Microsoft Azure Administrator Associate Training(AZ-104)

Module 7

Agenda

01 Azure Load Balancer

02 Azure Application Gateway

03 Azure Traffic Manager

04 Azure Front Door Service

05 Application Security Groups

06 Azure Firewall

07 Azure Bastion

08 Azure Network Watcher

09 Azure Express Route

10 Express Route Circuits

11 Express Route Peerings

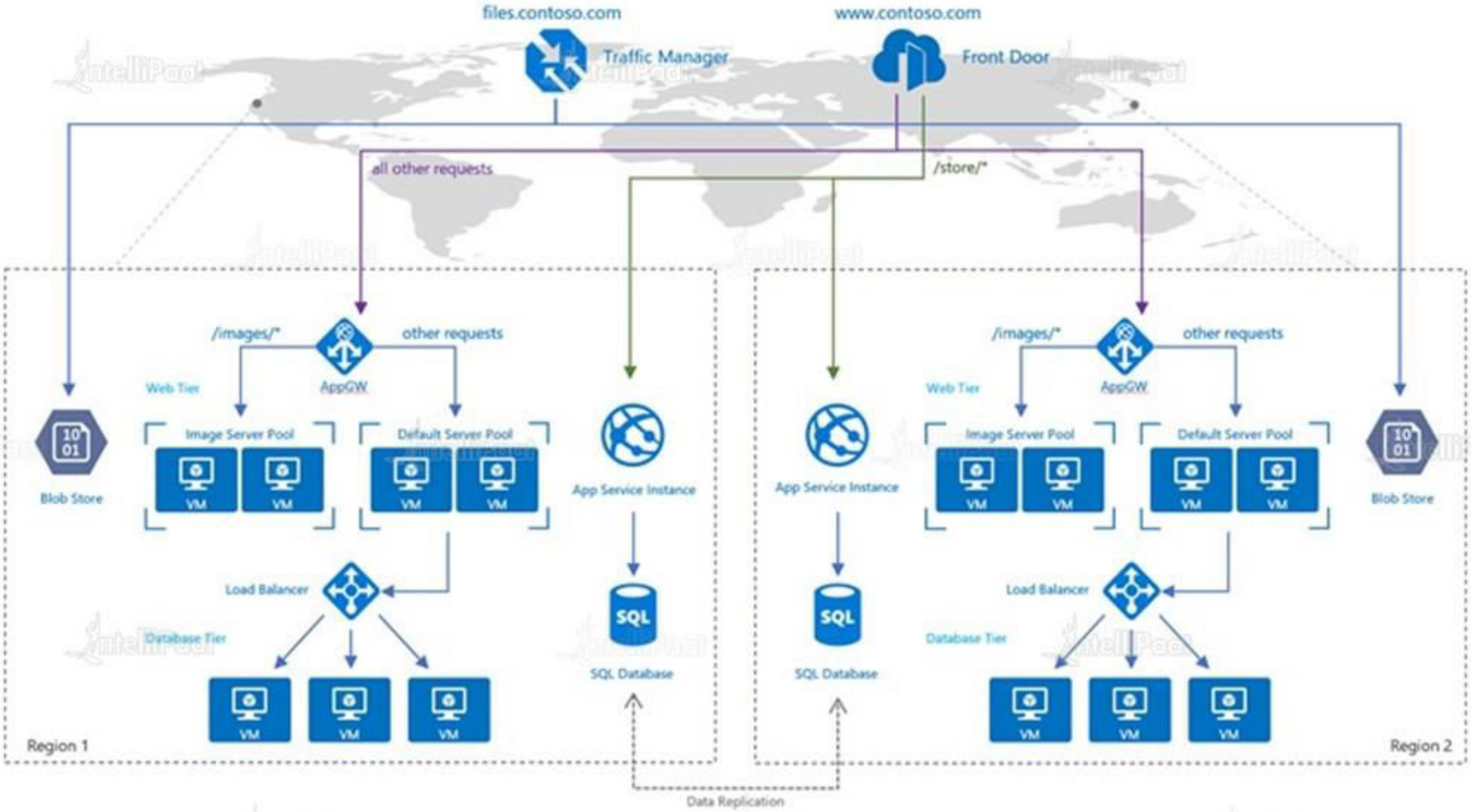
12 Quiz

Azure Load Balancing services Comparison

Comparison Chart

Azure Service	What is it?	OSI Layer	Use Case
Load Balancer	In-region scalability and availability	Layer 4	PaaS.news.com • AppG1 • AppG2 • AppG3
Application Gateway	URL/Content based routing and Load balancing	Layer 7	Cloud.com/recentupdates Cloud.com/blogs
Traffic Manager	Cross-region redirection and availability	DNS Routing	http://Cloud.com • Network.cloud.com • Storage.cloud.com • PaaS.cloud.com
Front Door Service	Cross-region redirection and availability	Layer 7 or HTTP/HTTPS layer and uses anycast protocol with split TCP	http://Cloud.com • Network.cloud.com • Storage.cloud.com • PaaS.cloud.com

Comparison Use Case



Azure Load Balancing services Concepts

Concepts

- **Frontend IP Address**
- **Backend Pool**
- **Health Probe**
- **Load Balancing Rule**

A Frontend IP Address is IP Address that is assigned to the load balancer and is used to access the resources being managed by the load balancer.

Concepts

- Frontend IP Address
- Backend Pool
- Health Probe
- Load Balancing Rule

A Backend Pool is a pool (group) of resources that are being managed by a load balancer. e.g. VM's.

