**What is Azure?**

The Azure cloud platform is more than 200 products and cloud services designed to help you bring new solutions to life—to solve today’s challenges and create the future. Build, run and manage applications across multiple clouds, on-premises, and at the edge, with the tools and frameworks of your choice.

**Benefits of Azure**

* You don’t need to invest in hardware upfront.
* You can terminate the resources whenever you don’t require them.
* You only pay for how much you use.
* **Azure Account**
* **Subscriptions** –This is a way of billing how much you use on Azure.
* **ACD (Azure Active Directory)** – This is an identity store (You can create users that have access to resources that you define in Azure)
* **Resource** – Every resource needs to be part of a resource group.
* **Regions or locationsA picture containing graphical user interface

  Description automatically generated**
* **RG (Resource Groups)** – The RG is used to go out and provide a logical grouping of resources. A resource needs to be mapped onto a resource group.
* **VM (Virtual Machine)**
  + **A Series | Entry Level** 
    - **Dev Test**
    - **Web Servers**
    - **Databases**
    - **Code Repositories**
  + **B Series | Burstable VMs**
  + **D Series | General Purpose Compute** – Run on Intel Xeon Processors
    - **Offer the vcpu’s, memory**
    - **And temporary storage**
  + **Da Series** - Use AMD Epic Processors
  + **Dc Series** – If you need additional Security
  + **E Series | Memory Optimized VMs**
  + **M Series is ideal for extremely large databases**
  + **Constrained vCPUs** – To reduce the cost of S/W
  + **F Series | Compute Optimized** – High CPU to memory ratio and great for medium traffic web servers, Network Appliances, Batch Processes, and Application servers as well as video encoding and rendering, AI inferencing, and gaming applications.
    - **F series runs on the latest Xeon Scalable processors and can scale up to 72 vcpu**.
  + **L Series | Storage Optimized** 
    - **Run Big data**
    - **No-SQL databases**
    - **Large Data warehousing**
    - **Up to 19.2TB of local storage which yields up to 3.8 Million IOPS**

**Virtual Machines in Azure**

|  |  |  |
| --- | --- | --- |
| Type | Sizes | Description |
| [General-purpose](https://docs.microsoft.com/en-us/azure/virtual-machines/sizes-general) | B, Dsv3, Dv3, Dasv4, Dav4, DSv2, Dv2, Av2, DC, DCv2, Dv4, Dsv4, Ddv4, Ddsv4, Dv5, Dsv5, Ddv5, Ddsv5, Dasv5, Dadsv5 | Balanced CPU-to-memory ratio. Ideal for testing and development, small to medium databases, and low to medium traffic web servers. |
| [Compute-optimized](https://docs.microsoft.com/en-us/azure/virtual-machines/sizes-compute) | F, Fs, Fsv2, FX | High CPU-to-memory ratio. Good for medium-traffic web servers, network appliances, batch processes, and application servers. |
| [Memory-optimized](https://docs.microsoft.com/en-us/azure/virtual-machines/sizes-memory) | Esv3, Ev3, Easv4, Eav4, Ebdsv5, Ebsv5, Ev4, Esv4, Edv4, Edsv4, Ev5, Esv5, Edv5, Edsv5, Easv5, Eadsv5, Mv2, M, DSv2, Dv2 | High memory-to-CPU ratio. Great for relational database servers, medium to large caches, and in-memory analytics. |
| [Storage optimized](https://docs.microsoft.com/en-us/azure/virtual-machines/sizes-storage) | Lsv2, Lsv3, Lasv3 | High disk throughput and IO are ideal for Big Data, SQL, NoSQL databases, data warehou,sing and large transactional databases. |
| [GPU](https://docs.microsoft.com/en-us/azure/virtual-machines/sizes-gpu) | NC, NCv2, NCv3, NCasT4\_v3, ND, NDv2, NV, NVv3, NVv4, NDasrA100\_v4, NDm\_A100\_v4 | Specialized virtual machines targeted for heavy graphic rendering and video editing, as well as model training and inferencing (ND) with deep learning. Available with single or multiple GPUs. |
| [High performance compute](https://docs.microsoft.com/en-us/azure/virtual-machines/sizes-hpc) | HB, HBv2, HBv3, HC, H | Our fastest and most powerful CPU virtual machines with optional high-throughput network interfaces (RDMA). |

**VM Connect**

* **RDP** (Remote Desktop Protocol)
* **SSH**
* **Bastion**

# Bastion

* Fully managed service that helps secure remote access to your virtual machines.
* Azure Bastion is a fully managed service that provides more secure and seamless Remote Desktop Protocol (RDP) and Secure Shell Protocol (SSH) access to virtual machines (VMs) without any exposure through public IP addresses.
* Steps 🡪 create vnet (subnet should be named “AzureBastionSubnet”> create bastion >

