Caltech | Center for Technology & Management Education

Post Graduate Program in Cloud Computing

Powered by simplilearn

Caltech | Center for Technology & Management Education

PG CC - Microsoft Azure Architect Technologies: AZ:303

Powerd by simplilearn

Implement Load Balancing and Network Security

A Day in the Life of an Azure Architect

You are working for an organization as an Azure Architect that uses load balancers that distribute incoming traffic to a web application based upon the availability.

These load balancers work with traditional on-premise servers where the application is running on instances and a load balancer is sitting in front of these servers and distributing load to them, based on some predefined algorithm and connection affinity settings.

Now the organization is planning to migrate to the cloud and needs to understand how they can achieve the same load balancing using Azure components.

A Day in the Life of an Azure Architect

- You have been asked to advise a solution that can help achieve load balancing in cloud applications that requires much more thought than having a simple load balancer in front of some servers, as we could have services hosted on PaaS, we should have services running on separate instances for various workloads and applications running on multiple servers that are geographically distributed across the world.
- Also, your company is looking for a solution that can help manage traffic to your Web Application.

To achieve all of the above along with some additional features, we will be learning a few concepts in this lesson that will help you find a solution for the given scenario.

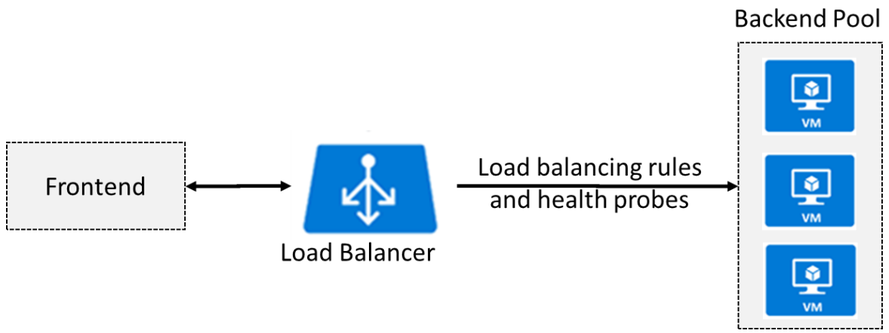
Learning Objectives

By the end of this lesson, you will be able to:

- Implement Azure Load Balancer and Application Gateway
- Configure a Web Application Firewall
- Illustrate the Azure Front Door
- Implement a Network and Application Security Group

Azure Load Balancer

Azure Load Balancer



- Distributes inbound traffic to backend resources
- Uses both inbound or outbound scenarios
- Protects on-premise web applications with secure remote access
- Extends Active Directory to the cloud

Azure Load Balancer

Public Load Balancer

Internal Load Balancer

The two types of Azure load balancers are:

Public Load Balancer

- Maps public IP addresses and port number of incoming traffic to the VM's private IP address and port number and vice versa.
- Applies load balancing rules to distribute traffic across Virtual Machines (VMs) or services.

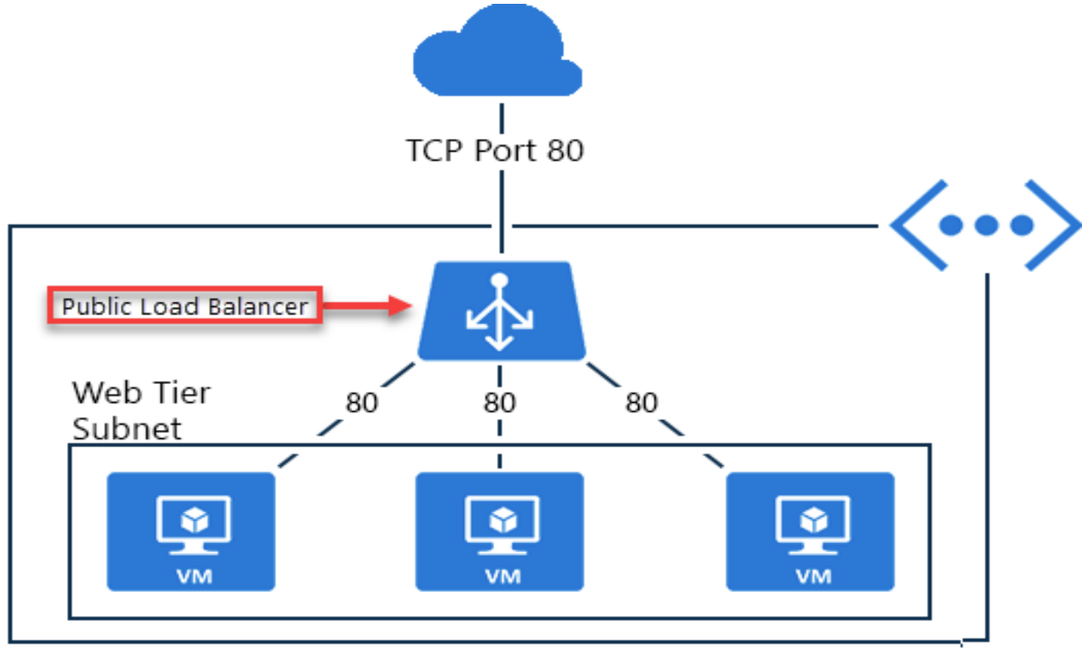


image source: https://docs.microsoft.com/en-in/

Internal Load Balancer

- Directs traffic only to resources inside a virtual network or to resources that use a VPN to access the Azure infrastructure
- Enables load balancing within a virtual network, for cross-premises virtual networks, multi-tier applications, and line-of-business applications

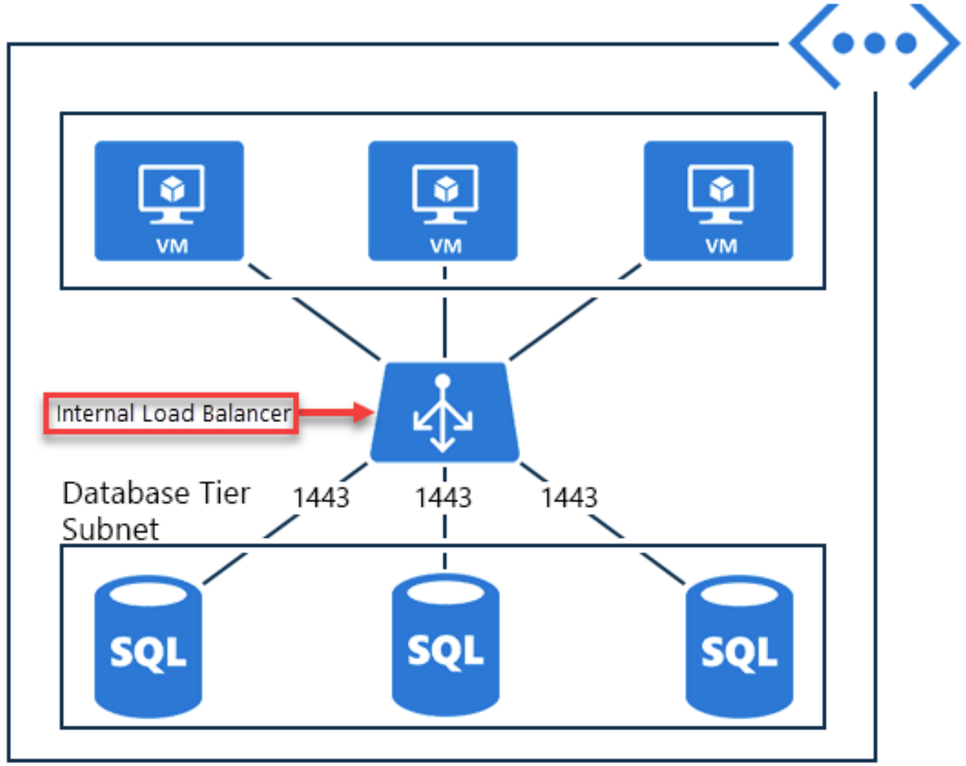


image source: https://docs.microsoft.com/en-in/

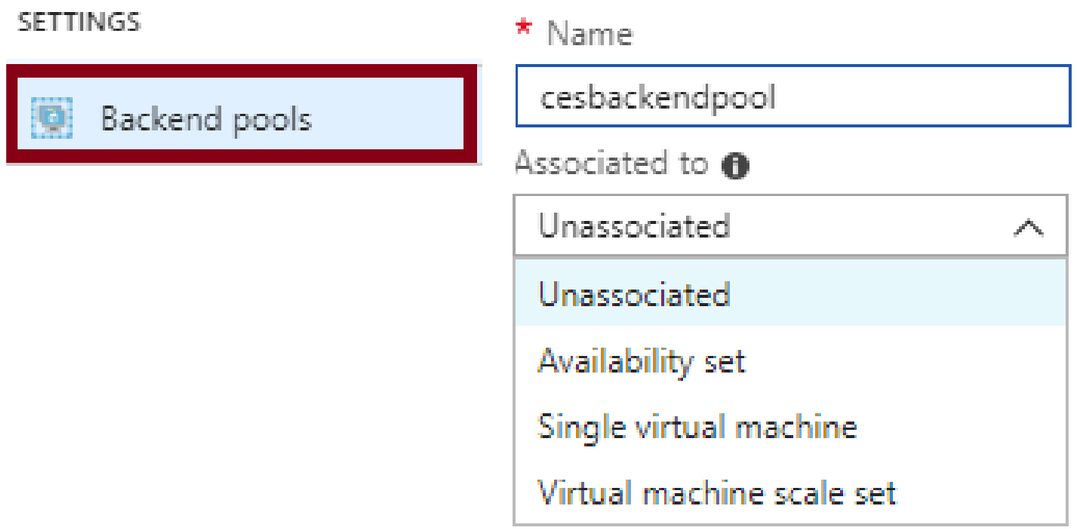
Load Balancer SKUs

- Load balancer supports both basic and standard (newer) SKUs
- SKUs are not mutable
- Load balancer rule cannot span two virtual networks
- Load balancer front-ends are not accessible across global Virtual Network peering

Backend Pools

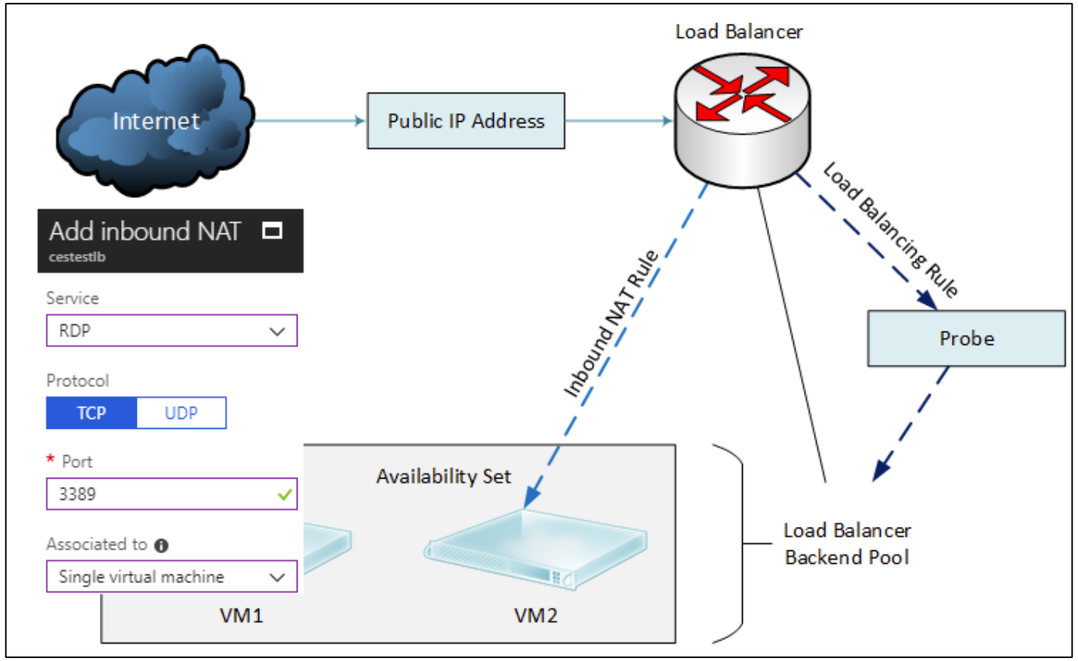
To distribute the traffic, a backend address pool contains the IP addresses of the virtual NICs that are connected to the load balancer.

SKU	Backend pool endpoints
Basic SKU	VMs in a single availability set or VM scale set.
Standard SKU	Any VM in a single virtual network, including a blend of VMs, availability sets, and VM scale sets.



Load Balancer Rules

- Maps a frontend IP and port combination to a set of backend IP addresses and port combinations.
- Rules can be used in combination with NAT rules.

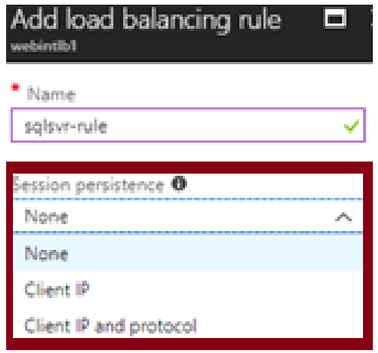


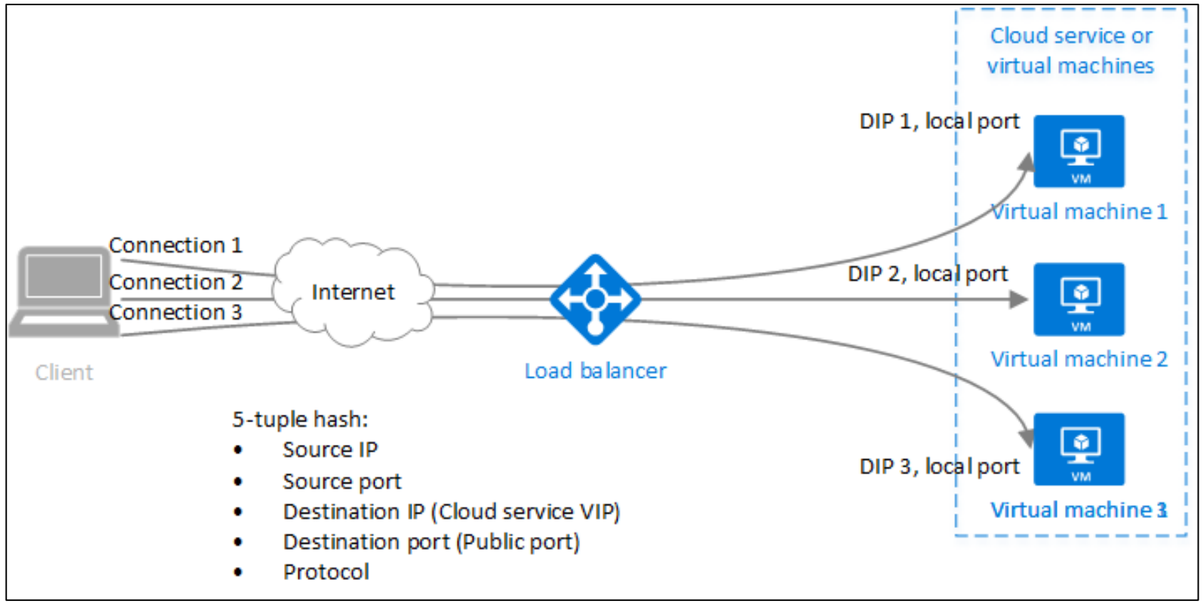
A NAT rule is explicitly attached to a VM (or a network interface) to complete the path to the target.

image source: https://docs.microsoft.com/en-in/

Session Persistence

Session persistence specifies how the client traffic is handled.