Concepts

- Frontend IP Address
- Backend Pool
- Health Probe
- Load Balancing Rule

A Health Probe is a special signal that is sent to each resource in the backend pool to check if it's healthy and available.

Concepts

- Frontend IP Address
- Backend Pool
- Health Probe
- **Load Balancing Rule**

A load balancing rule is used to associate the frontend IP, backend pool and heath probe together.

Azure Load Balancer

Azure Load Balancer

In Azure, Load Balancers are used to distribute incoming traffic across a pool of resources in order to maintain availability.

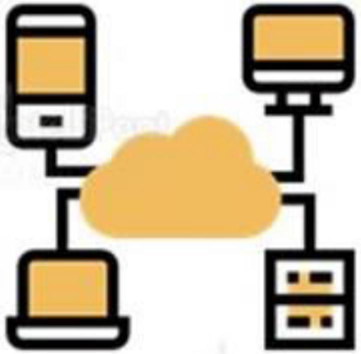
Types of Load Balancers

Types of Load Balancers

There are two types of load balancers in your Azure.

1. Internal Load balancer

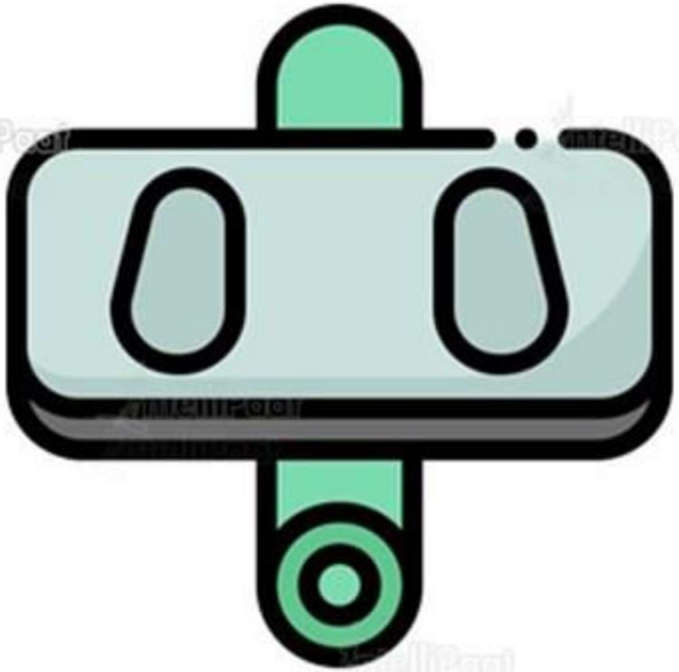
2. Public Load Balancer



Internal Load Balancer

Internal Load Balancer

An Internal Load Balancer is used to direct traffic only between either Azure's internal resources i.e. resources managed by the Azure infrastructure or resources connected to Azure infrastructure using a secure VPN.



Hands-on : Create an Internal Load Balancer

Hands-on

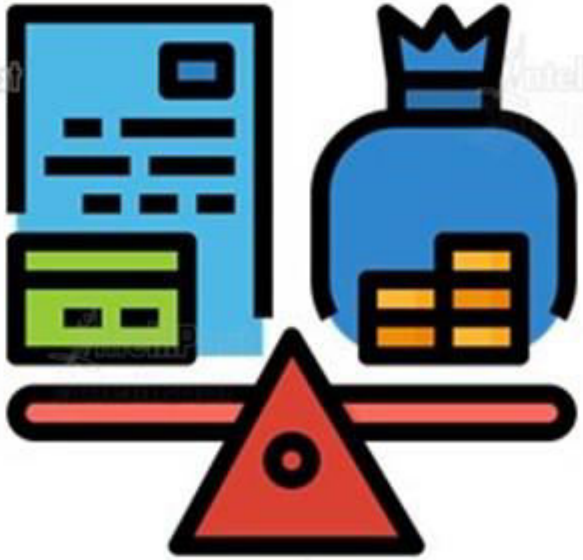
1. Create a Load balancer for an availability set containing two Virtual Machines in the same Virtual Network

2. Verify by using the Load balancer's frontend internal IP Address to access the website from the third VM in the same network

Public Load Balancer

Public Load Balancer

A Public Load Balancer is used to handle traffic between a public facing IP address of incoming traffic to private IP addresses of Azure resources.



Hands-on: Create a Public Load Balancer

Hands-on

1. Create a Public Load Balancer for an availability set with two VMs in the same Virtual Network

2. Connect to the Frontend IP address to check if it's working

Troubleshooting Load Balancer

Troubleshooting Load Balancer

There are two reason why you might have to troubleshoot a load balancer.

1. VM's are not responding to the health probe.

2. VM's are not responding to the traffic.

VM's are not responding to the health probe.

VM’s not responding to the health probe

There may be several reasons for this.

VM’s in the backend pool are unhealthy.

VM’s in the backend pool are not listening on the probe port.

The health probe port is blocked by firewall or NSG.

Misconfiguration in Load Balancer

VM’s not responding to the health probe

There may be several reasons for this.

VM’s in the backend pool are unhealthy.

VM’s in the backend pool are not listening on the probe port.

The health probe port is blocked by firewall or NSG.

Misconfiguration in Load Balancer

VM’s not responding to the health probe

There may be several reasons for this.

- VM’s in the backend pool are unhealthy.
- VM’s in the backend pool are not listening on the probe port.
- The health probe port is blocked by firewall or NSG.
- Misconfiguration in Load Balancer

VM’s not responding to the health probe

There may be several reasons for this.

VM’s in the backend pool are unhealthy.