**RDP Port = 3389**

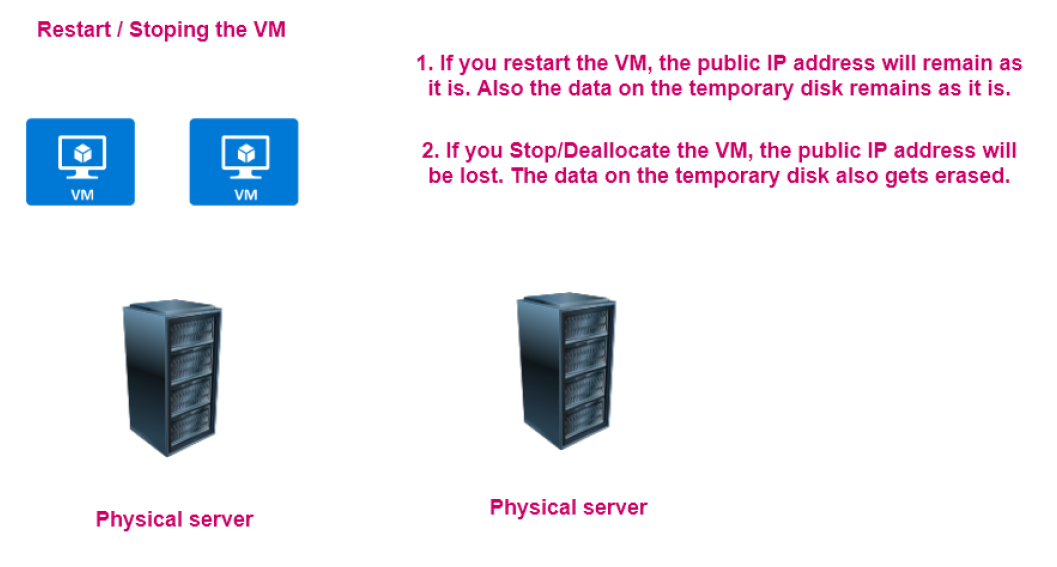
**Note: If we delete Resource Group then automatically all resources will be deleted, those that belong to that RG. And when you delete something then always check the deletion notification to confirm because sometimes some resources would not have been deleted because of some dependencies.**

**You can also create Budget alerts in Azure.**

**Graphical user interface, application

Description automatically generated**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

****

****

Graphical user interface, text

Description automatically generated

**Disk Types**

1. **Standard HDD**
   1. **This is ideal for backup environments and non-critical workloads.**
   2. **Max disk size –32,767 GiB**
   3. **Max throughput –500 MB/s**
   4. **Max IOPS -2000**
2. **Standard SSD**
   1. **This is ideal for Web Servers and Dev/Test Environments.**
   2. **Max disk size –32,767 GiB**
   3. **Max throughput –750 MB/s**
   4. **Max IOPS -6000.**
3. **Premium SSD**
   1. **This is ideal for Production environments.**
   2. **Max disk size –32,767 GiB**
   3. **Max throughput –950 MB/s**
   4. **Max IOPS –20,000.**
4. **Ultra Disk**
   1. **This is ideal for IO-intensive workloads –SQL, Oracle databases.**
   2. **Max disk size –32,767 GiB**
   3. **Max throughput –950 MB/s**
   4. **Max IOPS –20,000.**

**Server Side Disk Encryption**

**Server-Side Encryption** (also referred to as encryption-at-rest or Azure Storage encryption) automatically encrypts data stored on Azure managed disks (OS and data disks) when persisting on the Storage Clusters. For full details, see [Server-side encryption of Azure Disk Storage](https://docs.microsoft.com/en-us/azure/virtual-machines/disk-encryption).

### **Customer-managed keys**

You can choose to manage encryption at the level of each managed disk, with your keys. When you specify a customer-managed key, that key is used to protect and control access to the key that encrypts your data. Customer-managed keys offer greater flexibility to manage access controls.

**Networking Basics**

IPv4 = 32 bit

IPv6 = 128 bit

**5 Different Classes of IP Address (Classful IP Addressing)**

Yhan kisi ki demand as it is fulfill nhi hoti. Jese Kisi ko 1000 IP addresses chahiye to isme use fixed number of IP addresses nhi milenge

|  |  |  |  |
| --- | --- | --- | --- |
| N | H | H | H |

1. A = 0-126 (Network Bit = 1, Host Bit = 0)

(127 is LoopBack Address (Self Testing, Local Host) 127.0.0.1 )

|  |  |  |  |
| --- | --- | --- | --- |
| N | N | H | H |

1. B = 128-191

|  |  |  |  |
| --- | --- | --- | --- |
| N | N | N | H |

1. C = 192-223
2. D = 224-239
3. E = 240-255

Note – Class A, B, C me network address find krne ke lie Host bit ko 0 se replace kr denge or HostAddress/BroadCast Address find krne ke lie host bit ki value maximum kr denge.

Network Address & Broadcast address never assign to any system. We can only assign IP address between Network address and Broadcast address.

**Ports = 65535**

1. C Class Network = 256

Usable IP = 256-2 = 254

1. B Class Network IP = 256\*256 = 65536

Usable IP = 65536-2 = 65534

1. A Class Network IP = 256\*256\*256 = 16,777,216

Usable IP = 16,777,216-2 = 16,777,214

**Subnetting**

* Network within a network.
* Logically division of IP addresses.
* The process of dividing a network into smaller network sections is called **subnetting**.
* Subnetting is the strategy use to partition a single physical network into more than one smaller logical sub networks/subnets.
* Router is a internetworking device.

Subnet is a segmented piece of large network. More specifically, subnets are a logical partition of an IP network into multiple, smaller network segments.

**CIDR Notations (Classless Inter-Domain Routing)** (Classless IP Addressing 1993)

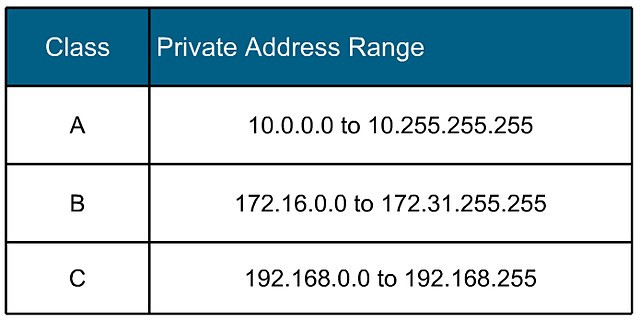
* A method of assigning Internet Protocol (IP) addresses that **improves the efficiency of address distribution** and replaces the previous system based on Class A, Class B and Class C networks.
* Classless addressing me IP addresses ki westing bahut kam hoti h.
* Isme user ki demand ki size ka block diya jata h.
* IANA provide that block size that user demands.
* No Classes
* Only Blocks

**Rules**

* Address should be continuous.
* No of addresses in a block must be in power of 2.
* First Address of every block must be evenly divisible with size of block.

