Azure fundamentals

Azure subscription overview

Introduction to Azure:-

AZURE means Auroral Zone Upwelling Release Experiment. Microsoft Azure is a cloud computing platform and an online portal that allows you to access and manage cloud services and resources provided by Microsoft. These services and resources include storing your data and transforming it, depending on your requirements. To get access to these resources and services, all you need to have is an active internet connection and the ability to connect to the Azure portal.

It is an open and flexible cloud platform which helps in development, data storage, service hosting, and service management.

Azure services can be managed through a web based portal,command line interface(Azure CLI and Azure Powershell) or software development kits(Java,Python..NET etc).

Cloud :-

Cloud refers to the servers that are accessed over the internet and the software and databases that run on those servers.

Cloud Computing :-

Simply put, cloud computing is the delivery of computing services—including servers, storage, databases, networking, software, analytics, and intelligence—over the Internet (“the cloud”) to offer faster innovation, flexible resources, and economies of scale. You typically pay only for cloud services you use, helping lower your operating costs, run your infrastructure more efficiently and scale as your business needs change.

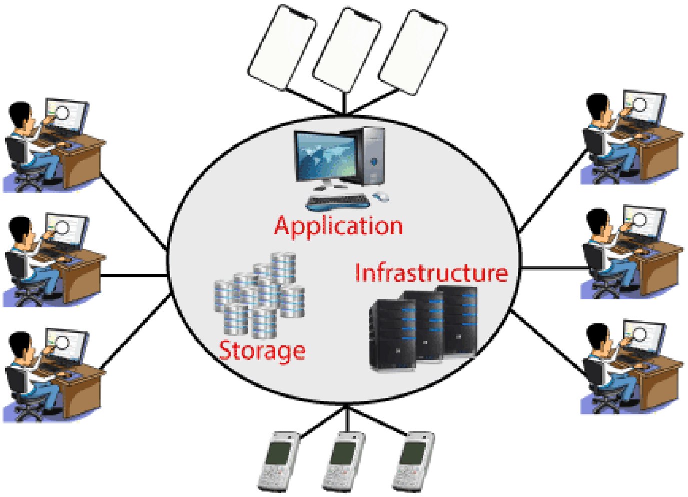


Diagram of cloud computing

Types of Cloud Computing:-

There are three different ways to deploy cloud services: on a public cloud, private cloud and hybrid cloud.

Public cloud

Public clouds are owned and operated by a third-party cloud service providers, which deliver their computing resources like servers and storage over the Internet. Microsoft Azure is an example of a public cloud. With a public cloud, all hardware, software and other supporting infrastructure is owned and managed by the cloud provider. You access these services and manage your account using a web browser.

Private cloud

A private cloud refers to cloud computing resources used exclusively by a single business or organization. A private cloud can be physically located on the company's on-site datacenter. Some companies also pay third-party service providers to host their private cloud. A private cloud is one in which the services and infrastructure are maintained on a private network.

Hybrid cloud

Hybrid clouds combine public and private clouds, bound together by technology that allows data and applications to be shared between them. By allowing data and applications to move between private and public clouds, a hybrid cloud gives your business greater flexibility, more deployment options and helps optimise your existing infrastructure, security and compliance.

Types of cloud services:

Infrastructure as a service (IaaS)

The most basic category of cloud computing services. With IaaS, you rent IT infrastructure—servers and virtual machines (VMs), storage, networks, operating systems—from a cloud provider on a pay-as-you-go basis.

Platform as a service (PaaS)

Platform as a service refers to cloud computing services that supply an on-demand environment for developing, testing, delivering and managing software applications. PaaS is designed to make it easier for developers to quickly create web or mobile apps, without worrying about setting up or managing the underlying infrastructure of servers, storage, network and databases needed for development.

Serverless computing

Overlapping with PaaS, serverless computing focuses on building app functionality without spending time continually managing the servers and infrastructure required to do so. The cloud provider handles the setup, capacity planning and server management for you. Serverless architectures are highly scalable and event-driven, only using resources when a specific function or trigger occurs.

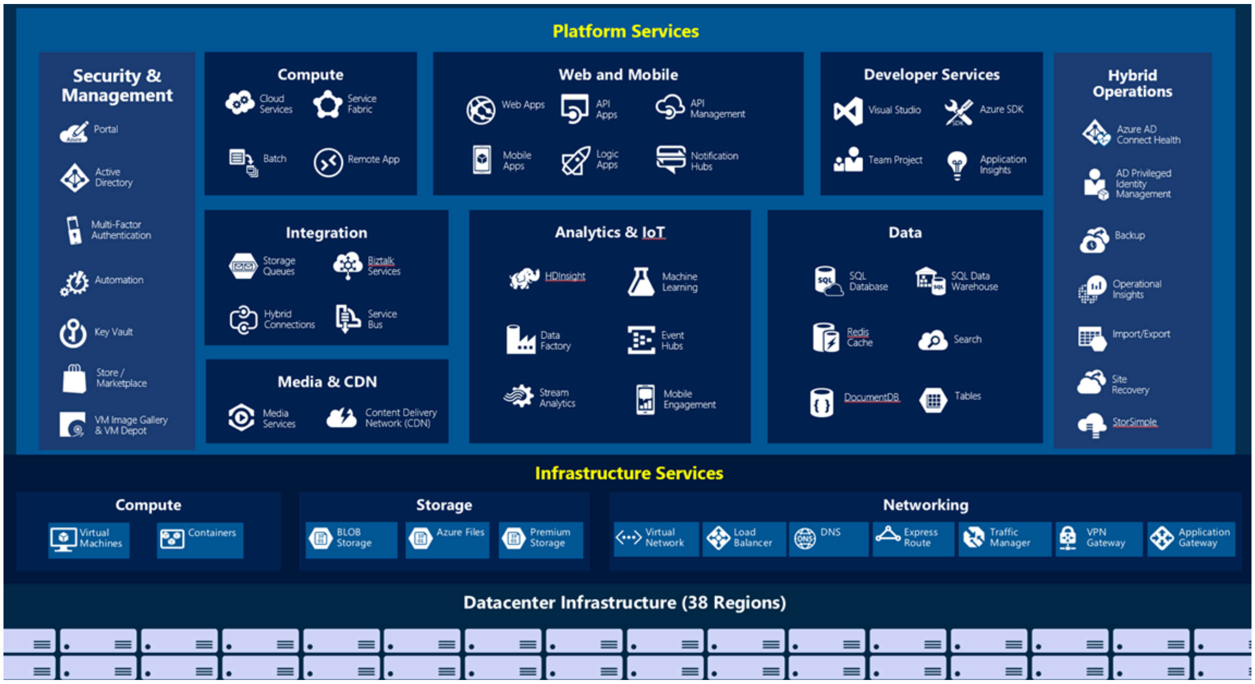
Software as a service (SaaS)

Software as a service is a method for delivering software applications over the Internet, on demand and typically on a subscription basis. With SaaS, cloud providers host and manage the software application and underlying infrastructure and handle any maintenance, like software upgrades and security patching. Users connect to the application over the Internet, usually with a web browser on their phone, tablet or PC.

Benefits of cloud computing:-

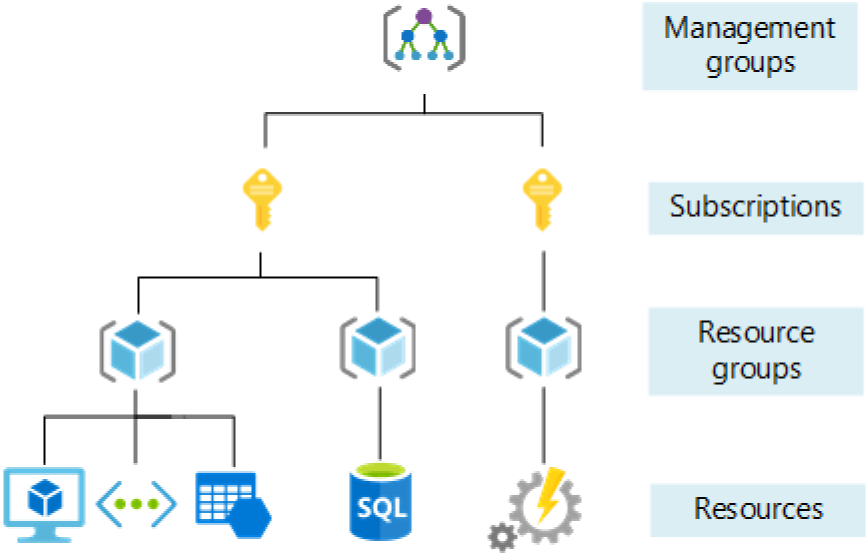
- Speed of service.
- Enhanced flexibility.
- Integrated delivery pipeline.
- Disaster recovery.
- Security.

Azure overview:-



Azure subscription:-

A subscription in Azure is a container that holds a collection of connected business or technical resources. The resources are used and billed as a group. Multiple subscriptions with various access management policies and invoicing procedures can be added to an Azure account**.**



Azure Powershell:-

Azure PowerShell is a set of cmdlets for managing Azure resources directly from PowerShell. Azure PowerShell is designed to make it easy to learn and get started with, but provides powerful features for automation. Azure PowerShell supports several authentication methods.

The Az PowerShell module is a wrapper module for Azure service related PowerShell modules, usually one module per Azure service such as Az.Network for Azure networking services and Az.AKS for Azure Kubernetes Service.

The cmdlets in the Azure PowerShell module are for managing legacy Azure resources that use Service Management APIs.

Features of Azure Powershell:-

The Az PowerShell module features the following benefits:

- Security and stability
  - Token cache encryption
  - Prevention of man-in-the-middle attack type
  - Username and password authentication in PowerShell 7
  - Support for features like continuous access evaluation

- Support for all Azure services
  - All generally available Azure services have a corresponding supported PowerShell module
  - Multiple bug fixes and API version upgrades since AzureRM
- New capabilities
  - Support in Cloud Shell and cross-platform
  - Can get and use access token to access Azure resources

Azure CLI(Command Line Interface):-

The Azure Command-Line Interface (CLI) is a cross-platform command-line tool to connect to Azure and execute administrative commands on Azure resources. It allows the execution of commands through a terminal using interactive command-line prompts or a script.

You can install the Azure CLI locally on Linux, Mac, or Windows computers. It can also be used from a browser through the Azure Cloud Shell or run from inside a Docker container.

Some commands in Azure are

1. get-command

By using this command to get all the commands

2. get-module -listavailable

By using this command to get all the module list

3. New-AzResourceGroup –Name “vinay” -location centralUS

(OR)

New-AzResourceGroup –n “vinil” -l centralUS

By using this command to create new resource group

PRACTICAL

How to create a WEBAPP in Azure Portal

1. Login to Azure portal.
2. Click on Create a resource and select web from marketplace.
3. Click on Web App and click on Create.
4. In resource group, click create new and enter the name then ok.