VM’s in the backend pool are not listening on the probe port.

The health probe port is blocked by firewall or NSG.

Misconfiguration in Load Balancer

VM’s are not responding to the traffic.

VM’s not responding to the traffic.

There may be several reasons for this.

VM’s in backend pool are not listening on the data port

Data port is being blocked by NSG

Accessing the Load Balancer from the same VM and NIC

Accessing the internal Load Balancer frontend from the participating VM in the same backend pool.

VM's not responding to the traffic.

There may be several reasons for this.

VM's in backend pool are not listening on the data port

Data port is being blocked by NSG

Accessing the Load Balancer from the same VM and NIC

Accessing the internal Load Balancer frontend from the participating VM in the same backend pool.

VM’s not responding to the traffic.

There may be several reasons for this.

VM’s in backend pool are not listening on the data port

Data port is being blocked by NSG

Accessing the Load Balancer from the same VM and NIC

Accessing the internal Load Balancer frontend from the participating VM in the same backend pool.

VM's not responding to the traffic.

There may be several reasons for this.

VM's in backend pool are not listening on the data port

Data port is being blocked by NSG

Accessing the Load Balancer from the same VM and NIC

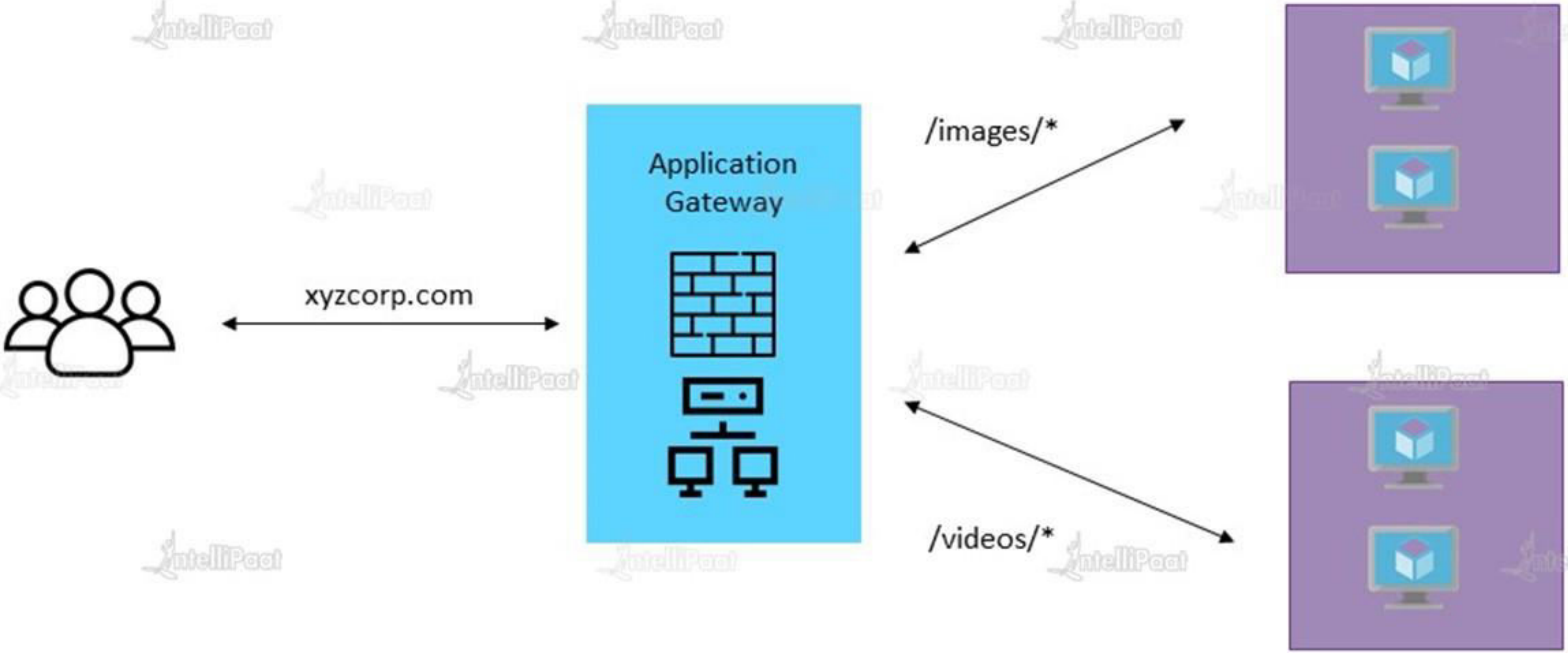
Accessing the internal Load Balancer frontend from the participating VM in the same backend pool.

Azure Application Gateway

Azure Application Gateway

Application gateway is a service provided by Microsoft azure that is based on path based routing to manage the traffic to your azure resources.

Application Gateway – Path Based Routing



Application Gateway - Features

- URL Based Routing
- Web Application Firewall
- Custom Error pages
- Secure Socket Layer Termination

Routing of traffic to back end server pools based on the URL path requests

Application Gateway - Features

- URL Based Routing
- Web Application Firewall
- Custom Error pages
- Secure Socket Layer Termination

Service provided by an application gateway that serves as a centralized protection of the web applications from general vulnerabilities

Application Gateway - Features

URL Based Routing

Web Application Firewall

Custom Error pages

Secure Socket Layer Termination

Custom error pages may be created here instead of showing the default Microsoft error pages.