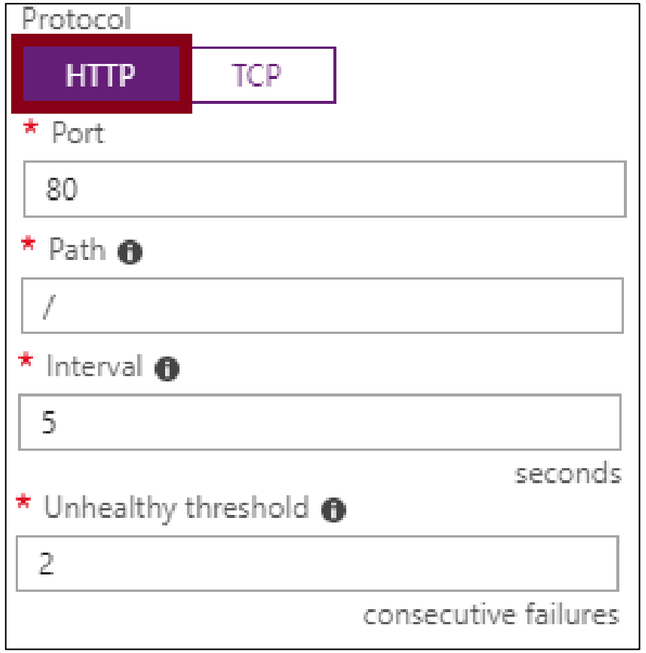
- Client IP requests can be handled by any virtual machine.
- Client IP and protocol specifies that successive requests from the same address and protocol will be handled by the same virtual machine.

image source: https://docs.microsoft.com/en-in/

Health Probes

- Allows the load balancer to monitor the status of an app
- Adds or removes VMs from the load balancer rotation, based on their response to health checks

- HTTP custom probe pings every 15 seconds
- TCP custom probe tries to establish a successful TCP session



Assisted Practice

Creating a Load Balancer

Duration: 10 Min.

Problem Statement:

You've been tasked with developing a load balancer that will distribute incoming traffic to a web application. To execute this operation, you can use an internal or external load balancer.

Assisted Practice: Guidelines

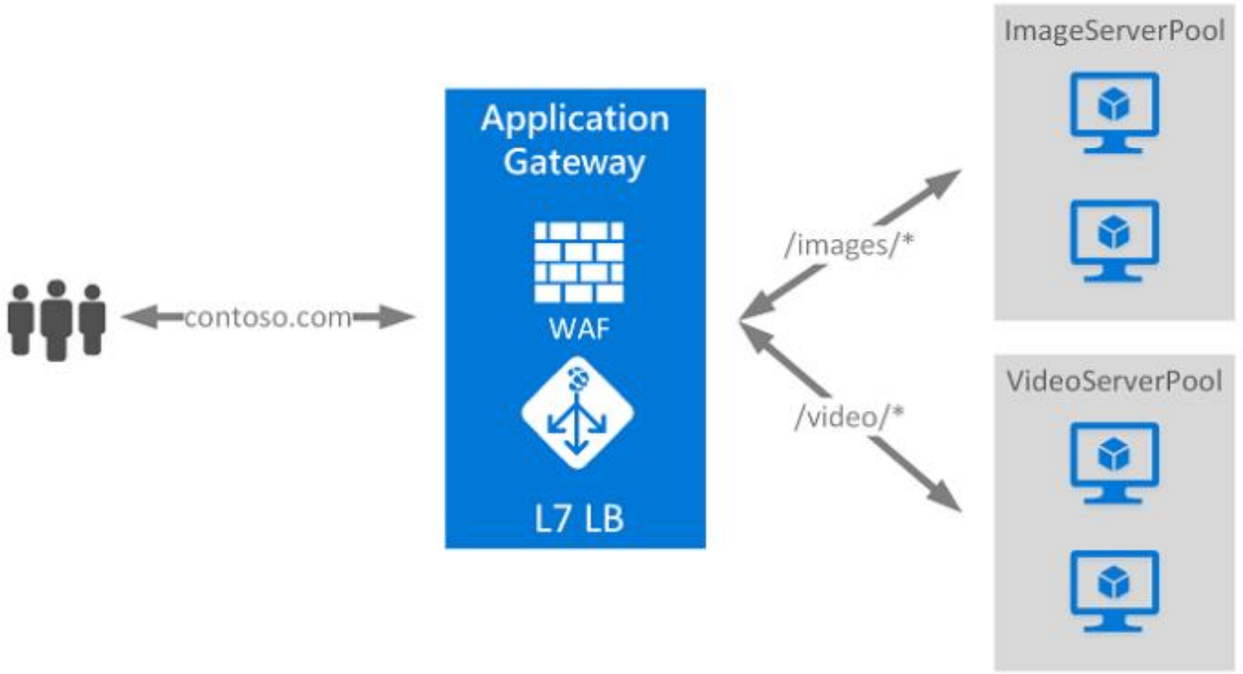
Steps to create a load balancer:

1. Go to the Azure portal
2. Click Create a resource
3. Select Networking, and click on Load Balancer
4. Create the Load Balancer

Azure Application Gateway

Application Gateway

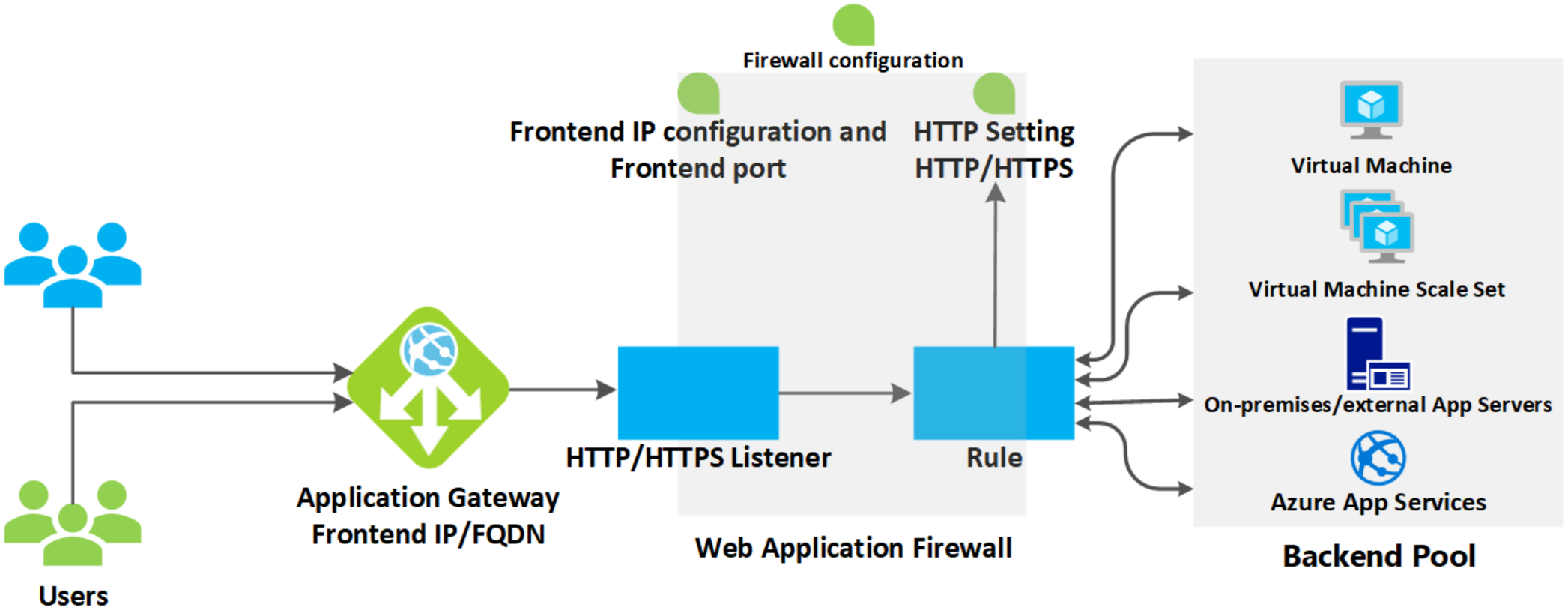
- It manages the requests that client applications can send to a web app.
- It routes the traffic to a pool of web servers, based on the URL of a request.



Source: https://docs.microsoft.com/en-us/azure/application-gateway/overview

Application Gateway

The following workflow shows how an application gateway accepts a request:



Source: https://docs.microsoft.com/en-us/azure/application-gateway/how-application-gateway-works

Application Gateway

Frontend port and listener

Backend pool

The components of an application gateway are:

Frontend Port and Listener

- Traffic enters the gateway through a frontend port.
- Listener is set up to listen for a specific host name and a specific port for a specific IP address.

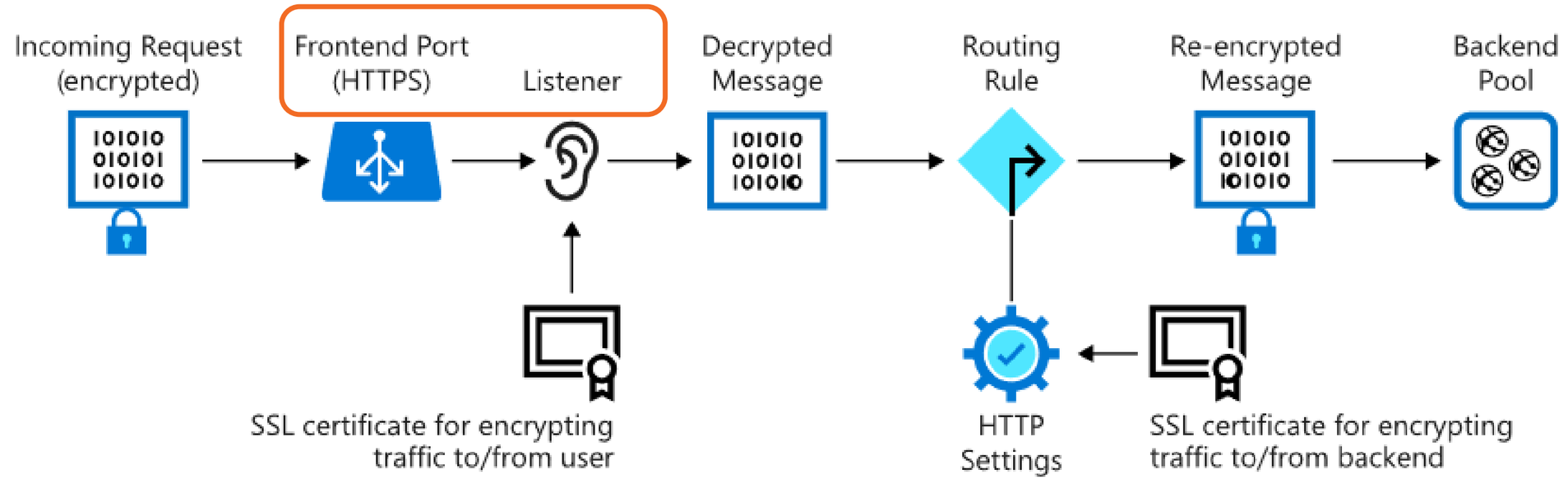
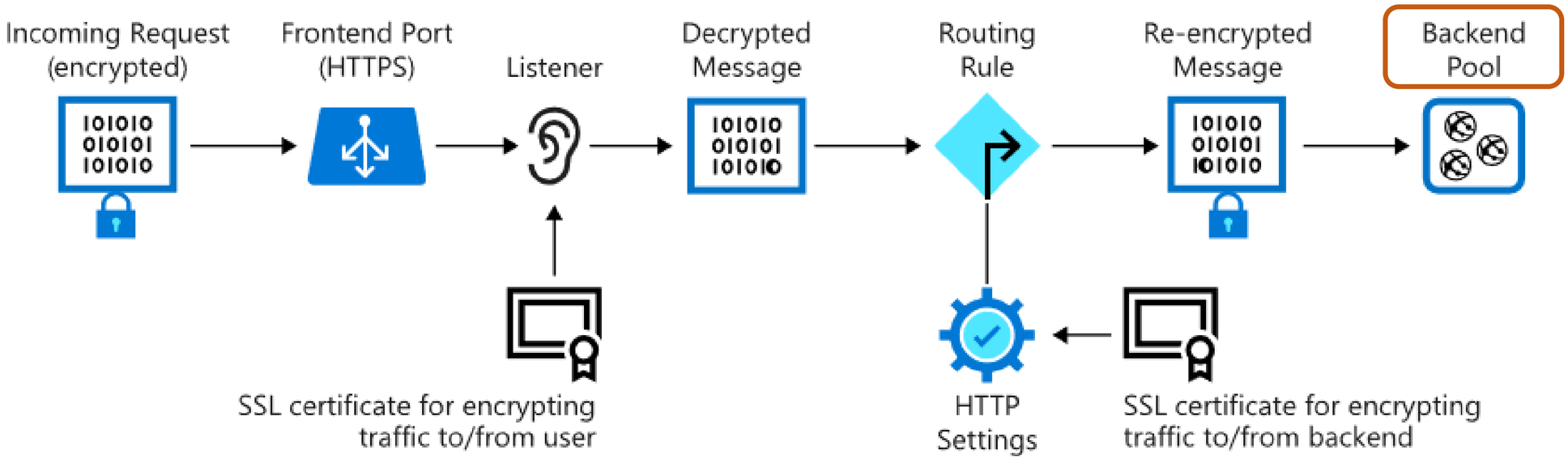


image source: https://docs.microsoft.com/en-in/

Backend Pool

The backend pool contains the application servers.