**Private IP Address**

* Used for communication within a private network. Cannot be directly contacted over the internet.
* Addresses can be reused per network.
* Assigned to a device by router.
* Has a small set range of possible addresses.
* A private IP address is **a range of non-internet facing IP addresses used in an internal network**.



**Public IP Address**

* Used to communicate over the public internet – outside a private network.
* Addresses are unique and cannot be reused.
* Assigned by and ISP.
* Addresses can be any combination of numbers not within the private IP range.
* Public is mainly for management traffic.
* A public IP address is **an IP address that can be accessed directly over the internet and is assigned to your network router by your internet service provider (ISP).**

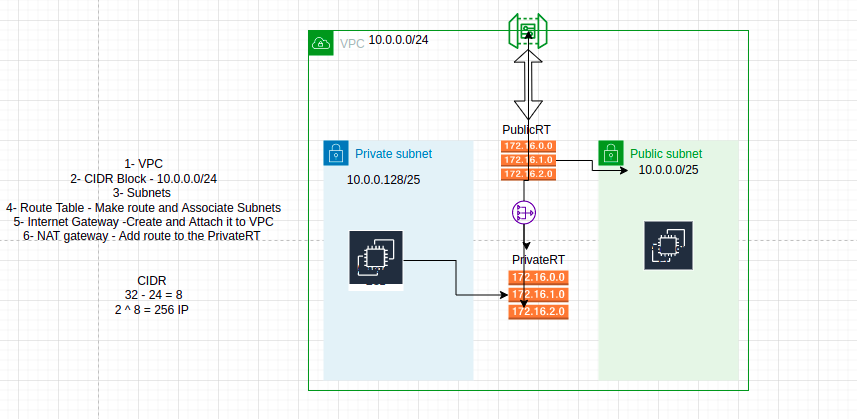
**IPv4**

* 32-bit logical address
* 4 Octet
* 0-255 Octet value
* IP Address = Network ID + Host ID

**Vnet**

Vnet enables you to launch Azure resources into a virtual network that you've defined. This virtual network closely resembles a traditional network that you'd operate in your own data center, with the benefits of using the scalable infrastructure of Azure.

Azure Virtual Network (VNet) is the fundamental building block for your private network in Azure. VNet enables many types of Azure resources, such as Azure Virtual Machines (VM), to securely communicate with each other, the internet, and on-premises networks. VNet is similar to a traditional network that you'd operate in your own data center, but brings with it additional benefits of Azure's infrastructure such as scale, availability, and isolation.

****

1. Vnet
2. CIDR Block
3. Subnets (Ex- Private Subnet, Public Sebnet)
4. Rout Table
5. Internet Gateway

**Subnet**

A subnet is a range of IP addresses in the virtual network. You can divide a virtual network into multiple subnets for organization and security. Each NIC in a VM is connected to one subnet in one virtual network.

**Public Subnet**

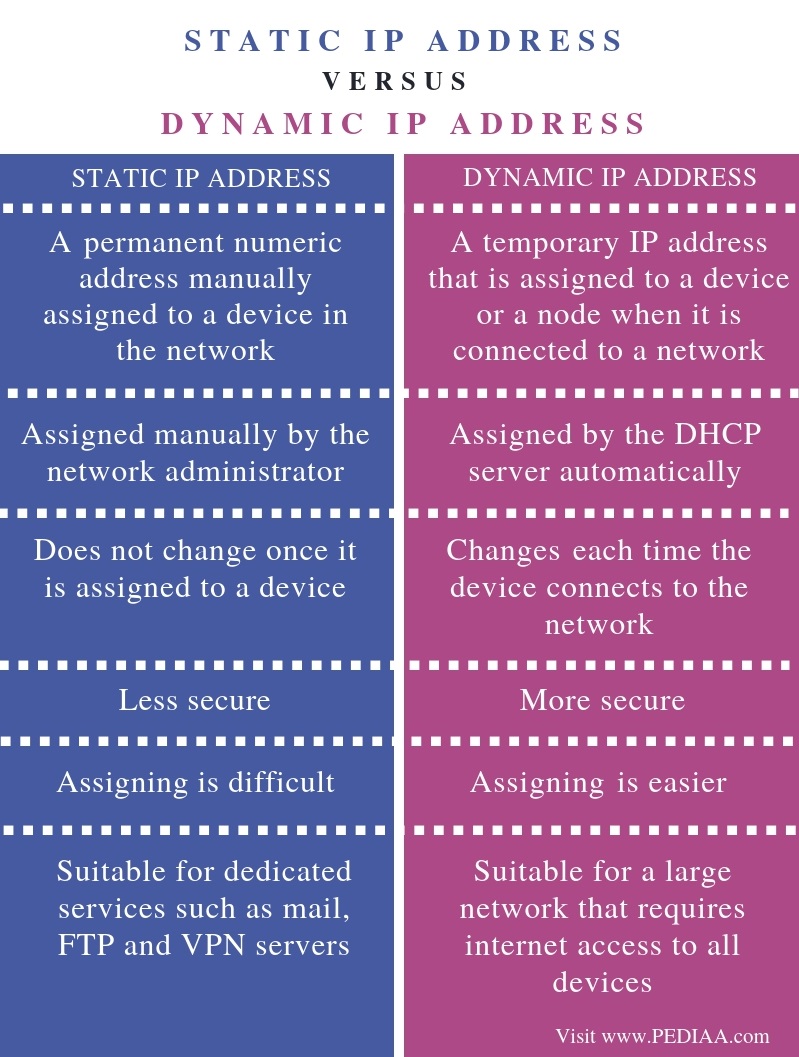
A public subnet is **a subnet that's associated with a route table that has a route to an internet gateway.**

**Private Subnet**

**If a subnet is associated with a route table that does not have a route to an internet gateway**, it's known as a private subnet.

