

Azure virtual network and Azure virtual machines

Review



Azure Virtual Network

This is a private network on Azure. It helps to host Azure resources such as your Azure virtual machines.

Its like having a traditional network in your on-premises data center.



Region

A virtual network needs to be hosted in a particular region.



Address space

You need to specify an address space for the virtual network



Subscription

A virtual network needs to be part of a subscription.



Subnets

This helps to segment the virtual network into one or more sub-networks.

Azure Virtual Machine

This service helps you to provision virtual machines on the cloud.



Compute

This is your compute service on the Azure platform. Here you can create compute resources on-demand.



Lifecycle

You can create the machine whenever you want. You can also terminate the machine whenever required.



Operating system

You can choose from operating systems such as Windows Server 2019 and different flavors of Linux.



Workload

You can then install different workloads on the machine.

Azure Virtual Machine



Less Management

You don't manage the infrastructure.



Less operations

Don't need to invest in managing the data center



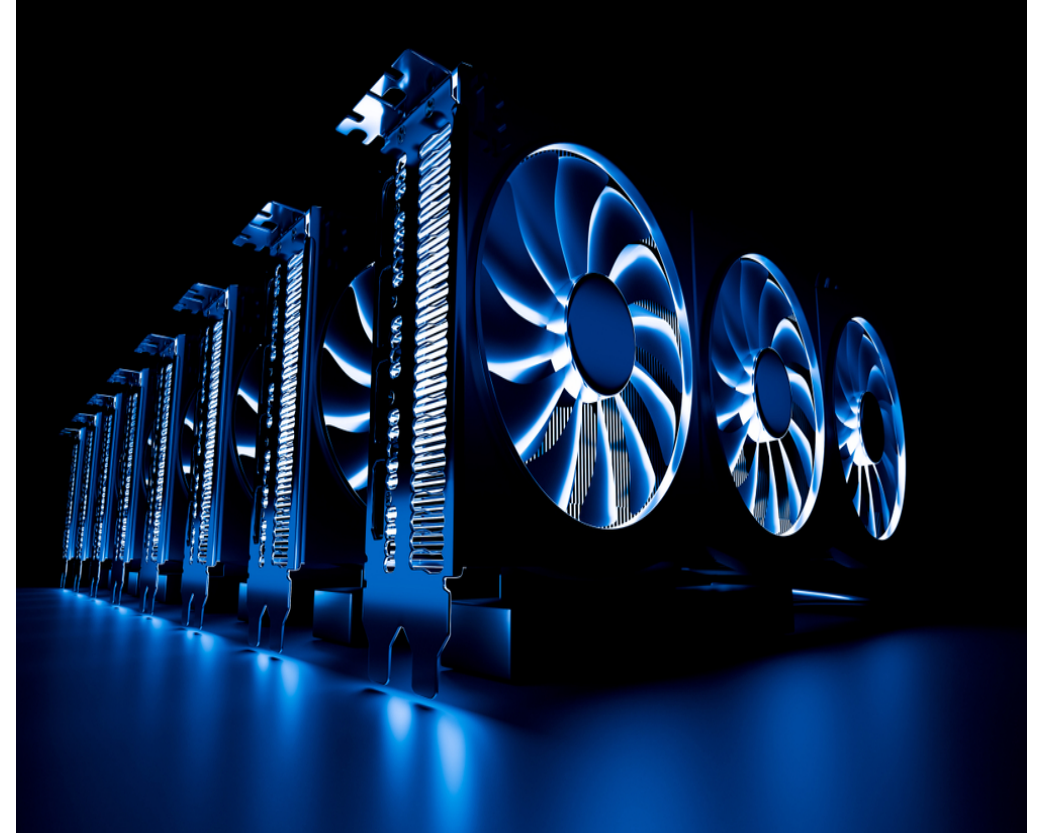
Less Investment

You only pay for how much you use.

