Contents

[ROUTING SERVICES IN AZURE 3](#_Toc152099189)

[LOAD BALANCER 4](#_Toc152099190)

[LOAD BALANCER CONCEPT 5](#_Toc152099191)

[COMPONENTS OF LOAD BALANCER 5](#_Toc152099192)

[LOAD BALANCER SKUs 5](#_Toc152099193)

[TYPES OF LOAD BALANCER 5](#_Toc152099194)

[BASIC LOAD BALANCER (VMs in AVAILABILITY SET) 6](#_Toc152099195)

[LOAD BALANCER NAT RULES 13](#_Toc152099196)

[MUTIPLE BACKEND POOL AND FRONTEND IP ADDRESS OF LB 14](#_Toc152099197)

[BASIC LOAD BALANCER (SCALE SET) 15](#_Toc152099198)

[STANDARD LOAD BALANCER 21](#_Toc152099199)

[AZURE APPLICATION GATEWAY 29](#_Toc152099200)

[APPLICATION GATEWAY FEATURES 30](#_Toc152099201)

[APPLICATION GATEWAY – PATH BASED ROUTING 31](#_Toc152099202)

[APPLICATION GATEWAY COMPONENTS 32](#_Toc152099203)

[SETTING UP APPLICATION GATEWAY – URL ROUTING 32](#_Toc152099204)

[APPLICATION GATEWAY – MULTIPLE SITES 37](#_Toc152099205)

[USER DEFINED ROUTES 37](#_Toc152099206)

[USECASE - SETTING UP USER DEFINED ROUTE 37](#_Toc152099207)

[NETWORK WATCHER 46](#_Toc152099208)

[AZURE BASTION SERVICE 46](#_Toc152099209)

[SETTING UP BASTION SERVICE 47](#_Toc152099210)

[AZURE FIREWALL 52](#_Toc152099211)

[WHAT IS A FIREWALL 52](#_Toc152099212)

[AZURE FIREWALL SERVICE 52](#_Toc152099213)

[AZURE TRAFFIC MANAGER 58](#_Toc152099214)

[GEOGRAPIC ROUTING METHOD 59](#_Toc152099215)

[AZURE TRAFFIC MANAGER SET UP 59](#_Toc152099216)

[AZURE TRAFFIC MANAGER ROUTING METHODS 59](#_Toc152099217)

[PRIORITY ROUTING METHOD 59](#_Toc152099218)

[PERFORMANCE ROUTING METHOD 62](#_Toc152099219)

[SUBNET ROUTING METHOD 62](#_Toc152099220)

[MULTIVALUED ROUTING METHOD 63](#_Toc152099221)

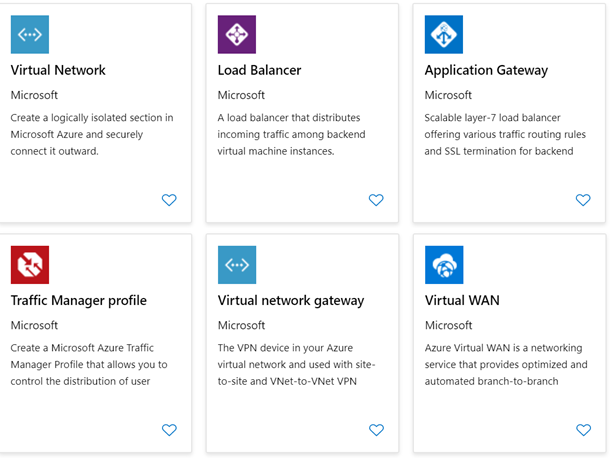
[WEIGHTED ROUTING METHOD 63](#_Toc152099222)

[AZURE FRONTDOOR 64](#_Toc152099223)

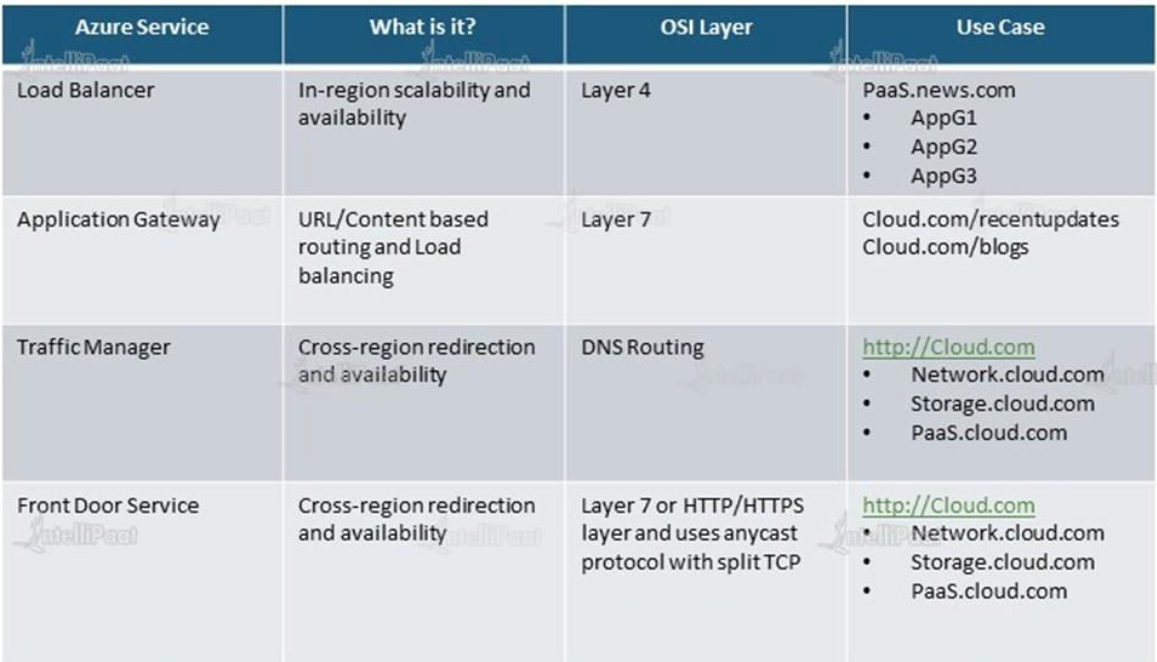
## ROUTING SERVICES IN AZURE

* In Azure, the Routing service refers to Azure routing capabilities that manage and control network traffic within the Azure environment.

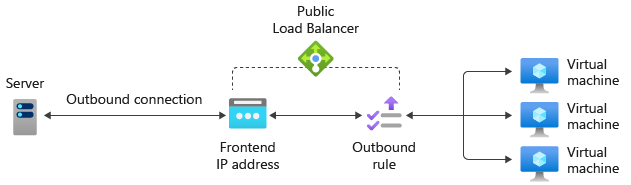
ROUTING SERVICES IN AZURE



1. AZURE VIRTUAL NETWORK (VNET):
   1. Azure Virtual Network is the foundation of the Routing service in Azure. It allows you to create isolated virtual networks where you can define subnets, IP address ranges, and network security groups. VNets serve as the logical boundaries for routing traffic within Azure.
2. AZURE VIRTUAL NETWORK GATEWAY
   1. Azure Virtual Network Gateway is a routing service that provides secure and private connectivity between Azure virtual networks and on-premises networks. It enables Site-to-Site VPN or ExpressRoute connections, allowing you to extend your on-premises network to Azure.
3. AZURE LOAD BALANCER
   1. Azure Load Balancer is a routing service that distributes incoming network traffic across multiple backend resources, such as virtual machines or virtual machine scale sets, to ensure high availability and scalability.
   2. It supports both internal and public-facing applications.
4. AZURE TRAFFIC MANAGER
   1. Azure Traffic Manager is a DNS-based global load balancing and routing service.
   2. It allows us to distribute incoming network traffic across multiple endpoints in different Azure regions or across different deployment environments.
   3. It helps optimize application performance and availability.
5. AZURE APPLICATION GATEWAY
   1. Azure Application Gateway is a web traffic load balancer and application delivery controller.
   2. It provides advanced routing and security features for HTTP/HTTPS traffic, such as URL-based routing, SSL termination, and web application firewall (WAF) protection.
6. AZURE FIREWALL
   * Azure Firewall is a managed network security service that provides stateful packet filtering and network address translation (NAT).
   * It helps secure Azure virtual network by enforcing application and network-level policies, including routing rules.