5. Enter the Appname
6. In publish select code
7. In Runtime stack select .NET5 or Python or Java etc.
8. Select operating system windows
9. Select region CentralUS
10. Select Review+create and select create
11. Go to All resources in left panel to see the list of created resources.
12. Click on Web app name.
13. Click on URL

To Clean up all resources

Azure networking services overview

The networking services in Azure provide a variety of networking capabilities that can be used together or separately. Click any of the following key capabilities to learn more about them:

- **Connectivity services** Connect Azure resources and on-premises resources using any or a combination of these networking services in Azure - Virtual Network (VNet), Virtual WAN, ExpressRoute, VPN Gateway, Virtual network NAT Gateway, Azure DNS, Peering service, and Azure Bastion.
- **Application protection services**: Protect your applications using any or a combination of these networking services in Azure - Load Balancer, Private Link, DDoS protection, Firewall, Network Security Groups, Web Application Firewall, and Virtual Network Endpoints.
- **Application delivery services**: Deliver applications in the Azure network using any or a combination of these networking services in Azure - Content Delivery Network (CDN), Azure Front Door Service, Traffic Manager, Application Gateway, Internet Analyzer, and Load Balancer.
- **Network monitoring**: Monitor your network resources using any or a combination of these networking services in Azure - Network Watcher, ExpressRoute Monitor, Azure Monitor, or VNet Terminal Access Point (TAP).

Connectivity services

This section describes services that provide connectivity between Azure resources, connectivity from an on-premises network to Azure resources, and branch to branch connectivity in Azure - Virtual Network (VNet), ExpressRoute, VPN Gateway, Virtual WAN, Virtual network NAT Gateway, Azure DNS, Azure Peering service, and Azure Bastion.

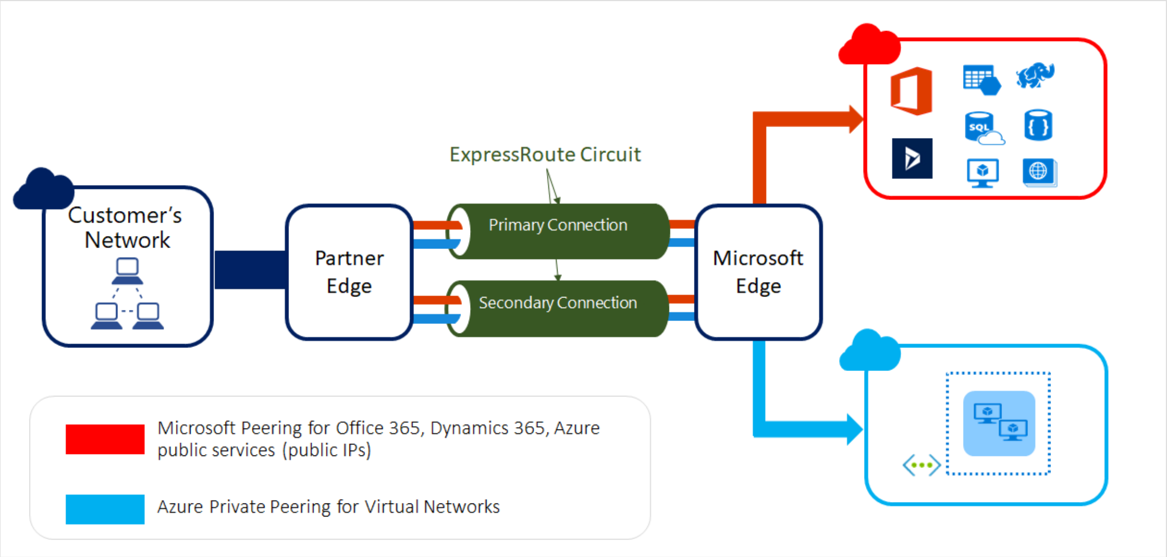
Virtual network

Azure Virtual Network (VNet) is the fundamental building block for your private network in Azure. You can use VNets to:

- **Communicate between Azure resources**: You can deploy VMs, and several other types of Azure resources to a virtual network, such as Azure App Service Environments, the Azure Kubernetes Service (AKS), and Azure Virtual Machine Scale Sets. To view a complete list of Azure resources that you can deploy into a virtual network.
- **Communicate between each other**: You can connect virtual networks to each other, enabling resources in either virtual network to communicate with each other, using virtual network peering. The virtual networks you connect can be in the same, or different, Azure regions.
- **Communicate to the internet**: All resources in a VNet can communicate outbound to the internet, by default. You can communicate inbound to a resource by assigning a public IP address or a public Load Balancer. You can also use Public IP addresses or public Load Balancer to manage your outbound connections.
- **Communicate with on-premises networks**: You can connect your on-premises computers and networks to a virtual network using VPN Gateway or ExpressRoute.

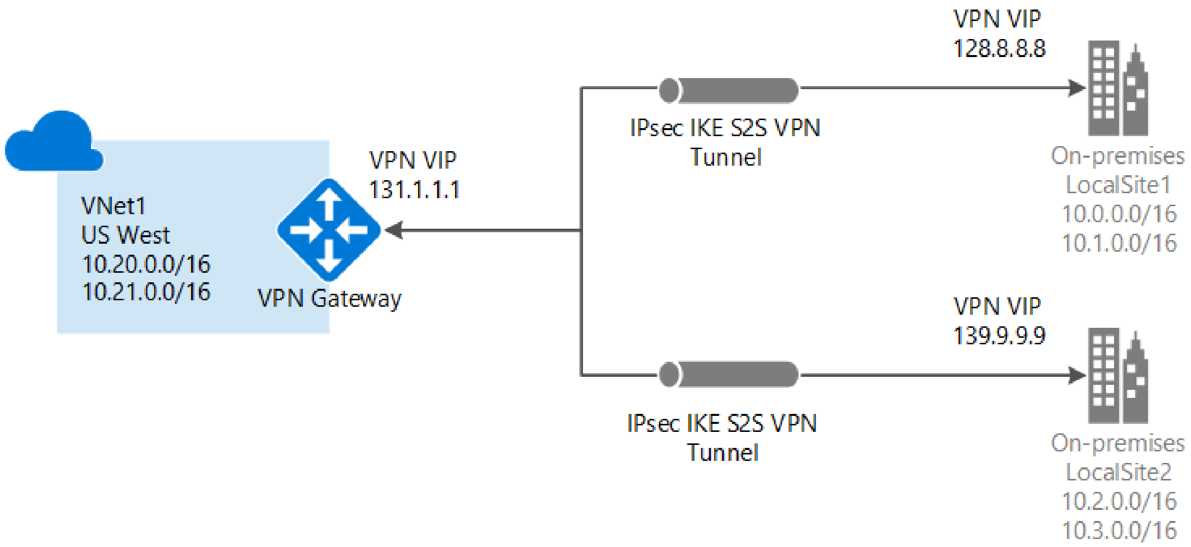
ExpressRoute

ExpressRoute enables you to extend your on-premises networks into the Microsoft cloud over a private connection facilitated by a connectivity provider. This connection is private. Traffic does not go over the internet. With ExpressRoute, you can establish connections to Microsoft cloud services, such as Microsoft Azure, Microsoft 365, and Dynamics 365.


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

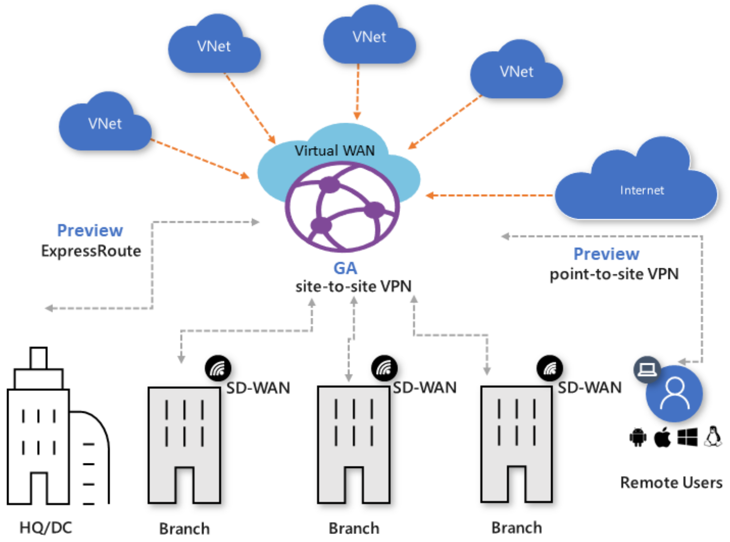
VPN Gateway

VPN Gateway helps you create encrypted cross-premises connections to your virtual network from on-premises locations or create encrypted connections between VNets. There are different configurations available for VPN Gateway connections, such as site-to-site, point-to-site, and VNet-to-VNet. The following diagram illustrates multiple site-to-site VPN connections to the same virtual network.



Virtual WAN

Azure Virtual WAN is a networking service that provides optimized and automated branch connectivity to, and through, Azure. Azure regions serve as hubs that you can choose to connect your branches to. You can leverage the Azure backbone to also connect branches for branch-to-VNet connectivity. Azure Virtual WAN brings together many Azure cloud connectivity services such as site-to-site VPN, ExpressRoute, and point-to-site user VPN into a single operational interface. Connectivity to Azure VNets is established by using virtual network connections.

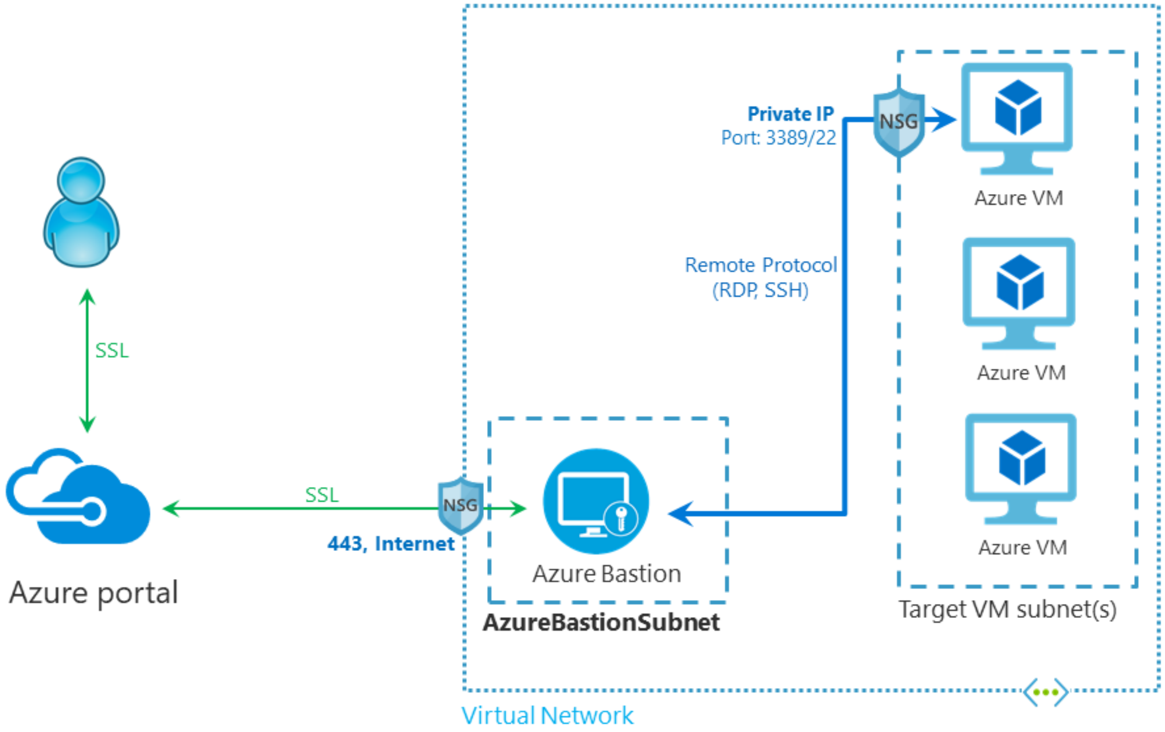


Azure DNS

Azure DNS is a hosting service for DNS domains that provides name resolution by using Microsoft Azure infrastructure. By hosting your domains in Azure, you can manage your DNS records by using the same credentials, APIs, tools, and billing as your other Azure services.

