$	0
001	$0 \times 2^2 + 0 \times 2^1 + 1 \times 2^0$	1
010	$0 \times 2^2 + 1 \times 2^1 + 0 \times 2^0$	2
011	$0 \times 2^2 + 1 \times 2^1 + 1 \times 2^0$	3
100	$1 \times 2^2 + 0 \times 2^1 + 0 \times 2^0$	4
101	$1 \times 2^2 + 0 \times 2^1 + 1 \times 2^0$	5

Address is separated by a decimal and ranges from 0 to 255. You will clearly understand the binary number, octets, and IP address formation in the below table. There are two different IP address one is private, and the other is public.

- **Private IP** is accessed only within a network like a simple school network with a LAN connection.
- **Public IP** is accessed globally via the Internet.

IP Address	Octet 1	Octet 2	Octet 3	Octet 4
10.2.7.4	00001010	00000010	00000111	0000010
192.124.249.161	11000000	01111100	11111001	1010000
255.255.140.40	11111111	11111111	10001100	0010100

The table below shows the Private IP address range assigned by IANA, and the rest are all Public IP address.

Private IP Range
10.0.0.1 – 10.255.255.255
172.16.0.0 – 172.31.255.255
192.168.0.0 – 192.168.255.255

What is IP Subnetting?

Subnetting is the process of dividing a network into many smaller networks. There are 5 classes of IP address and each with a unique purpose. Only the first octet is used for dividing an IP Address into different classes. The table below shows the range of IP address of the 5 classes.
research and development. So both these classes are reserved and can not be used. The below table shows the range of the first octet in an IP address with each class.
Note: The IP address with the first octet as 127 (in decimal) is a loopback address to check the network and address of the machine itself.

Class	Octet 1 Range (in Binary)	Octet 1 Range (in Decimal)
Class A	00000000-01111111	0-126

Class B	10000000-10111111	128-191
Class C	11000000-11011111	192-223
Class D	11100000-11101111	224-239
Class E	11110000-11110111	240-255

Class D is reserved for multitasking and broadcasting purpose, whereas **Class E** is reserved for
An IP address can further be divided into small networks depending on the use and purpose. The above classes are not sufficient for real-life use. Only 5 classes can not hold all the hosts on the same network, and the loss of IP address will be huge. So, the CIDR method was introduced.

Note: Every subnet's first and last address is not allocated to any host as it is reserved for network and broadcast.

SubNet	Total IP	Network IP	Broadcast IP	Range of Hosts	Total H
1	16	192.168.1.0	192.168.1.15	192.168.1.1-192.168.1.14	14
2	16	192.168.1.16	192.168.1.31	192.168.1.17-192.168.1.30	14
3	16	192.168.1.32	192.168.1.47	192.168.1.33-192.168.1.46	14
4	16	192.168.1.48	192.168.1.65	192.168.1.49-192.168.1.64	14