They are supported for the following two scenarios

1. Maintenance pages – Custom error is sent instead of 502 bad page.
2. Unauthorized Access Page – Error page is sent insteadd of a 403 unauthorized access page

Application Gateway - Features

- URL Based Routing
- Web Application Firewall
- Custom Error pages
- **Secure Socket Layer Termination**

Application gateway provides a service for the traffic to flow unencrypted to the backend servers, this is by supporting SSL/TLS termination at the gateway

Hands on - Application Gateway

Hands-on

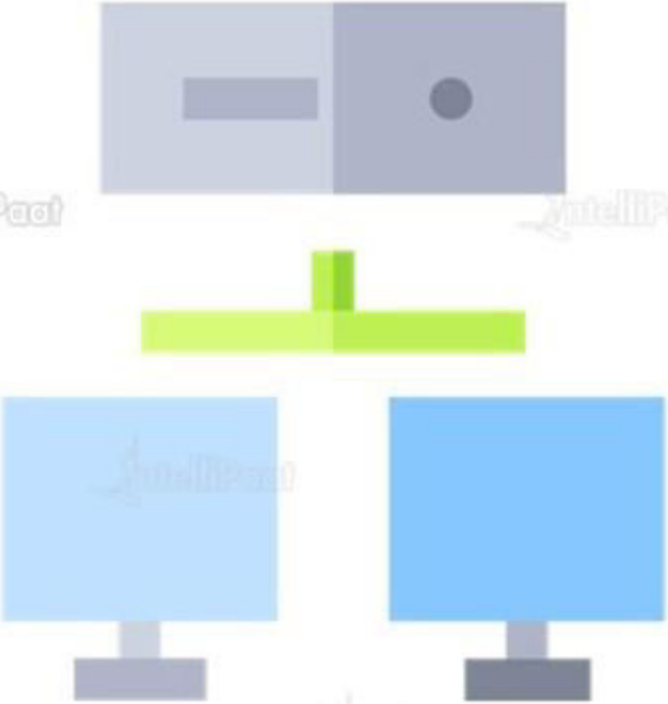
1. Configure Application gateway to enable path-based routing for two Virtual Machines

2. Check the path-based routing

Azure Front Door Service

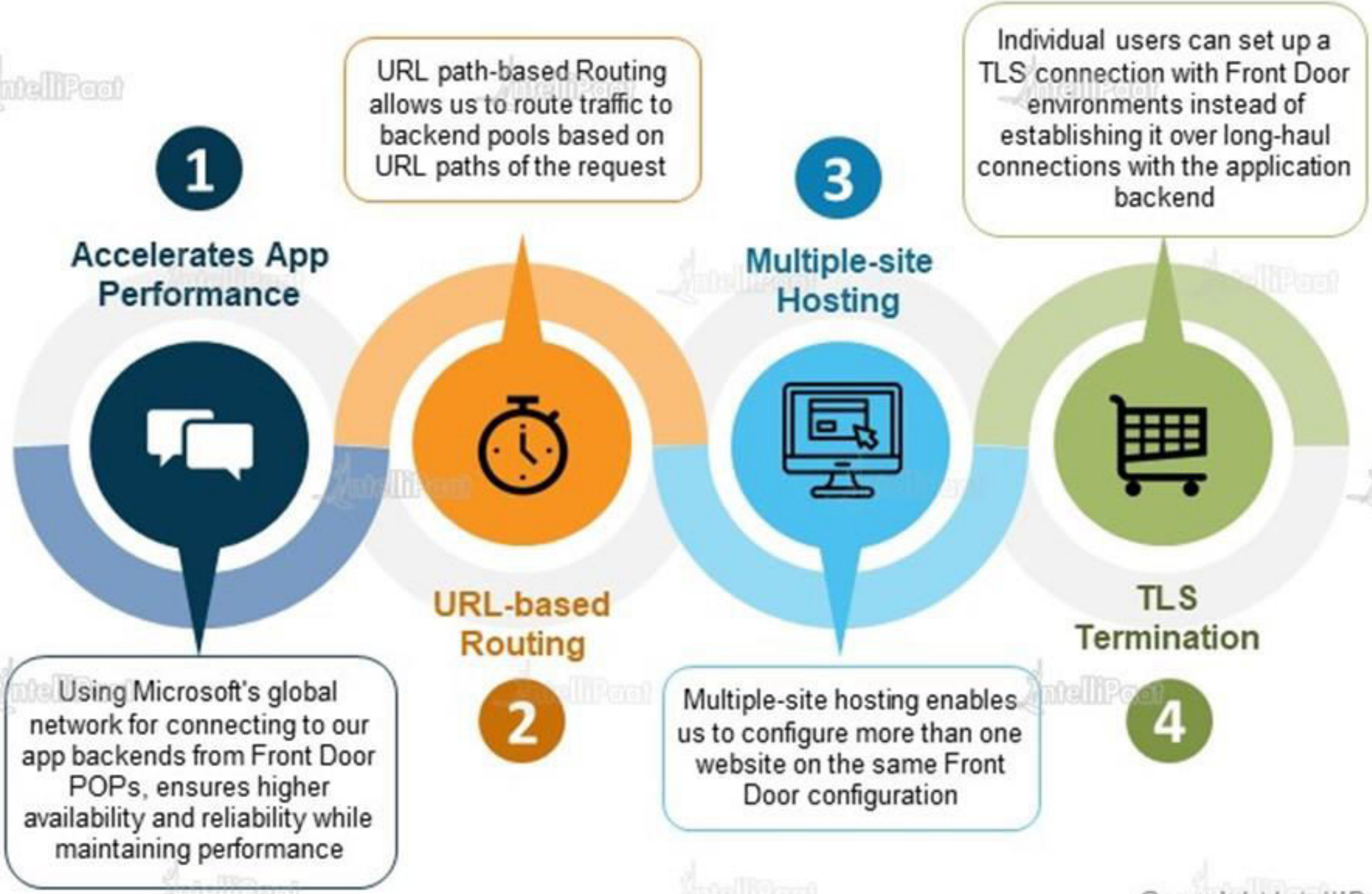
Azure Front Door Service: An Overview

Azure Front Door is a service offered by Azure that generates Layer 7 load-balancing capabilities for our applications



What is Azure Front Door Service?