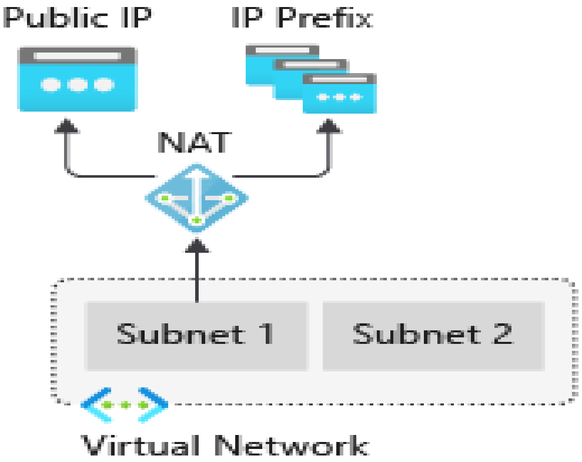
Azure Bastion

The Azure Bastion service is a fully platform-managed PaaS service that you provision inside your virtual network. It provides secure and seamless RDP/SSH connectivity to your virtual machines directly in the Azure portal over TLS. When you connect via Azure
.



Virtual network NAT Gateway

Virtual Network NAT (network address translation) simplifies outbound-only Internet connectivity for virtual networks. When configured on a subnet, all outbound connectivity uses your specified static public IP addresses. Outbound connectivity is possible without load balancer or public IP addresses directly attached to virtual machines.



Application protection services

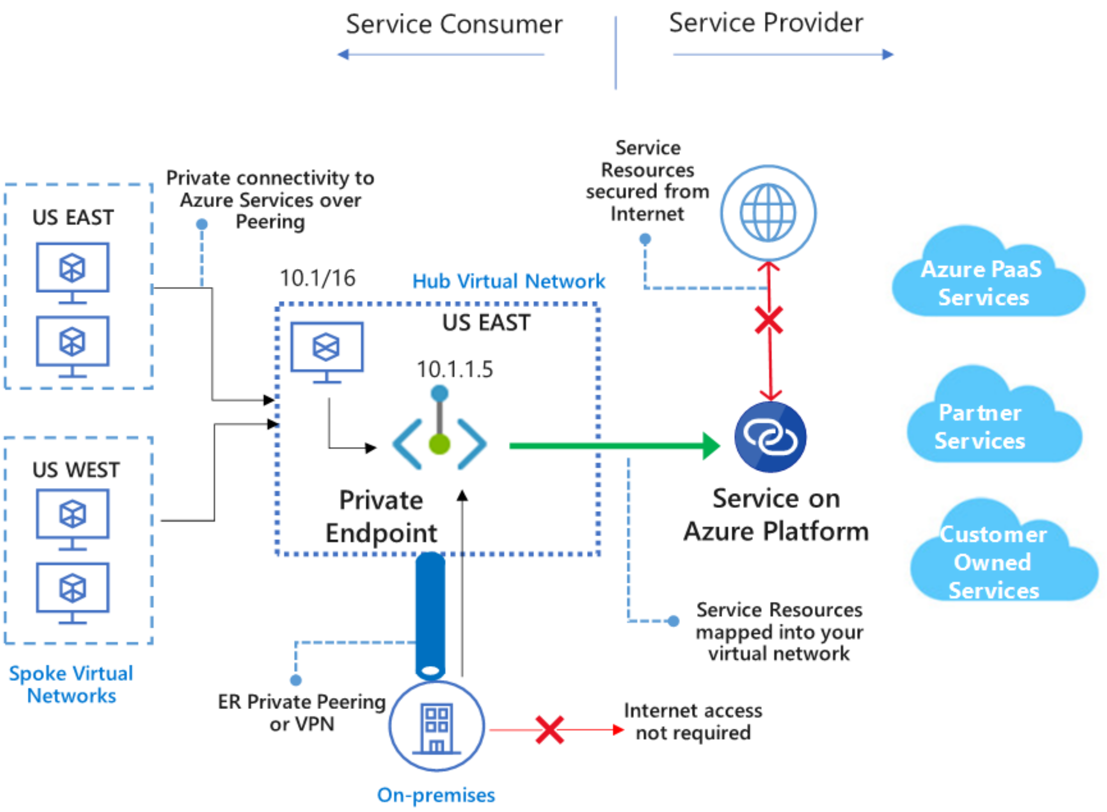
This section describes networking services in Azure that help protect your network resources - Protect your applications using any or a combination of these networking services in Azure - DDoS protection, Private Link, Firewall, Web Application Firewall, Network Security Groups, and Virtual Network Service Endpoints.

DDoS Protection

Azure DDoS Protection provides countermeasures against the most sophisticated DDoS threats.

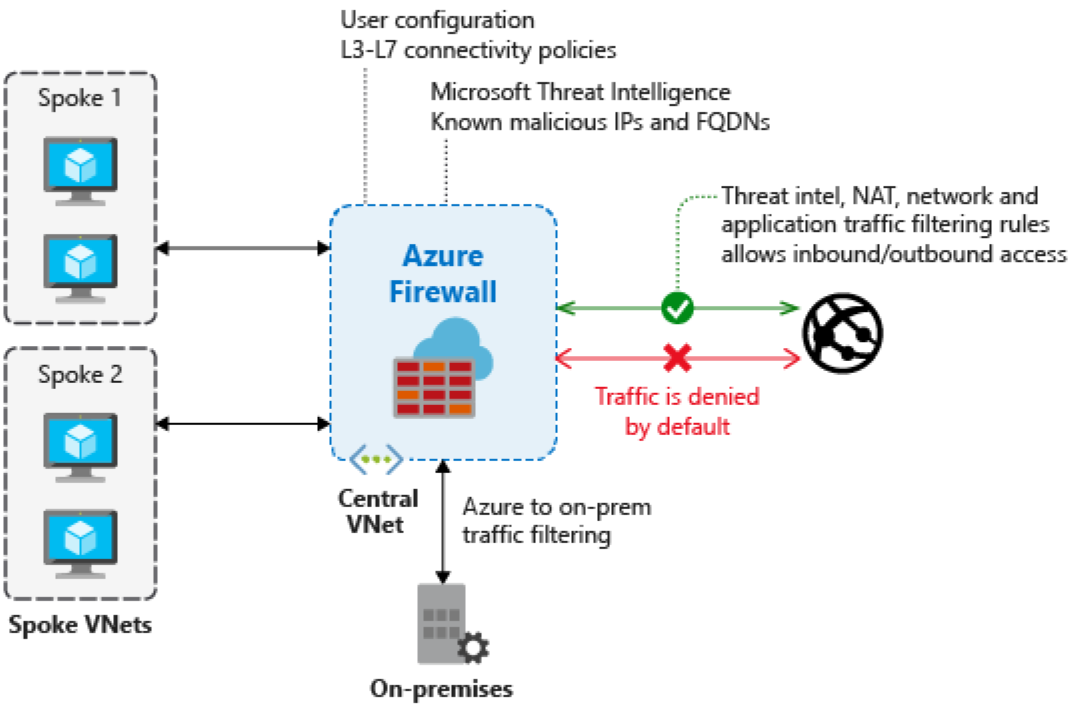
Azure Private Link

Azure Private Link enables you to access Azure PaaS Services (for example, Azure Storage and SQL Database) and Azure hosted customer-owned/partner services over a private endpoint in your virtual network. Traffic between your virtual network and the service travels through the Microsoft backbone network. Exposing your service to the public internet is no longer necessary. You can create your own private link service in your virtual network and deliver it to your customers.


Service Consumer
Service Provider
US EAST
Private connectivity to Azure Services over Peering
Service Resources secured from Internet
Azure PaaS Services
10.1/16
Hub Virtual Network
US EAST
10.1.1.5
Partner Services
US WEST
Private Endpoint
Service on Azure Platform
Customer Owned Services
Service Resources mapped into your virtual network
Spoke Virtual Networks
ER Private Peering or VPN
Internet access not required
On-premises

Azure Firewall

Azure Firewall is a managed, cloud-based network security service that protects your Azure Virtual Network resources. Using Azure Firewall, you can centrally create, enforce, and log application and network connectivity policies across subscriptions and virtual networks. Azure Firewall uses a static public IP address for your virtual network resources allowing outside firewalls to identify traffic originating from your virtual network.


User configuration
L3-L7 connectivity policies
Microsoft Threat Intelligence
Known malicious IPs and FQDNs
Spoke 1
Spoke 2
Spoke VNets
Azure Firewall
Threat intel, NAT, network and application traffic filtering rules allows inbound/outbound access
Traffic is denied by default
Central VNet
Azure to on-prem traffic filtering
On-premises

Web Application Firewall

Azure Web Application Firewall (WAF) provides protection to your web applications from common web exploits and vulnerabilities such as SQL injection, and cross site scripting.

Network security groups

You can filter network traffic to and from Azure resources in an Azure virtual network with a network security group.

Service endpoints

Virtual Network (VNet) service endpoints extend your virtual network private address space and the identity of your VNet to the Azure services, over a direct connection. Endpoints allow you to secure your critical Azure service resources to only your virtual networks. Traffic from your VNet to the Azure service always remains on the Microsoft Azure backbone network.

Application delivery services

This section describes networking services in Azure that help deliver applications - Content Delivery Network, Azure Front Door Service, Traffic Manager, Load Balancer, and Application Gateway.

Content Delivery Network

Azure Content Delivery Network (CDN) offers developers a global solution for rapidly delivering high-bandwidth content to users by caching their content at strategically placed physical nodes across the world.

Azure Front Door Service

Azure Front Door Service enables you to define, manage, and monitor the global routing for your web traffic by optimizing for best performance and instant global failover for high availability. With Front Door, you can transform your global (multi-region) consumer and enterprise applications into robust, high-performance personalized modern applications, APIs, and content that reach a global audience with Azure.

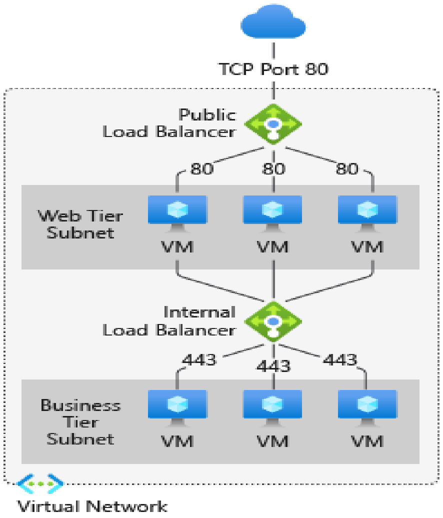
Traffic Manager

Azure Traffic Manager is a DNS-based traffic load balancer that enables you to distribute traffic optimally to services across global Azure regions, while providing high availability and responsiveness. Traffic Manager provides a range of traffic-routing methods to distribute traffic such as priority, weighted, performance, geographic, multi-value, or subnet.

Load Balancer

The Azure Load Balancer provides high-performance, low-latency Layer 4 load-balancing for all UDP and TCP protocols. It manages inbound and outbound connections. You can configure public and internal load-balanced endpoints. You can define rules to map inbound connections to back-end pool destinations by using TCP and HTTP health-probing options to manage service availability.

Azure Load Balancer is available in Standard, Regional, and Gateway SKUs.The following picture shows an Internet-facing multi-tier application that utilizes both external and internal load balancers:



Network monitoring services

This section describes networking services in Azure that help monitor your network resources - Network Watcher, Azure Monitor Network Insights, Azure Monitor, ExpressRoute Monitor, and Virtual Network TAP.