These servers might be virtual machines, a virtual machine scale set, or applications running on Azure App Service.

image source: https://docs.microsoft.com/en-in/

Application Gateway

The gateway routes the clients requests to a selected web server in the backend pool using a set of rules.

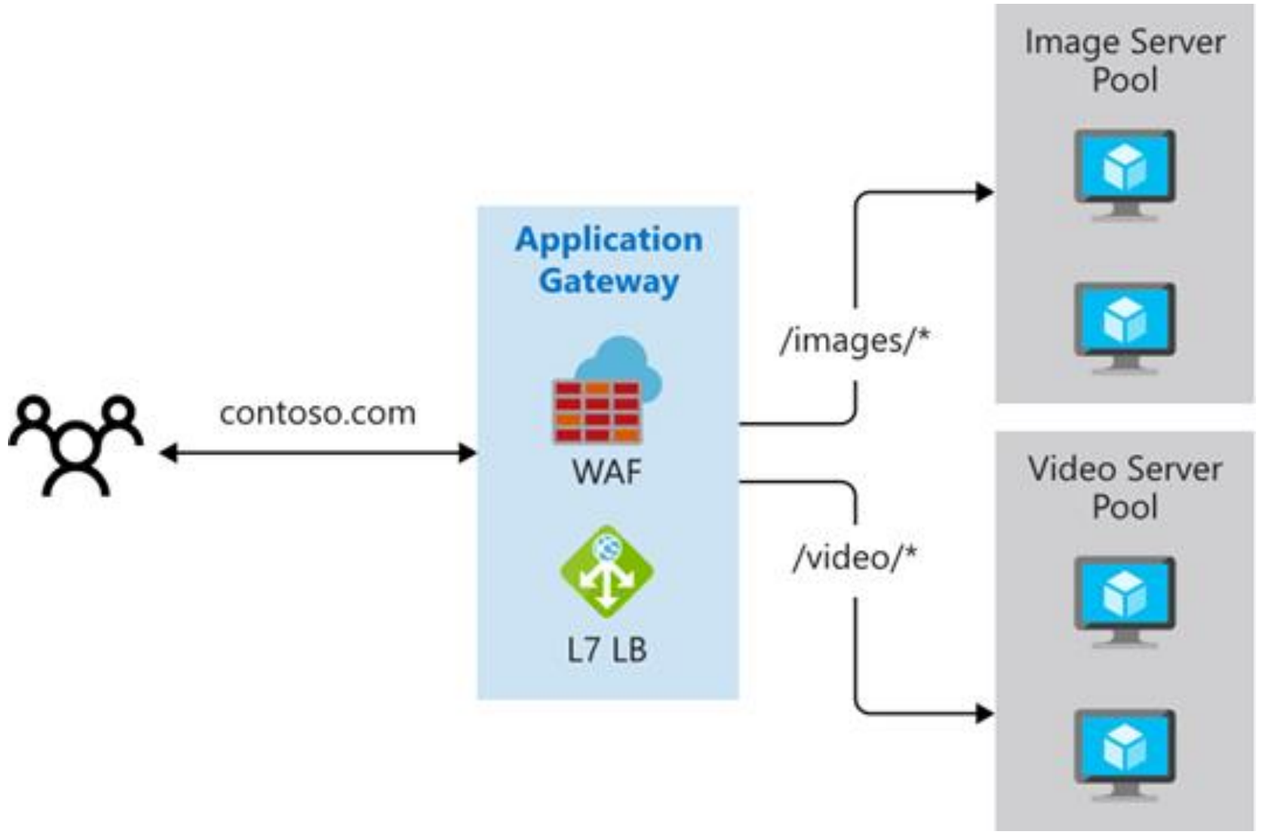
Path-based routing

Multiple site routing

The routing methods are:

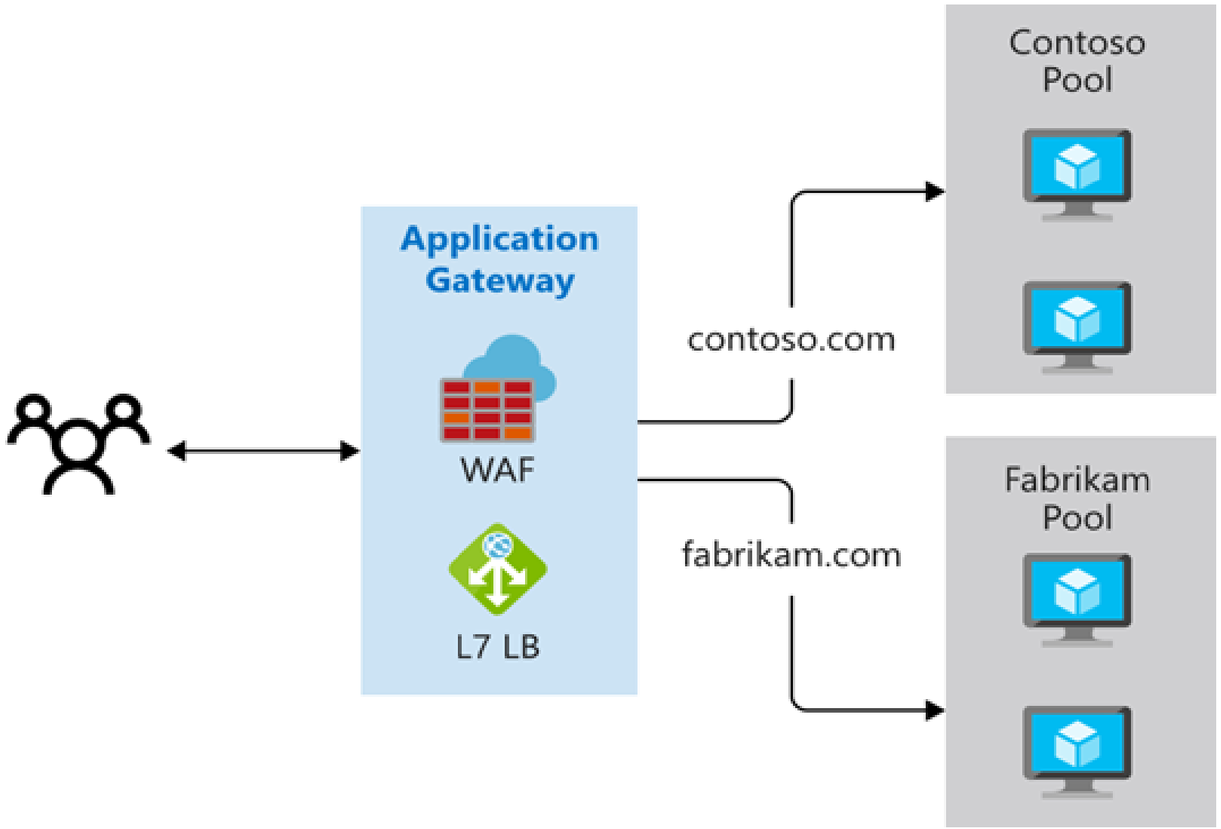
Path-based Routing

Path-based routing enables the user to send requests with different paths in the URL to a different pool of backend servers.



Multiple Site Hosting

Multiple site hosting enables the user to configure more than one web application on the same application gateway instance.

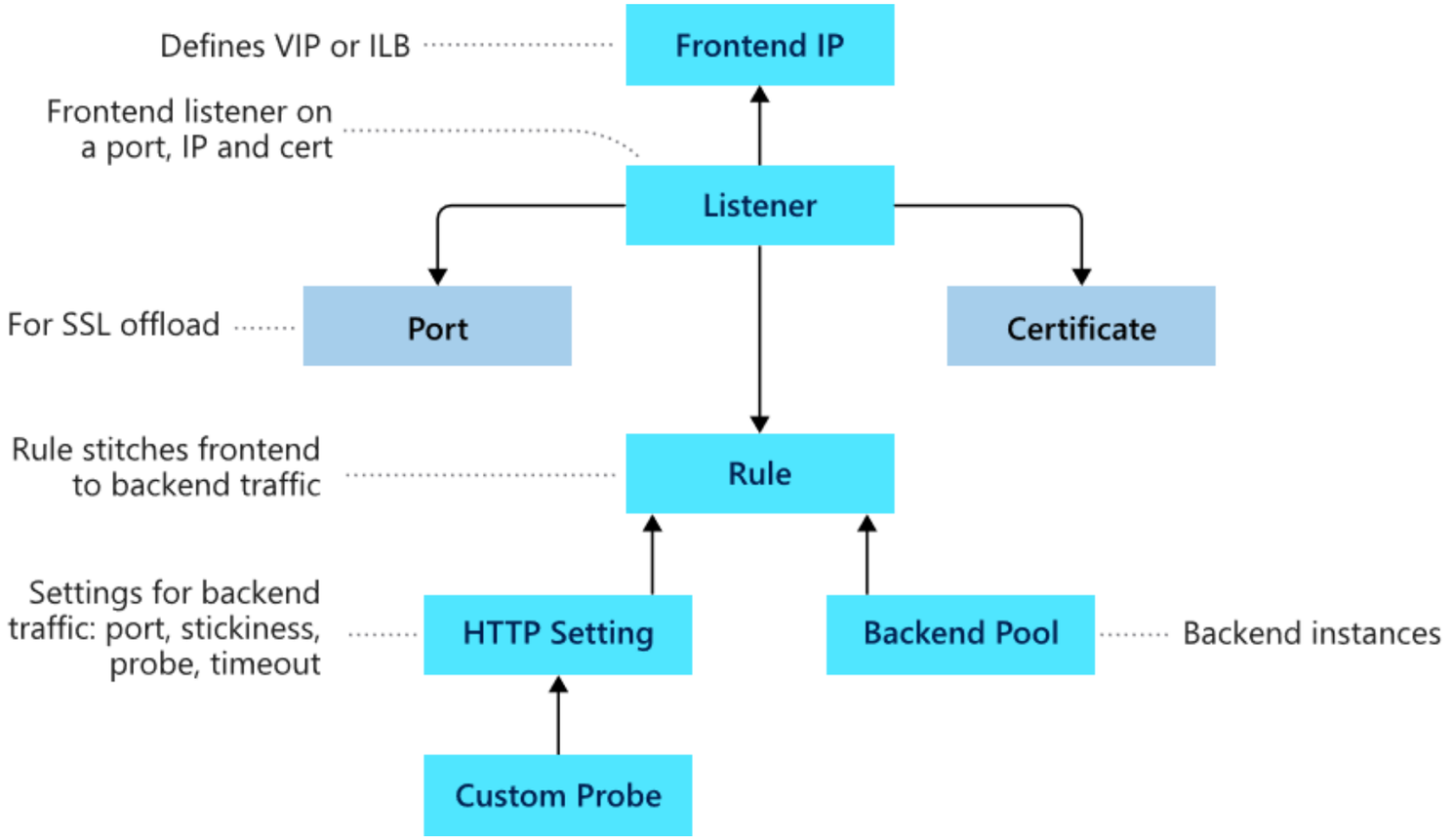


Application Gateway Configuration

An application gateway uses several components to distribute traffic.

The components are:

- Frontend IP address
- Listeners
- Routing rules
- Backend pools
- Web application firewall
- Health probes



Assisted Practice

Create an Application Gateway

Duration: 10 Min.

Problem Statement:

You are given a project to create an Application Gateway to manage traffic to your web applications.

Assisted Practice: Guidelines

Steps to create an application gateway:

1. Go to the Azure portal
2. Click on Create a resource
3. Create an application gateway

Web Application Firewall

Web Application Firewall

Web Application Firewall (WAF) provides a centralized protection to your web applications from common exploits and vulnerabilities.