IntelliPaat



1

Accelerates App Performance

Using Microsoft's global network for connecting to our app backends from Front Door POPs, ensures higher availability and reliability while maintaining performance

2

URL-based Routing

URL path-based Routing allows us to route traffic to backend pools based on URL paths of the request

3

Multiple-site Hosting

Multiple-site hosting enables us to configure more than one website on the same Front Door configuration

4

TLS Termination

Individual users can set up a TLS connection with Front Door environments instead of establishing it over long-haul connections with the application backend

Azure Front Door vs Application Gateway

Front Door

Application Gateway

Both Front Door and Application Gateway are **Layer 7 (HTTP/HTTPS) load balancers**. However, there are minor differences between the two that set them apart

- Front Door is a **global service**
- Front Door can load balance between our different-scale units/clusters/stamp units across regions

- Application Gateway is a **regional service**
- Application Gateway allows us to load balance between our VMs/containers ,etc., i.e., within the scale unit

Hands-on: Azure Front Door Service

Hands-on

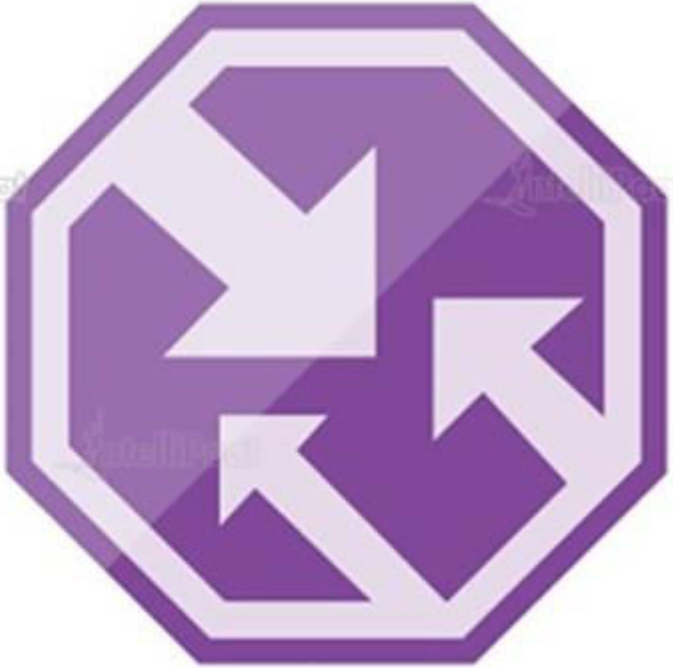
1. Deploy a Front Door service in the Azure portal with two Virtual Machines in the Backend pool and a routing rule

2. Verify the routing using the Frontend address of the Front Door Service

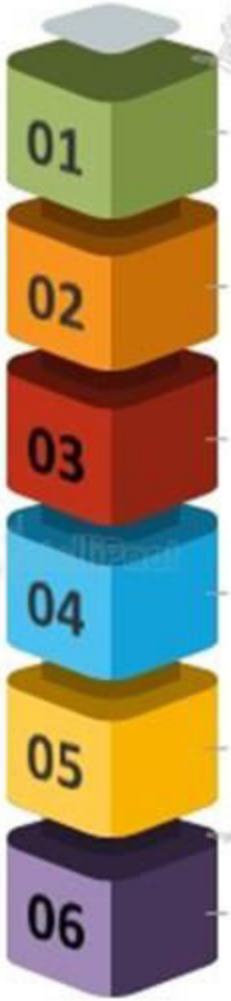
Azure Traffic Manager

What is Azure Traffic Manager?

Azure Traffic Manager is a **DNS-based load balancer** that allows us to distribute traffic optimally—while providing high availability and responsiveness across global Azure regions



Azure Traffic Manager: Routing Methods



Priority

It is used when the primary service endpoint is used for most of the times; backup is provided if the primary or backup endpoints are unavailable

Weighted

It is used to distribute traffic across a set of endpoints; this may be done evenly or according to the weight assigned

Performance

This works in accordance with the lowest network latency. If we have endpoints in different geographical locations, the 'closest' one is chosen

Geographic

Users are directed to specific endpoints (Azure, External, or Nested) based on the geographic location from where their DNS queries originate

Multivalue

The multivalue routing method is used for Traffic Manager profiles that can only have IPv4/IPv6 addresses as endpoints

Subnet

It is a traffic-routing method to map sets of end-users' IP address ranges to a specific endpoint within a Traffic Manager profile

Why do we need a Traffic Manager?

A Traffic Manager offers the following features:

01 Increases application availability

02 Improves application performance

03 Performs service maintenance without any downtime

Hands-on: Traffic Manager Profiles

Hands-on

1. **Configure traffic manager to enable traffic distribution for two endpoints**

2. **Verify the traffic manger based on the conditions**

Application Security Groups

Application Security Groups: An Overview

Application Security Groups allow us to create groups of virtual machines defined under the same network security group. It basically enables us to configure network security as an extension of the application's architecture

Azure Firewall

Azure Firewall

Azure firewall is a service provided by azure that is build to protect the azure virtual network resources.
It is a cloud based service that provides:

Built-in high availability

To increase the availability of resources, azure firewall spans multiple availability zone. This increases the uptime to 99.99%

Unrestricted cloud scalability

During peak traffic, There may be a need to accommodate changing network traffic flows. Azure firewall scales up to however much you need to without any extra budget.