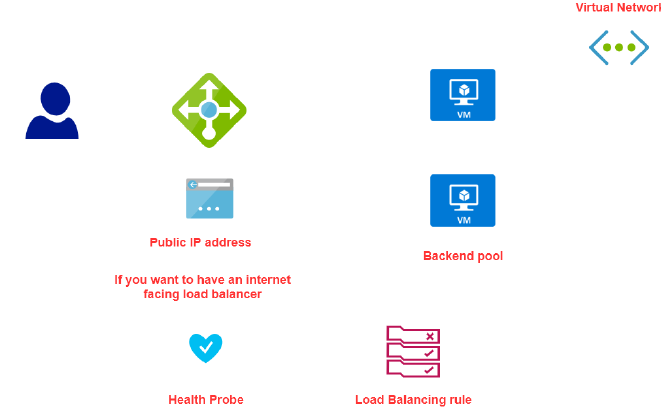


## LOAD BALANCER



* The Load Balancer Service, distribute the user requests across the pool of resources (e.g., Azure virtual machines) to maintain availability.
* *The azure load balancer works on Layer 4(Transport Layer) and Application Gateway (Application Layer) of the OSO Model*

### LOAD BALANCER CONCEPT



### COMPONENTS OF LOAD BALANCER

|  |  |
| --- | --- |
| **BACKEND POOL** | * When we create a load balancer, we specific the backend pool, which is a set of VMs to which the LB will route the traffic to. |
| **FRONTEND IP** | * The LB has a public IP address (called Frontend IP address). * The user can be able to access the VM via public IP of the load balancer. * The redirect of request from LB to VM are done via private IP of VM |
| **HEALTH PROBE** | * This helps the LB monitor the health of VMs in the backend pool |
| **LOAD BALANCING RULES** | * These rules drive how request can be distributed across the VM (which are part of backend pool) |

### LOAD BALANCER SKUs

* The Azure load balancer comes in 2 pricing model (SKU)
  + **BASIC LOAD BALANCER**
  + **STANDARD LOAD BALANCER**

|  |  |
| --- | --- |
| BASIC LOAD BALANCER | STANDARD LOAD BALANCER |
| *Free* | *Charges on Per hour basis* |
| *The VM in the backend pool must be part of availability set or scale set* | *VM can be an independent machine that are part of a VNET* |
| *Health Probes support TCP and HTTP only* | *Health Probes support TCP and HTTP and HTTPS* |
| *No support for availability zone* | *Support for availability zone* |
| *NO SLA* | *SLA of 99.99%* |

### TYPES OF LOAD BALANCER

There are 2 types of load balancer

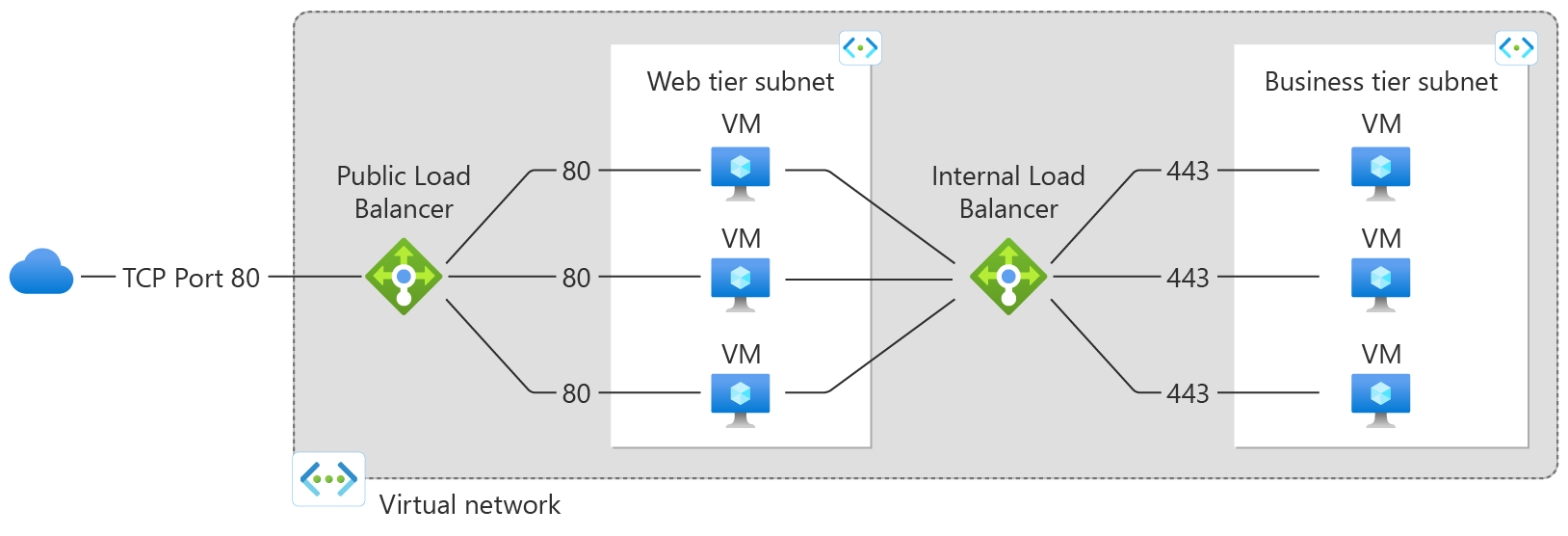
1. PUBLIC LOAD BALANCER

* A [public load balancer](https://learn.microsoft.com/en-us/azure/load-balancer/components#frontend-ip-configurations) can provide outbound connections for virtual machines (VMs) inside your virtual network.
* These connections are accomplished by translating their private IP addresses to public IP addresses.
* Public Load Balancers are used to load balance internet traffic to your VMs.

1. INTERNAL LOAD BALANCER

* An [internal (or private) load balancer](https://learn.microsoft.com/en-us/azure/load-balancer/components#frontend-ip-configurations) is used where private IPs are needed at the frontend only.
* Internal load balancers are used to load balance traffic inside a virtual network.
* A load balancer frontend can be accessed from an on-premises network in a hybrid scenario.

#### INTERNAL LOAD BALANCER



|  |  |
| --- | --- |
|  | * The internal load is used to direct traffic only between Azure’s internal resources i.e., the resources managed by Azure infrastructure or resources connected to Azure infrastructure using secure VPN * Internal load balancer can be used when want to divide the traffic to coming from other Azure Resources * It can also use internal load balancer or the traffic coming from on-premises network that is connected to an Azure resource via s secure VPN connection. |

#### PUBLIC LOAD BALANCER

* Public load balancer is used to handle the traffic between public facing IP address of incoming traffic to private IP address of Azure resources.

### BASIC LOAD BALANCER (VMs in AVAILABILITY SET)

|  |  |
| --- | --- |
|  | * **The VM has to part of Scale set or availibility set** |

#### SETTING UP BASIC LOAD BALANCER (VM IN AVALIBILITY SET)

* ***STEP 1*:**
  + *We will create VMs, which will be a part of an* ***Availability Set (Make sure the VMs are part of same VNET)***
  + *The VM will have no public IP address as the communication between LB and VMs will be done via private IPs*
  + *Availability Sets can be used in conjunction with Azure Load Balancer to distribute traffic across multiple VMs within the set, providing load balancing and scaling capabilities.*
* ***STEP 2:*** *Install IIS with a Default.html page.*
* ***STEP 3:*** 
  + *Create a Public IP address (Note public IP address is a separate resource in Azure).*
  + *The Public IP will be assigned to the Load Balancer. Also known as* ***Front End public IP address***
  + *We can use Basic SKU of Public Ip for Basic load balancer & Standard SKU for Standard load balancer.*
* ***STEP 5:*** *Create a NSG which will be attached to at the subnet level of which VM is part of. Note – the NSG created with the VMs must be detached.*
* ***STEP 6:*** *Create and configure a Load Balancer resource. As part of configuration -we need to set up a Backend pool of the VMs created in Step 1*
* ***STEP 7:*** *Configure the health probe to check the health of VM in the backend pool*
* ***STEP 8:***  *Create Load balancing Rules – which will give the routing of request to the VM in backend pool*
* ***STEP 9:*** *Now we can be able send the request to load balancer via its public IP address, which will then redirect the traffic to VM in the backend pool.*

#### SETTING UP BASIC LOAD BALANCER (VM IN SCALE SET)

STEP 1: *We will create VMs, which will be a part of an* ***Availability Set***

**In this step**

1. **Port 80 has been enabled**
2. **ISS has been installed on the VM**
3. **After validation of IIS installation – Disassociate the Public IP address of VM**