Network Watcher

Azure Network Watcher provides tools to monitor, diagnose, view metrics, and enable or disable logs for resources in an Azure virtual network.

Azure Monitor Network Insights

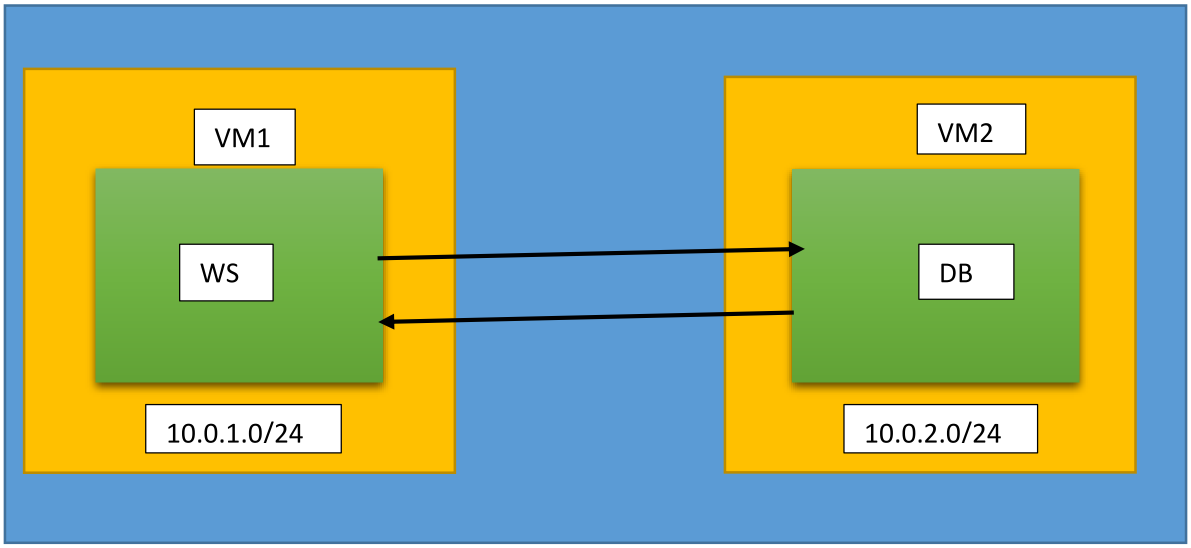
Azure Monitor for Networks provides a comprehensive view of health and metrics for all deployed network resources, without requiring any configuration. It also provides access to network monitoring capabilities like Connection Monitor, flow logging for network security groups, and Traffic Analytics.

Azure Monitor

Azure Monitor maximizes the availability and performance of your applications by delivering a comprehensive solution for collecting, analyzing, and acting on telemetry from your cloud and on-premises environments. It helps you understand how your applications are performing and proactively identifies issues affecting them and the resources they depend on.

Communicate two virtual machines

VNET 10.0.0.0/16



PRACTICAL

How to Create a virtual network

1. Select **Create a resource** in the upper left-hand corner of the portal.
2. In the search box, enter **Virtual Network**. Select **Virtual Network** in the search results.
3. In the **Virtual Network** page, select **Create**.
4. In **Create virtual network**, enter or select this information in the **Basics** tab:

Setting	**Value**
Project details	
Subscription	Select your subscription.
Resource group	Select **Create new**. Enter **myResourceGroup**. Select **OK**.
Instance details	
Name	Enter **myVNet**.
Region	Select **(US) Central US**.

5. Select the **IP Addresses** tab, or select the **Next: IP Addresses** button at the bottom of the page
6. In **IPv4 address space**, select the default address space or change it to **10.0.0.0/16**.
7. Select **+ Add subnet**, then enter **webserver** for **Subnet name** and **10.0.1.0/24** for **Subnet address range**.
8. Select **Add**
9. Select **+ Add subnet**, then enter **database** for **Subnet name** and **10.0.2.0/24** for **Subnet address range**.
10. Select **Add**.
11. Select the **Review + create** tab or select the **Review + create** button.
12. Select **Create**.

How to Create virtual machines

Create two VMs in the virtual network.

Create the first Virtual machine

1. On the upper-left side of the portal, select **Create a resource** > **Compute** > **Virtual machine**.
2. In **Create a virtual machine**, type or select the values in the **Basics** tab:

Setting	**Value**
Project Details	
Subscription	Select your Azure subscription
Resource Group	Select **myResourceGroup**
Instance details	
Virtual machine name	Enter **myVM1**
Region	Select **(US) CentralUS**
Availability Options	Select **No infrastructure redundancy required**
Image	Select **Windows 10 Pro,version 21H2 – Gen2**
Size	Choose VM size or take default setting
Administrator account	
Username	Enter a username
Password	Enter a password
Confirm password	Reenter password
Inbound port rules	
Public inbound ports	Select allow selected ports
Select inbound ports	RDP(3389)
Click licensing check box	

3. select **Next: Disks** select un check in **Delete with VM**, then **Next: Networking**.
4. In the Networking tab, select or enter:

Setting	**Value**
Network interface	
Virtual network	default
Subnet	Select **webserver**
Public IP	default
NIC network security group	Select **Basic**
Public inbound ports network	Select **Allow selected ports**
Delete NIC when VM is deleted	Click on checkbox

5. Select the **Management Tab**, then in **Boot Diagnostics** select **Disable**

6. Select the **Review + create** tab, or select the blue **Review + create** button at the bottom of the page.
7. Review the settings, and then select **Create**.

Create the second Virtual machine

1. On the upper-left side of the portal, select **Create a resource** > **Compute** > **Virtual machine**.
2. In **Create a virtual machine**, type or select the values in the **Basics** tab:

Setting	**Value**
Project Details	
Subscription	Select your Azure subscription
Resource Group	Select **myResourceGroup**
Instance details	
Virtual machine name	Enter **myVM2**
Region	Select **(US) CentralUS**
Availability Options	Select **No infrastructure redundancy required**
Image	Select **Windows 10 Pro,version 21H2 – Gen2**
Size	Choose VM size or take default setting
Administrator account	
Username	Enter a username
Password	Enter a password
Confirm password	Reenter password
Inbound port rules	
Public inbound ports	Select **Allow selected ports**
Select inbound ports	**RDP(3389)**
Click licensing check box	

3. Select **Next: Disks** select un check in **Delete with VM**, then **Next: Networking**.

4. In the Networking tab, select or enter:

Setting	**Value**
Network interface	
Virtual network	default
Subnet	Select **Database**
Public IP	default
NIC network security group	Select **Basic**
Public inbound ports network	Select **Allow selected ports**
Delete NIC when VM is deleted	Click on checkbox

5. Select the **Management Tab**,then in **Boot Diagnostics** select **Disable**
6. Select the **Review + create** tab, or select the blue **Review + create** button at the bottom of the page
7. Review the settings, and then select **Create**.

Connecting between two virtual machines.

1. Go to dashboard then select **myVM1**
2. In the VM menu bar, select **Connect**, then select **RDP**.
3. Click on **Download RDP file**
4. In that page, enter the username and password you created for the virtual machine previously.
5. Select **Connect** then virtual machine **myVM1 window** will be opened.
6. Go to control panel **Turn off** the **windows Defender Firewall.**
7. Go to dashboard then select **myVM2**
8. In the VM menu bar, select **Connect**, then select **RDP**.
9. Click on **Download RDP file**
10. In that page, enter the username and password you created for the virtual machine previously.
11. Select **Connect** then virtual machine **myVM2** window will be opened.
12. Go to control panel **Turn off** the **windows Defender Firewall.**
13. Open command prompt enter **ping myVM2 Private IPaddres.**

You'll receive a successful reply message like this:

```
C:\Users\myVM1> ping 10.0.2.4

Reply from 10.0.2.4: bytes=32 time=1ms TTL=128
Reply from 10.0.2.4: bytes=32 time=1ms TTL=128
Reply from 10.0.2.4: bytes=32 time=1ms TTL=128
Reply from 10.0.2.4: bytes=32 time=1ms TTL=128

Ping statistics for 10.0.2.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

14. Open virtual machine2 window Open command prompt
15. Enter **ping myVM2 Private IP address.**

You'll receive a successful reply message like this:

```
 C:\Users\myVM2> ping 10.0.1.4
Reply from 10.0.1.4: bytes=32 time=1ms TTL=128
Reply from 10.0.1.4: bytes=32 time=1ms TTL=128
Reply from 10.0.1.4: bytes=32 time=1ms TTL=128
Reply from 10.0.1.4: bytes=32 time=1ms TTL=128
```

```
Ping statistics for 10.0.1.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

Traffic Routing

Azure creates a route with an address prefix that corresponds to each address range defined within the address space of a virtual network. If the virtual network address space has multiple address ranges defined, Azure creates an individual route for each address range

Azure automatically creates a route table for each subnet within an Azure virtual network and adds system default routes to the table. Azure routes outbound traffic from a subnet based on the routes in a subnet's route table.

System routes

Azure automatically creates system routes and assigns the routes to each subnet in a virtual network. You can't create system routes, nor can you remove system routes, but you can override some system routes with custom routes. Azure creates default system routes for each subnet, and adds additional optional default routes to specific subnets, or every subnet, when you use specific Azure capabilities.

Each route contains an address prefix and next hop type. When traffic leaving a subnet is sent to an IP address within the address prefix of a route, the route that contains the prefix is the route Azure uses.

Azure automatically creates the following default system routes for each subnet within the virtual network:

Source	**Address prefixes**	**Next hop type**
Default	Unique to the virtual network	Virtual network
Default	0.0.0.0/0	Internet
Default	10.0.0.0/8	None
Default	192.168.0.0/16	None
Default	100.64.0.0/10	None

Network Interface

A network interface enables an Azure Virtual Machine to communicate with internet, Azure, and on-premises resources. When creating a virtual machine using the Azure portal, the portal creates one network interface with default settings for you.

VPN Gateway

VPN gateway is a specific type of virtual network gateway that is used to send encrypted traffic between an Azure virtual network and an on-premises location over the public Internet. You can also use a VPN gateway to send encrypted traffic between Azure virtual networks over the Microsoft network.

IP Address

An IP address is a unique address that identifies a device on the internet or a local network. IP stands for "Internet Protocol," which is the set of rules governing the format of data sent via the internet or local network.

Example of IPV4 Address

IPV4 Network address: it is a 32 bit address and represented in Decimal

10.0.0.0/24

Network 10.0.0.0

Subnet mask 255.255.255.0

Host (IP address range)

10.0.0.1 --- 10.0.0.254

10.0.0.1 first IP or Net ID

10.0.0.255 last IP or Broadcast ID

32-24 =8

Formula 2^N-2

2^8-2= 254

Class	Range
A	0-126
B	128-191
C	192-223
D	224-239
E	240-255

PRACTICAL

How to configure network interface and assigning IP address

Create a virtual network

1. Select **Create a resource** in the upper left-hand corner of the portal.
2. In the search box, enter **Virtual Network**. Select **Virtual Network** in the search results.
3. In the **Virtual Network** page, select **Create**.
4. In **Create virtual network**, enter or select this information in the **Basics** tab:

Setting	Value
Project details	
Subscription	Select your subscription.
Resource group	Select **Create new**. Enter **RG1**. Select **OK**.
Instance details	
Name	Enter **VNet**.
Region	Select **(US) Central US**.