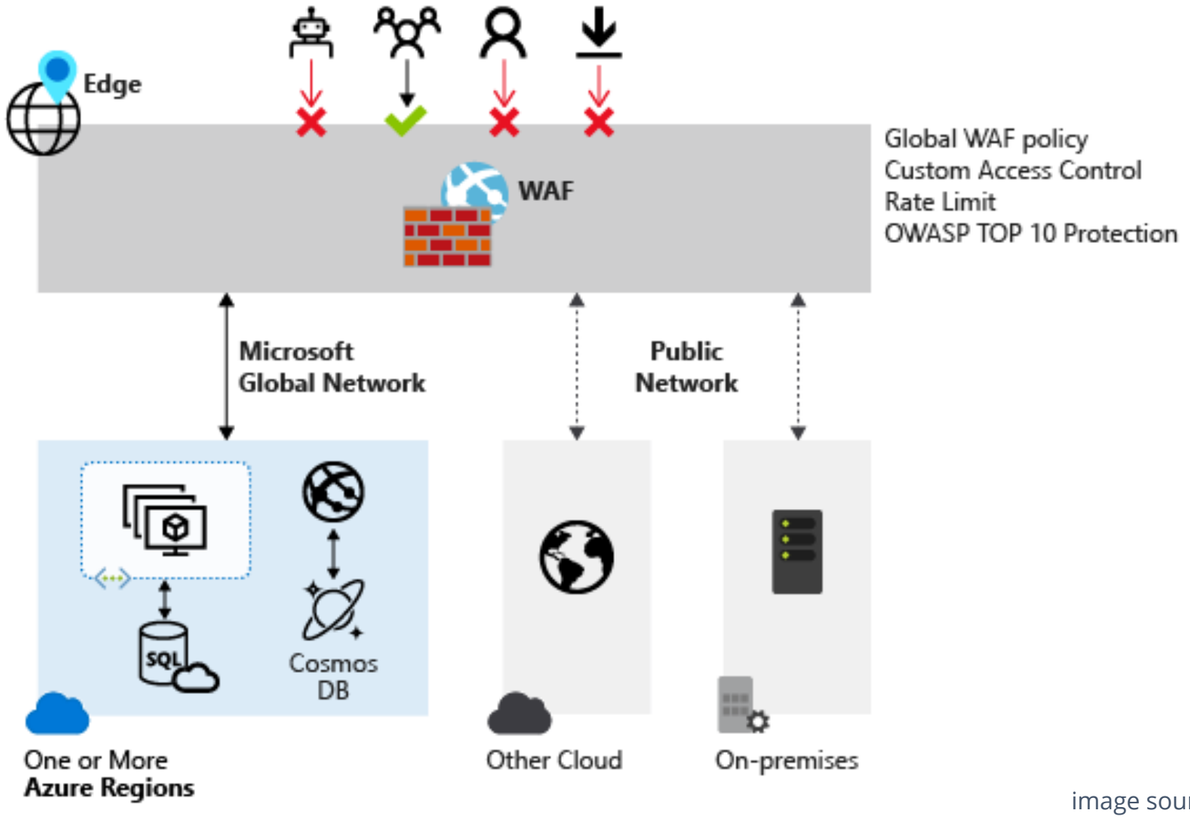
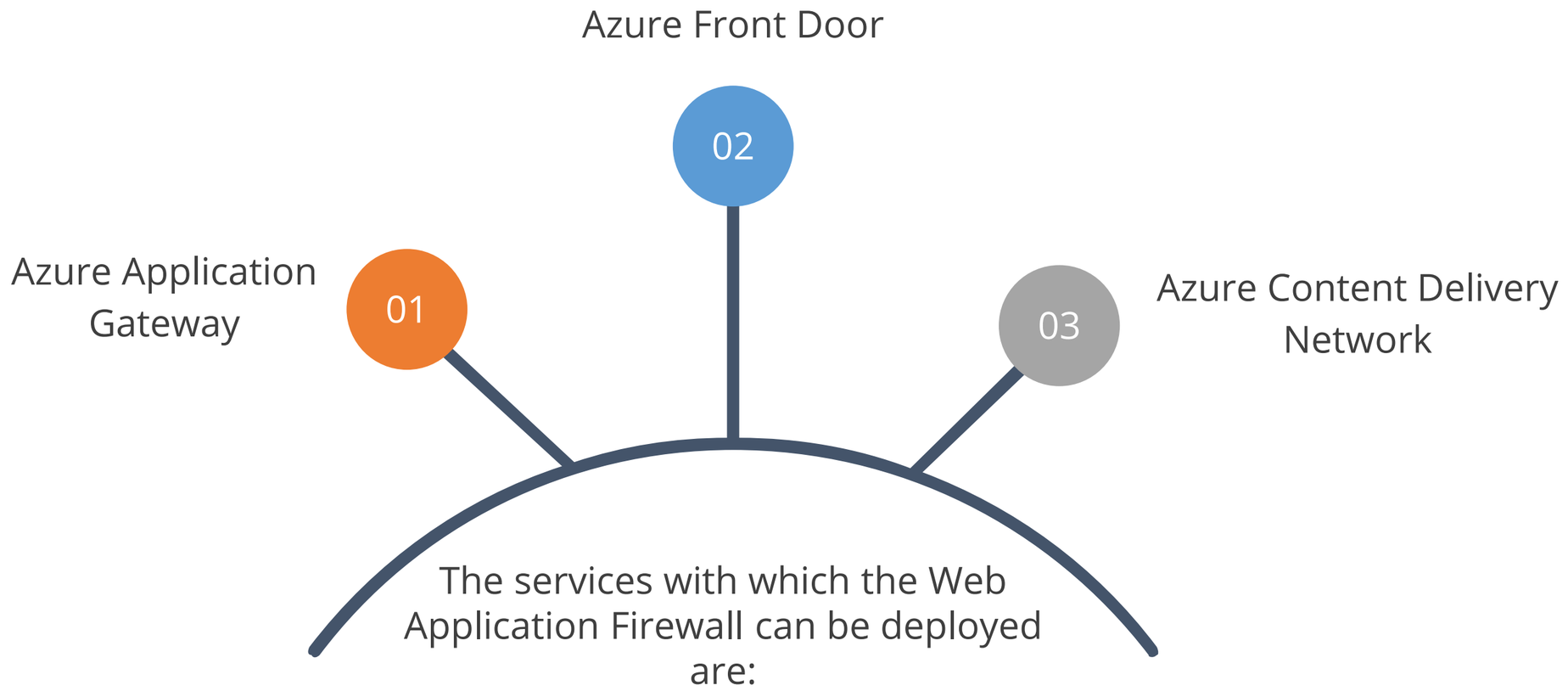


image source: https://docs.microsoft.com/en-in/

Web Application Firewall



Azure Firewall and Firewall Manager

Azure Firewall

Azure Firewall is a managed, cloud-based network security service that protects your Azure Virtual Network resources.

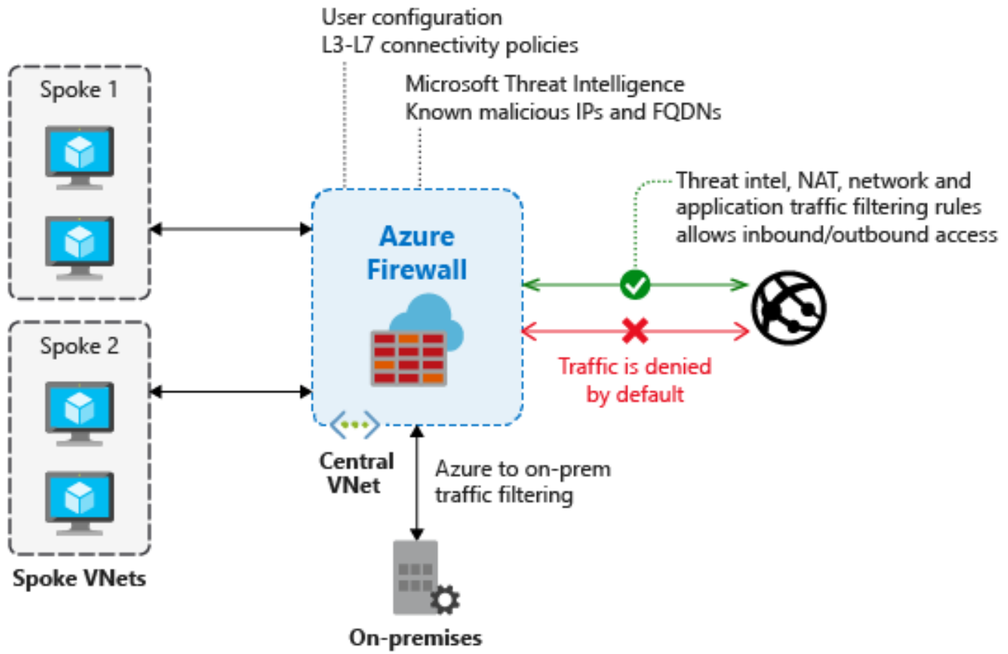
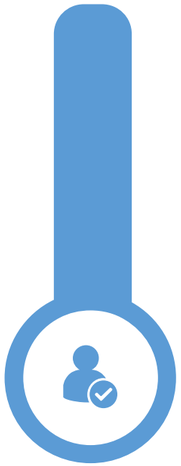


image source: https://docs.microsoft.com/en-in/

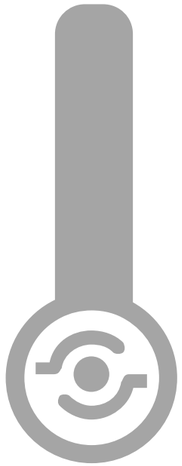
Azure Firewall Features

There are various features of Azure Firewall:



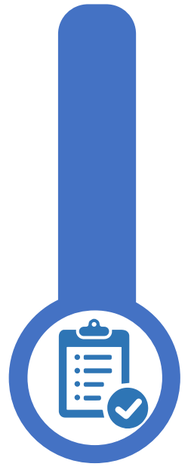
High built-in availability

Multiple availability zones



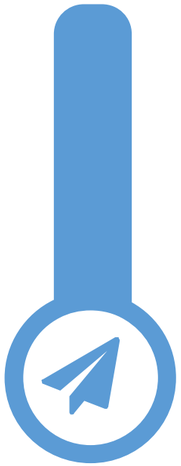
Unrestricted cloud scalability

Application FQDN filtering rules



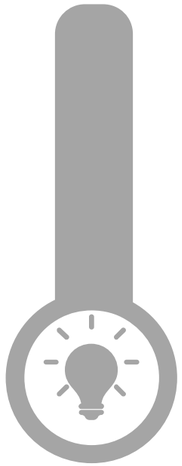
Network traffic filtering rules

Azure Firewall Features



FQDN tags

Service tags



Threat intelligence

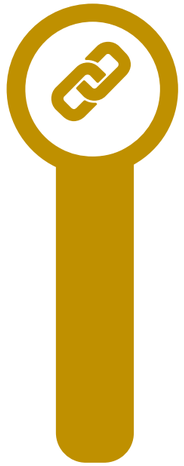
Outbound SNAT support

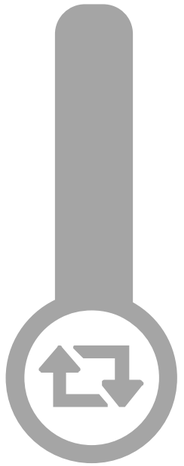
Inbound DNAT support

Azure Firewall Features

Multiple public IP addresses

Azure monitor logging





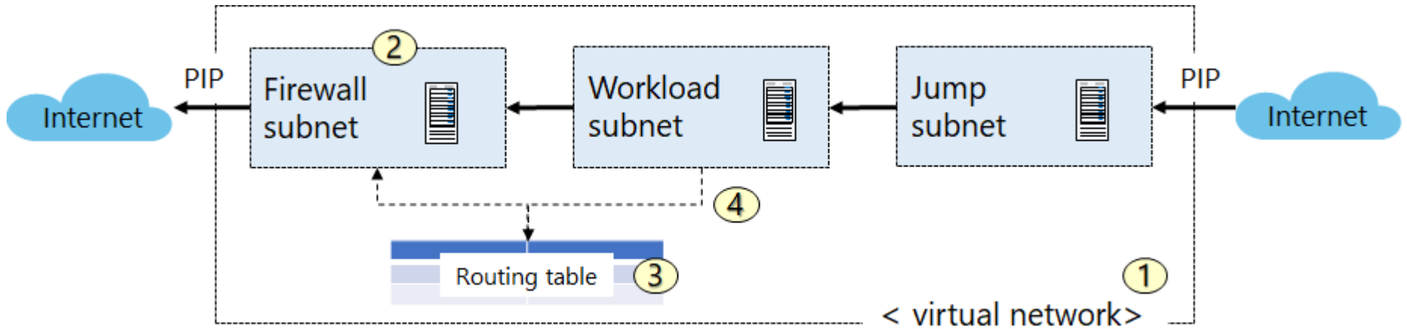
Forced tunneling

Web categories (preview)

Certifications

Implementing Azure Firewall

Consider an example where we want to use Azure Firewall to route protect our workload server by controlling the network traffic:



- Create the network infrastructure
- Deploy the firewall
- Create a default route
- Configure an application rule

Azure Firewall Manager

Azure Firewall Manager is a security management service for cloud-based security perimeters that offers central security policy and route management.

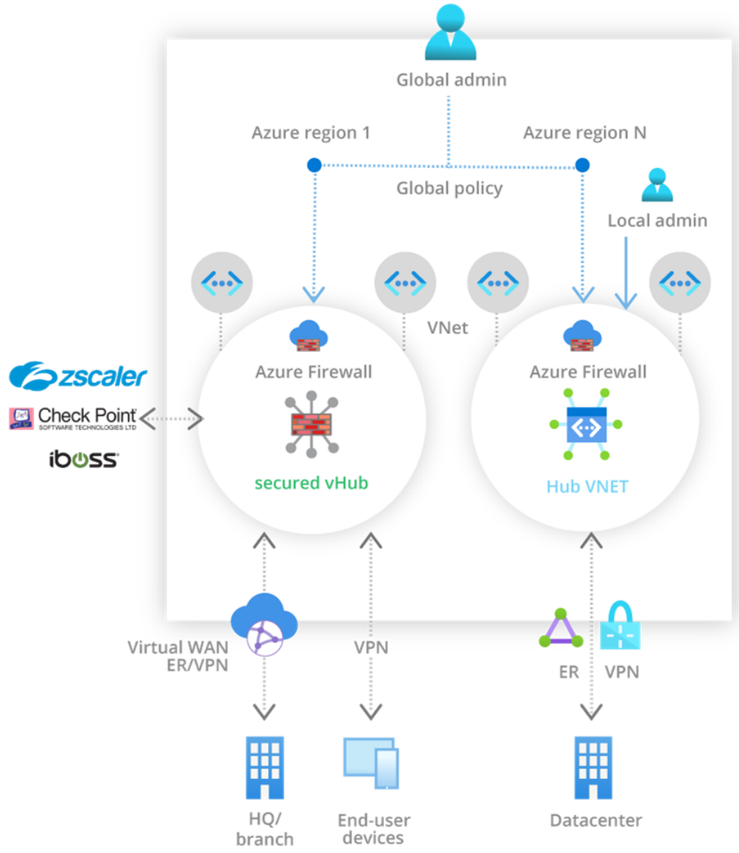


image source: https://docs.microsoft.com/en-in/

Azure Firewall Manager Features

Central Azure Firewall deployment and configuration

Centralized route management

Hierarchical policies (global and local)

Integrated with third-party security-as-a-service (SaaS) for advanced security

Azure Front Door

Azure Front Door

Azure Front Door is a global, scalable entry-point that uses the Microsoft global edge network to create fast, secure, and highly scalable web applications.