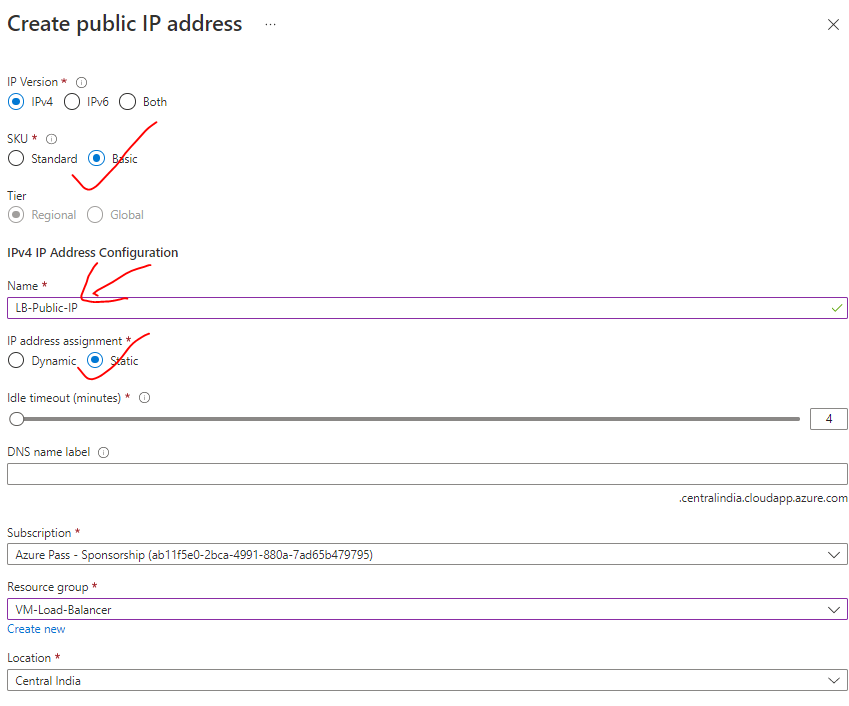


|  |  |
| --- | --- |
|  | * The communication between the Load balancer and the VMs in the backend pool – happens using private IP address. * For now – let’s keep the public IP address so that we can deploy IIS and validate it. * After that we can disassociate the public IP address from the VM as the communication between LB and VM are through private IPs |

**DISASSOCIATE PUBLIC IP FROM VM**

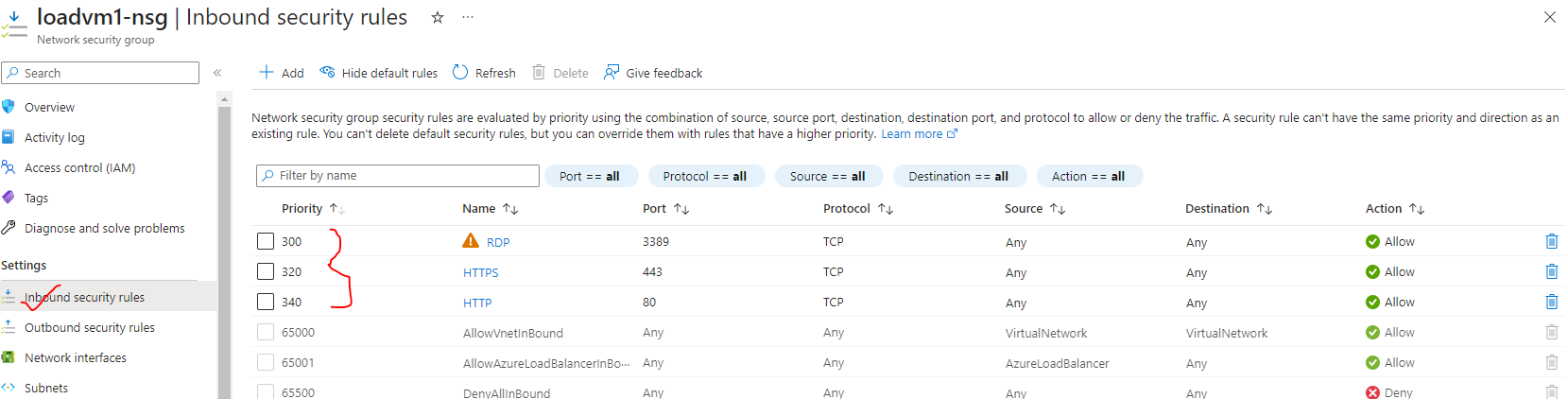
|  |  |
| --- | --- |
|  | 1. Go to VM 🡪 Networking 🡪Network Interface 🡪 IP Configuration 2. Disassociate the Public IP and make the provide IP as a static Ip 🡪 Save |

***STEP 3:*** *Create a Public IP address (Note public IP address is a separate resource in Azure). The Public IP will be assigned to the Load Balancer. Also known as Front End public IP address.* ***For basic load balancer the IP must be of type Basic SKU***