**Static and Dynamic IP addressing**

When a device is assigned a static IP address, the address does not change. Most devices use dynamic IP addresses, which are assigned by the network when they connect and change over time.



**Bastian Host**

Azure Bastion is a fully managed service that provides more secure and seamless Remote Desktop Protocol (RDP) and Secure Shell Protocol (SSH) access to virtual machines (VMs) without any exposure through public IP addresses.

**Attaching multiple network interface to single Virtual Machine**

****

**Note –** If you want to attach one or more NIC to the VM than you have to make a NIC first and then stop your VM because a new NIC will not connect to a VM in running state. So that you have to stop and then attach new NIC to VM.

**Note** – We can only attach NSG to the VM, NIC or SUBNET not to the VNet.

**Network Security Group & Rules** (Inbound Rules & Outbound Rules)

A network security group **contains security rules** (like inbound rule, outbound rule) **that allow or deny inbound network traffic to, or outbound network traffic from, several types of Azure resources.**

**Priority of Security Rules**

A number between 100 and 4096. Rules are processed in priority order, with lower numbers processed before higher numbers, because lower numbers have higher priority. Once traffic matches a rule, processing stops. As a result, any rules that exist with lower priorities (higher numbers) that have the same attributes as rules with higher priorities aren't processed.

Protocol = TCP, UDP, ICMP, ESP, AH, or Any.

**Azure Application Gateway Service / LB (Load Balancer) / Web Traffic Load Balancer**

* This service is a web traffic load balancer that is used to distribute traffic to web applications.
* The web applications can reside on Virtual Machines, Virtual Machines Scale sets or even on on-premises servers.
* The application gateway is on OSI Layer 7 load balancer.
* Secure Sockets Layer (SSL/TLS) termination.
* Here requests to the application gateway can be secure.
* And then the requests to the backend pool resource can go unencrypted.
* This can lift the burden of the backend pool for decrypting requests.
* The decryption of requests can be left to the Application gateway resource.
* You can also enable Autoscaling for your Application Gateway resource.
* This allows the Application Gateway to scale up or down based on traffic load patterns.
* You can also enable the web application firewall feature for the application gateway resource.
* Frontend components of the Application Gateway.
* Frontend IP address – Users will hit the Application Gateway via the frontend IP address.
* Listener – This is a logical entity that check for incoming connection requests. There can be multiple listeners attached to an application gateway.

There are two types of Listeners Configurations

1. Basic – Here the listener listens to a single domain site.
2. Multi-site – Here the Listeners maps to the multiple domain sites.

Different components of the application gateway.

**Routing Rules –** This is used to route the traffic from the listener to the backend pool.

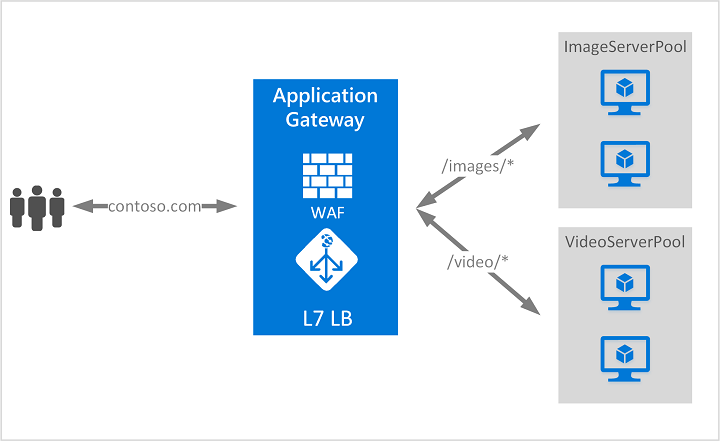
There are 2 types of routing rules.

1. **Basic -**  Here all requests are routed to backend pool directly.
2. **Path-Based –** Here requests are routed to the backend pool based on the URL in the request.

**Backend Pools –** These can be network interface cards, virtual machine scale sets, public or internal IP addresses, FQDN or backends such as app service.

Azure Application Gateway is a web traffic load balancer that enables you to manage traffic to your web applications. Traditional load balancers operate at the transport layer (OSI layer 4 - TCP and UDP) and route traffic based on source IP address and port, to a destination IP address and port.

Application Gateway can make routing decisions based on additional attributes of an HTTP request, for example URI path or host headers. For example, you can route traffic based on the incoming URL. So if /images is in the incoming URL, you can route traffic to a specific set of servers (known as a pool) configured for images. If /video is in the URL, that traffic is routed to another pool that's optimized for videos.



**Vnet Peering**

* Virtual Network Peering is used to connect two Azure virtual networks together via the backbone network.
* Azure supports connecting two virtual networks located in the same region or networks located across regions.
* Once you enable virtual network peering between two virtual networks, the virtual machines can then communicate via their private IP addresses across the peering connection.
* You can also peer virtual networks that are located across different subscriptions.
* The virtual networks can't have overlapping CIDR blocks.

Virtual network peering enables you to seamlessly connect two or more [Virtual Networks](https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-overview) 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.

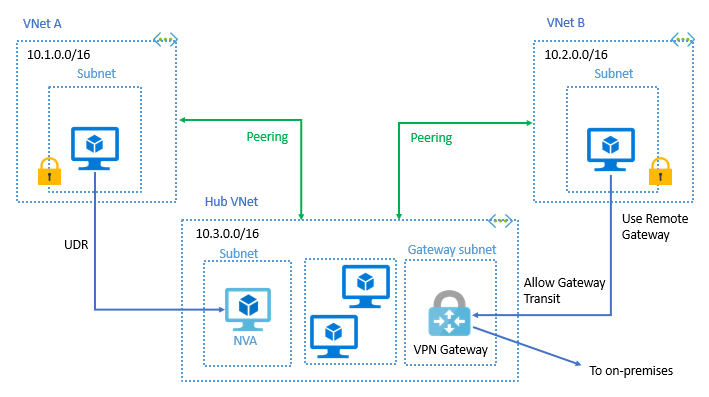
Azure supports the following 2 types of peering:

1. **Virtual network peering**: Connecting virtual networks within the same Azure region.