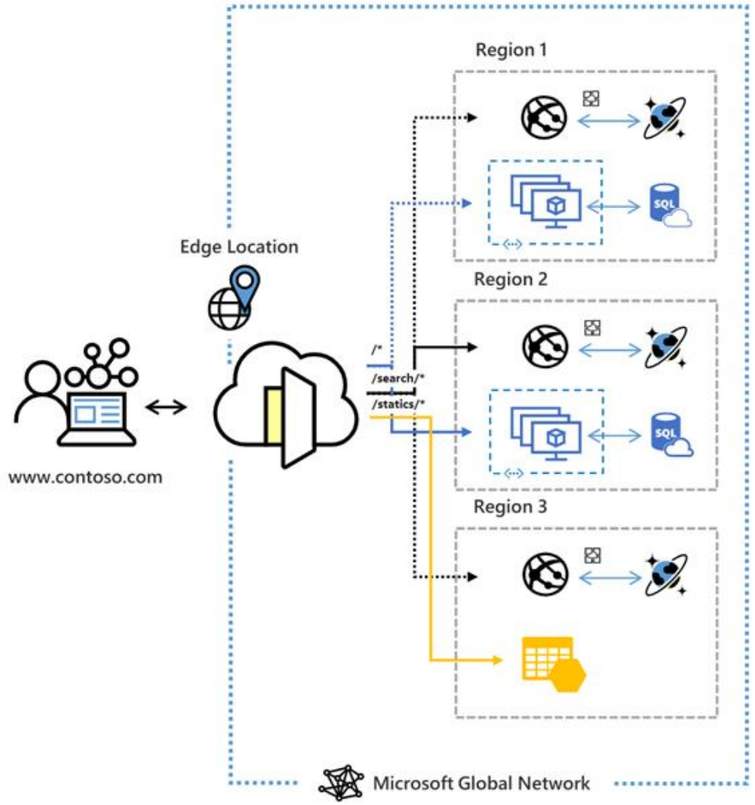


image source: https://docs.microsoft.com/en-in/

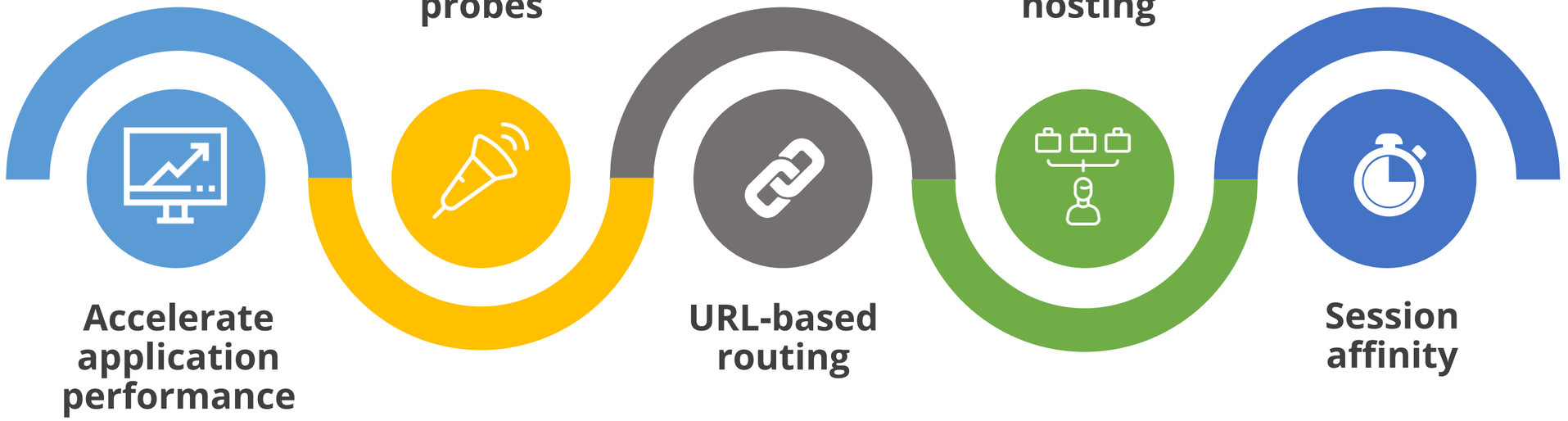
Source: https://docs.microsoft.com/

Benefits of Azure Front Door

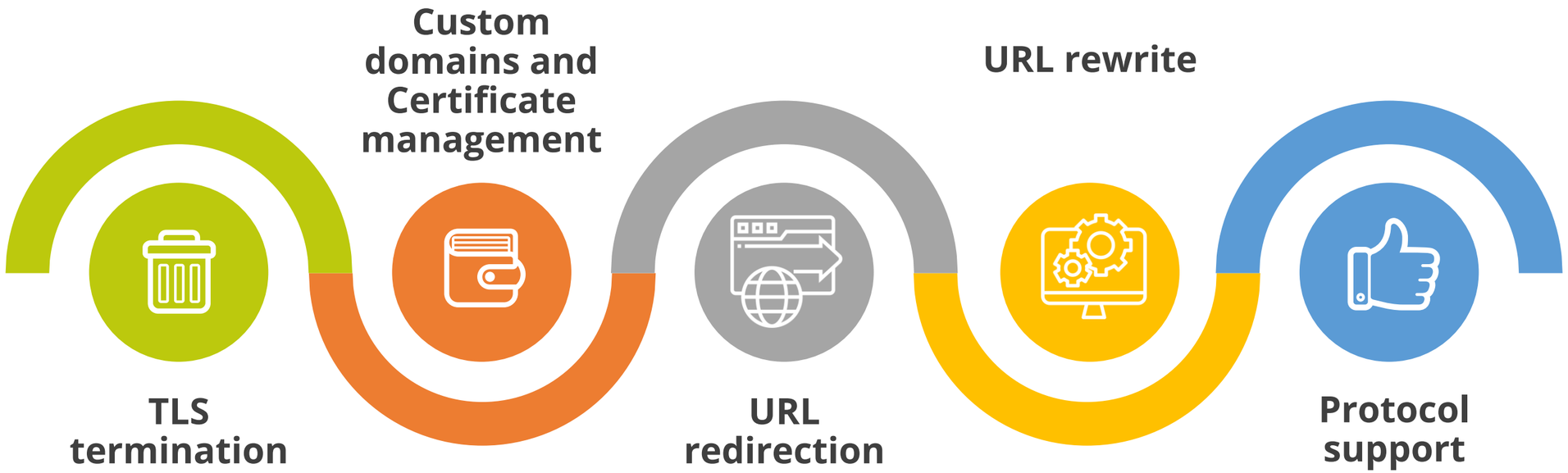
It allows the user to identify, manage, and track the global route for your web traffic by optimizing for best client-side performance and instant global failover for high availability.

Azure Front Door Features

Ten features of Azure Front Door:



Azure Front Door Features



Assisted Practice

Configure Azure Front Door Service

Duration: 10 Min.

Problem Statement:

You are given a project to configure Azure front door to create fast, secure, and widely scalable web applications.

Assisted Practice: Guidelines

Steps to configure Azure front door:

1. Go to the Azure portal
2. Click on Create a resource
3. Configure Azure front door

Azure Traffic Manager

Azure Traffic Manager

Traffic Manager is a network service that is used to route users to web app endpoints (deployments) in potentially different data centers located around the world.

Benefits

It ensures our apps are:

- Highly scalable
- Highly available

Prerequisites

You should have two or more deployments of your web app to leverage the features of Azure Traffic Manager.

Traffic Manager Overview

Below diagram is the overview of traffic manager:

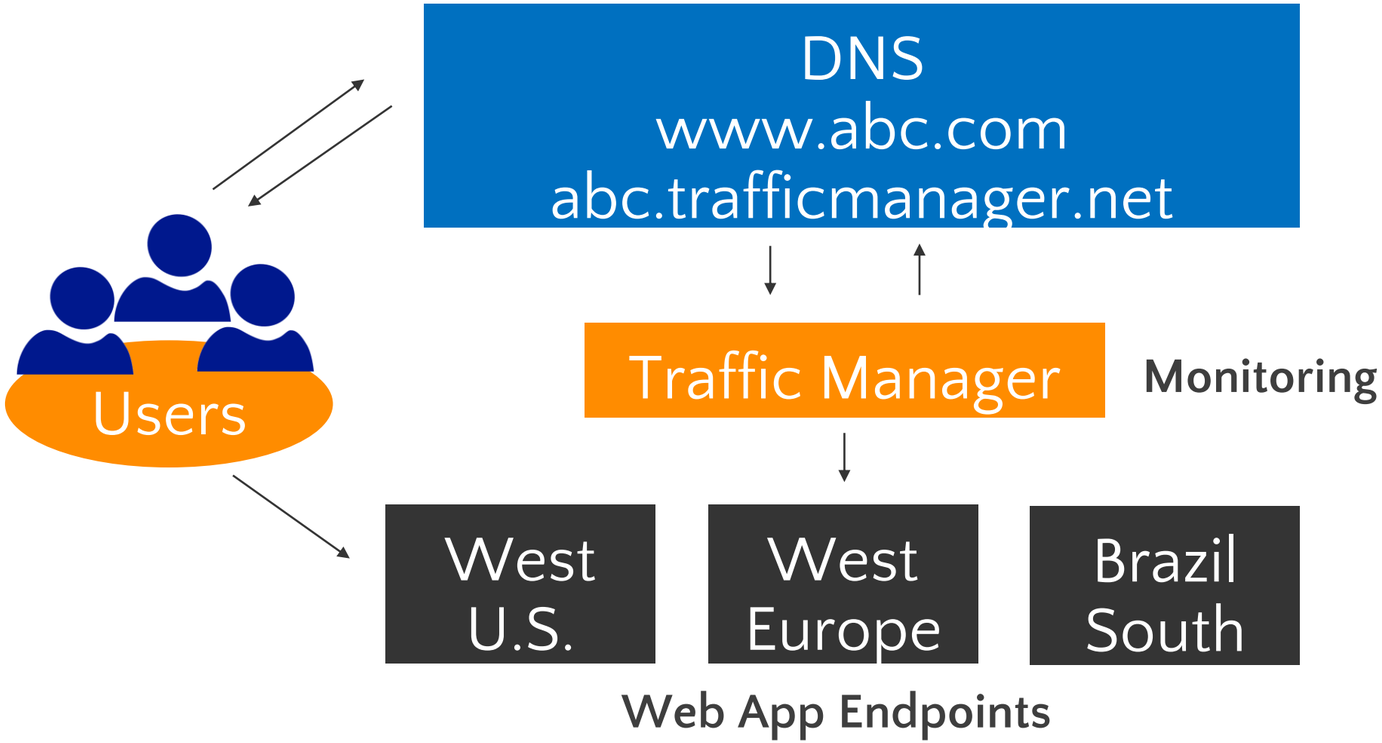


image source: https://docs.microsoft.com/en-in/

Traffic Manager Features

These are the features of traffic manager:

Increase application availability

Improve application performance

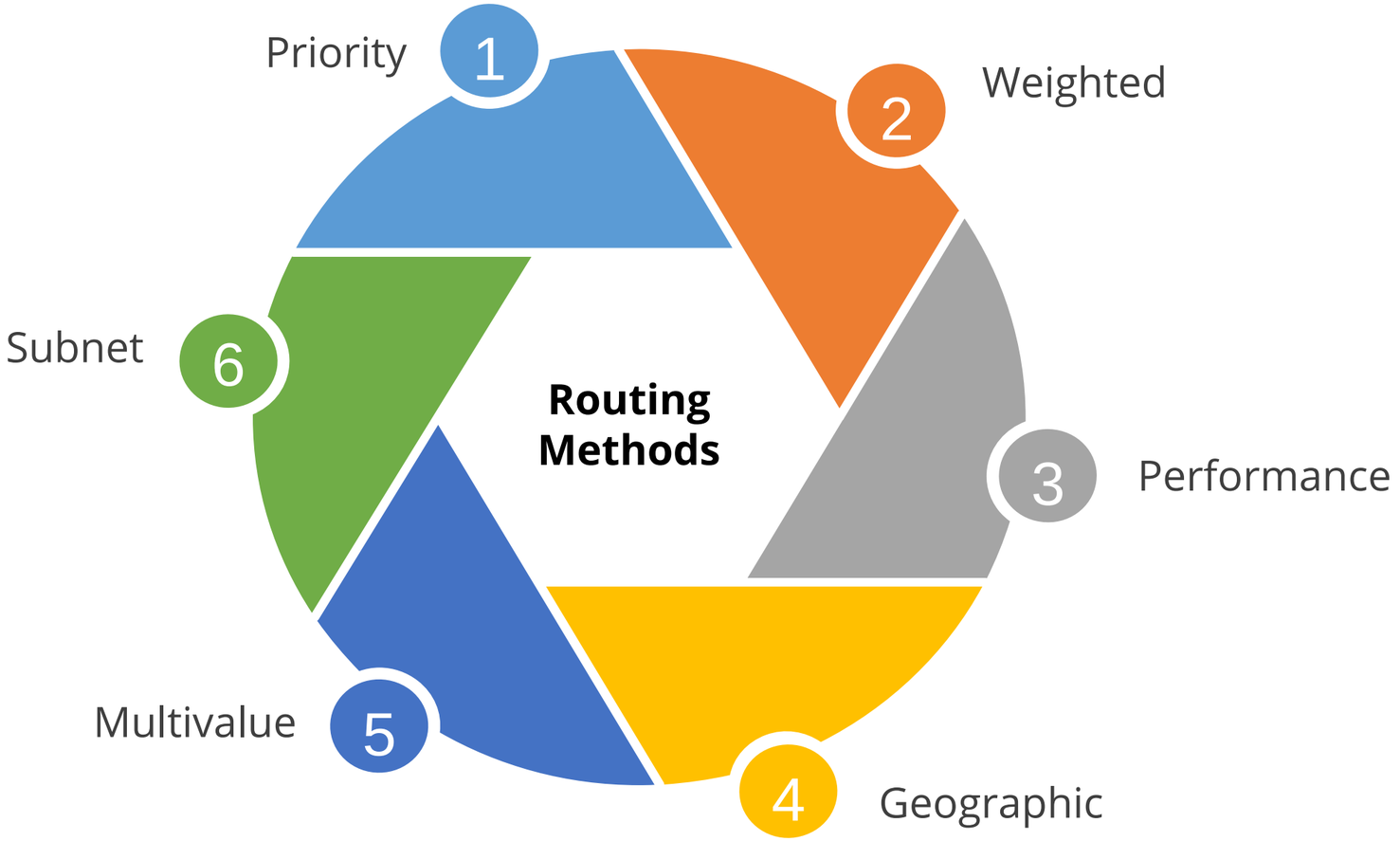
Service maintenance without downtime

Distribute traffic for complex deployments

Combine hybrid applications

Traffic Manager Routing Methods

These are the features of routing methods:



Priority Routing

The Priority traffic-routing method allows Azure customers to easily implement this failover pattern:

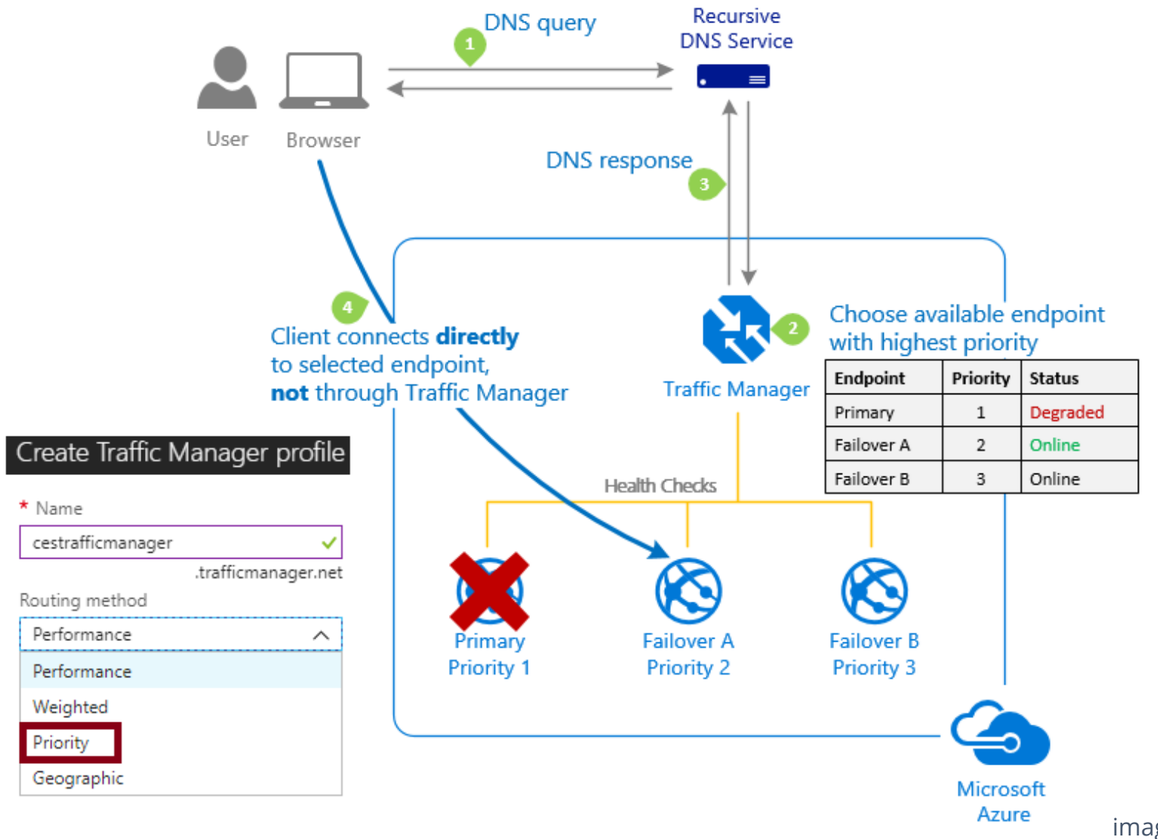


image source: https://docs.microsoft.com/en-in/

Weighted Routing

The Weighted traffic-routing method enables you to distribute traffic evenly or to use a predefined weighting.