Azure Firewall

Azure firewall is a service provided by azure that is build to protect the azure virtual network resources.
It is a cloud based service that provides:

Built-in high availability

To increase the availability of resources, azure firewall spans multiple availability zone. This increases the uptime to 99.99%

Unrestricted cloud scalability

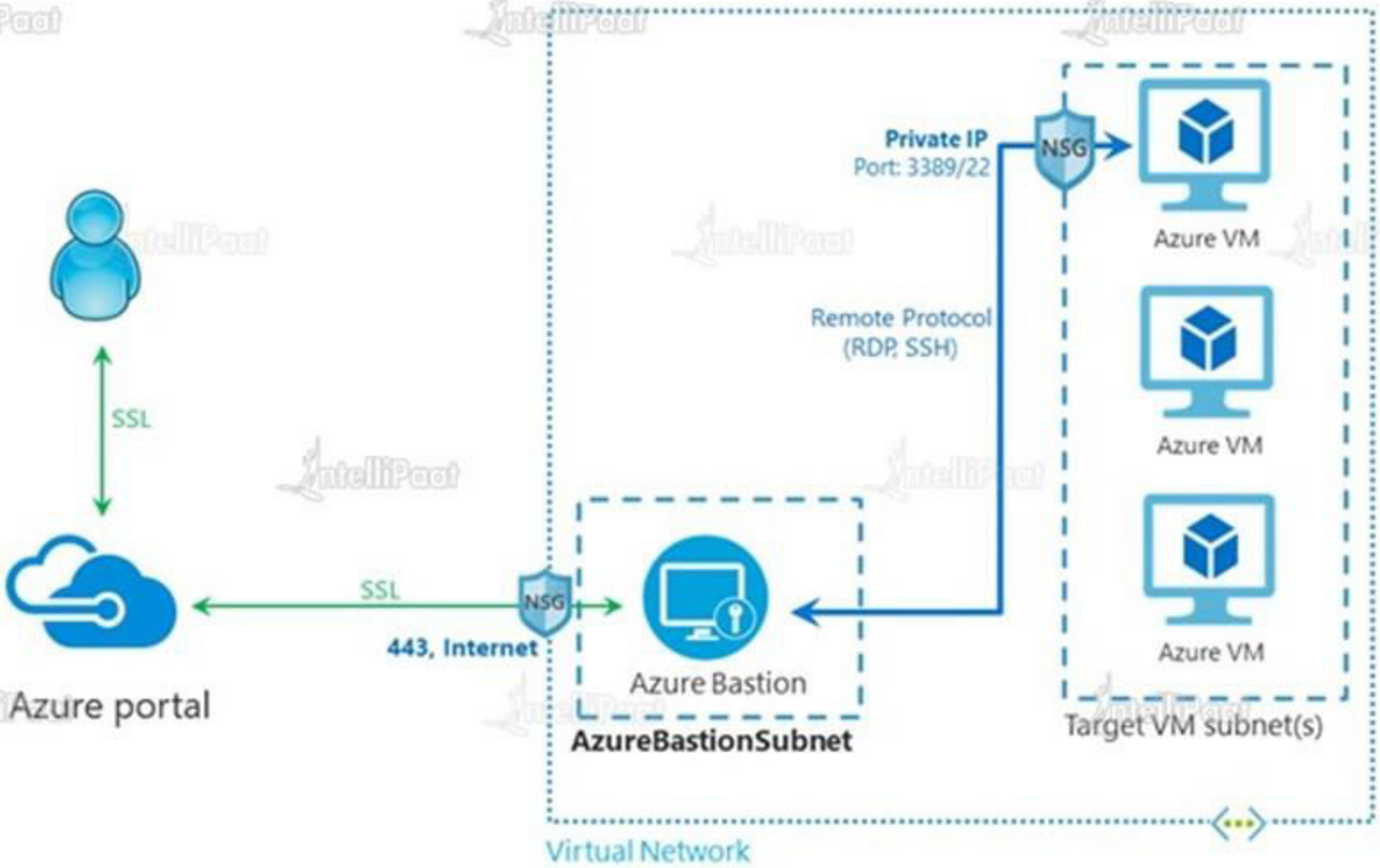
During peak traffic, There may be a need to accommodate changing network traffic flows. Azure firewall scales up to however much you need to without any extra budget.