1. **Global virtual network peering**: Connecting virtual networks across Azure regions.

**Benefits of Vnet Peering whether local or global, include:**

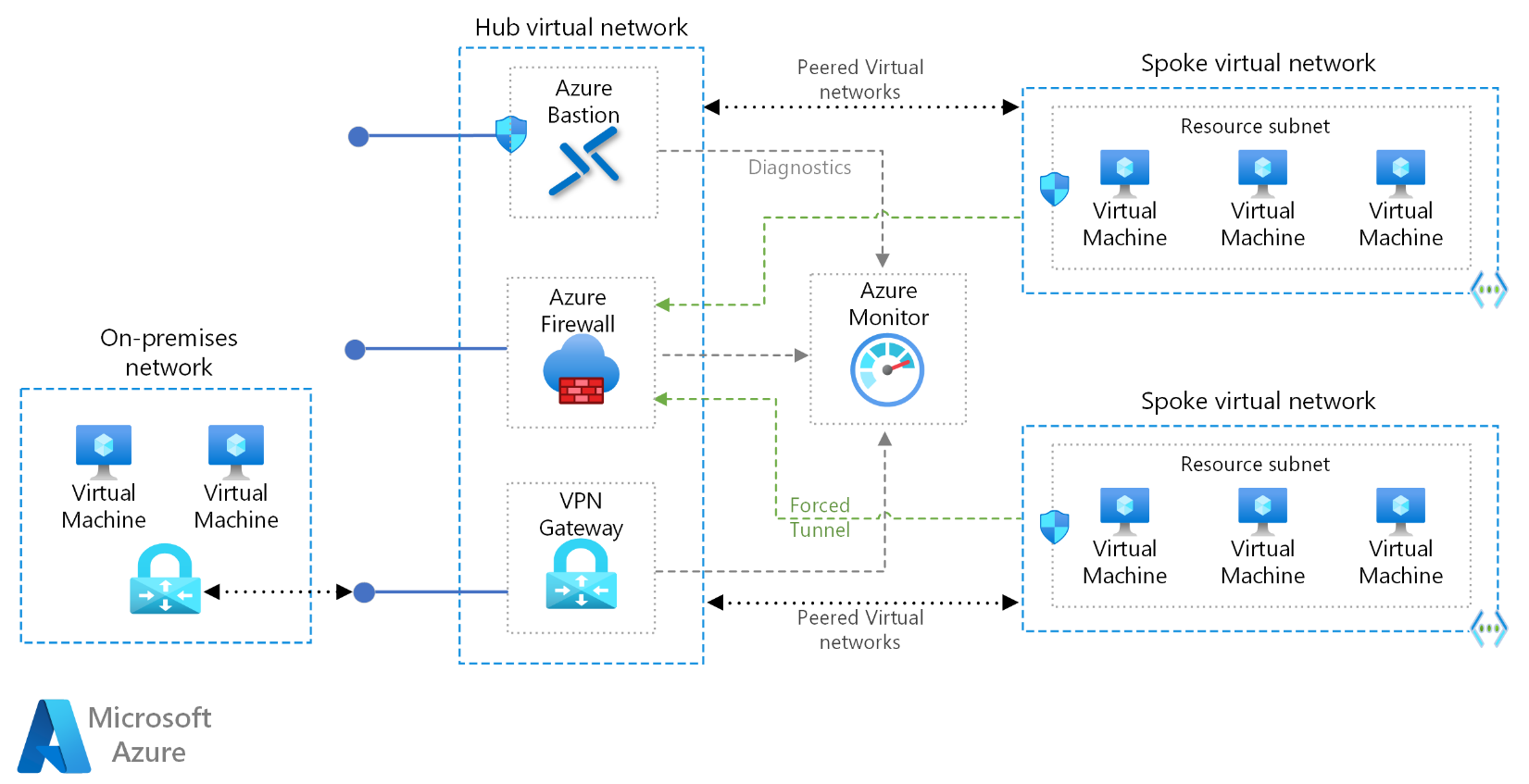
* Network traffic between peered virtual networks is private.
* Low-latency, high-bandwidth connection between resources in different virtual networks.
* Ability for resources in one virtual network to communicate with resources in a different virtual network.
* Ability to transfer data between virtual networks across Azure subscriptions.
* No downtime to resources in either virtual network when creating the peering, or after the peering is created.
* No public Internet, gateways, or encryption is required in the communication between the virtual networks.
* Peerings are not transitive.



**Hub and Spoke**

This reference architecture details a hub-spoke topology in Azure. The hub virtual network acts as a central point of connectivity to many spoke virtual networks. The hub can also be used as the connectivity point to your on-premises networks. The spoke virtual networks peer with the hub and can be used to isolate workloads.

## **Architecture**



### **Workflow**

The architecture consists of the following aspects:

**Hub virtual network:** The hub virtual network is the central point of connectivity to your on-premises network. It's a place to host services that can be consumed by the different workloads hosted in the spoke virtual networks.

**Spoke virtual networks:** Spoke virtual networks are used to isolate workloads in their own virtual networks, managed separately from other spokes. Each workload might include multiple tiers, with multiple subnets connected through Azure load balancers.

**Virtual network peering:** Two virtual networks can be connected using a [peering connection](https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-peering-overview). Peering connections are non-transitive, low latency connections between virtual networks. Once peered, the virtual networks exchange traffic by using the Azure backbone without the need for a router.