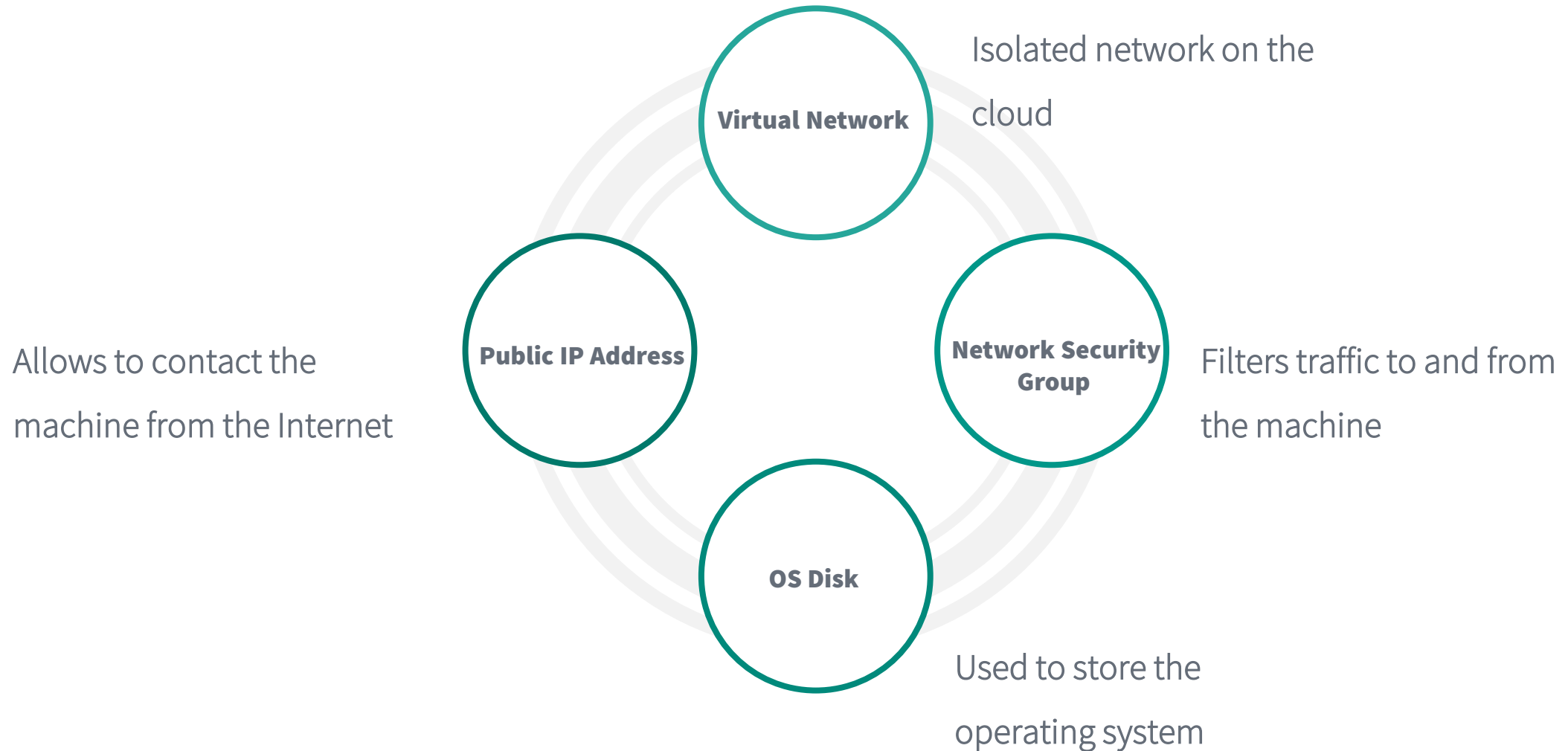


Configure


You can configure various aspects of your virtual machine




Azure Virtual Machine





Private IP Address

 Azure assigns private IP addresses to resources from the address range of the subnet.

 The first four addresses of each subnet range are reserved by Azure.



 By default, Azure assigns a dynamic IP address.

 You can also mark a private IP address as static

Public IP Address



This allows internet resources to communicate with Azure resources



Here the allocation of the public IP address can be static or dynamic depending upon the SKU



Basic SKU – Dynamic or Static. Does not support availability zones.



Standard SKU – Only Static allocation. Does support zone-redundancy.

Azure Virtual Network

REVIEW



Azure Virtual Network

Isolation

This is a private network in Azure



Internet

All resources in the virtual network can communicate with the Internet by default



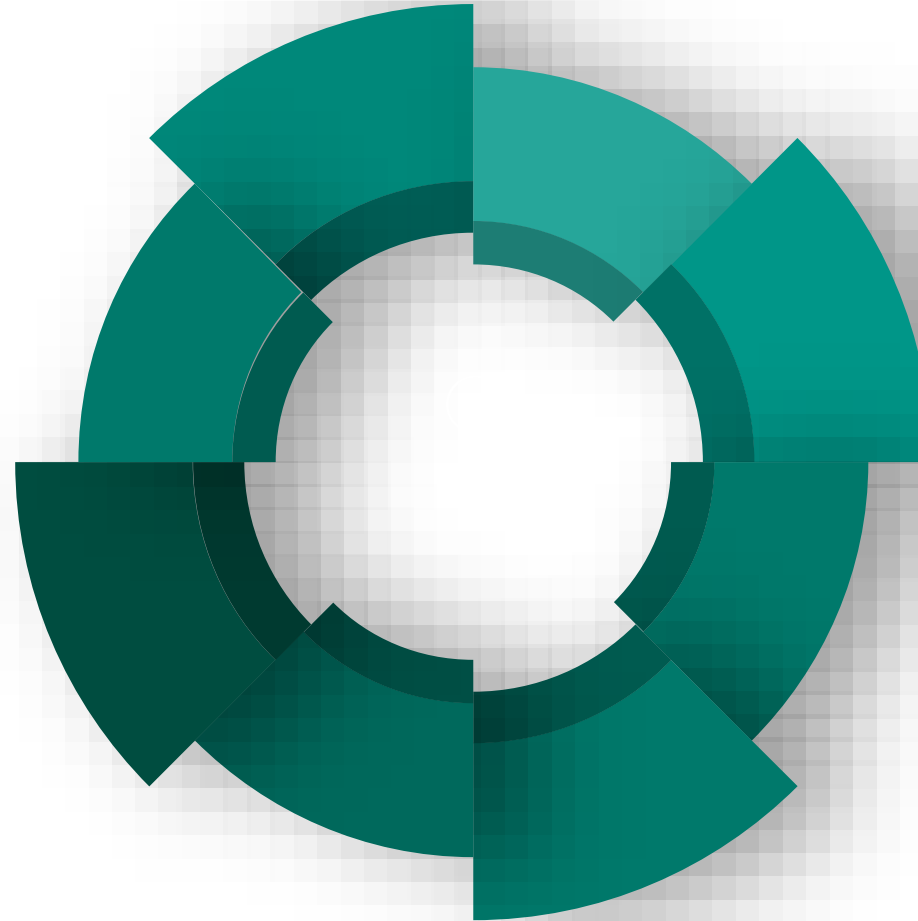
Subnet

This is a range of IP addresses within the virtual network. Subnets help to have better organization and security



Network Interface

This is the interconnection between the virtual machine and the virtual network.