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.
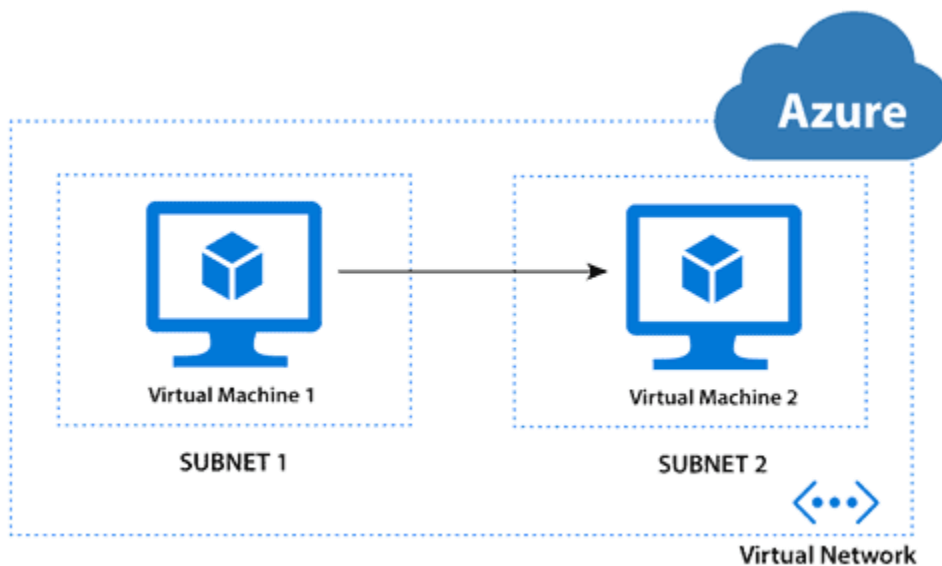
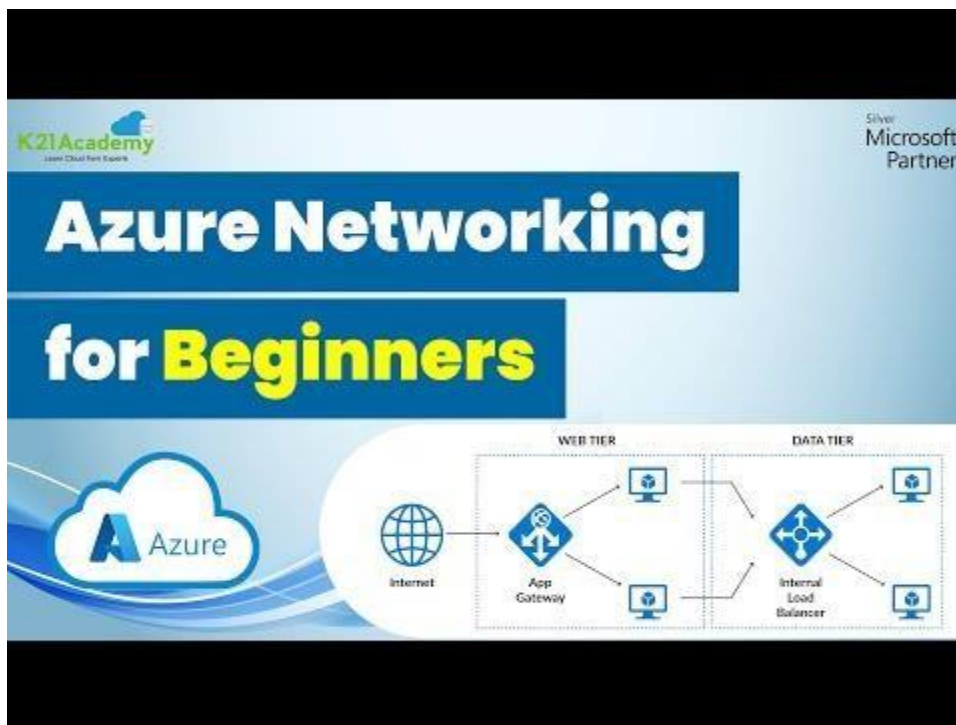# Azure Networking : Brief Introduction of Azure Virtual Network

June 15, 2021 by Krishan kumar 4 Comments
 6087 views

Overview of Azure | Getting Familiar with IP Addressing | Azure Virtual Network (VNet) | Azure Network Security | Azure Network Models | Conclusion

Azure Networking is a communication protocol for connecting multiple resources via the Internet. Microsoft provides various services and tools under Azure that make your network strong and easy to manage. This blog will cover the basics of networking concepts and an overview of Azure networking architecture with the following topics.

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.

Getting Familiar with IP Addressing

Before understanding IP Address, we need to learn the binary numbers. If you are not familiar with binary and decimal conversion, look at the brief explanation below.