**Bastion Host:** Azure Bastion lets you securely connect to a virtual machine using your browser and the Azure portal. An Azure Bastion host is deployed inside an Azure Virtual Network and can access virtual machines in the virtual network (VNet), or virtual machines in peered VNets.

**Azure Firewall:** Azure Firewall is a managed firewall as a service. The Firewall instance is placed in its own subnet.

**VPN virtual network gateway or ExpressRoute gateway**. The virtual network gateway enables the virtual network to connect to the VPN device, or ExpressRoute circuit, used for connectivity with your on-premises network. For more information, see [Connect an on-premises network to a Microsoft Azure virtual network](https://docs.microsoft.com/en-us/microsoft-365/enterprise/connect-an-on-premises-network-to-a-microsoft-azure-virtual-network?view=o365-worldwide).

**VPN device**. A device or service that provides external connectivity to the on-premises network. The VPN device may be a hardware device or a software solution such as the Routing and Remote Access Service (RRAS) in Windows Server 2012.

**VPN**

* A VPN **provides an encrypted server and hides your IP address from corporations, government agencies and would-be hackers**.
* A VPN protects your identity even if you are using public or shared Wi-Fi, and your data will be kept private from any prying internet eyes.
* A VPN circumvents your personal ISP, instead of sending your internet connection to a hosted server. With servers located all over the world, users then have the ability to “relocate” themselves and access the internet from nearly anywhere. Encryption adds an extra layer of security, particularly for businesses that are frequently utilizing remote access. It can also be a helpful tool for travel, gaming and streaming.

**3 Types of VPN Connections**

1. [Point-to-Site VPN connections](https://docs.microsoft.com/en-us/azure/vpn-gateway/design#P2S)
2. [Site-to-Site VPN connections](https://docs.microsoft.com/en-us/azure/vpn-gateway/design#s2smulti)
3. [VNet-to-VNet VPN connections](https://docs.microsoft.com/en-us/azure/vpn-gateway/design#V2V)
4. **Point-to-Site VPN connection**

A Point-to-Site VPN connection is used to establish a secure connection between multiple client machines and an Azure virtual network via the Internet.

Below is a diagram from the Microsoft documentation on a sample scenario

Diagram

Description automatically generated

* This sort of connection is based off certificates for authentication.
* You need to have a root certificate in place that needs to be uploaded to Azure for the point-to-site connection.
* A client certificate needs to be generated from the root certificate. This client certificate needs to be on each client computer that needs to connect to the Azure virtual network via the Point-to-Site connection.
* To generate the certificates, you can use a Certificate authority or generate a self-signed certificate using PowerShell. Some commands are given below

**// To generate the root certificate**

$cert = New-SelfSignedCertificate -Type Custom -KeySpec Signature `

-Subject "CN=RootCertificate" -KeyExportPolicy Exportable `

-HashAlgorithm sha256 -KeyLength 2048 `

-CertStoreLocation "Cert:\CurrentUser\My" -KeyUsageProperty Sign -KeyUsage CertSign

**// To generate the client certificate**

New-SelfSignedCertificate -Type Custom -DnsName P2SChildCert -KeySpec Signature `

-Subject "CN=ClientCertificate" -KeyExportPolicy Exportable `

-HashAlgorithm sha256 -KeyLength 2048 `

-CertStoreLocation "Cert:\CurrentUser\My" `

-Signer $cert -TextExtension @("2.5.29.37={text}1.3.6.1.5.5.7.3.2")

**Gateway Subnet:** The gateway subnet is part of the virtual network IP address range that you specify when configuring your virtual network. It contains the IP addresses that the virtual network gateway resources and services use.

**Virtual Network Gateway:** A 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.

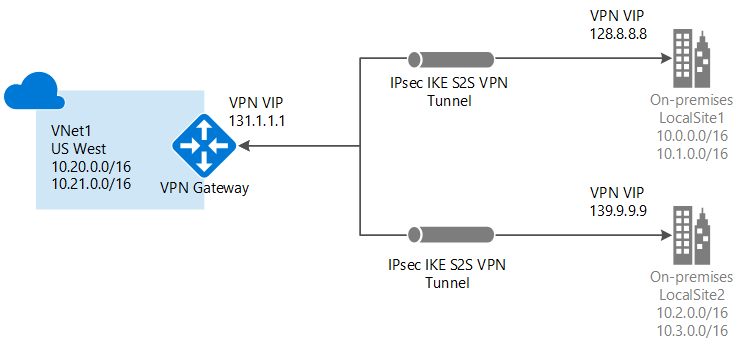
Point-to-site VPN can use one of the following protocols:

* **OpenVPN® Protocol**, an SSL/TLS based VPN protocol. A TLS VPN solution can penetrate firewalls, since most firewalls open TCP port 443 outbound, which TLS uses. OpenVPN can be used to connect from Android, iOS (versions 11.0 and above), Windows, Linux, and Mac devices (macOS versions 10.13 and above).
* **Secure Socket Tunneling Protocol (SSTP)**, a proprietary TLS-based VPN protocol. A TLS VPN solution can penetrate firewalls, since most firewalls open TCP port 443 outbound, which TLS uses. SSTP is only supported on Windows devices. Azure supports all versions of Windows that have SSTP and support TLS 1.2 (Windows 8.1 and later).
* **IKEv2 VPN**, a standards-based IPsec VPN solution. IKEv2 VPN can be used to connect from Mac devices (macOS versions 10.11 and above).

Note - IKEv2 and OpenVPN for P2S are available for the [**Resource Manager deployment model**](https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/deployment-models) only. They are not available for the classic deployment model.