IP addresses



Public IP address

This allows for outbound communication with the Internet.



Private IP address

This is used for communication within the virtual network.



Virtual Network peering



Connection

Helps to connect two or more virtual networks together. The traffic moves via the Microsoft backbone infrastructure.



IP addresses

The virtual networks in the peering connection must have non-overlapping IP address spaces.



Locations

You can connect virtual networks that are in the same region or across regions.



Peering Connection

A peering connection is created for each virtual network.



Azure DNS

DNS Zone

This is used to host the DNS records for a particular domain.



Public zone

Here Azure DNS can resolve host names in your public domain.



Private zone

Here domain names can be resolved within the virtual network.



Virtual Network link

To ensure that the virtual network can use the private DNS zone, you need to link the virtual network to the zone.



Autoregistration

Here DNS records for your virtual machines get automatically created in the zone.



Domain Name System

Review



Domain Name System



Azure Private DNS

This provides a reliable and secure DNS service for your virtual network.

Here you can use your own custom private DNS zones



Virtual Network link

To resolve records, the virtual network needs to be linked to a zone



Automatic updates

DNS records can be updated whenever a virtual machine gets created, changes its IP address or gets deleted.



Autoregistration

Here DNS records get automatically registered for the virtual machines in the virtual network



Records

Supports the common DNS record types – A, AAAA, CNAME, MX , SOA, TXT.

Azure Public DNS

This is a hosting service that provides name resolution by using Microsoft Azure Infrastructure.

You can manage your records in Azure DNS



Reliability

Here you can make use of Azure's global network of DNS name servers.



Records

Supports the common DNS record types – A, AAAA, CNAME, MX, SOA, TXT.



Tools

You can use tools such as PowerShell to manage your DNS zones.



Domain name

Currently you can't buy a domain name when it comes to Azure DNS.

Azure Virtual Machine

This service helps you to provision virtual machines on the cloud.



Compute

This is your compute service on the Azure platform. Here you can create compute resources on-demand.



Lifecycle

You can create the machine whenever you want. You can also terminate the machine whenever required.



Operating system

You can choose from operating systems such as Windows Server 2019 and different flavors of Linux.



Workload

You can then install different workloads on the machine.

Azure Virtual Machine



Less Management

You don't manage the infrastructure.



Less Investment

You only pay for how much you use.