***STEP 4:*** *Disassociate the NSG associated with the VM*

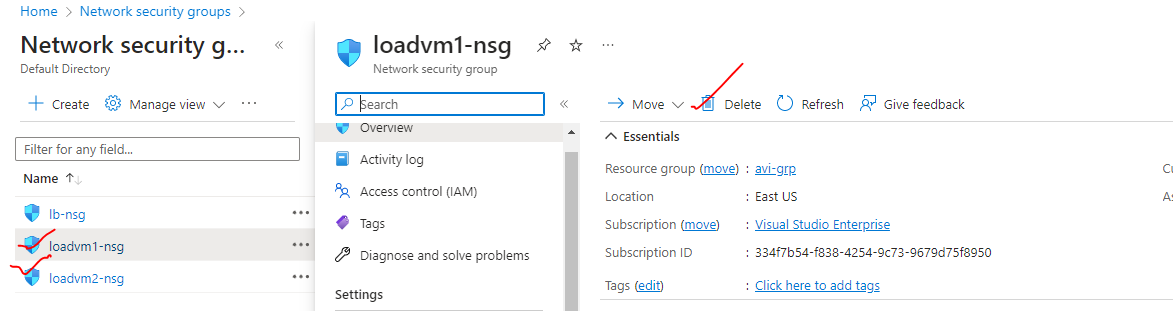
1. Delete the NSG Rule



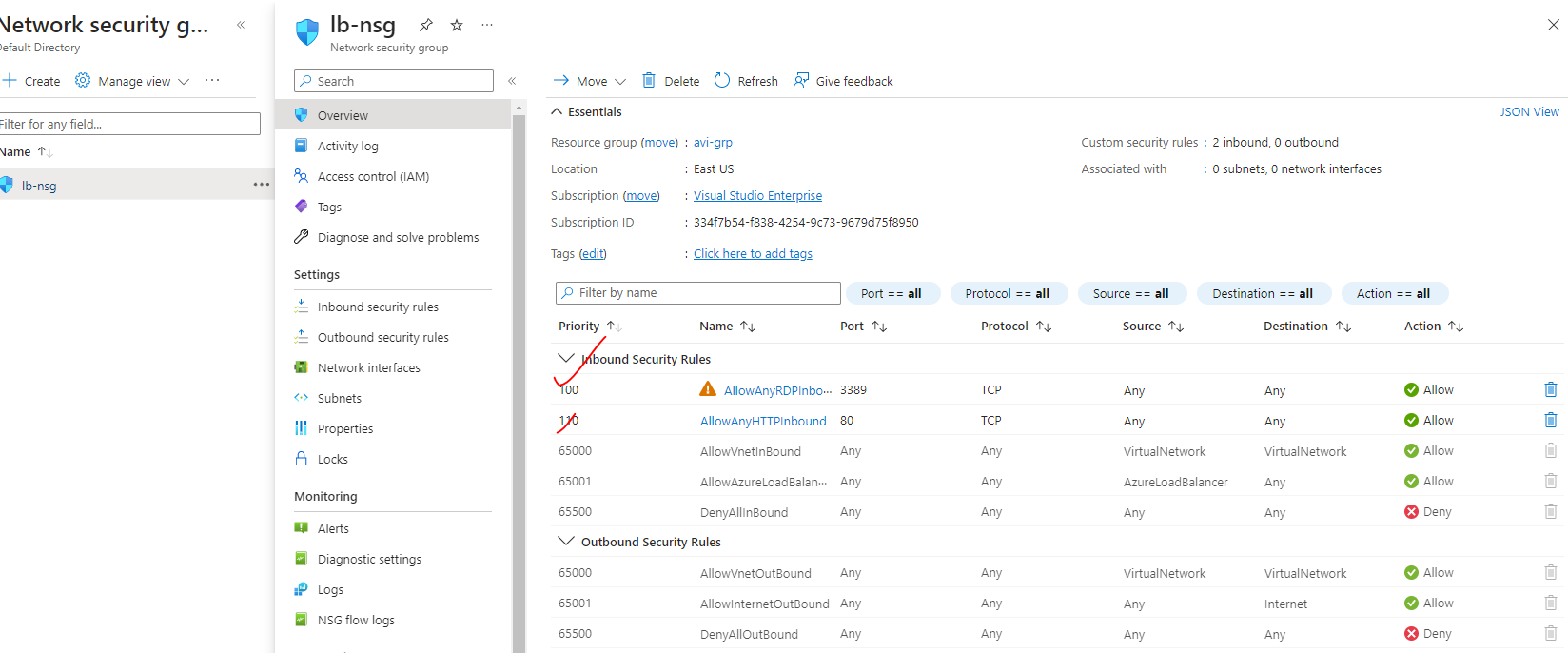
1. Disassociate the NSG from the NIC

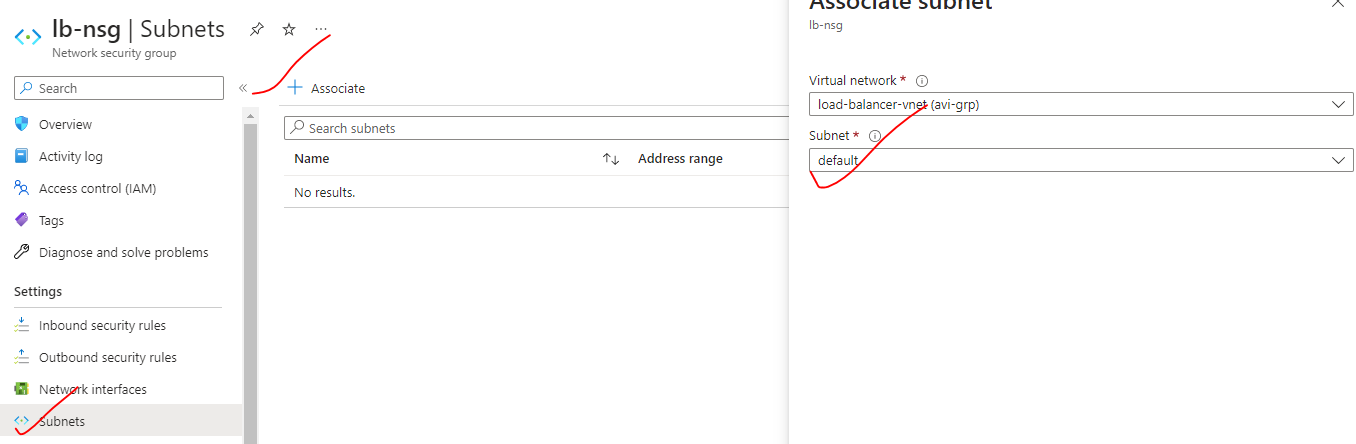


1. Delete the NSG



***STEP 5:*** *Create NSG and attach it to the subnet level of the VM.(Associate the subnet with the NSG)*





***STEP 7:*** *Create and configure a Basic Load Balancer resource. As part of configuration -we need to set up a Backend pool of the VMs created in Step 1*

|  |  |
| --- | --- |
| BASIC | FRONT END CONFIGURATION |
|  | Create the Load balancer  Note – Backend pool configuration can be done while configuring the LB  **TIER CONFIGURATION**  REGIONAL – VMs is a region will be load balanced  **GLOBAL –** VMs across multiple regions can be load balanced. |

##### LOAD BALANCER CONFIGURATIONS

###### CONFIGURING BACKEND POOL

|  |  |
| --- | --- |
|  | Add the VMs in the backend pool |

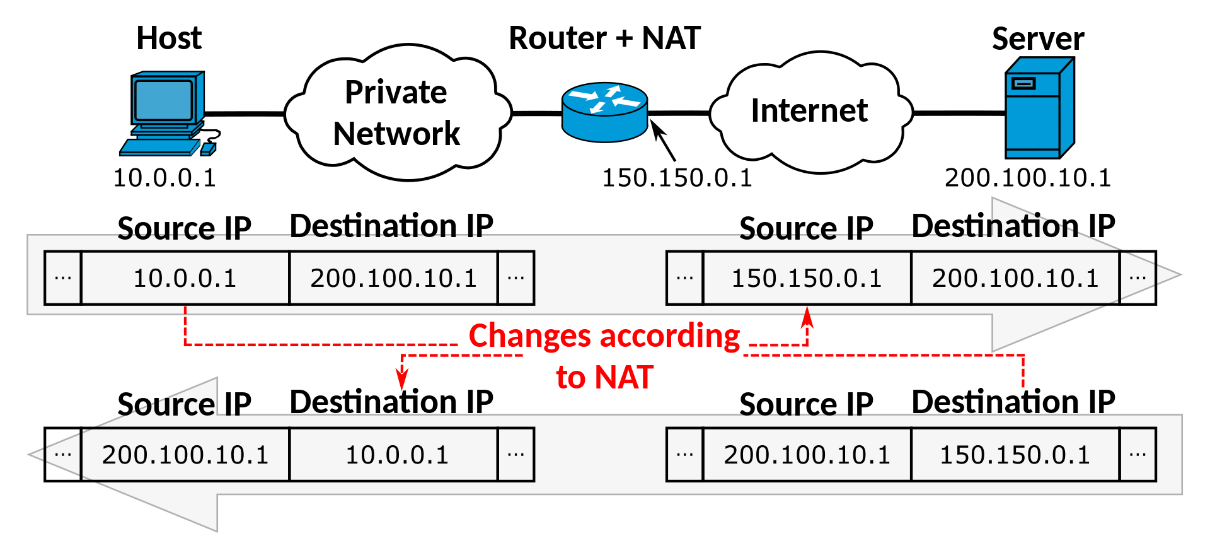
###### CONFIGURING HEALTH PROBE

|  |  |
| --- | --- |
|  | * After the interval of every 5 second – Load balancer will initiate a TCP handshake. if the VM acknowledge the TCP request – then the LB will know that VM is healthy |

###### CONFIGURING LOAD BALACING RULES

|  |  |
| --- | --- |
|  | * PORT- 80 - This setting is the port associated with the frontend IP that you want traffic to be distributed based on this load-balancing rule. * **BACKEND PORT** – It’s the Port in the VM which is the PORT of the IIS- This means – If the request comes to port number 80 of the load balancer (normal HTTP web request default port is 80) – then it will be distributing the traffic to backend pool port.   Load balancer rule reference diagram |

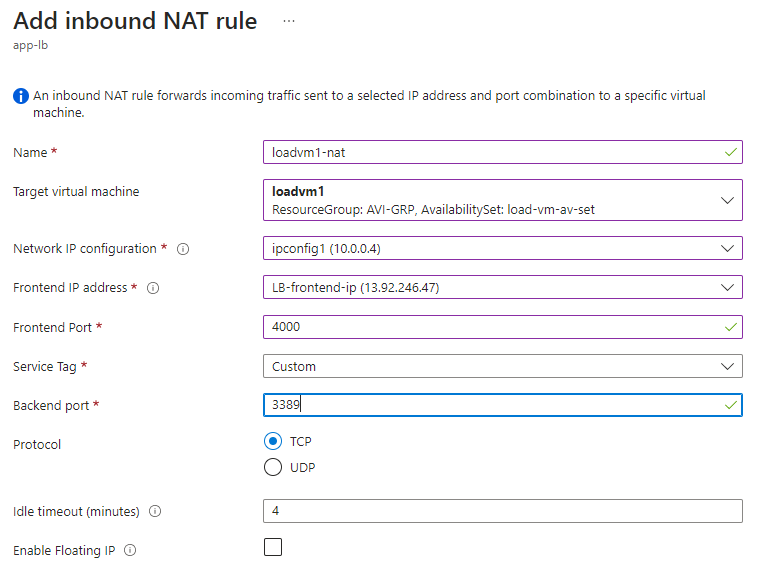
### LOAD BALANCER NAT RULES

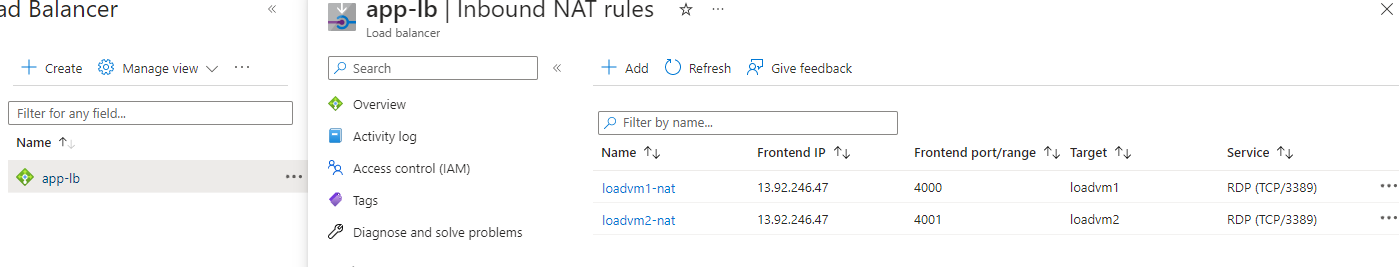


The primary purpose of NAT is to conserve public IP addresses, as the number of available public IP addresses is limited. With NAT, a router or firewall device sits between the private network and the internet, acting as a mediator. It translates the private IP addresses used within the local network to a single public IP address when communicating with external networks.