5. Select the **IP Addresses** tab, or select the **Next: IP Addresses** button at the bottom
6. In **IPv4 address space**, select the default address space or change it to **10.0.0.0/16**.
7. Select **default subnet**, or **Add subnet** then enter **webserver** for **Subnet name** and **10.0.1.0/24** for **Subnet address range**.
8. Select the **Review + create** tab then Select **Create**.

Create a Network Interface

1. Select **Create a resource** in the upper left-hand corner of the portal.
2. In the search box, enter **Network Interface**. Select **Network Interface** in the search results.

Setting	Value
Project details	
Subscription	Select your subscription.
Resource group	Select **RG1**

Instance details	
Network interface name	Select **VNetIN**
Region	Select **CentralUS**
Virtual network	Select **VNet**
Subnet	default
Private IP address assignment	Select **Dynamic**
NIC network security group	Select **None**

3. Select the **Review + create** tab then Select **Create**.
4. Go to **VNet** in that click on **IPconfigurations** then **enabled** the default IPaddress will be created.
5. To **Add ip address** dynamically then click **Add** and enter the Name **Ipconfig2**
6. Click ok.
7. To **Add ip address** statically then click **Add** and enter the Name **Ipconfig3.**

8. Select **static** mode in private IP address settings and enter the IP address as per range of **VNe**t IP address
9. Click ok then the IP address added successful.

VPN Peering

VPN means Virtual Private Network.it is securely connected from one location to another location through Tunnel.

Virtual network peering enables you to seamlessly connect two or more Virtual Networks in Azure. The virtual networks appear as one for connectivity purposes. The traffic between virtual machines in peered virtual networks uses the Microsoft backbone infrastructure. Like traffic between virtual machines in the same network, traffic is routed through Microsoft's private network only.

Azure supports the following types of peering:

- **Virtual network peering**: Connect virtual networks within the same Azure region.
- **Global virtual network peering**: Connecting virtual networks across Azure regions.

Benefits of using virtual network peering

- A low-latency, high-bandwidth connection between resources in different virtual networks.
- The ability for resources in one virtual network to communicate with resources in a different virtual network.
- The ability to transfer data between virtual networks across Azure subscriptions, Azure Active Directory tenants, deployment models, and Azure regions.
- The ability to peer virtual networks created through the Azure Resource Manager.

PRACTICAL FOR VPN PEERING AND VIRTUAL NETWORK GATEWAY

Connection of two VM's through VPN PEERING AND VPN GATEWAY

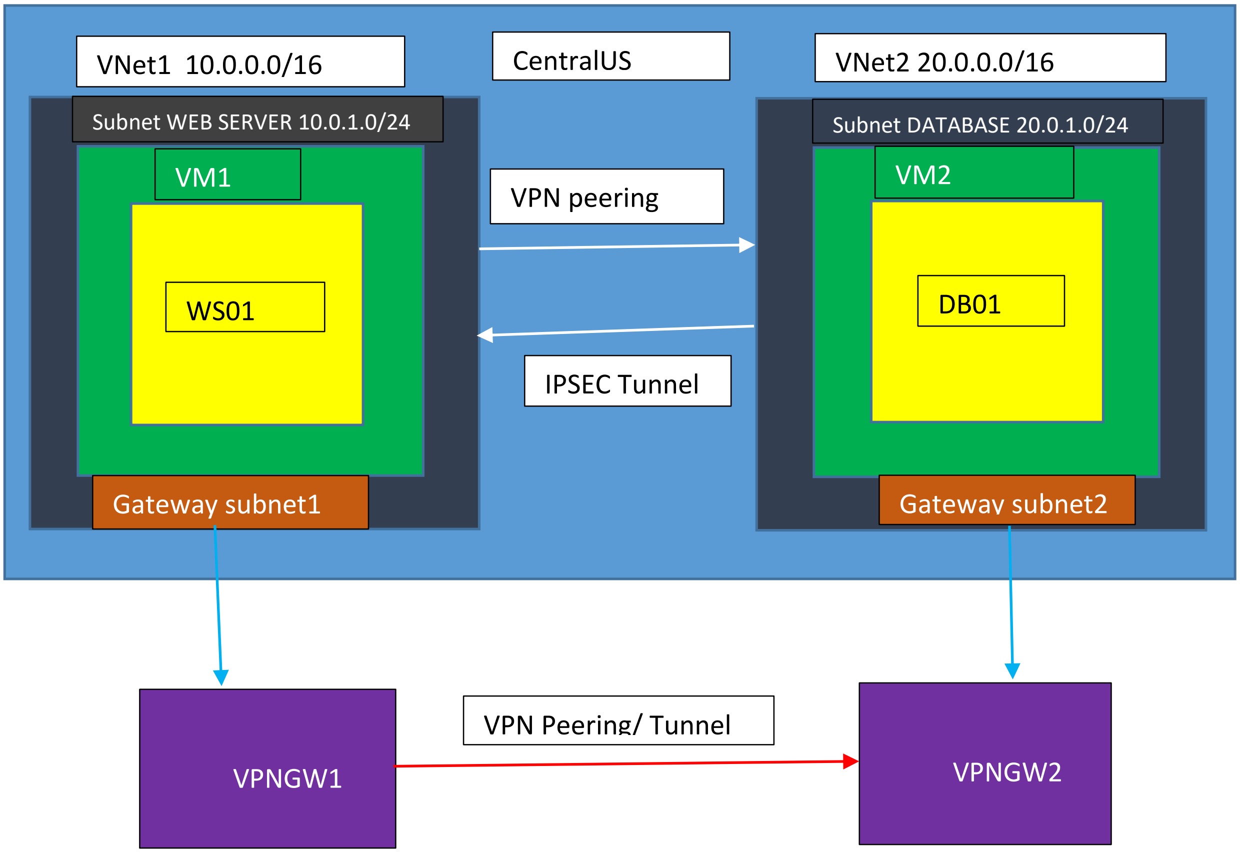


Diagram for connection of two VM's through VPN PEERING AND VPN GATEWAY

How to connect Virtual machines in same region

1.First create two virtual networks with different IP addresses

Create a virtual network 1

1. Select **Create a resource** in the upper left-hand corner of the portal.
2. In the search box, enter **Virtual Network**. Select **Virtual Network** in the search results.
3. In the **Virtual Network** page, select **Create**.
4. In **Create virtual network**, enter or select this information in the **Basics** tab:

Setting	Value
Project details	
Subscription	Select your subscription.
Resource group	Select **Create new**. Enter **RG1**. Select **OK**.
Instance details	
Name	Enter **VNet1**.
Region	Select **(US) Central US**.

5. Select the **IP Addresses** tab, or select the **Next: IP Addresses** button at the bottom of the page
6. In **IPv4 address space**, select the default address space or change it to **10.0.0.0/16**.
7. Select **+ Add subnet**, then enter **webserver** for **Subnet name** and **10.0.1.0/24** for **Subnet address range**.
8. Select **Add**.
9. Select the **Review + create** tab or select the **Review + create** button.
10. Select **Create**

Create a virtual network 2

1. Select **Create a resource** in the upper left-hand corner of the portal.
2. In the search box, enter **Virtual Network**. Select **Virtual Network** in the search results.
3. In the **Virtual Network** page, select **Create**.
4. In **Create virtual network**, enter or select this information in the **Basics** tab:

Setting	Value
Project details	
Subscription	Select your subscription.
Resource group	Select **Create new**. Enter **RG2**. Select **OK**.
Instance details	
Name	Enter **VNet2**.
Region	Select **(US) Central US**.

5. Select the **IP Addresses** tab, or select the **Next: IP Addresses** button at the bottom of the page
6. In **IPv4 address space**, select the address space change it to **20.0.0.0/16**.
7. Select **+ Add subnet**, then enter **database** for **Subnet name** and **20.0.1.0/24** for **Subnet address range**.
8. Select **Add**.
9. Select the **Review + create** tab or select the **Review + create** button.
10. Select **Create**

2.Create a virtual machines

Create the first Virtual machine

1. On the upper-left side of the portal, select **Create a resource** > **Compute** > **Virtual machine**.
2. In **Create a virtual machine**, type or select the values in the **Basics** tab:

Setting	**Value**
Project Details	
Subscription	Select your Azure subscription
Resource Group	Select **RG1**
Instance details	
Virtual machine name	Enter **myVM1**
Region	Select **(US) CentralUS**
Availability Options	Select **No infrastructure redundancy required**
Image	Select **Windows 10 Pro,version 21H2 – Gen2**
Size	Choose VM size or take default setting
Administrator account	
Username	Enter a username
Password	Enter a password
Confirm password	Reenter password
Inbound port rules	
Public inbound ports	Select allow selected ports
Select inbound ports	RDP(3389)
Click licensing check box	

3. select **Next: Disks** select un check in **Delete with VM**, then **Next: Networking**.
4. In the Networking tab, select or enter:

Setting	**Value**
Network interface	
Virtual network	Select **VNet1**
Subnet	Select **webserver**
Public IP	default
NIC network security group	Select **Basic**
Public inbound ports network	Select **Allow selected ports**
Delete NIC when VM is deleted	Click on checkbox

5. Select the **Management Tab**, then in **Boot Diagnostics** select **Disable**
6. Select the **Review + create** tab, or select the blue **Review + create** button at the bottom of the page.
7. Review the settings, and then select **Create**.

Create the second Virtual machine

1. On the upper-left side of the portal, select **Create a resource** > **Compute** > **Virtual machine**.
2. In **Create a virtual machine**, type or select the values in the **Basics** tab:

Setting	**Value**
Project Details	
Subscription	Select your Azure subscription
Resource Group	Select **RG2**
Instance details	
Virtual machine name	Enter **myVM2**
Region	Select **(US) CentralUS**
Availability Options	Select **No infrastructure redundancy required**
Image	Select **Windows 10 Pro,version 21H2 – Gen2**
Size	Choose VM size or take default setting
Administrator account	
Username	Enter a username
Password	Enter a password
Confirm password	Reenter password
Inbound port rules	
Public inbound ports	Select allow selected ports
Select inbound ports	RDP(3389)
Click licensing check box	

3. select **Next: Disks** select un check in **Delete with VM**, then **Next: Networking**.
4. In the Networking tab, select or enter:

Setting	**Value**
Network interface	
Virtual network	Select **VNet2**
Subnet	Select **database**
Public IP	default
NIC network security group	Select **Basic**
Public inbound ports network	Select **Allow selected ports**
Delete NIC when VM is deleted	Click on checkbox

5. Select the **Management Tab**, then in **Boot Diagnostics** select **Disable**
6. Select the **Review + create** tab, or select the blue **Review + create** button at the bottom of the page.
7. Review the settings, and then select **Create**.

3. To Add peering

1. Go to VNet1 then go to peerings.
2. Click on **+ Add**
3. Enter the **peer1** in first **peering link name.**
4. Enter the **peer2** in second **peering link name.**
5. Select virtual network **VNet2**
6. Click **add** then peering connected successful

Connecting between two virtual machines.