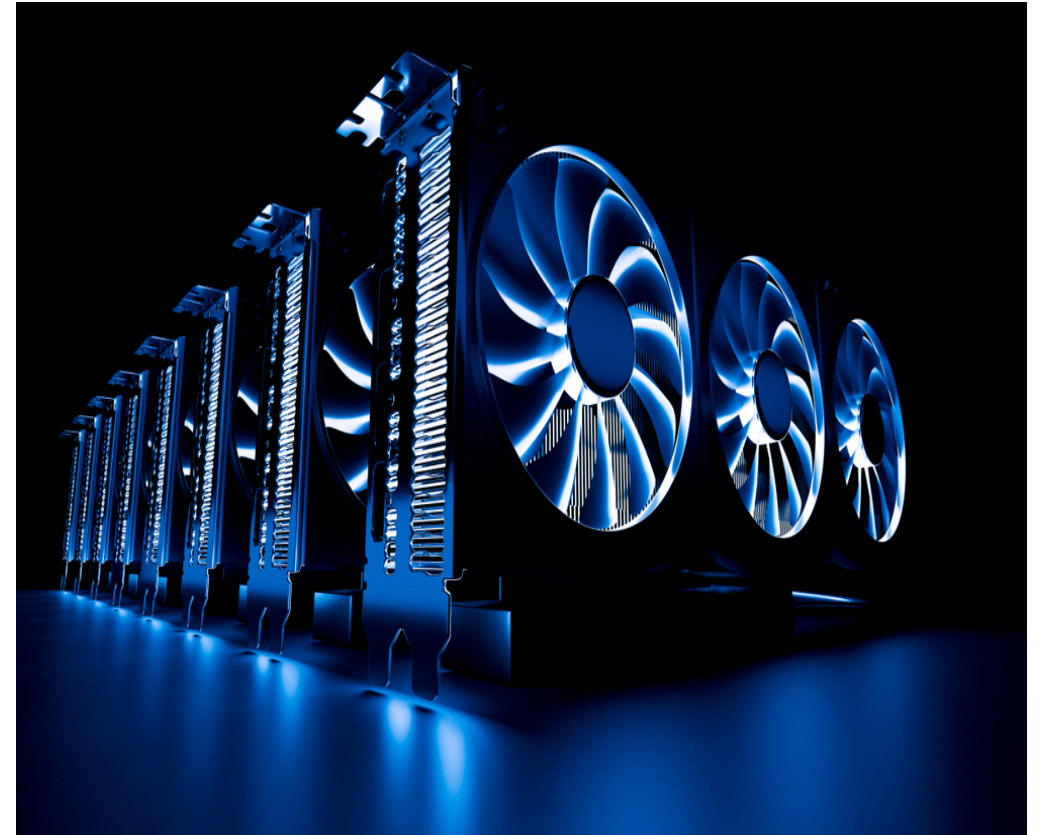
Less operations

Don't need to invest in managing the data center

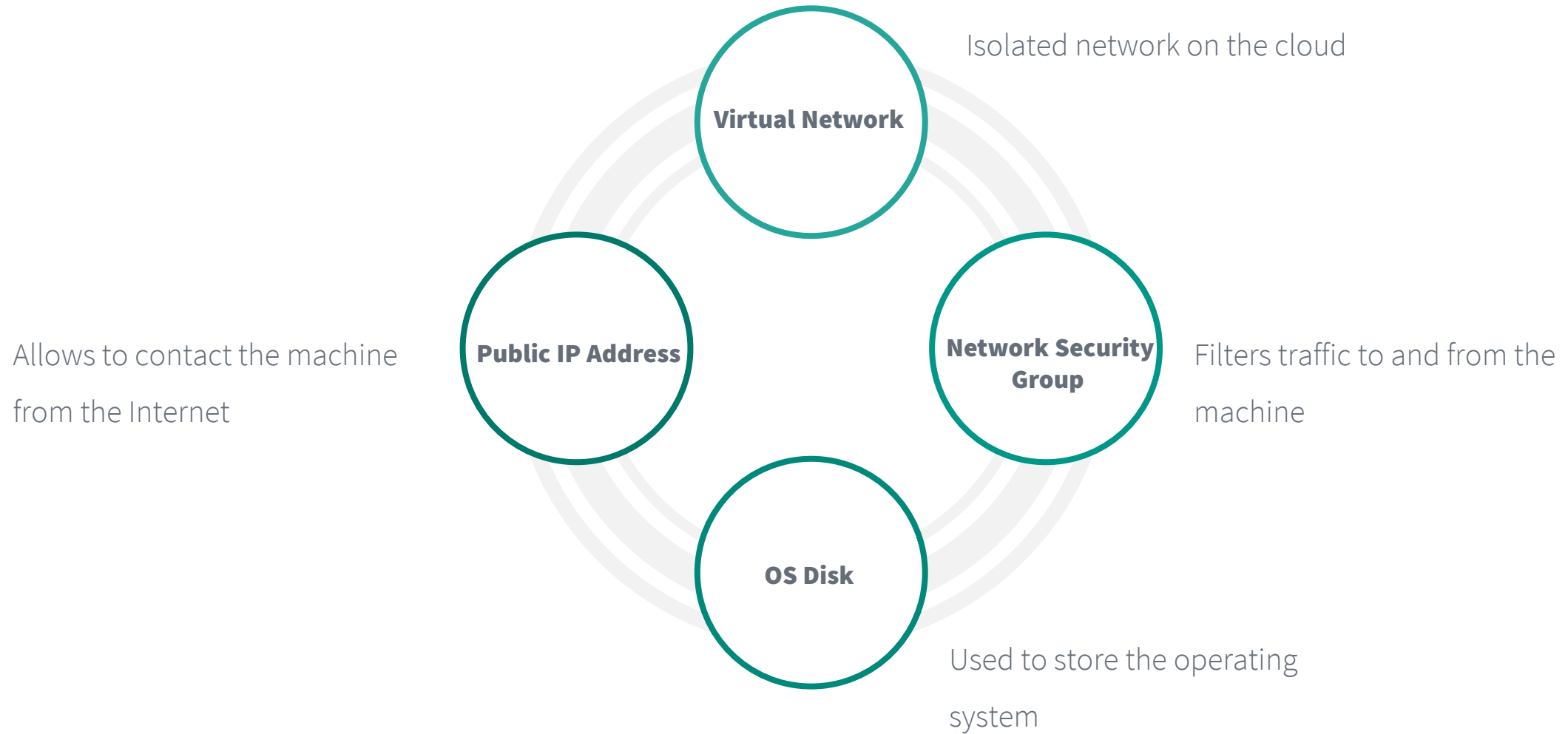


Configure

You can configure various aspects of your virtual machine



Azure Virtual Machine



Private IP Address



Azure assigns private IP addresses to resources from the address range of the subnet.



The first four addresses of each subnet range are reserved by Azure.



By default, Azure assigns a dynamic IP address.



You can also mark a private IP address as static

Public IP Address



This allows internet resources to communicate with Azure resources



Here the allocation of the public IP address can be static or dynamic depending upon the SKU



Basic SKU – Dynamic or Static. Does not support availability zones.



Standard SKU – Only Static allocation. Does support zone-redundancy.

Azure Load Balancer

Review



Azure Availability sets



Failure

This feature helps to protect against infrastructure level failures.