1. **Site-to-Site VPN connection**

A Site-to-Site (S2S) VPN gateway connection is a connection over IPsec/IKE (IKEv1 or IKEv2) VPN tunnel. S2S connections can be used for cross-premises and hybrid configurations. A S2S connection requires a VPN device located on-premises that has a public IP address assigned to it.



VPN Gateway can be configured in active-standby mode using one public IP or in active-active mode using two public IPs. In active-standby mode, one IPsec tunnel is active and the other tunnel is in standby. In this setup, traffic flows through the active tunnel, and if some issue happens with this tunnel, the traffic switches over to the standby tunnel. Setting up VPN Gateway in active-active mode is *recommended* in which both the IPsec tunnels are simultaneously active, with data flowing through both tunnels at the same time. An additional advantage of active-active mode is that customers experience higher throughputs.

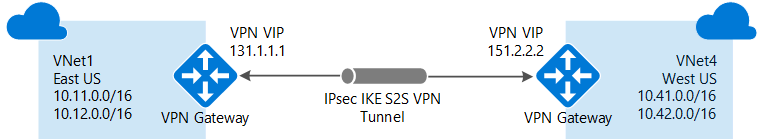
You can create more than one VPN connection from your virtual network gateway, typically connecting to multiple on-premises sites. When working with multiple connections, you must use a RouteBased VPN type (known as a dynamic gateway when working with classic VNets). Because each virtual network can only have one VPN gateway, all connections through the gateway share the available bandwidth. This type of connection is sometimes referred to as a "multi-site" connection.

**3. VNet-to-VNet VPN connections**

Connecting a virtual network to another virtual network (VNet-to-VNet) is similar to connecting a VNet to an on-premises site location. Both connectivity types use a VPN gateway to provide a secure tunnel using IPsec/IKE. You can even combine VNet-to-VNet communication with multi-site connection configurations. This lets you establish network topologies that combine cross-premises connectivity with inter-virtual network connectivity.

The VNets you connect can be:

* in the same or different regions
* in the same or different subscriptions
* in the same or different deployment models



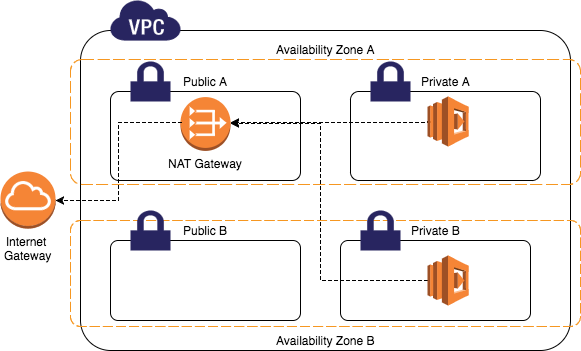
**VPN Gateway**

VPN Gateway sends encrypted traffic between an Azure virtual network and an on-premises location over the public Internet. You can also use VPN Gateway to send encrypted traffic between Azure virtual networks over the Microsoft network. A VPN gateway is a specific type of virtual network gateway. Each virtual network can have only one VPN gateway. However, you can create multiple connections to the same VPN gateway. When you create multiple connections to the same VPN gateway, all VPN tunnels share the available gateway bandwidth.

**NAT Gateway**

For private subnet to talk external world.

A NAT gateway is **a Network Address Translation (NAT) service**. You can use a NAT gateway so that instances in a private subnet can connect to services outside your VPC but external services cannot initiate a connection with those instances.



**What is NAT and Internet gateway?**

A NAT device forwards traffic from the instances in the private subnet to the internet or other AWS services, and then sends the response back to the instances while Internet Gateway is used to allow resources in your VPC to access internet.

**Route Table**

Azure Route Tables, or User Defined Routing, **allow you to create network routes so that your CloudGen Firewall VM can handle the traffic both between your subnets and to the Internet**.

A **Route Table** is used to direct traffic in/out of a subnet. It contains a number of CIDRs (IP address ranges) and where to direct the appropriate traffic.

How traffic will route.

**Express Route**

* The ExpressRoute connection does not go over the puclic internet.
* Your connections are more reliable, faster and you get less latency.
* You get two connections for each Express route circuit for redundancy.
* ExpressRoute is **a service that enables you to create private connections between Azure datacenters and infrastructure that's on your premises or in a colocation environment**.

Diagram

Description automatically generated

**Azure WAN**

Azure Virtual WAN is a networking service that brings many networking, security, and routing functionalities together to provide a single operational interface. Some of the main features include:

* Branch connectivity (via connectivity automation from Virtual WAN Partner devices such as SD-WAN or VPN CPE).
* Site-to-site VPN connectivity.
* Remote user VPN connectivity (point-to-site).
* Private connectivity (ExpressRoute).
* Intra-cloud connectivity (transitive connectivity for virtual networks).
* VPN ExpressRoute inter-connectivity.
* Routing, Azure Firewall, and encryption for private connectivity.

You don't have to have all of these use cases to start using Virtual WAN. You can get started with just one use case, and then adjust your network as it evolves.

The Virtual WAN architecture is a hub and spoke architecture with scale and performance built in for branches (VPN/SD-WAN devices), users (Azure VPN/OpenVPN/IKEv2 clients), ExpressRoute circuits, and virtual networks. It enables a [global transit network architecture](https://docs.microsoft.com/en-us/azure/virtual-wan/virtual-wan-global-transit-network-architecture), where the cloud hosted network 'hub' enables transitive connectivity between endpoints that may be distributed across different types of 'spokes'.

**Network Watcher**

Azure Network Watcher provides tools to monitor, diagnose, view metrics, and enable or disable logs for resources in an Azure virtual network. Network Watcher is designed to monitor and repair the network health of IaaS (Infrastructure-as-a-Service) products which includes Virtual Machines, Virtual Networks, Application Gateways, Load balancers, etc.

**Connection Monitor**

Check the network connectivity between machines. These can be in Azure or on your on-premises environments.