1. Go to dashboard then select **myVM1**
2. In the VM menu bar, select **Connect**, then select **RDP**
3. Click on **Download RDP file**
4. In that page, enter the username and password you created for the virtual machine previously.
5. Select **Connect** then virtual machine **myVM1 window** will be opened.
6. Go to control panel **Turn off** the **windows Defender Firewall.**
7. Go to dashboard then select **myVM2**
8. In the VM menu bar, select **Connect**, then select **RDP**.
9. Click on **Download RDP file**
10. In that page, enter the username and password you created for the virtual machine previously.
11. Select **Connect** then virtual machine **myVM2** window will be opened.
12. Go to control panel **Turn off** the **windows Defender Firewall.**
13. Open command prompt enter **ping myVM2 Private IP address.**

You'll receive a successful reply message like this:

```
C:\Users\myVM1> ping 10.0.2.4

Reply from 10.0.2.4: bytes=32 time=1ms TTL=128
Reply from 10.0.2.4: bytes=32 time=1ms TTL=128
Reply from 10.0.2.4: bytes=32 time=1ms TTL=128
Reply from 10.0.2.4: bytes=32 time=1ms TTL=128

Ping statistics for 10.0.2.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

14. Open virtual machine2 window Open command prompt
15. Enter **ping myVM2 Private IPaddress.**

You'll receive a successful reply message like this:

```
 C:\Users\myVM2> ping 10.0.1.4
Reply from 10.0.1.4: bytes=32 time=1ms TTL=128
Reply from 10.0.1.4: bytes=32 time=1ms TTL=128
Reply from 10.0.1.4: bytes=32 time=1ms TTL=128
Reply from 10.0.1.4: bytes=32 time=1ms TTL=128

Ping statistics for 10.0.1.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

How the virtual machines connected through gateway

1. Go to **VNet1** then go to **subnets.**
2. Click on **+ Add Gateway subnet**
3. Enter **IP address** in **subnet address range.**
4. Click **Save**
5. Follow the above process in **VNet2** also.

Create a virtual network gateway1

1. Go to **Home** in the upper left-hand corner of the portal.
2. In the search box, enter **Virtual Network gateway**. Select **Virtual Network gateway** in the search results.
3. In the **Virtual Network gateway** page, select **Create**.
4. In **Create virtual network gateway1**, enter or select this information in the **Basics** tab:

Setting	**Value**
Project details	
Subscription	Select your subscription.
Instance details	
Name	Enter **VPNGW1**.
Region	Select **(US) Central US**.
Gateway type	Select **VPN**
VPN Type	Select **Route based**
Generation	Select **Generation1**
Virtual network	Select **VNet1**
Public IP address	Enter **VPNGW1_IP**
Availability	Select **1**

5. Select the **Review + create** tab, or select the blue **Review + create** button at the bottom of the page.
6. Review the settings, and then select **Create**.

Create a virtual network gateway 2

1. Go to **Home** in the upper left-hand corner of the portal.
2. In the search box, enter **Virtual Network gateway**. Select **Virtual Network gateway** in the search results.
3. In the **Virtual Network gateway** page, select **Create**.
4. In **Create virtual network gateway2**, enter or select this information in the **Basics** tab:

Setting	Value
Project details	
Subscription	Select your subscription.
Instance details	
Name	Enter **VPNGW2**.
Region	Select **(US) Central US**.
Gateway type	Select **VPN**
VPN Type	Select **Route based**
Generation	Select **Generation1**
Virtual network	Select **VNet2**
Public IP address	Enter **VPNGW2_IP**
Availability	Select **1**

5. Select the **Review + create** tab, or select the blue **Review + create** button at the bottom of the page.
6. Review the settings, and then select **Create**.

How to Add connection

1. Go to **VPNGW1** then go to **connections**.
2. Click on **+ Add .**
3. Enter the **connection1** in **name.**
4. Select connection type **VNet to VNet.**
5. Select **VPNGW2** in second virtual network **gateway.**
6. Enter **123345** in shared key.
7. Click **ok .**
8. Follow the above same process simultaneously in **VPNGW2.**
9. It shows the status **connected.**
10. Go to virtual machine windows and pinging the private IP addresses.
11. You'll receive a successful reply message.

CLEAN UP ALL RESOURCES

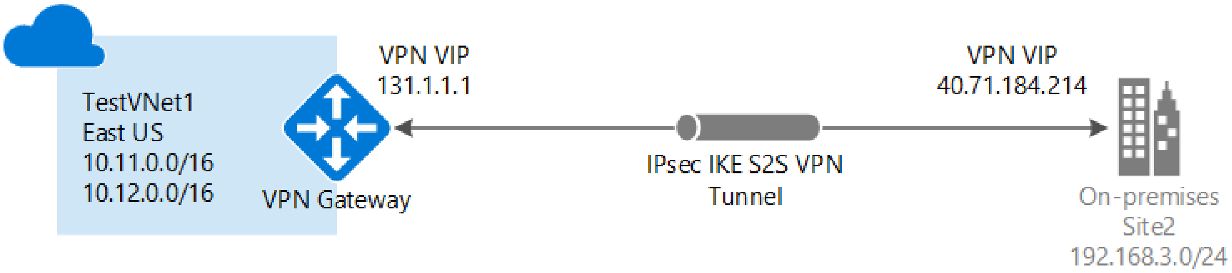
SITE –TO-SITE VPN CONNECTION

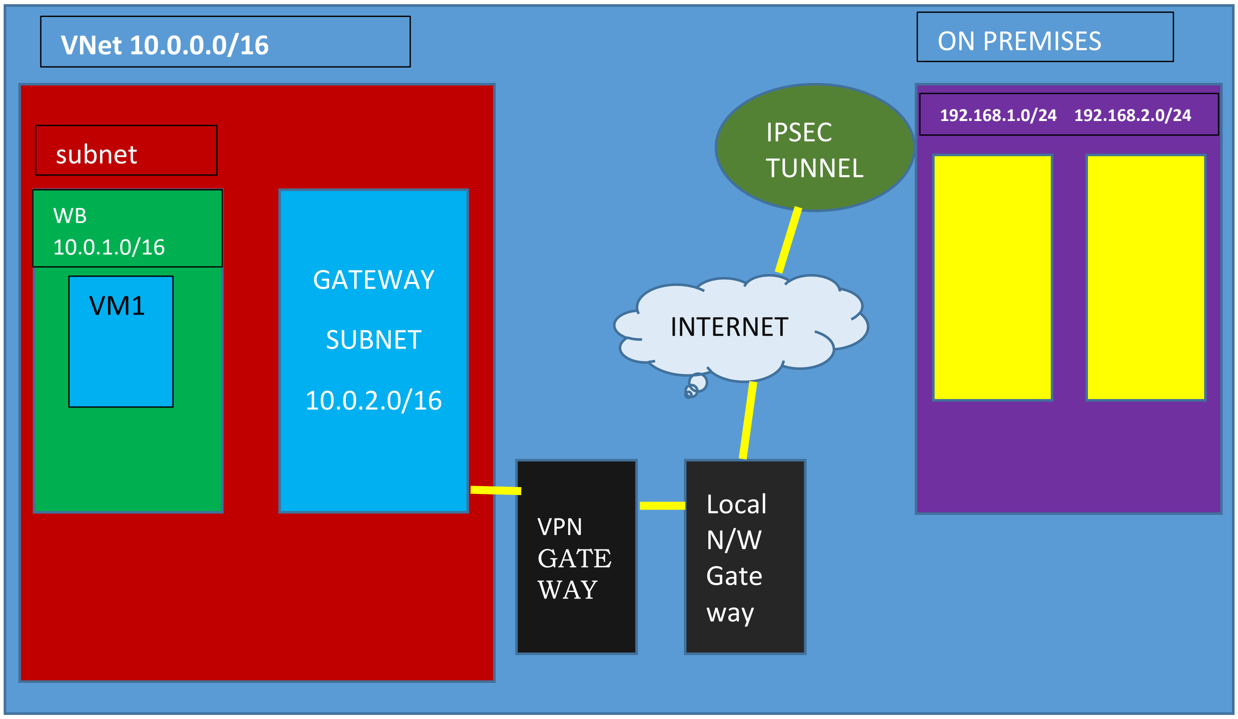
A site-to-site virtual private network (VPN) refers to a connection set up between multiple networks. A Site-to-Site VPN gateway connection is used to connect your on-premises network to an Azure virtual network over an IPsec/IKE (IKEv1 or IKEv2) VPN tunnel. This type of connection requires a VPN device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

It works by creating a "tunnel" between two networks. With a site-to-site VPN, these tunnels go from one location to another, and the only people who can see the data being transferred are users logged onto the network. The VPN uses gateways at each location, which encrypt all traffic that passes through.

Site-to-Site VPN configuration

A site-to-site Virtual Private Network (VPN) provides this by creating an encrypted link between VPN gateways located at each of these sites. A site-to-site VPN tunnel encrypts traffic at one end and sends it to the other site over the public Internet where it is decrypted and routed on to its destination.





Benefits of Site-to-Site VPN

1. **Watertight Internal Network**
   When a business utilizes a site-to-site VPN across its operations, they can expect a far more secure footing as far as their data is concerned.
2. **Operational efficiency**
   Because users don't have to have client apps installed on any of their devices, using a site-to-site offers ease-of-use opportunities for businesses.
3. **scalability**
   One of the biggest benefits of implementing a site-to-site VPN for an organization is its scalability.

PRACTICAL

Site-to-Site connection in azure portal

Create a virtual network

1. Select **Create a resource** in the upper left-hand corner of the portal.
2. In the search box, enter **Virtual Network**. Select **Virtual Network** in the search results.
3. In the **Virtual Network** page, select **Create**.
4. In **Create virtual network**, enter or select this information in the **Basics** tab:

Setting	**Value**
Project details	
Subscription	Select your subscription.
Resource group	Select **Create new**. Enter **RG1**. Select **OK**.
Instance details	
Name	Enter **VNet**.
Region	Select **(US) Central US**.

5. Select the **IP Addresses** tab, or select the **Next: IP Addresses** button at the bottom of the page
6. In **IPv4 address space**, select the default address space or change it to **10.0.0.0/16**.
7. Select **+ Add subnet**, then enter **webserver** for **Subnet name** and **10.0.1.0/24** for **Subnet address range**.
8. Select **Add**.
9. Select the **Review + create** tab or select the **Review + create** button.
10. Go to **VNet1** then go to **subnets.**
11. Click on **+ Add Gateway subnet**
12. Enter **IP address** in **subnet address range.**
13. Click **Save**

Create a Virtual machine

1. On the upper-left side of the portal, select **Create a resource** > **Compute** > **Virtual machine**.
2. In **Create a virtual machine**, type or select the values in the **Basics** tab:

Setting	**Value**
Project Details	
Subscription	Select your Azure subscription
Resource Group	Select **RG1**
Instance details	
Virtual machine name	Enter **myVM1**
Region	Select **(US) CentralUS**
Availability Options	Select **No infrastructure redundancy required**
Image	Select **Windows server 2016 Datacenter-Gen2**
Size	Choose VM size or take default setting
Administrator account	
Username	Enter a username
Password	Enter a password
Confirm password	Reenter password
Inbound port rules	
Public inbound ports	Select allow selected ports
Select inbound ports	RDP(3389)
Click licensing check box	

3. select **Next: Disks** select un check in **Delete with VM**, then **Next: Networking**.
4. In the Networking tab, select or enter:

Setting	**Value**
Network interface	
Virtual network	Select **VNet.**
Subnet	Select **webserver.**
Public IP	default
NIC network security group	Select **Basic**
Public inbound ports network	Select **Allow selected ports**
Delete NIC when VM is deleted	Click on checkbox

5. Select the **Management Tab**, then in **Boot Diagnostics** select **Disable**
6. Select the **Review + create** tab, or select the blue **Review + create** button at the bottom of the page.
7. Review the settings, and then select **Create**.