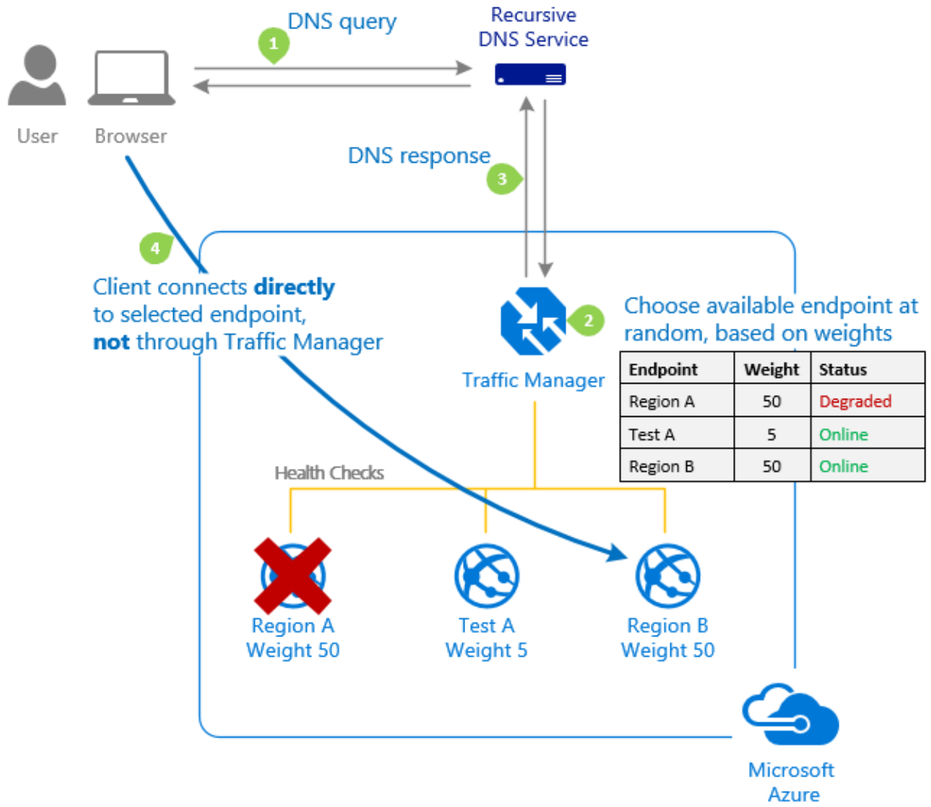


image source: https://docs.microsoft.com/en-in/

Performance Routing

The Performance traffic-routing method helps you route traffic to the location that is closest to you.

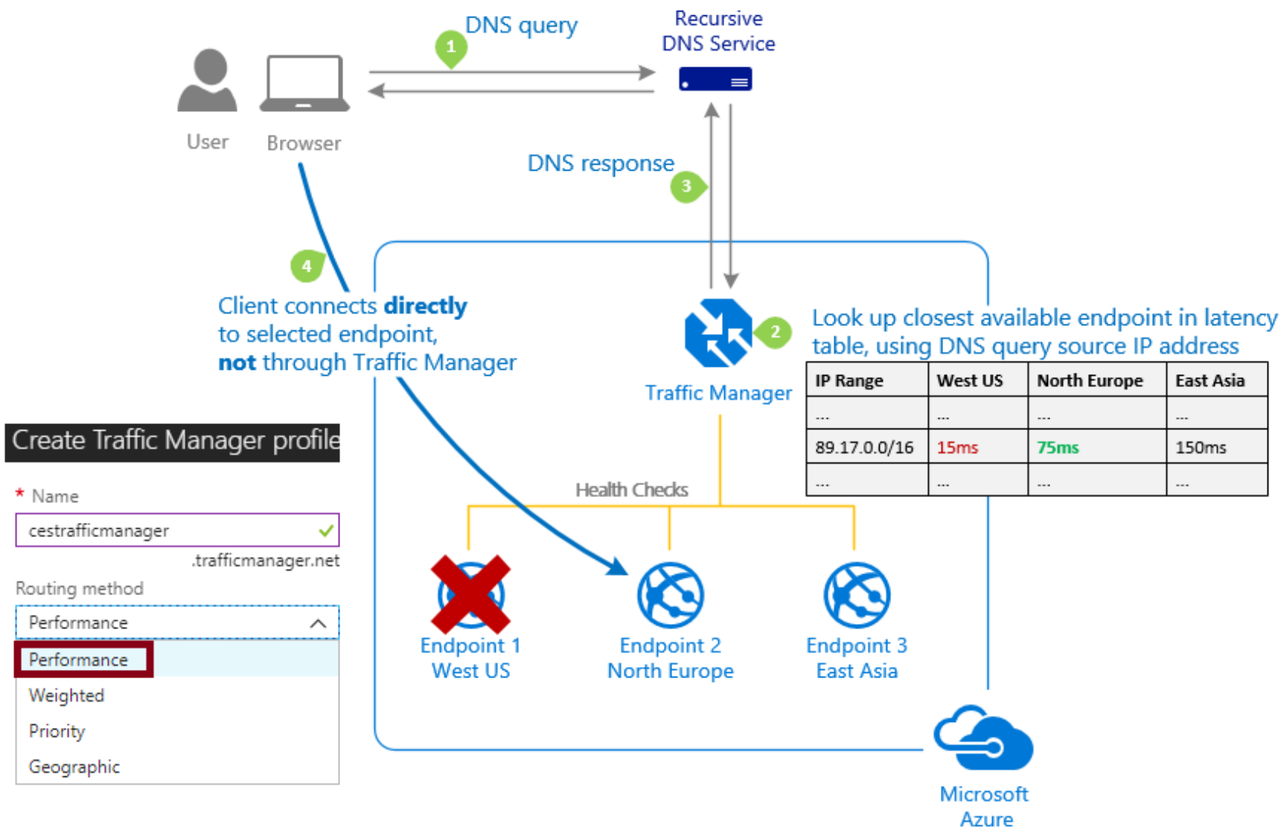


image source: https://docs.microsoft.com/en-in/

Geographic Routing

The Geographic traffic-routing method helps you in measuring traffic from different regions.

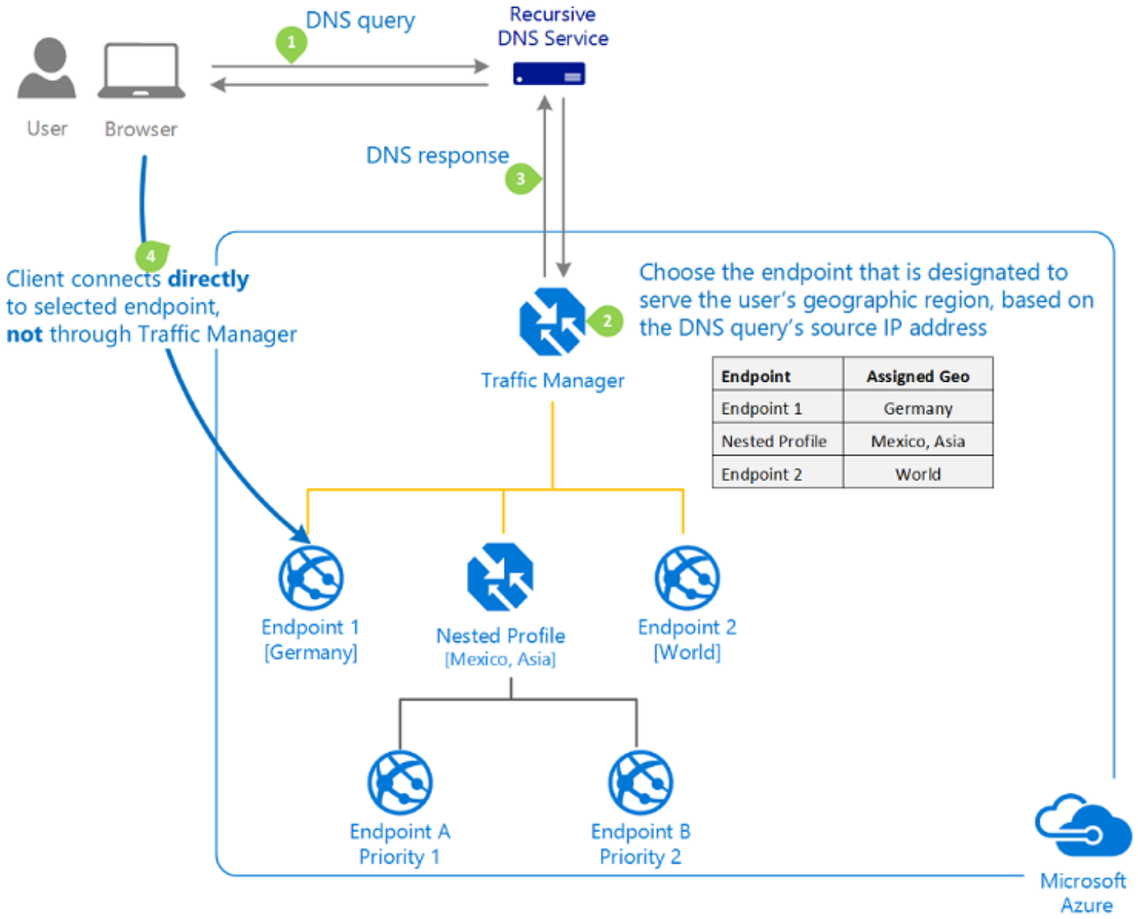


image source: https://docs.microsoft.com/en-in/

Points to Remember

- All Azure Traffic Manager profiles use the shared domain ***.trafficmanager.net***.
- Web apps in the same data centers will automatically be load balanced.
- Web apps spread across multiple data centers will need to be load balanced.
- Endpoints need to be in the same subscription to provide load balancing between the apps.

Distributing Network Traffic

The network traffic table explained below:

Service	Azure Load Balancer	Application Gateway	Traffic Manager	Azure Front Door
Technology	Transport layer (Level 4)	Transport layer (Layer 7)	DNS resolver	Layer 7 or HTTP/HTTPS
Protocols	Any TCP or UDP protocol	HTTP, HTTPS, HTTP/2, and Web sockets	DNS resolution	Split TCP-based anycast protocol
Backends and Endpoints	Azure VMs and Azure VM scale sets	Azure VMs, Azure VM scale sets, Azure app services, IP addresses, and hostnames	Azure cloud services, Azure app services, Azure app services slots, and public IP addresses	Internet-facing services hosted inside or outside of Azure
Network connectivity	External and Internal	External and Internal	External	External and Internal

Assisted Practice

Implement Traffic Manager

Duration: 10 Min.

Problem Statement:

You've been assigned the task of implementing Traffic Manager, which will route client requests to the proper service endpoint using a traffic-routing method.

Assisted Practice: Guidelines

Steps to implement traffic manager:

1. Log into the Azure portal
2. Create a resource
3. Create Traffic Manager Profile
4. View Traffic Manager Profile

Azure Security Groups

Network Security Groups (NSG)

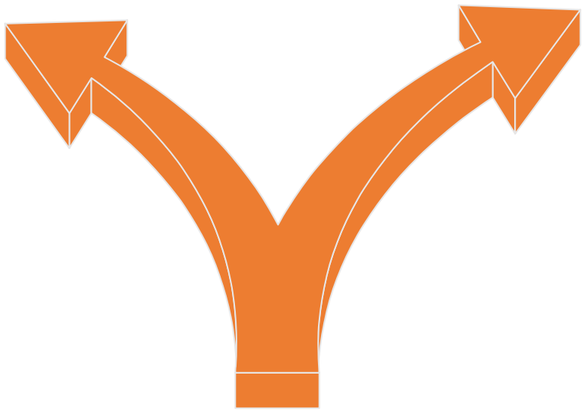
Features

- A user can limit network traffic to resources in a virtual network using an NSG.
- NSG contains a list of security rules that allow or deny inbound or outbound network traffic.
- NSG can be associated with a subnet or a network interface.
- NSGs operate in layers 3 & 4 allowing communication between network interfaces.
- NSGs are used to isolate applications between environments, tiers, and services.
- NSGs lock down network communication between virtual machines.