Unplanned events

This is when the underlying infrastructure fails unexpectedly. The failures could be attributed to network failures , local disk failures or even rack failures



Planned maintenance events

Here Microsoft needs to make planned updates to the underlying physical environment. In such cases , a reboot might be required on your virtual machine



Availability sets

Here when a machine is assigned to an availability set, it is assigned to a fault and update domain.

Azure Availability zones



Failure

This features help provides better availability for your application by protecting them from datacenter failures.



Zones

Each Availability zone is a unique physical location in an Azure region. Each zone comprises of one or more data centers that has independent power, cooling, and networking



Protection

Hence the physical separation of the Availability Zones helps protect applications against data center failures



Availability

Using Availability Zones, you can be guaranteed an availability of 99.99% for your virtual machines. You need to ensure that you have 2 or more virtual machines running across multiple availability zones.

Azure Load Balancer

This is a service that is used to distribute incoming traffic across a group of backend resources or servers.

This service operates at Layer 4 of the OSI model.



Public Load Balancer

This provides outbound connections for virtual machines inside the virtual network.



Performance

The Load balancer provides low latency and high throughput.



Internal Load Balancer

This is used to load balance traffic inside a virtual network.



Scaling

The Load Balancer can scale up to millions of flows for all TCP and UDP applications.

Azure Load Balancer SKUs

Basic SKU



This is a free version of the Load Balancer



The backend virtual machines need to be part of an availability set or scale set



Supports health probes of TCP and HTTP



Does not have an SLA

Standard SKU



Here there is an hourly charge



Here the backend virtual machines can also be independent machines that are part of a virtual network

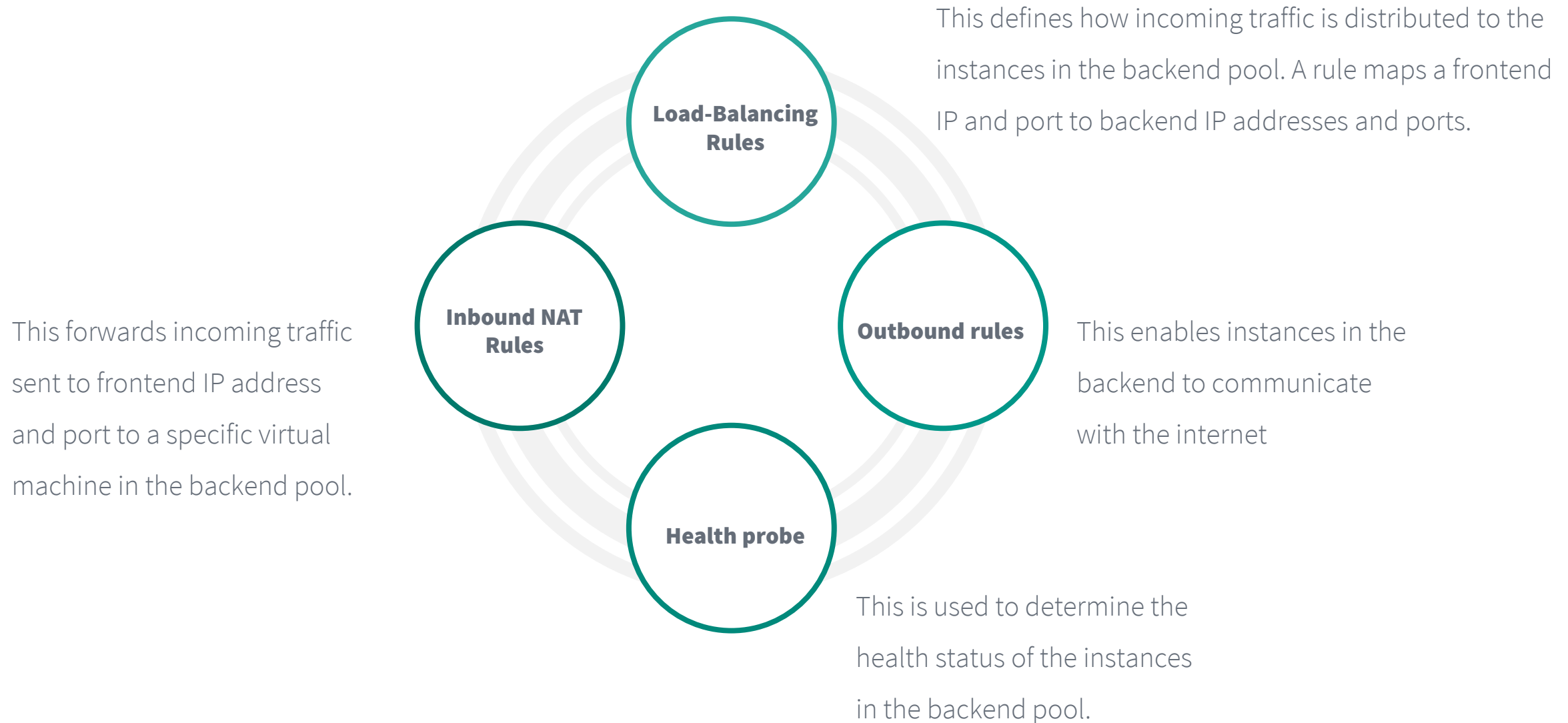


Supports health probes of TCP ,HTTP and HTTPS



Has an SLA of 99.99%

Azure Load Balancer Components



Azure Virtual Machine Scale Set

This service helps to create and manage a group of load balanced VM's.