Create a virtual network gateway

1. Go to **Home** in the upper left-hand corner of the portal.
2. In the search box, enter **Virtual Network gateway**. Select **Virtual Network gateway** in the search results.
3. In the **Virtual Network gateway** page, select **Create**.
4. In **Create virtual network gateway1**, enter or select this information in the **Basics** tab:

Setting	**Value**
Project details	
Subscription	Select your subscription.
Instance details	
Name	Enter **VPNGW**.
Region	Select **(US) Central US**.
Gateway type	Select **VPN**
VPN Type	Select **Route based**
Generation	Select **Generation1**
Virtual network	Select **VNet**
Public IP address	Enter **VPNGW_IP**
Availability Zone	Select **1**

5. Select the **Review + create** tab, or select the blue **Review + create** button at the bottom of the page.
6. Review the settings, and then select **Create**.

Create a local network gateway

1. Go to **Home** in the upper left-hand corner of the portal.
2. In the search box, enter **Local Network gateway**. Select **Local Network gateway** in the search results.
3. In the **Local Network gateway** page, select **Create**.
4. In **Create Local network gateway**, enter or select this information in the **Basics** tab:

Setting	**Value**
Project details	
Subscription	Select your subscription.
Resource group	**RG1**
Instance details	
Name	Enter **VPNLNG**.
Region	Select **(US) Central US**.
End point	Select **IP address**
IP address	Enter the IP address of **myVM1**
Address space	**10.101.0.0/16**

5. Select the **Review + create** tab, or select the blue **Review + create** button at the bottom of the page.
6. Review the settings, and then select **Create**.

To Add connection

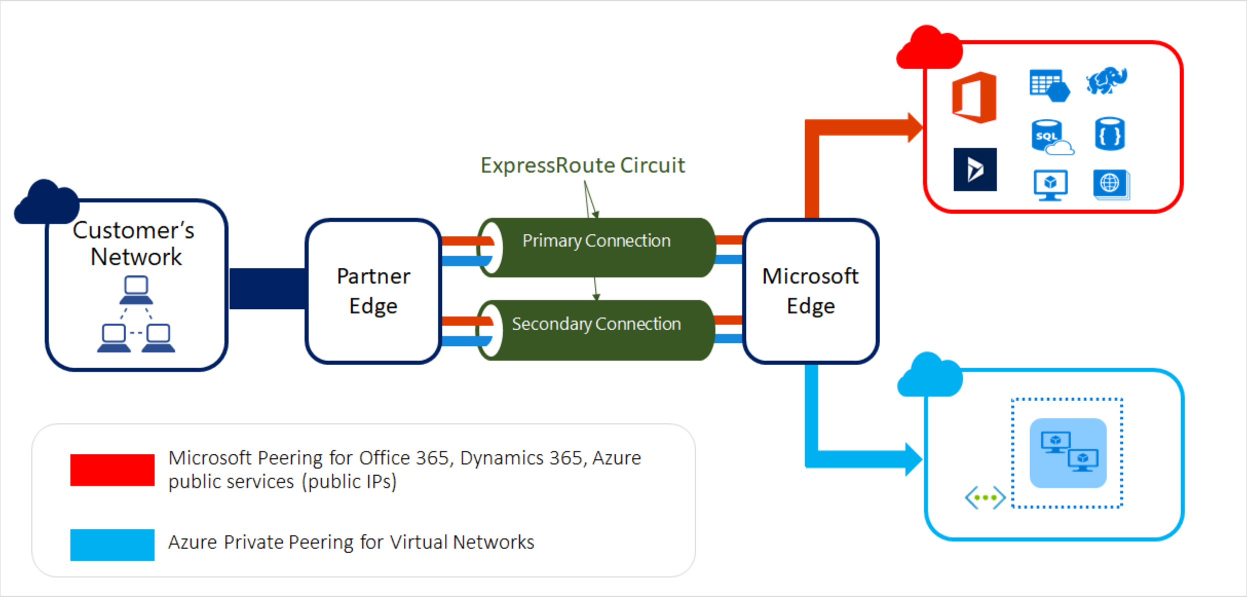
1. Go to **VPNGW** then go to **connections**.
2. Click on **+ Add .**
3. Enter the **site to site vpn** in **name.**
4. Select connection type **Site-to-site (IPSEC)**
5. Select **VPNLNG** in **Local network gateway.**
6. Enter **123345** in shared key.
7. Select **IKEv2** in **IKE protocol.**
8. Click **ok** then the connection will be created**.**
9. Go to dashboard then select **myVM1**
10. In the VM menu bar, select **Connect**, then select **RDP**
11. Click on **Download RDP file**
12. In that page, enter the username and password you created for the virtual machine previously.
13. Select **Connect** then virtual machine **myVM1 window** will be opened.
14. Go to control panel **Turn off** the **windows Defender Firewall.**
15. Go to **server manager** then go to **Add roles and features**.
16. Click **Next**. In **server roles** select **Remote access**.
17. Select **Direct access and VPN** and **Routing** in **server roles**.
18. Click **Add features** then click **Next**.
19. Click **Install**.
20. Go to **Dashboard** then go to **Tools.**
21. Click the **Routing and Remote access**. In that right click on **VNet** then click on **configure enable routing and remote access** then click on **Next.**
22. In **configuration** select **custom configuration** then click on **Next.**
23. In **custom configuration** select **VPN access and Dail up access** then click on **Next** and click on **Finish.**
24. Click on **VNet** then go to **Network interface** then right click on **Network interface** enter the **name** click on **Next.**
25. In **connection type** select **Connect using private virtual networking** then click on **Next**.
26. In **VPN type** select **IKEv2** then click on **Next**.
27. In **Destination address** enter the **virtual network gateway IP address** then click on **Next.**
28. In **protocols and security** select **Route IP packets** on this interface and click on **Nex**t then click on **finish** the network interface will be added.
29. Click on the **network interface** then go to **security** enter the **shared key** in the bottom of the tab.
30. Go to **virtual network gateway** then **Refresh it** then it will be connected.

CLEAN UP ALL RESOURCES

EXPRESS ROUTE

Express Route lets you extend your on-premises networks into the Microsoft cloud over a private connection with the help of a connectivity provider. With Express Route, you can establish connections to Microsoft cloud services, such as Microsoft Azure and Microsoft 365.

Connectivity can be from any-to-any (IP VPN) network, a point-to-point Ethernet network, or a virtual cross-connection through a connectivity provider at a colocation facility. Express Route connections don't go over the public Internet. This allows Express Route connections to offer more reliability, faster speeds, consistent latencies, and higher security than typical connections over the Internet. For information on how to connect your network to Microsoft using Express Route


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

Benefits of Express Route

- Layer 3 connectivity between your on-premises network and the Microsoft Cloud through a connectivity provider. Connectivity can be from any-to-any (IPVPN) network, a point-to-point Ethernet connection, or through a virtual cross-connection via an Ethernet exchange.
- Connectivity to Microsoft cloud services across all regions in the geopolitical region.
- Global connectivity to Microsoft services across all regions with the Express Route premium add-on.
- Dynamic routing between your network and Microsoft via BGP.
- Built-in redundancy in every peering location for higher reliability.

How to create Express Route

Create a virtual network

1. Select **Create a resource** in the upper left-hand corner of the portal.
2. In the search box, enter **Express Route**. Select **Express Route** in the search results.
3. In the **Express Route** page, select **Create**.
4. In **Express Route**, enter or select this information in the **Basics** tab:

Setting	Value
Project details	
Subscription	Select your subscription.
Resource group	Select **Create new**. Enter **RG1**. Select **OK**.
Instance details	
Name	Enter **Express Route**.
Region	Select **(US) Central US**.

5. Select the **Configuration** tab, or select the **Next: Configuration** button at the bottom of the page

Instance details	
Name	Enter **Express Route**.
Region	Select **(US) Central US**.
Provider	Select **Airtel**
Peering location	Select **Mumbai**
Bandwidth	Select **10gbps**
SKU	Select **Standard**
Billing model	Select **Metered**
Allow classic operations	Select **NO**

6. Select the **Review + create** tab or select the **Review + create** button.
7. Select **create.**

CLEAN UP ALL RESOURCES

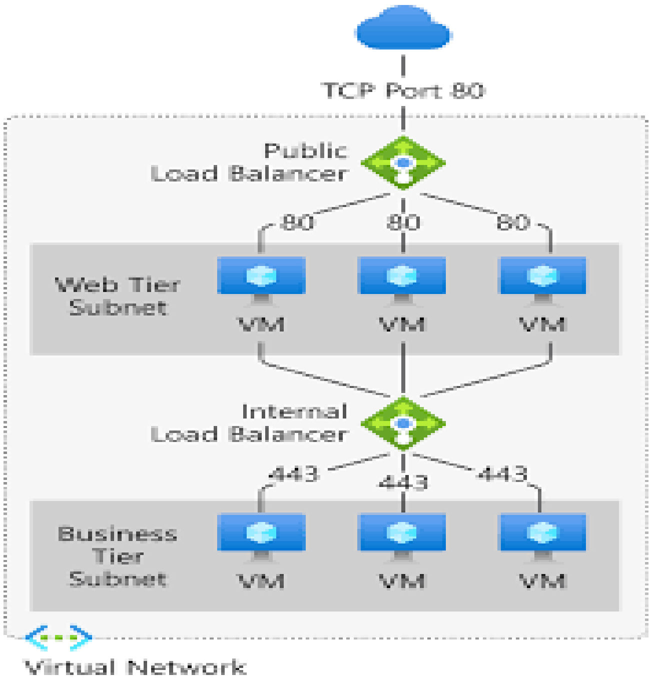
LOAD BALANCER

Load balancing refers to evenly distributing load (incoming network traffic) across a group of backend resources or servers.

Azure Load Balancer operates at layer 4 of the Open Systems Interconnection (OSI) model. It's the single point of contact for clients. Load balancer distributes inbound flows that arrive at the load balancer's front end to backend pool instances. These flows are according to configured load-balancing rules and health probes. The backend pool instances can be Azure Virtual Machines or instances in a virtual machine scale set.

A **public load balancer** can provide outbound connections for virtual machines (VMs) inside your virtual network. These connections are accomplished by translating their private IP addresses to public IP addresses. Public Load Balancers are used to load balance internet traffic to your VMs.

An **internal (or private) load balancer** is used where private IPs are needed at the frontend only. Internal load balancers are used to load balance traffic inside a virtual network. A load balancer frontend can be accessed from an on-premises network in a hybrid scenario.



.

USES OF LOAD BALANCER

- Load balance **internal** and **external** traffic to Azure virtual machines.
- Increase availability by distributing resources **within** and **across** zones.
- Configure **outbound connectivity** for Azure virtual machines.
- Use **health probes** to monitor load-balanced resources.
- Employ **port forwarding** to access virtual machines in a virtual network by public IP address and port.
- Enable support for **load-balancing** of **IPv6**.
- Standard load balancer provides multi-dimensional metrics through Azure Monitor. These metrics can be filtered, grouped, and broken out for a given dimension. They provide current and historic insights into performance and health of your service. Insights for Azure Load Balancer offers a preconfigured dashboard with useful visualizations for these metrics. Resource Health is also supported.
- Load balance services on **multiple ports, multiple IP addresses, or both**.
- Move **internal** and **external** load balancer resources across Azure regions.
- Load balance TCP and UDP flow on all ports simultaneously using **HA ports**.

Secure by default

- Standard load balancer is built on the zero trust network security model.
- Standard Load Balancer is secure by default and part of your virtual network. The virtual network is a private and isolated network.
- Standard load balancers and standard public IP addresses are closed to inbound connections unless opened by Network Security Groups. NSGs are used to explicitly permit allowed traffic. If you don't have an NSG on a subnet or NIC of your virtual machine resource, traffic isn't allowed to reach this resource.
- Basic load balancer is open to the internet by default.
- Load balancer doesn't store customer data.