Azure Bastion

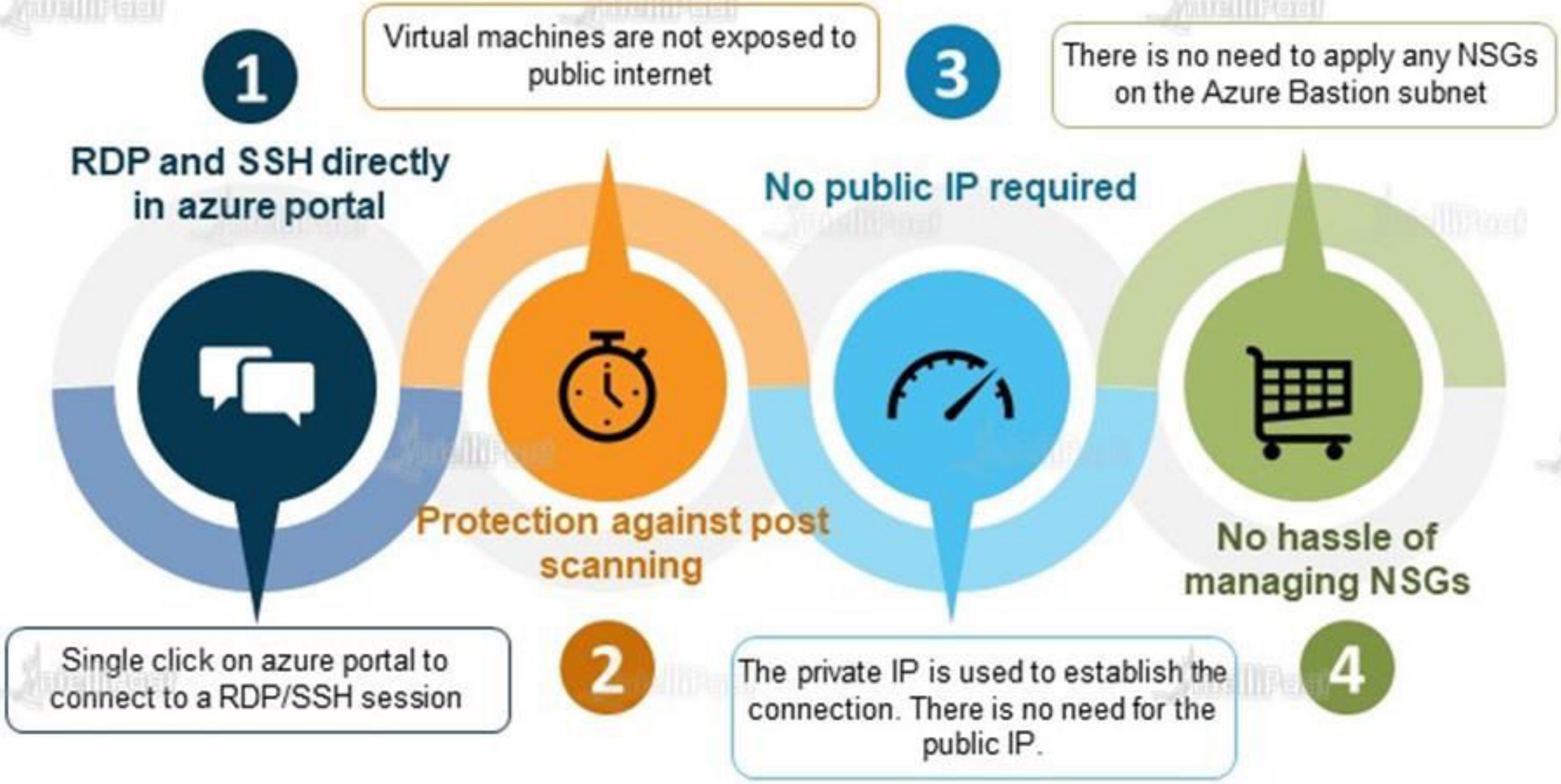
What is Azure Bastion?

Azure Bastion is a PaaS service that provides you RDP/SSH connectivity to the virtual machines directly in the azure portal over SSL such that the RDP/SSH ports are not exposed to the outside world without the need of an additional client or software.

Azure Bastion Architecture



Azure Bastion Features



1

RDP and SSH directly in azure portal

Single click on azure portal to connect to a RDP/SSH session

2

Protection against post scanning

Virtual machines are not exposed to public internet

3

No public IP required

The private IP is used to establish the connection. There is no need for the public IP.

4

No hassle of managing NSGs

There is no need to apply any NSGs on the Azure Bastion subnet

Hands-on: Bastion

Hands-on

1. Deploy a Bastion subnet in the Virtual Machine Virtual Network

2. Connect to the Virtual Machine using the Bastion host service

What Is Azure Network Watcher?

What Is Azure Network Watcher?

Azure Network Watcher is a service that contains multiple tools used to diagnose and monitor our Azure Networks.

Azure Network Watcher Features

Azure Network Watcher Features

- Monitoring
- Diagnostics
- Metrics
- Logs

Network Watcher allows us to monitor traffic between virtual machines and other endpoints. Such as Virtual Machines, URI's etc.

Azure Network Watcher Features

Monitoring

Diagnostics

Metrics

Logs

Azure Network Watcher allows us to diagnose problems related to filtering, routing, connectivity etc.

Azure Network Watcher Features

- Monitoring
- Diagnostics
- **Metrics**
- Logs

In Network Watcher we can analyze how many of each network resource we have deployed in a region and what the current limit is.

Azure Network Watcher Features

Monitoring

Diagnostics

Metrics

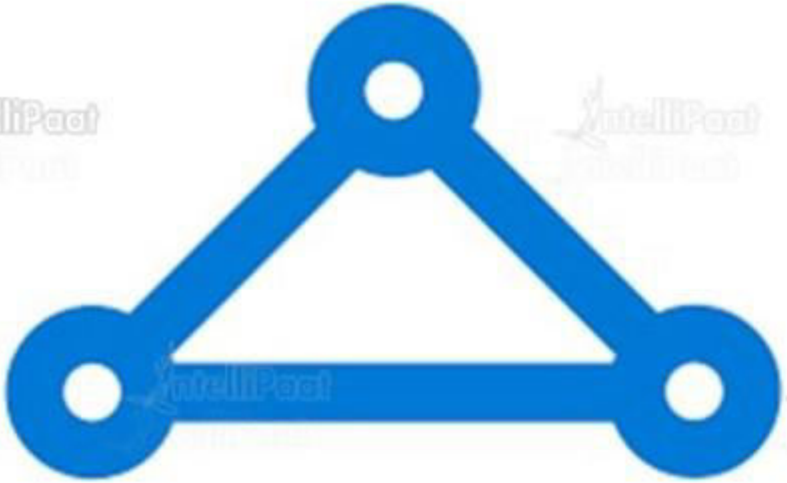
Logs

In Network Watcher we analyze log files for our Network Security Groups and diagnostic logs for network resources.