Here VM's can be created on demand.



Integration

This service can be used with the Load Balancer.



Rules

You can use rules and conditions to scale out or scale in the number of virtual machines.



Virtual Machines

Here VM's are created based on the base image for the machine.



Availability

This service can automatically distribute the virtual machines across Availability zones and Availability sets.

Azure Application Gateway

Review



Azure Application Gateway



Load Balancer

This is a web traffic load balancer. This makes routing decisions based on the attributes of the HTTP request.



Autoscaling

The Standard_v2 SKU supports autoscaling that can scale up and down based on traffic load patterns.



High Availability

For the Standard_v2 SKU , the gateway can span multiple Availability Zones.



Layer 7

This load balancer operates at Layer 7

Azure Application Gateway features

Here requests can be routed to the back-end
Server pools based on the URL paths of the request.

**URL-based
routing**

**Rewrite HTTP
Headers or URL**

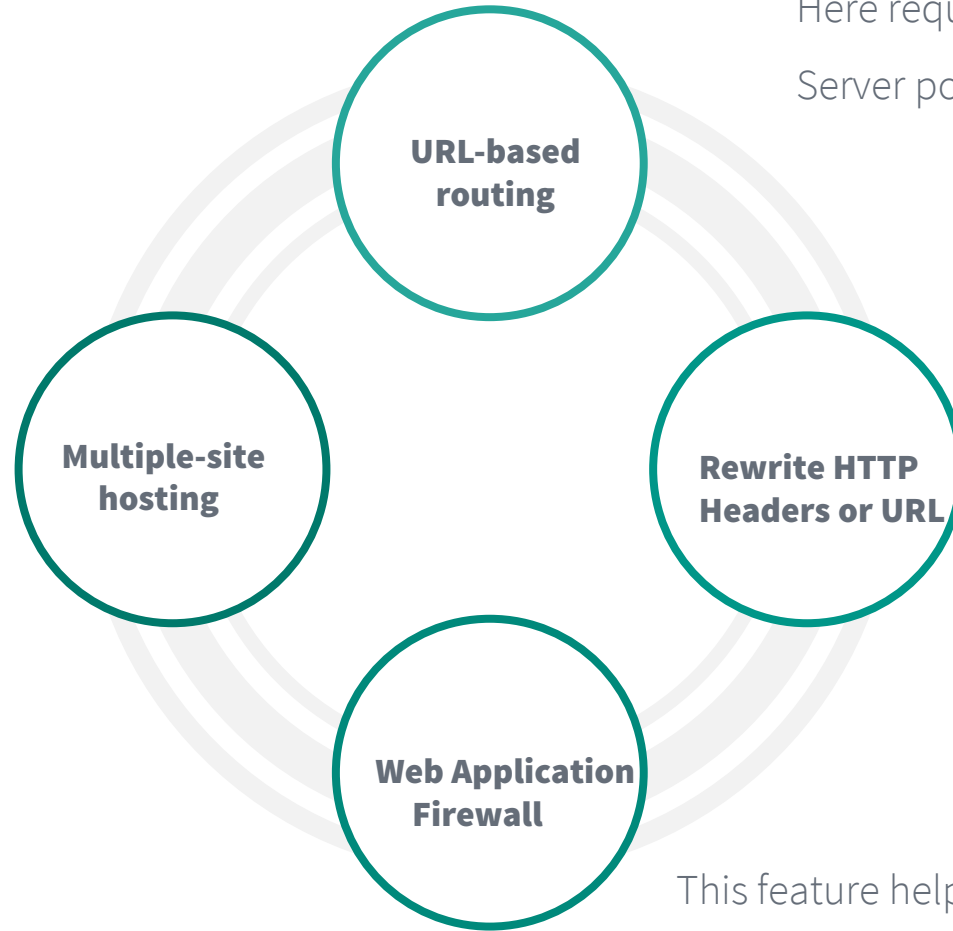
Here you can create rules to
rewrite the headers and URLs.

**Web Application
Firewall**

This feature helps to protect
your web applications.

**Multiple-site
hosting**

Here you can configure
routing based on the host
name or domain name.



Azure Application Gateway components

Frontend IP addresses

This is the IP address that is associated with the Application Gateway



Listeners

This is a logical entity that checks for incoming requests



Request Routing Rule

The rule binds the listener, the back-end server pool and the backend HTTP settings.



HTTP settings

The settings determine how requests are routed to the backend servers.