PRACTICAL

How the Load Balancer work in azure portal

1.First create virtual networks

Create a virtual network

1. In the search box at the top of the portal, enter **Virtual network**. Select **Virtual Networks** in the search results.
2. In **Virtual networks**, select **+ Create**.
3. In **Create virtual network**, enter or select the following information in the **Basics** tab:

Setting	**Value**
Project Details	
Subscription	Select your Azure subscription

Setting	Value
Resource Group	Select **Create new**. In **Name** enter **CreatePubLBQS-rg**. Select **OK**.
Instance details	
Name	Enter **myVNet**
Region	Select **CentralUS**

4. Select the **IP Addresses** tab or select **Next: IP Addresses** at the bottom of the page.
5. In the **IP Addresses** tab, enter this information:

Setting	Value
IPv4 address space	Enter **10.1.0.0/16**

6. Under **Subnet name**, select the word **default**. If a subnet isn't present, select **+ Add subnet**.
7. In **Edit subnet**, enter this information:

Setting	Value
Subnet name	Enter **myBackendSubnet**
Subnet address range	Enter **10.1.0.0/24**

8. Select **Save** or **Add**.
9. Select the **Security** tab.
10. Under **BastionHost**, select **Enable**. Enter this information:

Setting	value
Bastion name	Enter **myBastionHost.**
AzureBastionSubnet address	Enter **10.1.1.0/27**
Public IP Address	Select **CreateNew.** Enter **myBastionIP.** Select **OK.**

11. Select the **Review + create** tab or select the **Review + create** button.
12. Select **Create**.

Create Load Balancer

1. In the search box at the top of the portal, enter **Load balancer**. Select **Load balancers** in the search results.
2. In the **Load balancer** page, select **+ Create**.
3. In the **Basics** tab of the **Create load balancer** page, enter or select the following information:

Setting	Value
Project details	
Subscription	Select your subscription.

Setting	**Value**
Resource group	Select **CreatePubLBQS-rg**.
Instance details	
Name	Enter **myLoadBalancer**
Region	Select **CenralUS**.
SKU	Leave the default **Standard**.
Type	Select **Public**.
Tier	Leave the default **Regional**.

4. Select **Next: Frontend IP configuration** at the bottom of the page.
5. In **Frontend IP configuration**, select **+ Add a frontend IP configuration**.
6. Enter **myFrontend** in **Name**.
7. Select **IPv4** or **IPv6** for the **IP version**.
8. Select **IP address** for the **IP type**
9. Select **Create new** in **Public IP address**.
10. In **Add a public IP address**, enter **myPublicIP** for **Name**.
11. Select **Zone-redundant** in **Availability zone**
12. Leave the default of **Microsoft Network** for **Routing preference**.
13. Select **OK**.
14. Select **Add**.
15. Select **Next: Backend pools** at the bottom of the page.
16. In the **Backend pools** tab, select **+ Add a backend pool**.
17. Enter **myBackendPool** for **Name** in **Add backend pool**.
18. Select **myVNet** in **Virtual network**.
19. Select **NIC** or **IP Address** for **Backend Pool Configuration**.
20. Select **IPv4** or **IPv6** for **IP version**.
21. Select **Add**.
22. Select **Next: Inbound rules** at the bottom of the page.
23. In **Load balancing rule** in the **Inbound rules** tab, select **+ Add a load balancing rule**.
24. In **Add load balancing rule**, enter or select the following information:

Setting	**value**
Name	Enter **myHTTPRule**
IP Version	Select **IPv4** or **IPv6** depending on your requirements.
Frontend IP address	Select **myFrontend**.
Backend pool	Select **myBackendPool**.
Protocol	Select **TCP**.
Port	Enter **80**.
Backend port	Enter **80**.
Health probe	Select **Create new**. In **Name**, enter **myHealthProbe**. Select **TCP** in **Protocol**. Leave the rest of the defaults, and select **OK**.
Session persistence	Select **None**.

Setting	value
Idle timeout (minutes)	Enter or select **15**.
TCP reset	Select **Enabled**.
Floating IP	Select **Disabled**.
Outbound source network address translation (SNAT)	Leave the default of **(Recommended) Use outbound rules to provide backend pool members access to the internet.**

25. Select **Add**.
26. Select the blue **Review + create** button at the bottom of the page.
27. Select **Create**.

Create NAT gateway

1. In the search box at the top of the portal, enter **NAT gateway**. Select **NAT gateways** in the search results.
2. In **NAT gateways**, select **+ Create**.
3. In **Create network address translation (NAT) gateway**, enter or select the following information:

Setting	Value
Project details	
Subscription	Select your subscription.
Resource group	Select **CreatePubLBQS-rg**.
Instance details	
NAT gateway name	Enter **myNATgateway**.
Region	Select **CentralUS**.
Availability zone	Select **None**.
Idle timeout (minutes)	Enter **15**.

4. Select the **Outbound IP** tab or select **Next: Outbound IP** at the bottom of the page.
5. In **Outbound IP**, select **Create a new public IP address** next to **Public IP addresses**.
6. Enter **myNATgatewayIP** in **Name**.
7. Select **OK**.
8. Select the **Subnet** tab or select the **Next: Subnet** button at the bottom of the page.
9. In **Virtual network** in the **Subnet** tab, select **myVNet**.
10. Select **myBackendSubnet** under **Subnet name**.
11. Select the blue **Review + create** button at the bottom of the page, or select the **Review + create** tab.
12. Select **Create**.

Create a virtual machines in different zones

Create a virtual machine 1

1. In the search box at the top of the portal, enter **Virtual machine**. Select **Virtual machines** in the search results.
2. In **Virtual machines**, select **+ Create** > **Virtual machine**.
3. In **Create a virtual machine**, enter or select the following values in the **Basics** tab:

Setting	**Value**
Project Details	
Subscription	Select your Azure subscription
Resource Group	Select **CreatePubLBQS-rg**
Instance details	
Virtual machine name	Enter **myVM1**
Region	Select **CentralUS**
Availability Options	Select **Availability zones**
Availability zone	Select **Zone 1**
Security type	Select **Standard**.
Image	Select **Windows Server 2022 Datacenter: Azure Edition - Gen2**
Azure Spot instance	Leave the default of unchecked.
Size	Choose VM size or take default setting
Administrator account	
Username	Enter a username
Password	Enter a password
Confirm password	Reenter password
Inbound port rules	
Public inbound ports	Select **None**

4. Select the **Networking** tab, or select **Next: Disks**, then **Next: Networking**.
5. In the Networking tab, select or enter the following information:

Setting	**Value**
Network interface	
Virtual network	Select **myVNet**
Subnet	Select **myBackendSubnet**
Public IP	Select **None**.
NIC network security group	Select **Advanced**
Configure network security group	Select **Create new**. In the **Create network security group**, enter **myNSG** in Name. Under **Inbound rules**, select **+Add** an inbound rule. Under **Service**, select **HTTP**. Under **Priority**, enter **100.**

Setting	**Value**
	In Name, enter **myNSGRule** Select **Add** Select **OK**
Delete NIC when VM is deleted	Leave the default of **unselected**.
Accelerated networking	Leave the default of **selected**.
Load balancing	
Place this virtual machine behind an existing load-balancing solution?	Select the check box.
Load balancing settings	
Load-balancing options	Select **Azure load balancer**
Select a load balancer	Select **myLoadBalancer**
Select a backend pool	Select **myBackendPool**

6. Select **Review + create**.
7. Review the settings, and then select **Create**.

Create a virtual machine 2

1. In the search box at the top of the portal, enter **Virtual machine**. Select **Virtual machines** in the search results.
2. In **Virtual machines**, select **+ Create** > **Virtual machine**.
3. In **Create a virtual machine**, enter or select the following values in the **Basics** tab:

Setting	**Value**
Project Details	
Subscription	Select your Azure subscription
Resource Group	Select **CreatePubLBQS-rg**
Instance details	
Virtual machine name	Enter **myVM2**
Region	Select **CentralUS**
Availability Options	Select **Availability zones**
Availability zone	Select **Zone 2**
Security type	Select **Standard**.
Image	Select **Windows Server 2022 Datacenter: Azure Edition - Gen2**
Azure Spot instance	Leave the default of unchecked.
Size	Choose VM size or take default setting
Administrator account	
Username	Enter a username
Password	Enter a password
Confirm password	Reenter password
Inbound port rules	
Public inbound ports	Select **None**

4. Select the **Networking** tab, or select **Next: Disks**, then **Next: Networking**.

5. In the Networking tab, select or enter the following information:

Setting	Value
Network interface	
Virtual network	Select **myVNet**
Subnet	Select **myBackendSubnet**
Public IP	Select **None**.
NIC network security group	Select **Advanced**
Configure network security group	Select **myNSG**
Delete NIC when VM is deleted	Leave the default of **unselected**.
Accelerated networking	Leave the default of **selected**.
Load balancing	
Place this virtual machine behind an existing load-balancing solution?	Select the check box.
Load balancing settings	
Load-balancing options	Select **Azure load balancer**
Select a load balancer	Select **myLoadBalancer**
Select a backend pool	Select **myBackendPool**

6. Select **Review + create**.
7. Review the settings, and then select **Create.**

Install IIS

1. In the search box at the top of the portal, enter **Virtual machine**. Select **Virtual machines** in the search results.
2. Select **myVM1**.
3. On the **Overview** page, select **Connect**, then **Bastion**.
4. Enter the username and password entered during VM creation.
5. Select **Connect**.
6. In the PowerShell Window, run the following commands to:
    1. Install the IIS server
    2. Remove the default iisstart.htm file
    3. Add a new iisstart.htm file that displays the name of the VM:

PowerShellCopy

```
 # Install IIS server role
 Install-WindowsFeature -name Web-Server -IncludeManagementTools

 # Remove default htm file
 Remove-Item  C:\inetpub\wwwroot\iisstart.htm

 # Add a new htm file that displays server name
 Add-Content  -Path  "C:\inetpub\wwwroot\iisstart.htm"  -Value  $("Hello  World
from " + $env:computername)
```

7. Close the Bastion session with **myVM1**.
8. Repeat steps 1 to 8 to install IIS and the updated iisstart.htm file on **myVM2**.

Test the load balancer

1. In the search box at the top of the page, enter **Public IP**. Select **Public IP addresses** in the search results.
2. In **Public IP addresses**, select **myPublicIP**.
3. Copy the item in **IP address**. Paste the public IP into the address bar of your browser. The custom VM page of the IIS Web server is displayed in the browser.

CLEAN UP ALL RESOURCES

TRAFFIC MANAGER

Azure Traffic Manager is a DNS-based traffic load balancer. This service allows you to distribute traffic to your public facing applications across the global Azure regions. Traffic Manager also provides your public endpoints with high availability and quick responsiveness.

Traffic Manager uses DNS to direct the client requests to the appropriate service endpoint based on a traffic-routing method. Traffic manager also provides health monitoring for every endpoint. The endpoint can be any Internet-facing service hosted inside or outside of Azure. Traffic Manager provides a range of traffic-routing methods and endpoint monitoring options to suit different application needs and automatic failover models. Traffic Manager is resilient to failure, including the failure of an entire Azure region.

Features of Traffic Manager

- Increase application availability.
- Improve application performance.
- Service maintenance without downtime.
- Combine hybrid applications.
- Distribute traffic for complex deployments.