|  |  |
| --- | --- |
|  | * As the backend VMs don’t have public IP addresses, we can’t be able to connect these VM to internet or RDP onto these machines. * For such use cases, Load balancer provide option to connect to those VMs using its own public IP address, this is done with the help of ***NAT (Network Address Translation)*** * *Go to the load balancer 🡪 Inbound NAT rules 🡪 Add* * **Note- We need to add the NAT rules for all the connected VMs** |

* The Frontend port is a random port given for each connected VM. The will be used to connect (RDP) with the VM
* Backend port is the default port number for RPD

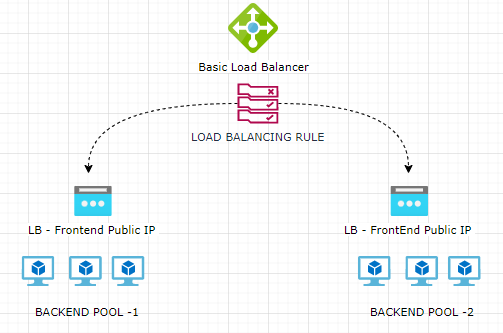




|  |  |
| --- | --- |
|  | * To connect with the respective VM we use   **<LOAD\_BALANCE\_FRONTEND\_IP>:<FRONT END PORT CONFIGURED FOR THE VM>** |

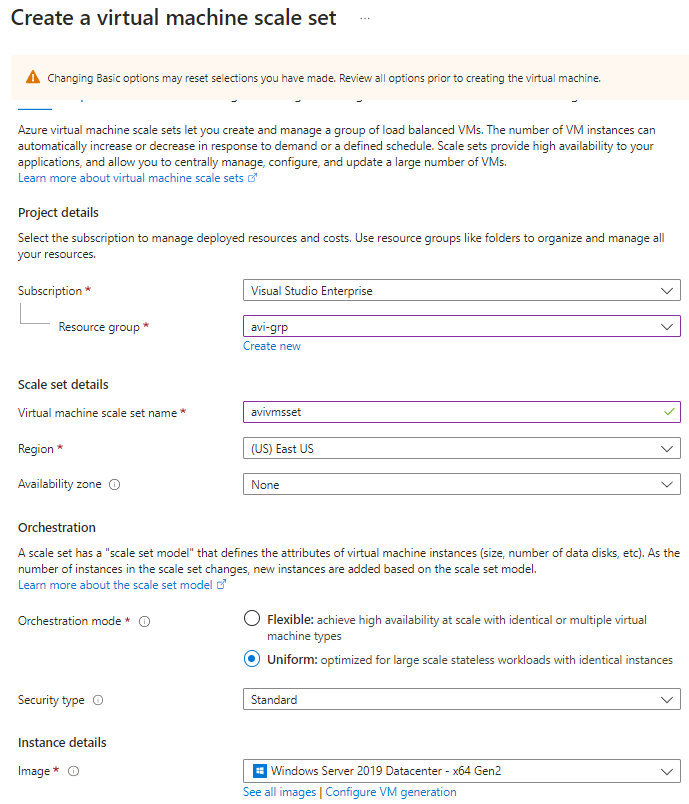
### MUTIPLE BACKEND POOL AND FRONTEND IP ADDRESS OF LB

* The load balancer can have multiple frontend public IP addesss through which it can manage multiple backend pools using the load balacing rules
* <https://learn.microsoft.com/en-us/azure/load-balancer/load-balancer-multivip-overview>

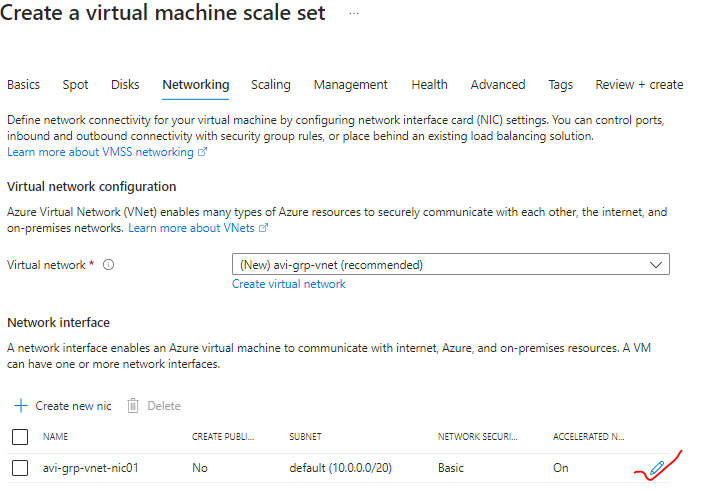


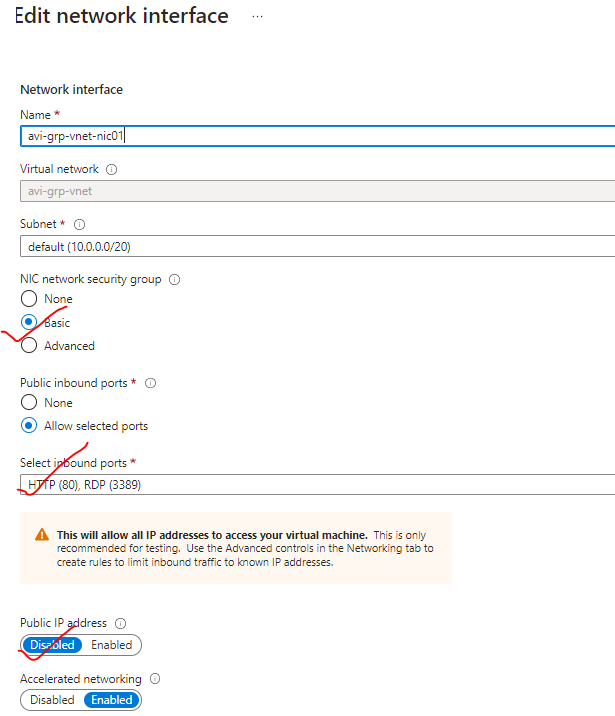
### BASIC LOAD BALANCER (SCALE SET)

#### STEP 1: CREATE A VM SCALE SET



**NETWORKING**: Allow the HTTP & RDP ports





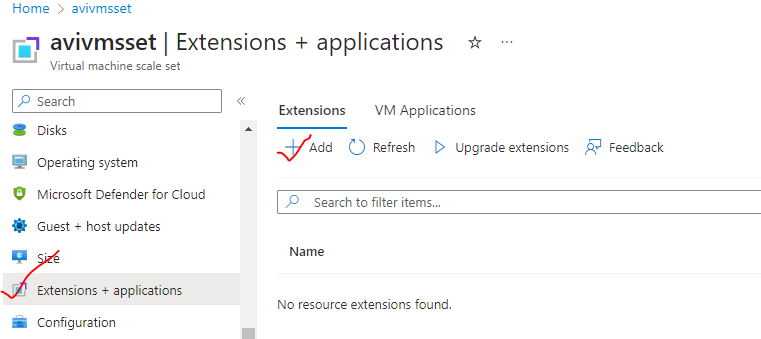
|  |  |
| --- | --- |
|  | * Let’s keep the initial instance count as :1 |
|  |  |