Network Security Group Rules

Inbound Rules

- Allow VNet Inbound
- Allow Azure Load Balancer Inbound
- Deny All Inbound



Outbound Rules

- Allow VNet OutBound
- Allow Internet OutBound
- Deny All OutBound

NSG has two default security rules

NSG Rules

Every network security group you build in Azure comes with the following default rules:

VM1-nsg - Inbound security rules
Network security group

PRIORITY	NAME	PORT	PROTOCOL	ACTION
65000	AllowVnetInBound	Any	Any	Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	Allow
65500	DenyAllInBound	Any	Any	Deny

VM1-nsg - Outbound security rules
Network security group

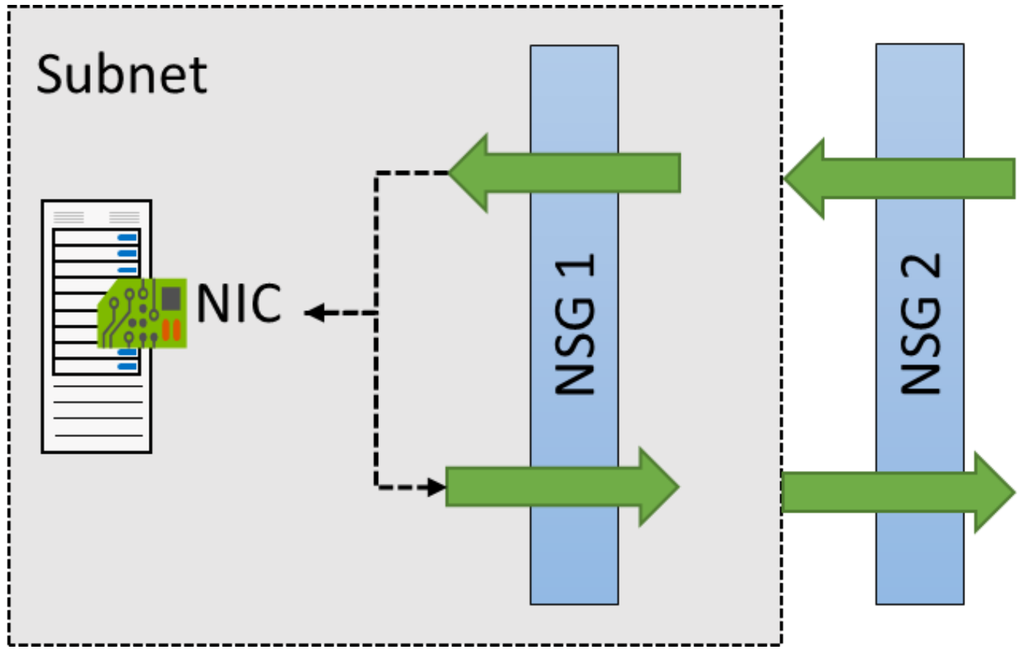
PRIORITY	NAME	PORT	PROTOCOL	ACTION
65000	AllowVnetOutBound	Any	Any	Allow
65001	AllowInternetOutBound	Any	Any	Allow
65500	DenyAllOutBound	Any	Any	Deny

Note

The default rules cannot be removed, but they can be overridden by developing rules with higher priorities.

NSG Effective Rules

The effective security rules for a network interface are a combination of the rules in the NSG associated with the network interface and the subnet in which the network interface is located.



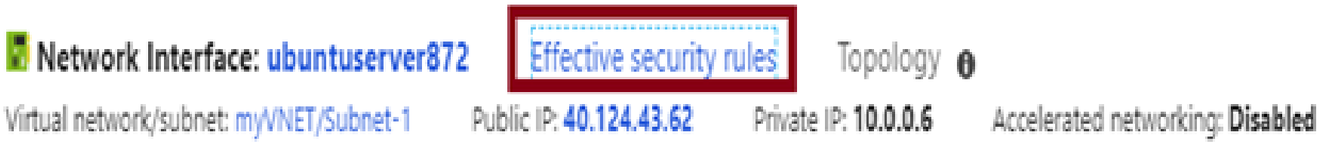


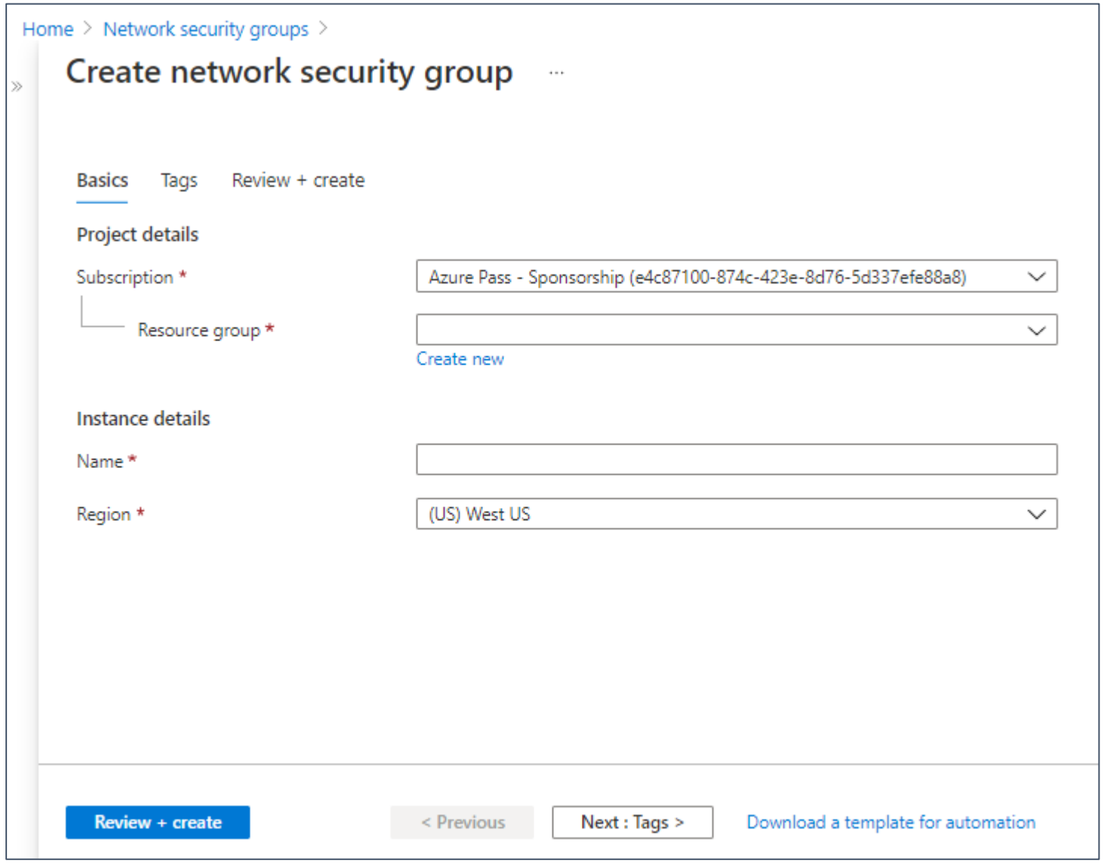
image source: https://docs.microsoft.com/en-in/

Creating NSG Rules

1. Pick Create a resource from the Azure portal menu or the Home tab and then pick Network protection category from drop-down

1. Set values for the following settings on the Create network security group page, under the **Basics tab**

1. Select a **subscription plan**

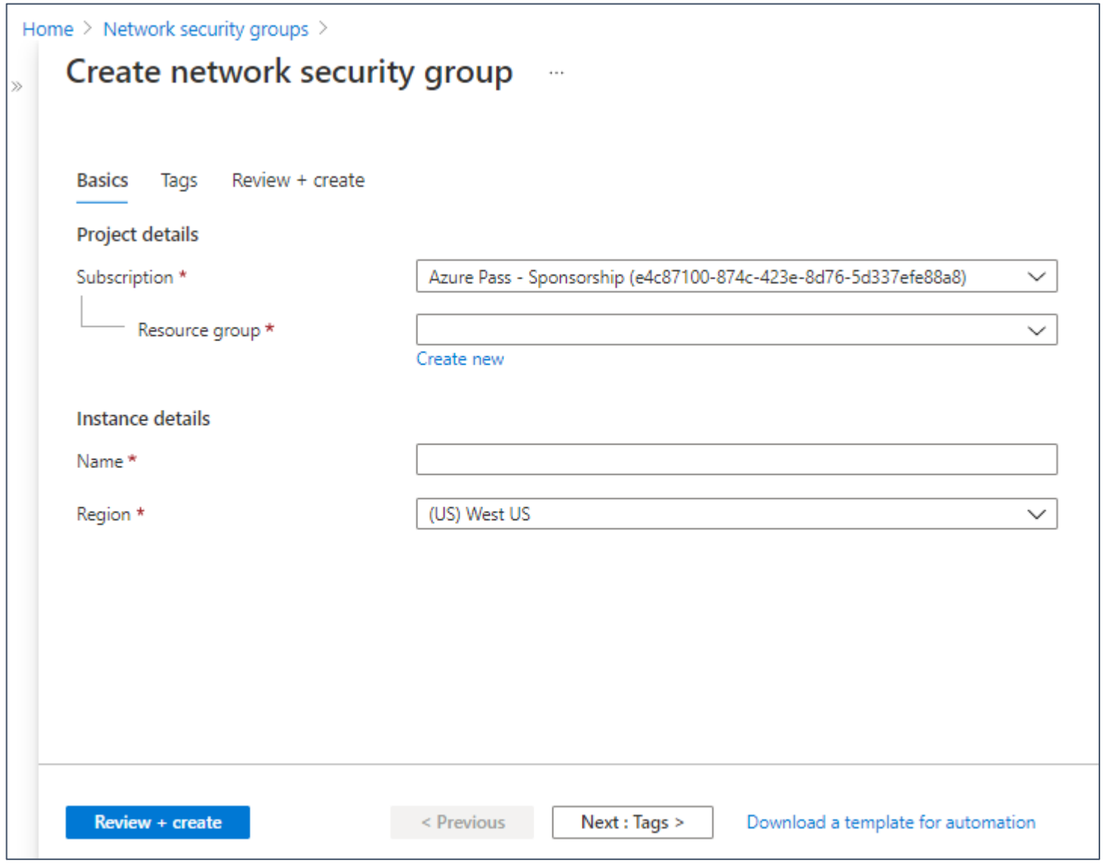


Creating NSG Rules

4. Choose an existing resource group or create a new resource group by selecting Create new

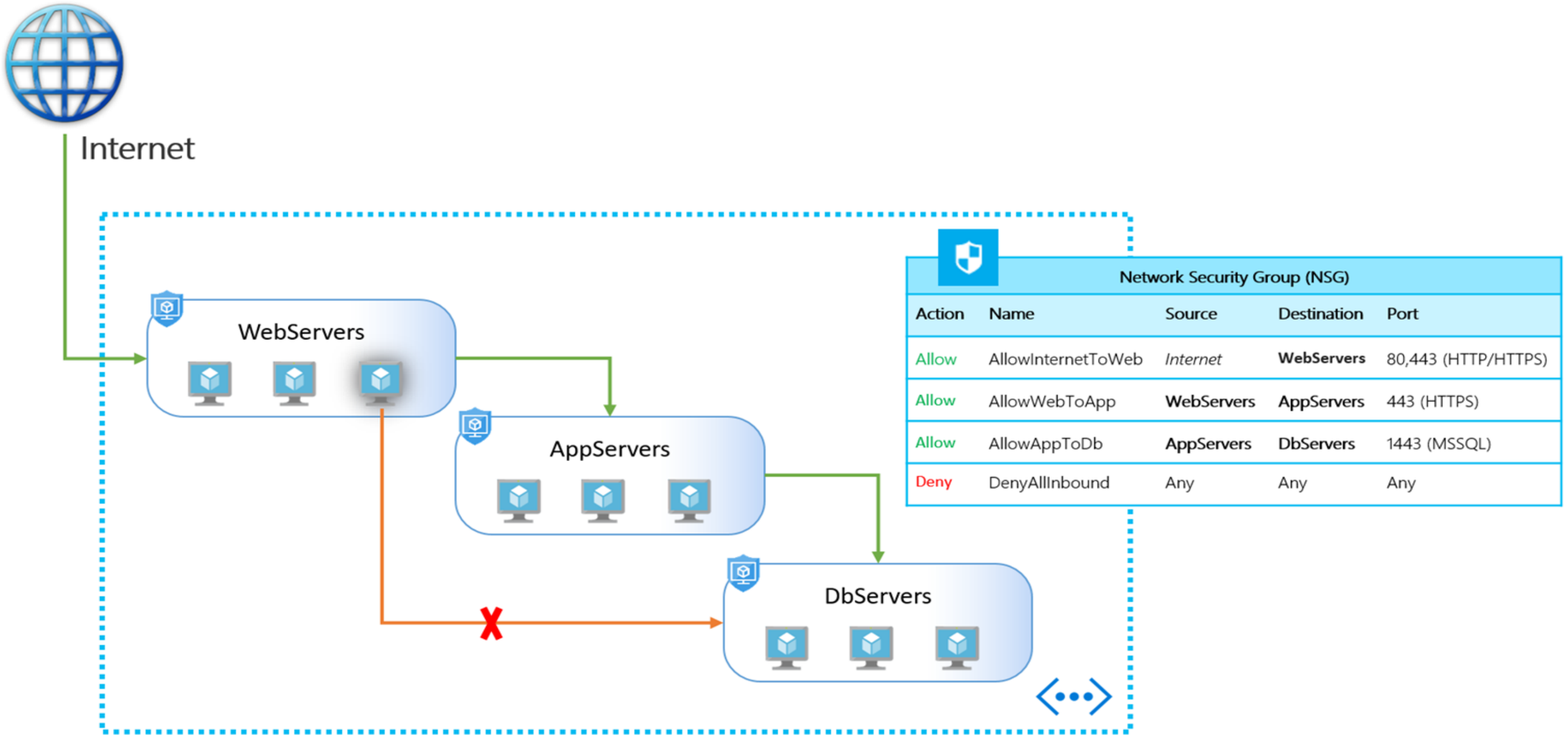
5. Type a unique text string in the Name section

6. Select the desired spot in the Region section, then select Review + Create from the menu and then select Create after you see the Validation passed post



Application Security Groups (ASG)

The diagram depicts the architecture of the Application Security Groups:



Application Security Groups (ASG)

Features

- Azure Security Groups enables the user to define fine-grained network security policies based on workloads and centralized on applications.
- ASGs enables the user to group VMs based on their monikers and secure our applications by filtering traffic.
- By providing a moniker descriptive name that suits our architecture, the user can identify application classes.
- It can be used for everything, including applications, frameworks, environments, workload forms, tiers, and even functions.