**Next Hop**

Here you can see the next route for a packet of data. This helps you understand whether the packet is being routed to the correct destination.

**IP Flow Verify**

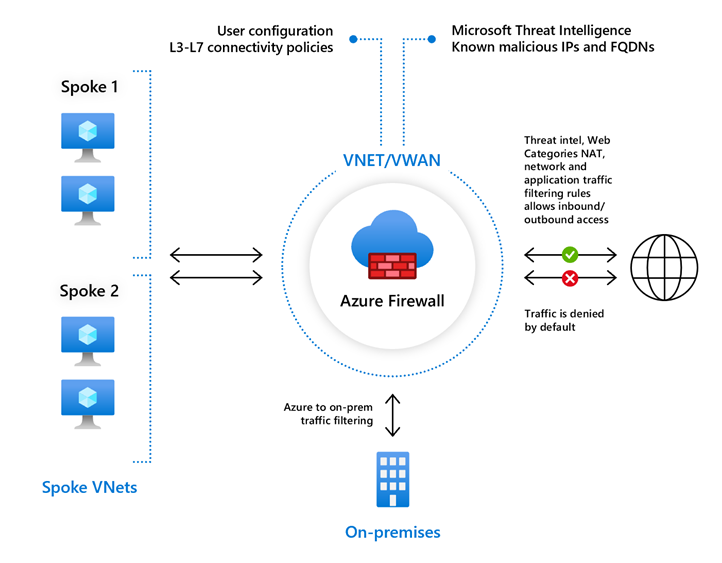
This can be used to check if a packet is allowed or denied to or from a virtual machine. If a packet is being denied by a security group, you can see which rule is denying the packet.

**Connection Troubleshoot**

Check the connection from a virtual machine to a virtual machine, fully qualified domain name, URI or IPv4 address.

**Azure Firewall**

Azure Firewall is a cloud-native and intelligent network firewall security service that provides the best of breed threat protection for your cloud workloads running in Azure. It's a fully stateful, firewall as a service with built-in high availability and unrestricted cloud scalability. It provides both east-west and north-south traffic inspection.



**DNS**

Azure DNS allows you to host your DNS domain in Azure, so you can manage your DNS records using the same credentials, billing and support contract as your other Azure services. Zones can be either public or private, where Private DNS Zones (in Managed Preview) are only visible to VMs that are in your virtual network. Our global network of name servers uses Anycast routing to provide outstanding performance and availability.

**COMPUTE**

**Virtualization**

Virtualization is **the fundamental technology that powers cloud computing**. Virtualization is software that manipulates hardware, while cloud computing refers to a service that results from that manipulation. You can't have cloud computing without virtualization.

**Cloud Computing**

Cloud computing is the on-demand availability of computer system resources, especially data storage and computing power, without direct active management by the user. Large clouds often have functions distributed over multiple locations, each location being a data center.

## **Difference between Cloud Computing and Virtualization**

| **Cloud Computing** | **Virtualization** |
| --- | --- |
| Cloud computing refers to the distribution of computer services such as servers, storage, networking, and intelligence via the Internet, or the cloud. | Virtualization is a technology that lets you use a single physical hardware system to create many virtual environments or dedicated resources. |
| Deliver a range of resources to users in groups for a variety of objectives. | Packaged resources are delivered to specified consumers for a specific purpose. |
| Scalable to a large extent | Low-scalability |
| Cloud computing entails the use of several machines in the event of a disaster recovery | It is reliant on a single peripheral. |
| Cloud computing has a greater total cost than virtualization. | Virtualization has a lower total cost than virtualization. |
| Many pieces of specialized hardware are required. | While a single dedicated piece of hardware can perform admirably. |

**Data Disk**

A data disk is **a managed disk that's attached to a virtual machine to store application data, or other data you need to keep**. Data disks are registered as SCSI drives and are labeled with a letter that you choose. Each data disk has a maximum capacity of 32,767 gibibytes (GiB).

**IOPS**

* **IOPS measures the number of read and write operations per second**
* Input/output operations per second is an input/output performance measurement used to characterize computer storage devices like hard disk drives, solid state drives, and storage area networks.

**Throughput**

* **Throughput measures the number of bits read or written per second**.

**Data Disk Snapshot**

A snapshot is **a full, read-only copy of a virtual hard disk (VHD)**. You can use a snapshot as a point-in-time backup, or to help troubleshoot virtual machine (VM) issues. You can take a snapshot of both operating system (OS) or data disk VHDs.

**Shared Disks**

Azure shared disks is a feature for Azure managed disks that allow you to attach a managed disk to multiple virtual machines (VMs) simultaneously. Attaching a managed disk to multiple VMs allows you to either deploy new or migrate existing clustered applications to Azure.

**Custom Script Extensions**

The Custom Script Extension downloads and runs scripts on Azure virtual machines (VMs). This extension is useful for post-deployment configuration, software installation, or any other configuration or management task. You can download scripts from Azure Storage or GitHub, or provide them to the Azure portal at extension runtime.

The Custom Script Extension integrates with Azure Resource Manager templates. You can also run it by using the Azure CLI, PowerShell, the Azure portal, or the Azure Virtual Machines REST API.

* This tool can be used on Azure virtual machines to download and execute scripts.
* This is ideal when you want to deploy any custom configuration of any software installation on a VM.
* The scripts can be located in an Azure storage account or even in Github.
* A time duration of 90 minutes is allowed for the script to run. Any longer and the result will be a failed extension provision.
* It is ideal not to place reboots inside the script because the extension will not continue after the reboot. Hence if you have other commands that need to run via the extension after the reboot, they won’t run.
* If your script does need a reboot, then maybe you can look at other tools such as desired state configuration, Chef, or Puppet.
* The script will run only once.
* The custom script extension will run under the impersonation of the local system account.