In the decimal number system, the combinations are made using only the numbers from 0 to 9. In other words, it is the number system with a base of 10 (0 to 9). Similarly, in the Binary Number System base of 2 (0 and 1) is used. Each value in a binary number is made with 2^N ('N' is the place value that increases from right to left). The below table shows the basic conversion between binary and decimal.
Also Check: ARM Template. What
is IP Address?

Binary	Conversion	Decimal
000	$0\times2^2+0\times2^1+0\times2^0$	0
001	$0\times2^2+0\times2^1+1\times2^0$	1
010	$0\times2^2+1\times2^1+0\times2^0$	2
011	$0\times2^2+1\times2^1+1\times2^0$	3
100	$1\times2^2+0\times2^1+0\times2^0$	4
101	$1\times2^2+0\times2^1+1\times2^0$	5

IANA is the Internet Assigned Numbers Authority that manages and assigns the IP address in the world. IP Address identifies each device on a network uniquely. There are currently two IP Adress that is IPv4 and IPv6. An **IPv4** address contains a total of 32 binary bits divided into 4 equal octets (8-bit block), whereas **IPv6** is written in hexadecimal notation, separated into 8 groups of 16 **bits** by the colons, thus (8 x 16 = 128) bits in total. We will focus on IPv4 as it is the most used. Each octet of an IP Address is separated by a decimal and ranges from 0 to 255. You will clearly understand the binary number, octets, and IP address formation in the below table. There are two different IP address one is private, and the other is public.

IP Address	Octet 1	Octet 2	Octet 3	Octet 4
10.2.7.4	00001010	00000010	00000111	0000010
192.124.249.161	11000000	01111100	11111001	1010000
255.255.140.40	11111111	11111111	10001100	0010100

- **Private IP** is accessed only within a network like a simple school network with a LAN connection.
- **Public IP** is accessed globally via the Internet.

Class	Octet 1 Range (in Binary)	Octet 1 Range (in Decimal)

Class A	00000000-01111111	0-126

The table below shows the Private IP address range assigned by IANA, and the rest are all Public IP address.

Private IP Range
10.0.0.1 – 10.255.255.255
172.16.0.0 – 172.31.255.255
192.168.0.0 – 192.168.255.255

Check Out: [Azure Service Bus Pricing](). What is IP Subnetting?

Subnetting is the process of dividing a network into many smaller networks. There are 5 classes of IP address and each with a unique purpose. Only the first octet is used for dividing an IP Address into different classes. The table below shows the range of IP address of the 5 classes.

Class D is reserved for multitasking and broadcasting purpose, whereas **Class E** is reserved for research and development. So both these classes are reserved and can not be used. The below table shows the range of the first octet in an IP address with each class.

Note: The IP address with the first octet as 127 (in decimal) is a loopback address to check the network and address of the machine itself.

An IP address can further be divided into small networks depending on the use and purpose. The above classes are not sufficient for real-life use. Only 5 classes can not hold all the hosts on the same network, and the loss of IP address will be huge. So, the CIDR method was introduced.

CIDR (Classless Inter-Domain Routing)

Class B	10000000-10111111	128-191
Class C	11000000-11011111	192-223
Class D	11100000-11101111	224-239
Class E	11110000-11110111	240-255

CIDR is a method for allocating IP Address. Using this method, we can apply a subnet mask to an IP Address. This mask defines the number of bits used as a network, and the host will use the other bits that left. To understand CIDR better, we will decode a simple IP address with a subnet mask.

Suppose 192.168.1.30/28 is an IP address with 28 as the subnet mask. By comparing with IP address classes in the above table, this IP comes under Class C. Now, 24 bits are made of 3 octets, so the network will take four extra bits from the next octet to complete 28 bits. Using 2^N('N' is the number of borrowed bits from the host), a total of 16 subnets is formed. After taking the four bits, the last octet is left with only 4 bits that a host will use. Using 2^H('H' is the number of host bits left), each subnet will contain a block of 16 IP address. The first and last IP is reserved for network and broadcast in each subnet, so the total number of hosts will be 2^H-2('H' is the number of host bits) equals 14.