Application Security Groups

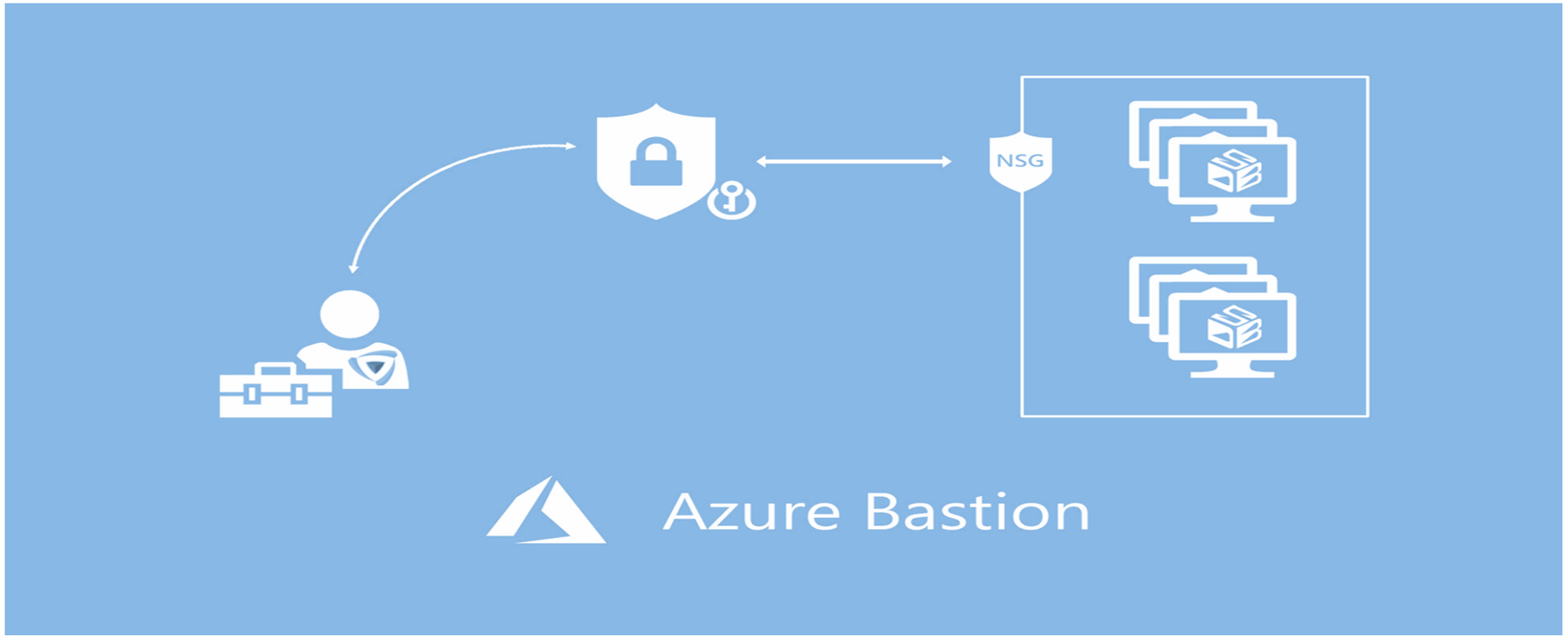
Benefits

- The user will be able to scale at his own rate. He should render the VMs representatives of the relevant ASGs when they're being deployed.
- ASGs give the user the ability to run multiple applications on the same subnet while also isolating traffic.
- The user can reduce the number of Network Security Groups in our subscription by using Azure Security Groups.
- The user no longer needs to be concerned about protection description.

Azure Bastion

Azure Bastion

Azure Bastion is a new completely managed PaaS service that can be deployed within virtual network. It allows user to connect to their VMs via RDP/SSH over SSL directly from the Azure portal.

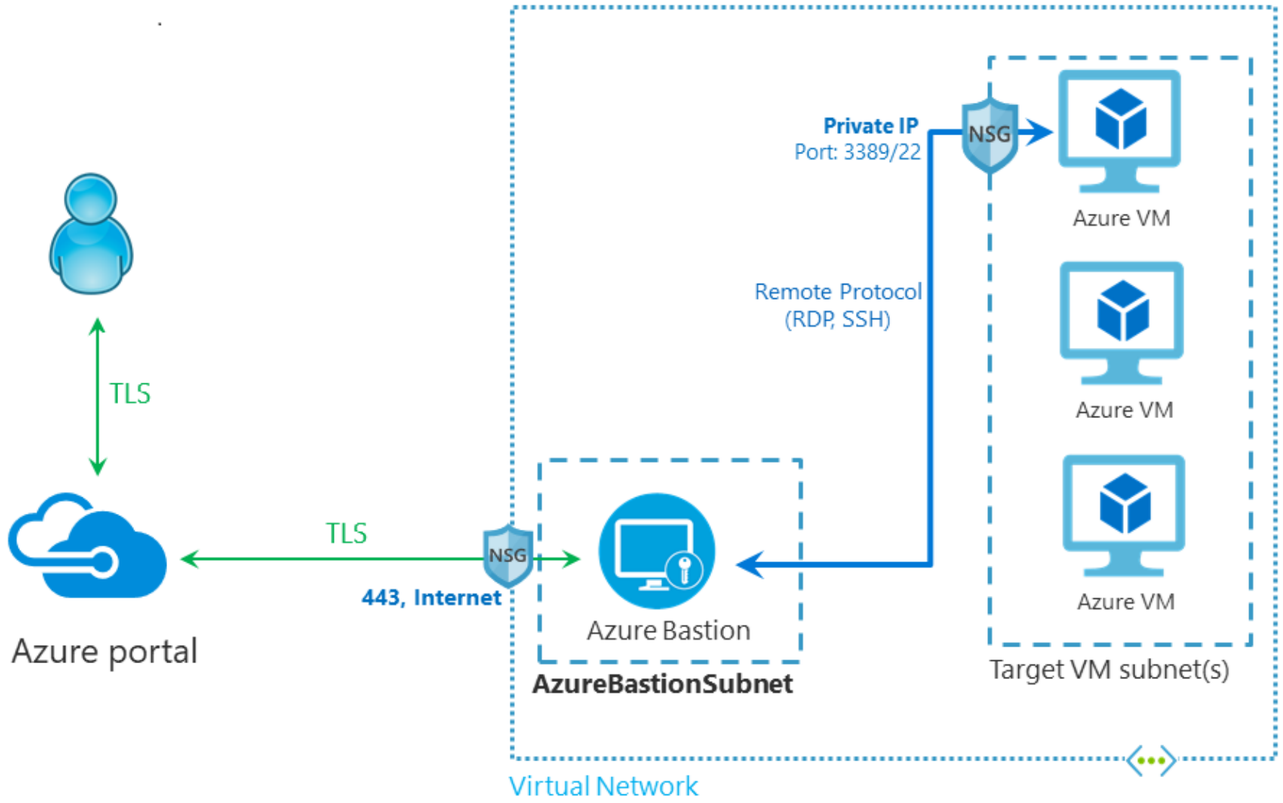


The virtual machines do not need a public IP address when connected via Azure Bastion.

image source: https://docs.microsoft.com/en-in/

Azure Bastion Architecture

The architecture of an Azure Bastion deployment is depicted in this diagram.

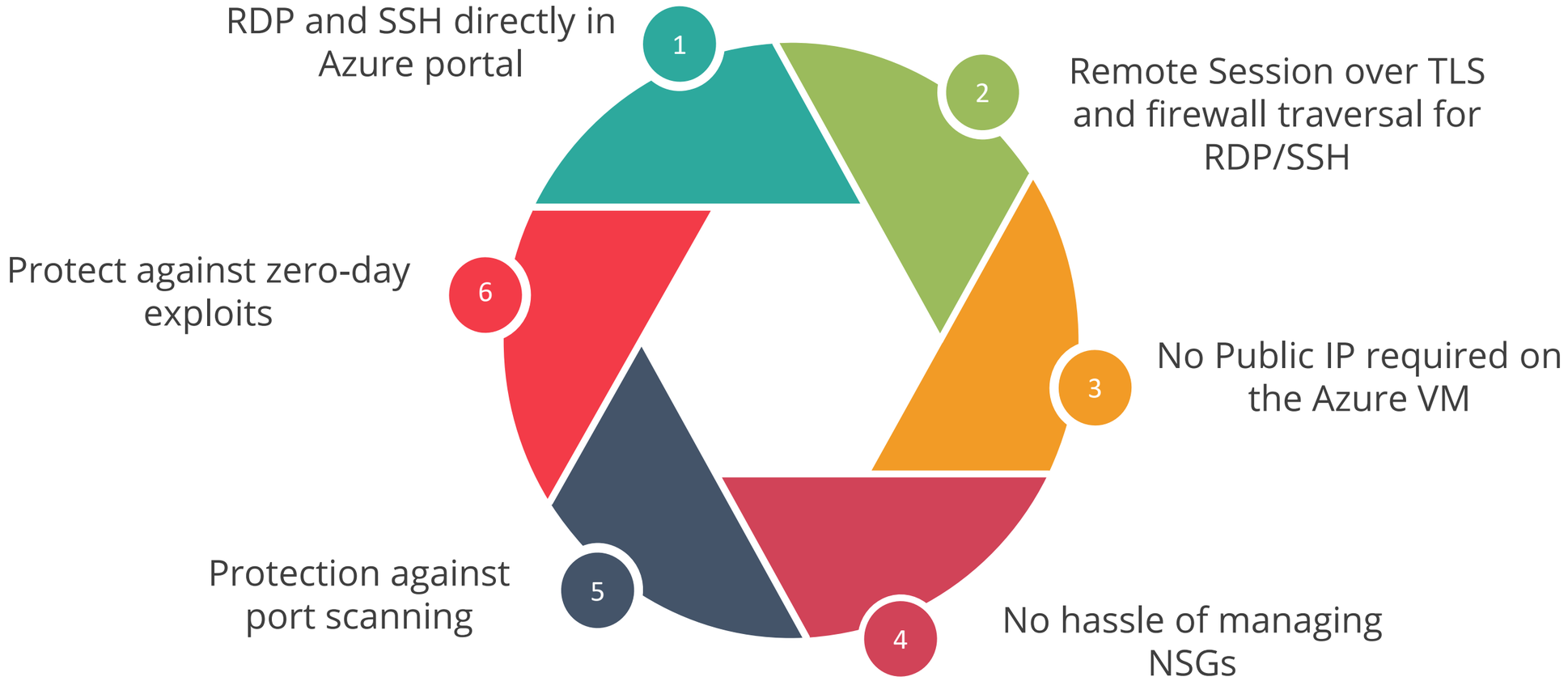


- The Bastion host is installed in a virtual network that includes the AzureBastionSubnet , which has a minimum prefix of /27.
- Any HTML5 browser can be used to link to the Azure portal.
- The virtual machine to which the user connects is chosen by the user.

image source: https://docs.microsoft.com/en-in/

Key Features

These are the key features of Azure Bastion:



Key Features

RDP and SSH directly in Azure Portal

With a single click, you can access RDP and SSH sessions directly from the Azure portal.

Remote Session over TLS and firewall traversal for RDP/SSH

Azure Bastion uses an HTML5-based web client that is automatically streamed to your local computer.

No Public IP required on the Azure VM

Azure Bastion connects to the Azure virtual machine via RDP/SSH using the VM's private IP address. Your virtual machine does not need a public IP address.

Key Features

No hassle of managing NSGs

On the Azure Bastion subnet, no NSGs are needed. You should configure your NSGs to only enable RDP/SSH from Azure Bastion since it connects to your virtual machines over a private IP.

Protection against port scanning

The virtual machines are safe from port scanning by rogue and malicious users outside the user's virtual network because the user doesn't have to expose them to the public Internet.

Protection against zero day exploits

By keeping the Azure Bastion hardened and up to date for the user, the Azure platform protects the user from zero-day exploits.

Assisted Practice

Azure Bastion

Duration: 10 Min.

Problem Statement:

You've been assigned a project to build Azure Bastion, which will allow you to access to your virtual machines through RDP/SSH directly from the Azure portal using SSL.

Assisted Practice: Guidelines

Steps to create Azure Bastion:

1. Log into the Azure portal
2. Select the virtual machine
3. Create Azure Bastion

Key Takeaways

- Azure Load balancer distributes inbound traffic to backend resources
- Application Gateway manages requests and routes traffic to a pool of web servers.
- Azure Firewall is a managed, cloud-based network security service that protects your Azure Virtual Network resources.
- Traffic Manager is a network service used to route users to web app endpoints in potentially different data centers located around the world.

Key Takeaways

- A network security group is used to trigger a rule or access control list that allows or blocks network traffic.
- Azure Security Groups enables the user to define fine-grained network security policies based on workloads and centralized on applications.
- Azure Bastion is a new completely managed PaaS service that can be deployed within virtual network.

Implementing Traffic Manager for traffic management

Duration: 25 Min.

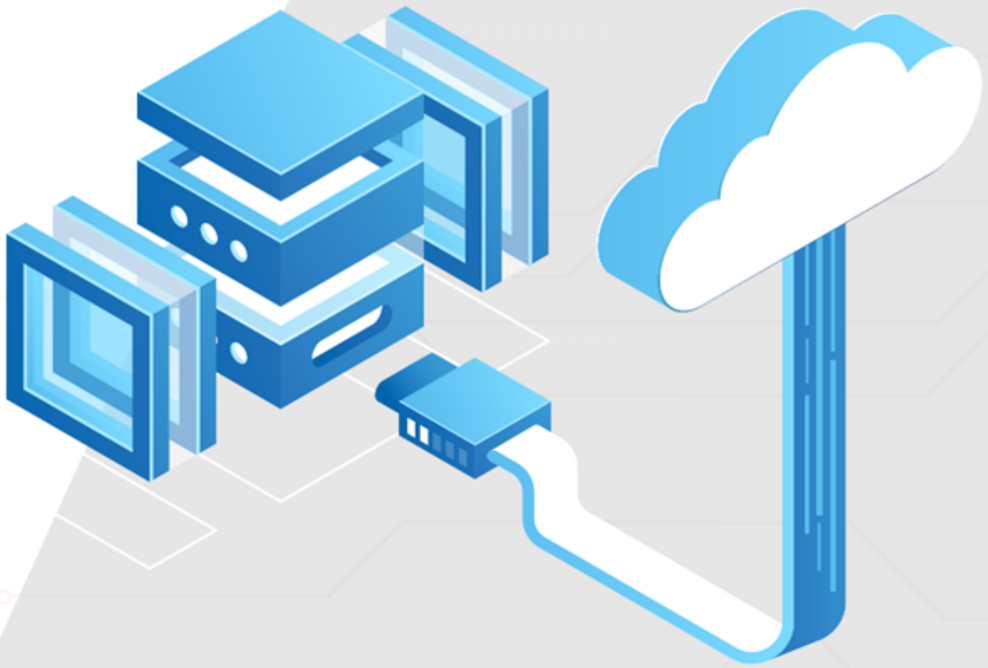
Project agenda: To Implement Traffic Manager for traffic management for a web application

Description: You have been given a project to create a traffic manager to route the traffic for a web application based on performance. As a part of this you need to create two web applications each in two different regions and place these behind the traffic manager to route the traffic to appropriate applications based on performance.

Perform the following:

Create two web application in two different region and use a traffic manager to route the traffic based upon the performance.

LESSON-END PROJECT



Thank you