Why Azure Express Route

Why Azure Express Route

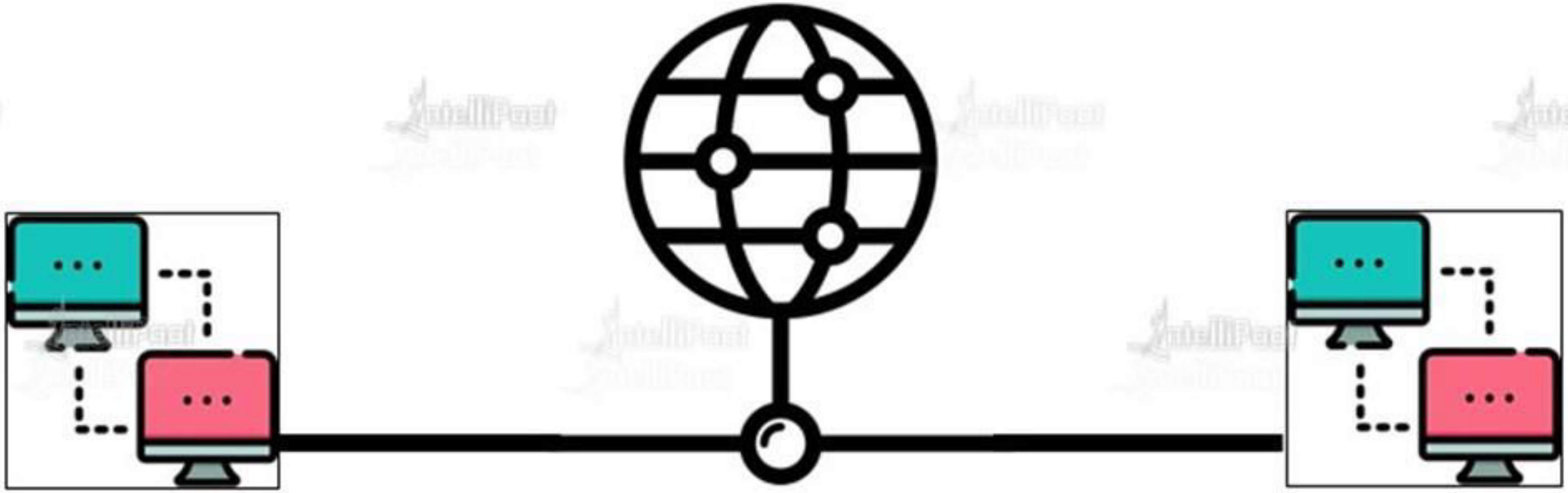
Azure Express Route enables you to connect your on premises network to Azure Cloud privately with low latency.



What is Azure Express Route

What is Azure Express Route

Microsoft Azure Express Route allows us to connect our on premises network to Microsoft Cloud services like Azure, Office 365 etc. using a private connection established via a connection provider.



Azure Express Route Benefits

Azure Express Route Benefits

- **Secure**
- **Fast**
- **Cloud Services**
- **Flexible Billing**

Express Route creates a private connections between Microsoft datacenters and infrastructure.

Azure Express Route Benefits

- Secure
- **Fast**
- Cloud Services
- Flexible Billing

Express Route supports bandwidth up to 10Gbps

Azure Express Route Benefits

- Secure
- Fast
- Cloud Services
- Flexible Billing

Express Route connections can be used to access: Microsoft Azure services, Microsoft Office 365 services, Microsoft Dynamics 365

Azure Express Route Benefits

- Secure
- Fast
- Cloud Services
- **Flexible Billing**

Express Route supports the following billing system: Unlimited data, Metered Data.

Azure Express Route Components

Azure Express Route Components

Azure Express Route has two major components.

1. Circuits

2. Peering

Express Route Circuits

Express Route Circuits

An Express Route circuit is a logical connection between your on-premises network and Microsoft cloud services through a connectivity provider.

An Express Route circuit is identified and referenced by a unique identifier called a Service Key.

Each circuit has a fixed bandwidth that is shared by all the network peerings.

Express Route Peerings

Express Route Peerings

A Peering is an connection between two separate networks.

Each Express Route Circuit has three types of peering associated with it: Azure Public, Azure Private and Microsoft Peering

Types of Express Route Peering

Types of Express Route Peering

Private

Microsoft

Public

Private peering is used to connect to Azure compute services like virtual machines, cloud services etc. that are deployed in your VNet.

Types of Express Route Peering

Private

Microsoft

Public

Microsoft Peering is used to connect to Microsoft online services like Office 365, Dynamic 365 etc.

Types of Express Route Peering

Private

Microsoft

Public

Public peering is used to connect to service like Azure Storage, SQL databases, Websites etc. Public peering is deprecated for new circuits and it is advised that you use Microsoft peering in its place.

IntelliPaat

India: +91-7847955955

US: 1-800-216-8930 (TOLL FREE)

support@intellipaat.com

24/7 Chat with Our Course Advisor