Although a total of 16 subnets or network are possible for this example, the table below listed the initial 4 subnets that can be formed using 28 as the subnet mask. Each subnet contains a total of 16 IP address, and the number of hosts will be 14 as the other two are reserved for network and broadcast.

After comparing the IP given in the example that is 192.168.1.30/28 with the table below, it is clearly visible that it belongs to the second subnet ranging from 192.168.1.16 to 192.168.1.31.

Note: Every subnet's first and last address is not allocated to any host as it is reserved for network and broadcast.

Check Out: Azure Bastion.
IP Address in Azure

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

SubNet	Total IP	Network IP	Broadcast IP	Range of Hosts	Total H
1	16	192.168.1.0	192.168.1.15	192.168.1.1-192.168.1.14	14
2	16	192.168.1.16	192.168.1.31	192.168.1.17-192.168.1.30	14
3	16	192.168.1.32	192.168.1.47	192.168.1.33-192.168.1.46	14
4	16	192.168.1.48	192.168.1.65	192.168.1.49-192.168.1.64	14

- **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 publicfacing 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.

Also Read: Azure Load Balancer.
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.
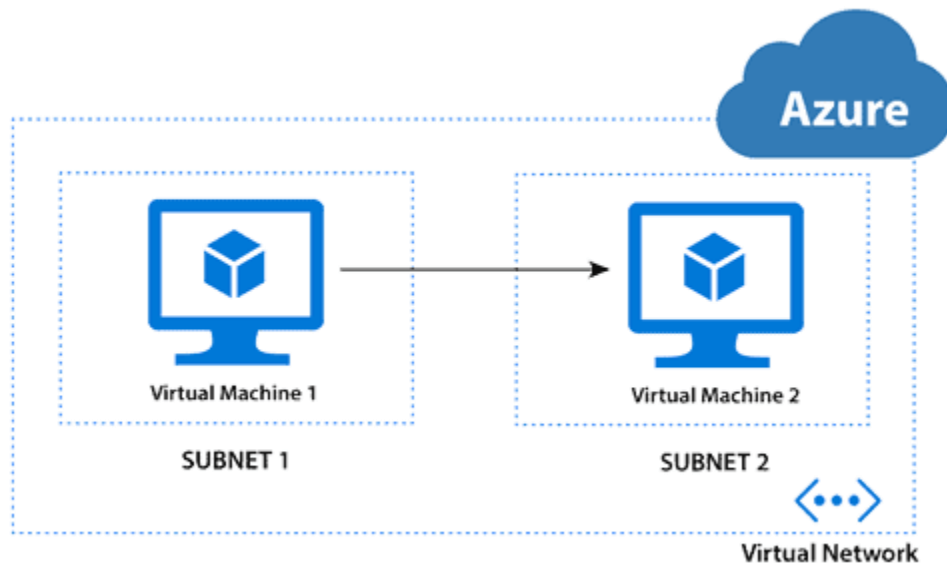