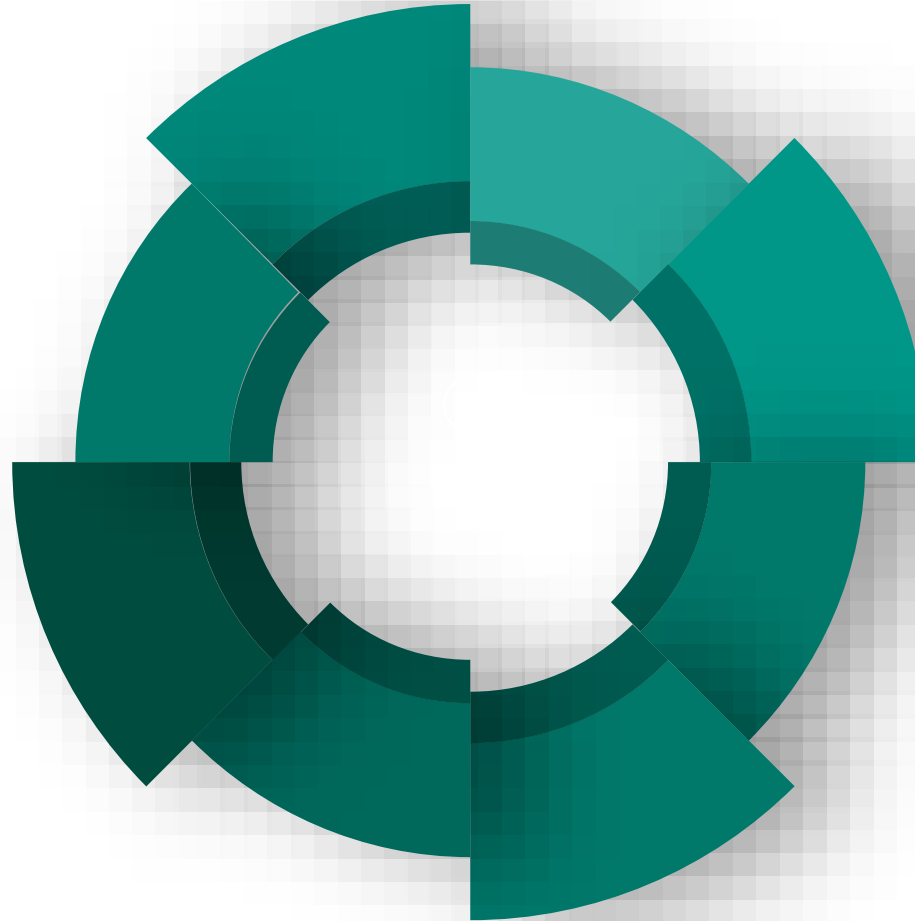
Backend pool

This contains the backend Servers.



Health probes

Here you can define your own custom health probes.



Azure Traffic Manager

Review



Azure Traffic Manager

Priority

Here you can direct users to a secondary endpoint if the primary one fails



Weighted

Here you can assign weights to each endpoint



Performance

Here users can be directed to the closest endpoint with the lowest network latency



Geographic

Here users are directed to endpoints based on their geographic location



Multivalue

Here multiple endpoints are sent to the user.



Subnet

Here the endpoint is decided based on the subnet the user is located in.



Endpoint Types



Azure endpoints

This can be PaaS cloud services, Web Apps, Web App Slots, Public IP Addresses that are assigned to virtual machines. Here the VM's need to also have a DNS name assigned.



External Endpoints

This can be IP addresses or FQDN's that are located outside of Azure.



Nested Endpoints

This can be another Traffic Manager profile

Azure Point-to-Site VPN Connections

REVIEW



Point-to-Site VPN



Secure Connection

Allows clients that run Windows, Linux or macOS to securely connect to an Azure virtual network.



Few clients

This is ideal when you have a few clients that need to connect to the Azure virtual network.



VPN Connection

The VPN connection is created over SSTP(Secure Socket Tunneling Protocol) or IKEv2.



Authentication

You have different authentication methods that can be used – Certificates, Azure AD



Point-to-Site VPN



Gateway subnet

Your virtual network needs to have a Gateway subnet in place. Here the VM's that will manage the VPN will be deployed here.



Certificates

You can use self-signed certificates. The public key of the root certificate is uploaded to the Azure Virtual Network gateway.



Virtual Network Gateway

This allows you to configure the Virtual Network Gateway connection.



Client

Each client needs to have the client certificate installed.



Point-to-Site VPN

Protocols



SSTP

Secure Socket Tunneling Protocol – Developed by Microsoft. Here the encrypted tunnel is created over TCP port 443. Uses SSL/TLS protocol.



IKEv2

Internet Key Exchange uses the IPsec protocol suite to establish a secure connection.



OpenVPN

This is an open standard created to implement secure connections. Used the OpenSSL library.



Azure Site-to-Site VPN Connections

REVIEW



Site-to-Site VPN



Secure Connection

Here the connection is established over IPsec/IKE VPN tunnel.



Public IP Address

The on-premises network needs to have a software or hardware device that has a public routable IP address



On-premises network

Here you connect your entire on-premises network to the Azure virtual network.



Site-to-Site VPN



Gateway subnet

Your virtual network needs to have a Gateway subnet in place. Here the VM's that will manage the VPN will be deployed here.



Local Network gateway

This will be a representation of the on-premises network configuration.



Virtual Network Gateway

This allows you to configure the Virtual Network Gateway connection.



Azure ExpressRoute

REVIEW



Azure ExpressRoute



Connection

Allows you to connect your on-premises networks to Microsoft cloud over a private connection.



Redundancy

Each ExpressRoute circuit has two connections for redundancy purposes.



Private peering

Azure private peering allows you to connect to your Azure virtual network resources.



Microsoft peering

This allows you to connect to public services such as Microsoft 365 and Azure PaaS services.



Azure ExpressRoute



Gateway

Your Azure virtual network needs to have a virtual network gateway in place that is configured to use ExpressRoute.