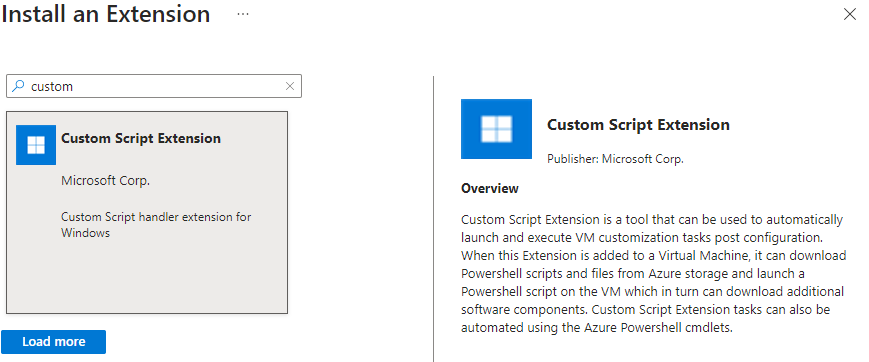
#### STEP 2: UPLOAD THE SCRIPT IN THE STORAGE ACCOUNT

* CREATE STORAGE ACCOUNT
* UPLOAD THE SCRIPT IN THE EXTENSION
* To install IIS on VM scale set – we can make use of ***custom script extension***. For that we need to **Create Storage Account and upload a script to install IIS**

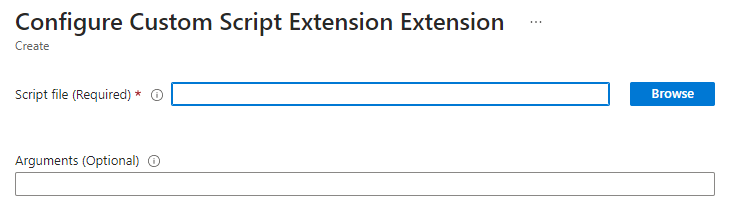
|  |  |
| --- | --- |
| WINDOWS VM (installing IIS)  NEED TO CREATE POWERSHELL FILE – e.g – iis.ps1 | LINUX VM(install nginx)  Need to create Bash file : install\_web.sh |
| import-module servermanager  add-windowsfeature web-server -includeallsubfeature  set-content -path "C:\inetpub\wwwroot\Default.html" -Value "<h1>Sever name: $($env:computername)</h1>" | apt-get update -y && apt-get upgrade -y  apt-get install -y nginx |

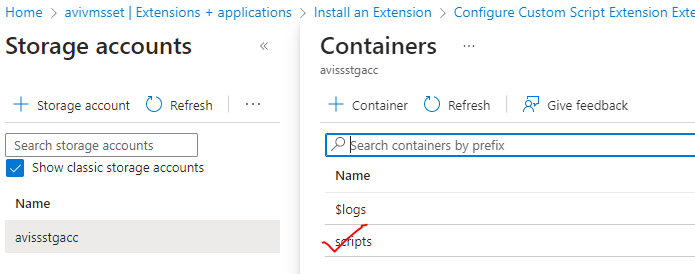
#### STEP 3: INSTALL CUSTOM SCRIPT EXTENSION AND RUN



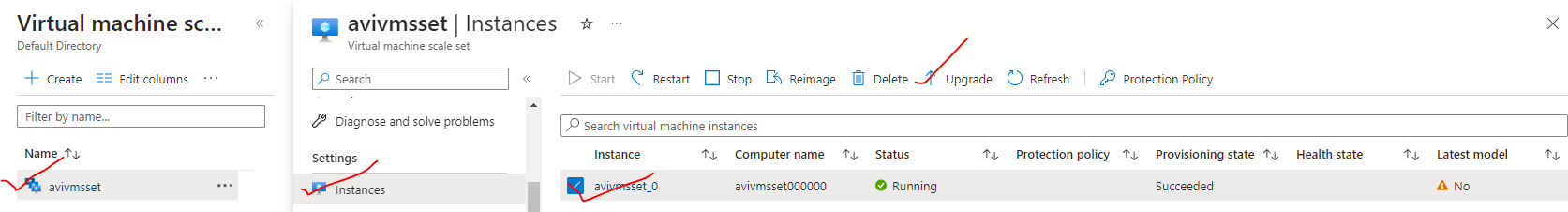


1. Browse the Storage account container (scripts)
2. Then select the script 🡪 Create

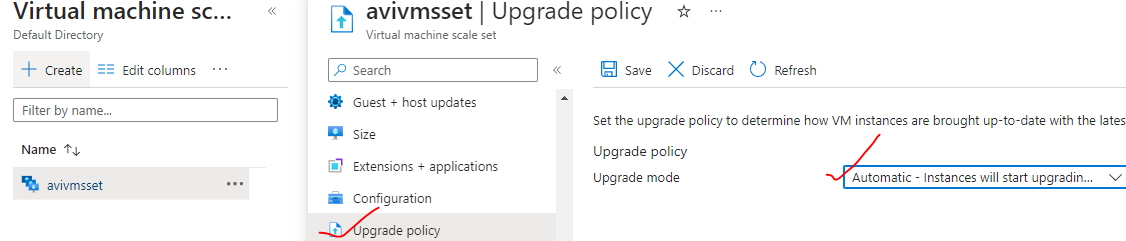




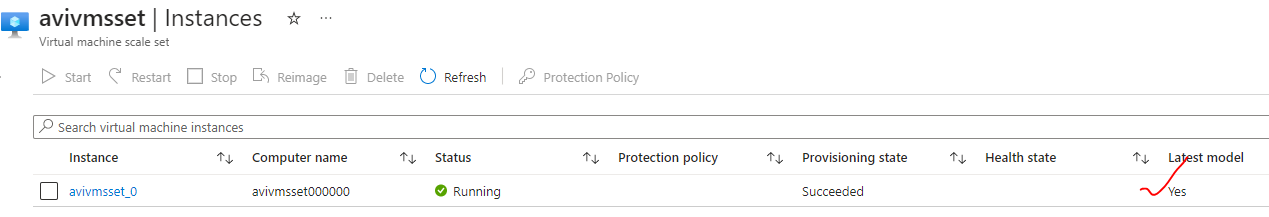
#### STEP 4: UPGRADE THE SCALE SET TO APPLY CUSTOM SCRIPT CHANGES



* **SET THE UPGRADE POLICY TO BE AUTOMATIC**



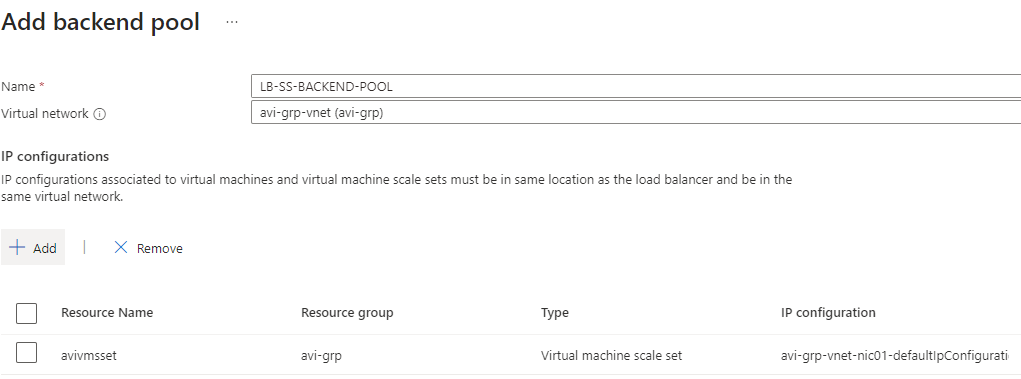
Since we setup the upgrade policy to Automatic – the scale set is showing Latest model as “Yes”