Azure Subnet

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)
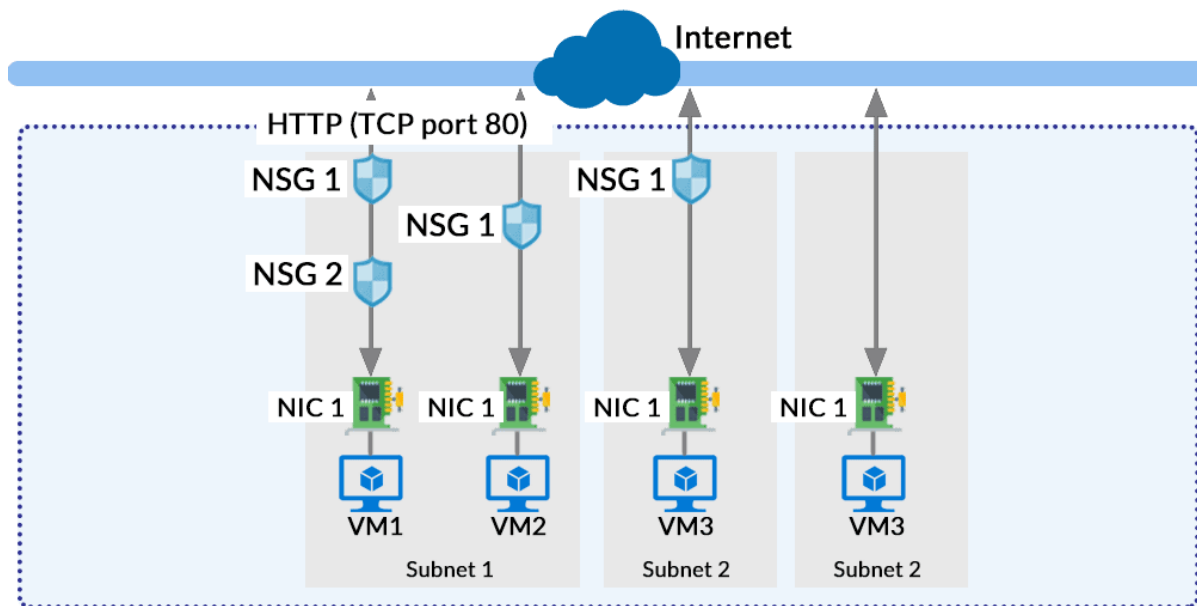
The Network Security Group in Azure acts like a firewall at the network level. It filters the traffic passing through Azure Resources in a virtual network. NSG is a group of security rules that defines the priority, source or destination, protocol, direction, port range and action. Using these rules, NSG allows or deny inbound and outbound traffic. The rules for entering traffic inside a resource is also called 'Ingress', and the rules for exiting the traffic or going out of the resource is called 'Egress'. When all the rules are created, the NSG can be used in a Virtual Machine that will interact with a network.

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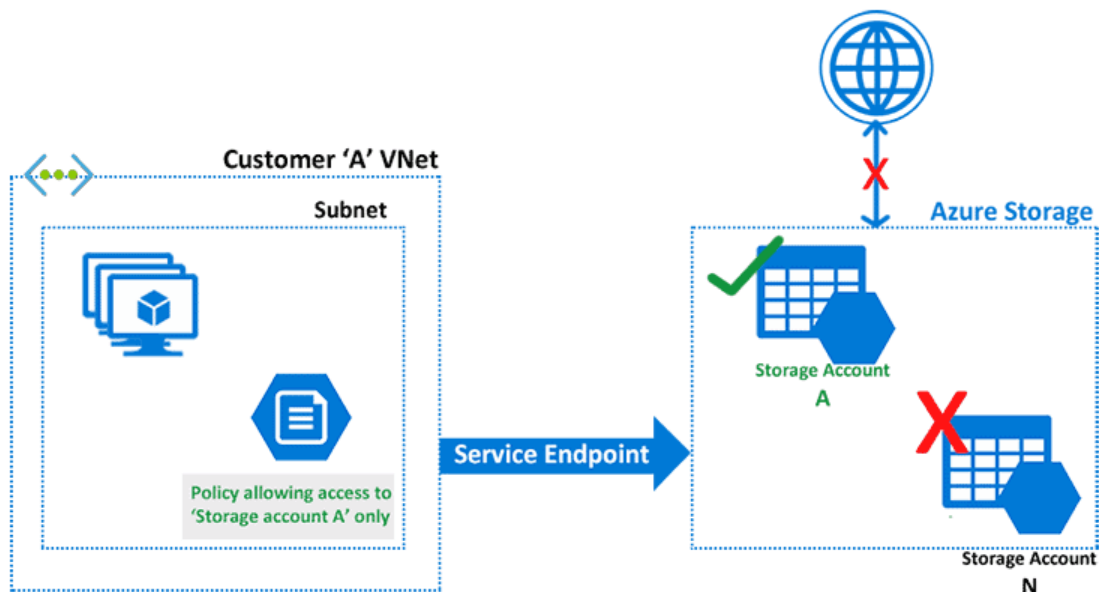
Service Endpoints in Azure provides secure connectivity over the optimized route of the Azure Network. Without needing a public IP address, Service Endpoints allows Private IP address in a VNet to reach the endpoint of an Azure Service. It is simple to set up and improves security for the Azure resources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