Global Reach

This allows you to connect your on-premises networks together via their individual ExpressRoute circuits.



FastPath

This improves data path performance between on-premises network and the Azure virtual network. Virtual network gateway – Ultra Performance, ErGw3AZ.



Azure ExpressRoute SKU's



Local

Here the circuit only gives access to one or two Azure regions in or near the same metro. Here you can save on costs. You only have Unlimited billing model.



Standard/Performance

You get more connections per second, better performance. You can connect to any Azure region. You get both Unlimited and Metered billing.



Section

REVIEW



Network Security Groups



Filter traffic

Filter traffic to and from Azure resources in an Azure virtual network.



Rules

Here you can create Inbound and Outbound Network Group Security rules.



Attachment

The Network Security Group can be attached to a network interface or to a subnet.



Default

Each Network Security Group has default rules that can't be edited or deleted.



Network Security Groups Rules

Priority

Here the rules with lower numbers are processed first. Once a matching rule is found, the processing is stopped.



Source/Destination

Can be an IP address, a service tag or an application group.



Protocol

TCP, UDP, ICMP etc.



Port Range

Here you can specify the port range for the traffic.



Direction

Whether it is an Inbound or Outbound rule.



Action

Allow or Deny.



Azure Firewall

Protection

Helps to protect your Azure virtual network resources. It has built-in high availability.



Application rules

You can restrict outbound traffic to fully qualified domain names.



Network rules

You can also limit traffic at the network layer.



Threat Intelligence

Can alert and deny traffic based on known malicious IP addresses and domains.

NAT Rules

Define Network address translation rules for resources in the virtual network.



Forced tunneling

Can route all Internet-bound traffic to a designated next hop instead of directly being routed to the Internet.



Azure Traffic Manager

Review



Azure Traffic Manager

Priority

Here you can direct users to a secondary endpoint if the primary one fails



Weighted

Here you can assign weights to each endpoint



Performance

Here users can be directed to the closest endpoint with the lowest network latency



Geographic

Here users are directed to endpoints based on their geographic location



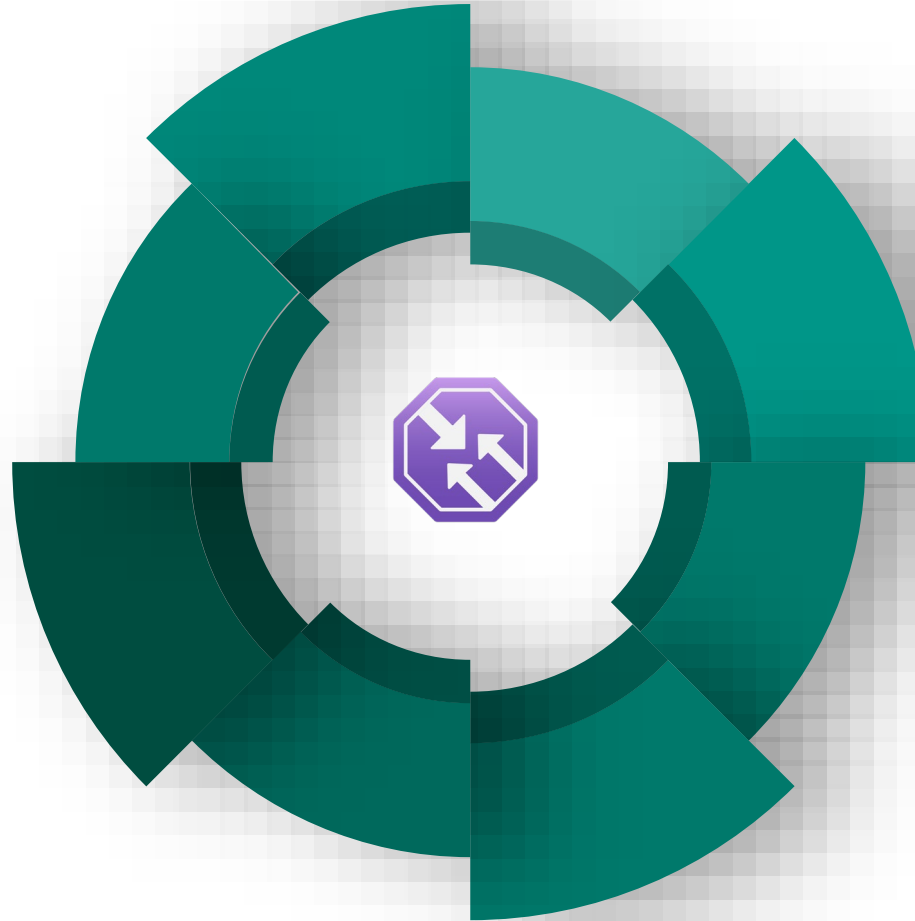
Multivalue

Here multiple endpoints are sent to the user.



Subnet

Here the endpoint is decided based on the subnet the user is located in.



Endpoint Types



Azure endpoints

This can be PaaS cloud services, Web Apps, Web App Slots, Public IP Addresses that are assigned to virtual machines. Here the VM's need to also have a DNS name assigned.



External Endpoints

This can be IP addresses or FQDN's that are located outside of Azure.



Nested Endpoints

This can be another Traffic Manager profile