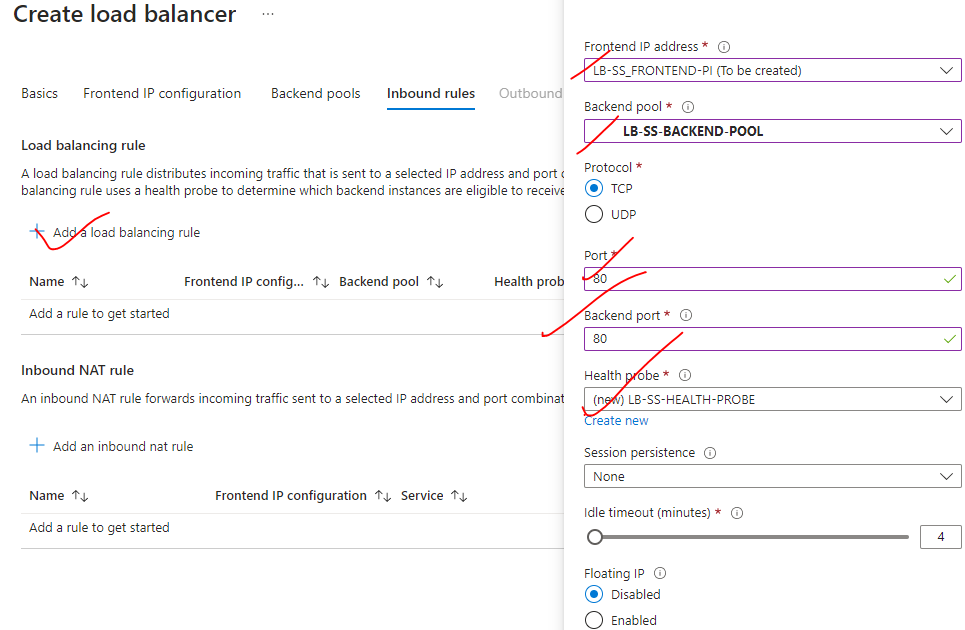
#### STEP 5: SET UP THE LOAD BALANCER

Create a basic load balancer. Configure the

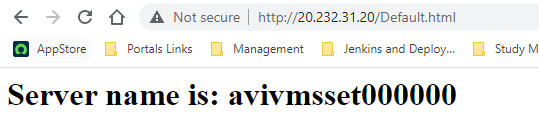
1. Frontend IP
2. Public IP
3. Backend pool as VM scale set



1. Set up the load balancing rule



#### STEP 6: ACCESS THE VM IN THE SCALE SET VIA LB FRONT END IP

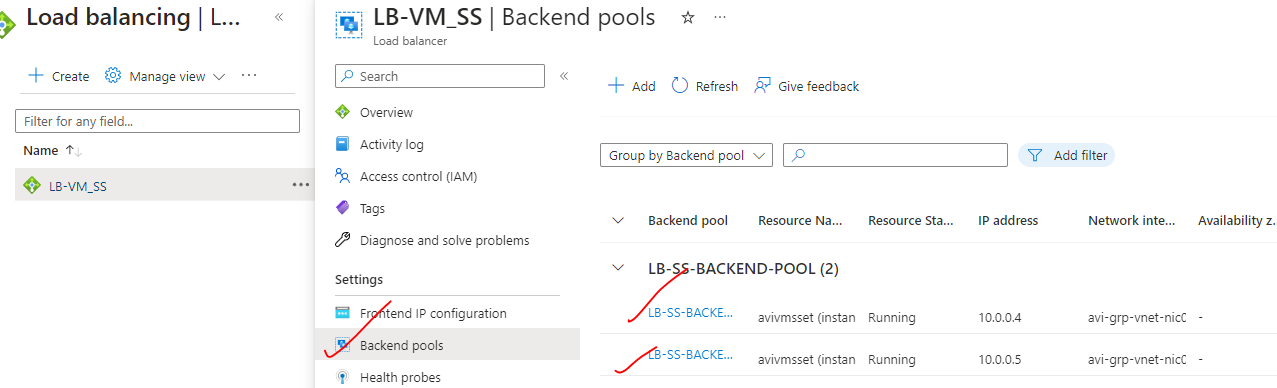


#### STEP 7: ADDING INSTANCES TO VM SCALE SET (MANUAL SCALING)

* While setting up the scale set we added just one instance to the scale set.
* To validate – whether the load balancer is load balancing the traffic withing the VMs of the Scale set – we can more instances.
* The new instance will be added on to the virtual machine scale set for that new instance. The custom script extension, installing internet information services and having the Default.html page in place at the same time.
* Along with that - the instance will be also reachable from the Azure load balancer.
* In the below example – lets increase the instance count = 2

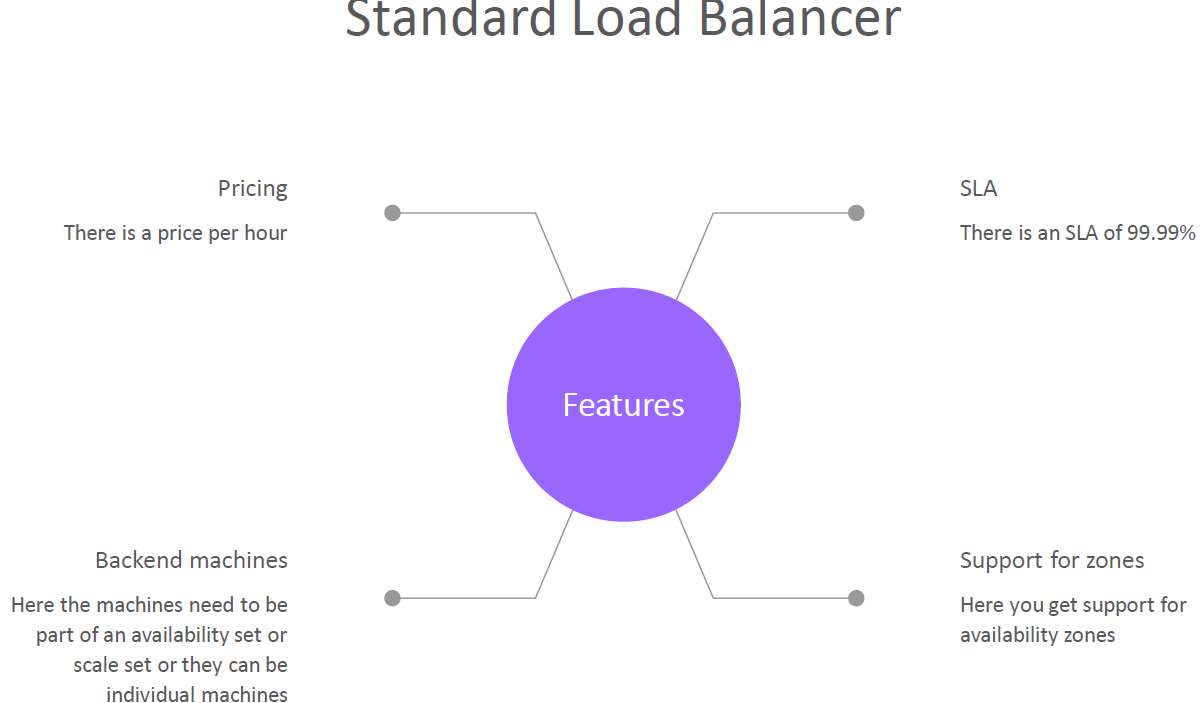


The instance will automatically get added to the backend pool of the load balancer



### STANDARD LOAD BALANCER

* Comparison between Basic and Standard load balancer: <https://learn.microsoft.com/en-us/azure/load-balancer/skus#skus>
* For high availability – we should choose Standard load balancer.
* ***For standard load balancer- any virtual machines or virtual machine scale sets, but they have to part of same virtual network***. They need not to be part of VMSS or Availability Set as needed in basic load balancer



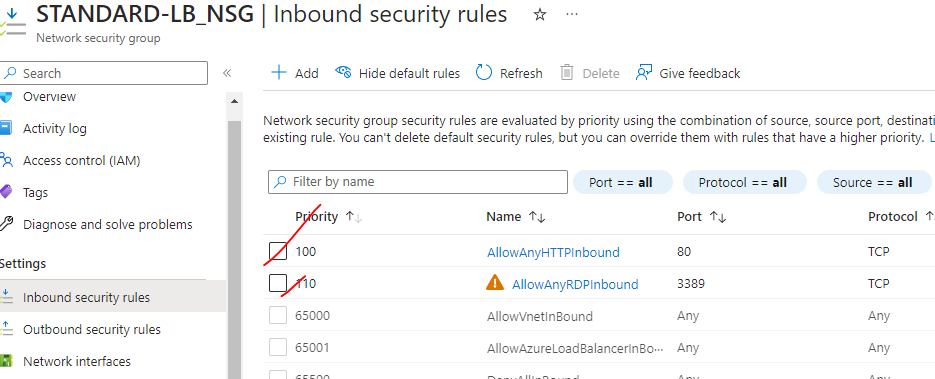
#### SETTING UP STANDARD LOAD BALANCER

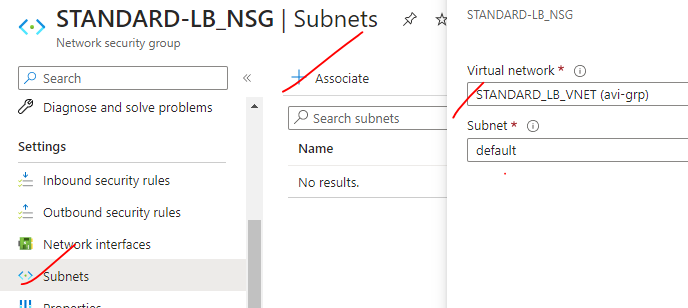
1. **Step 1: Create a Storage account and upload the custom script to install IIS to all VMs**

|  |  |
| --- | --- |
|  | **Step 2: Create 2 VMs**   1. The VMs will have no public IP address. 2. The VMs will have no NSG attached – we will create NSG as separate resource and attach it at subnet level. |
|  | **Step 3:**   1. Install the custom script extension. 2. Browse to the custom script in the storage account container |