Web Application Firewall (WAF)
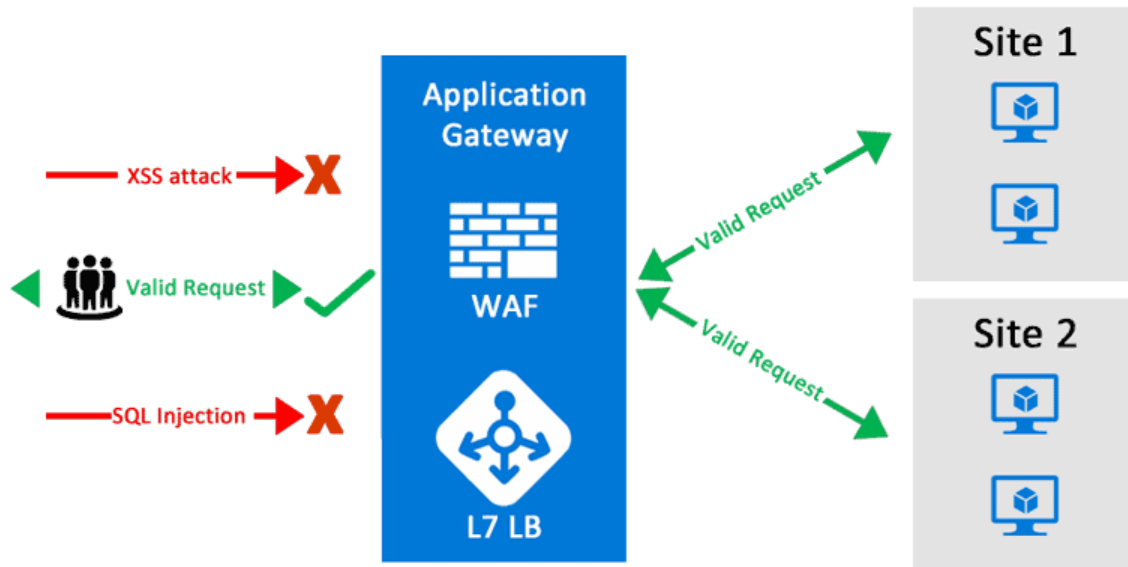
Web applications are a common target for hackers to steal user information. So, protection from the most common attacks like SQL injection, cross-site scripting, etc., is a must. Web Application Firewall by Azure is a firewall for protecting the web application from these common threats. It provides 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
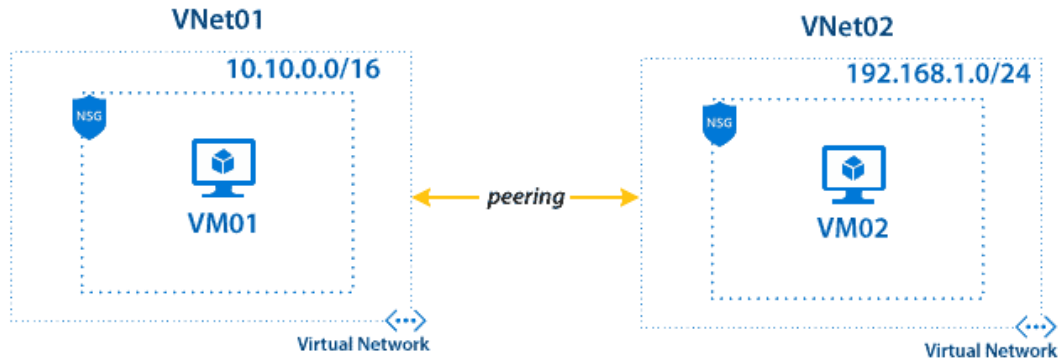
Virtual Network peering enables to connect the two or more Virtual Networks in Azure. It also allows transferring data between deployment models, Azure Subscriptions, Azure Active Directory Tenants and Azure regions without downtime and failure. The traffic between the peered virtual networks use Microsoft's 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.
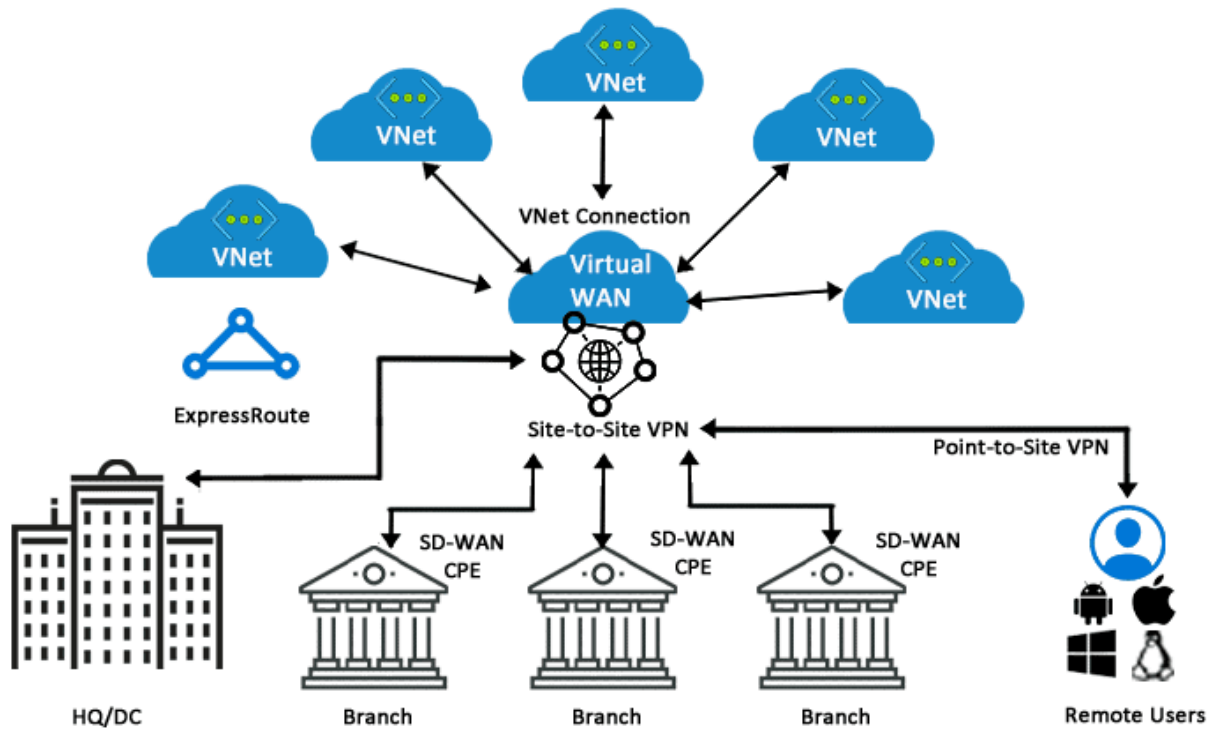
In the above diagram, a Virtual WAN at the centre acts as a single operational hub to manage all the traffic coming from multiple resources in a VNet. Instead of contacting the multiple branches separately, a VNet can contact the central hub to connect with all the branches connected to it.