**Step 4: Create the NSG**

1. **Add the inbound rule for HTTP and RDP traffic.**
2. **Attach it to the Subnet**

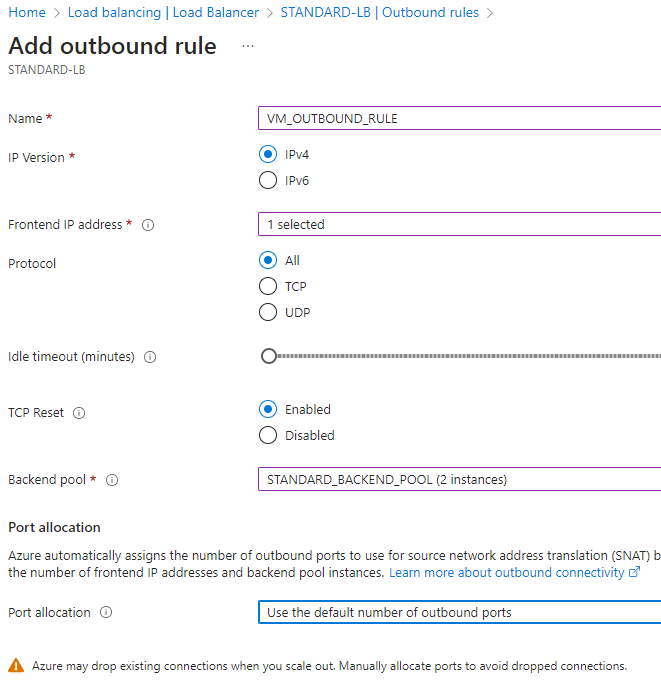




|  |  |  |
| --- | --- | --- |
|  | **STEP 5: CREATE THE LOAD BALANCER**  **Note – The Standard load balancer supports HTTPS health probe too.**  ***What's the difference between the TCP protocol and HTTP protocol in the standard load balancer?***  In HTTP health probe - The probe is going to make a HTTP request onto the path configured in the path. If it gets a response back, then it will consider backend instance has healthy. | |
|  | For the Standard load balancer:   * The public IP should also be of Standard SKU * The standard SKU creates a “***static public IP address***” | |
| **SET UP THE LOAD BALANCING RULE** |  | |
|  | | **INBOUND NAT RULES**   * To access the VMs using RDP – we need to configure the NAT rules. * We need to use the frontend IP of the Load balance for RDP   **<Public\_ip>:<frontendport of vm>**   * By default, the outbound connection from the standard LB to internet will be disabled – which must be enabled explicitly |
|  | |  |

#### OUTBOUND RULE

* When we access the VM via LB’s public IP. The outgoing internet connection from the VM are disabled.
* To enable it we need to configure the outbound rule - ***Go to the Outbound rules of the LB*** 🡪 configure the following.

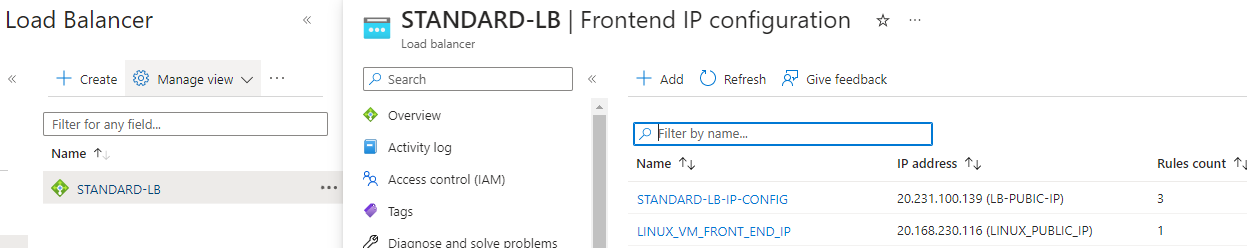


#### MULTIPLE BACKEND POOL

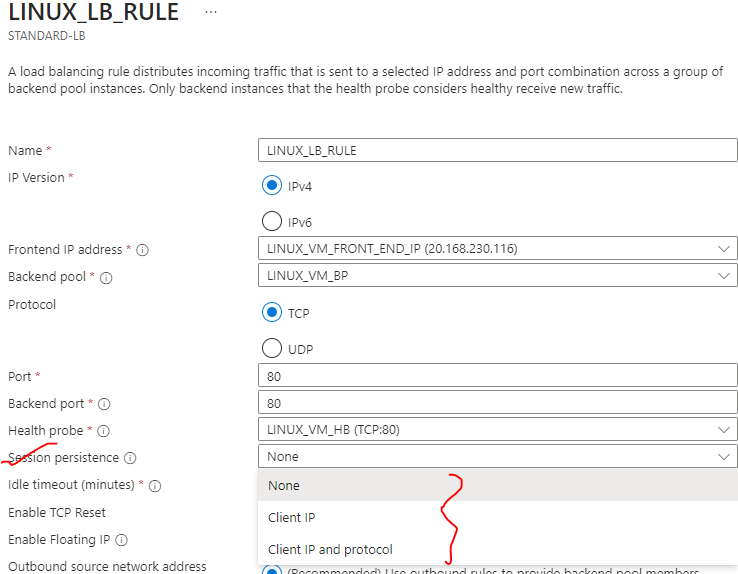
|  |  |
| --- | --- |
|  | * **The standard load balancer can have multiple backend pool.** * **To route the traffic to respective backend pool we can have dedicated frontend IP address.** |

To configure the Multiple backend pool

|  |  |
| --- | --- |
|  | Create a VM that can be added to the backend pool. |
|  | CREATE NEW FRONTEND IP FOR NEW BACKEND POOL |
|  | CREATE A NEW HEALTH PROBE FOR NEW BACKEND POOL |
|  | CREATE A NEW LOAD BALANCING RULE FOR NEW BACKEND POOL |

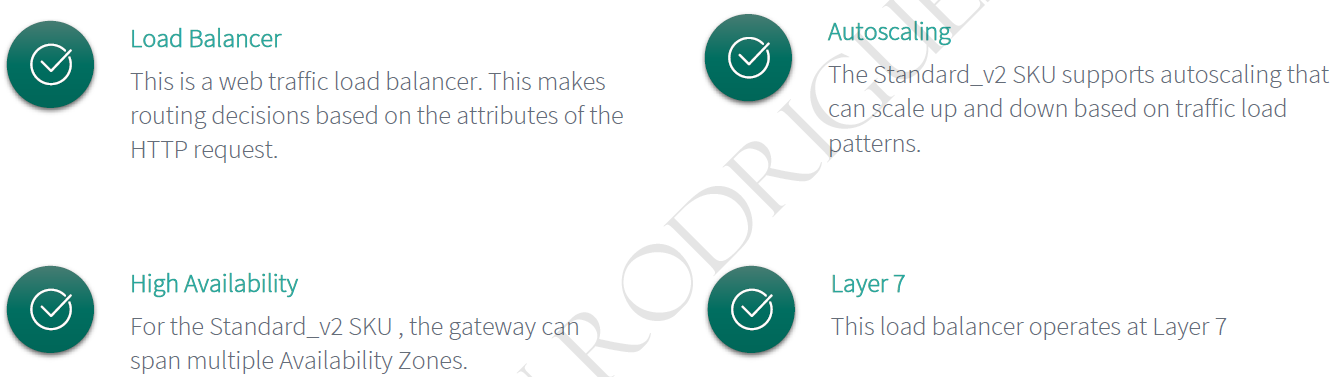


#### LOAD BALANCER SESSION PERSISTENCE



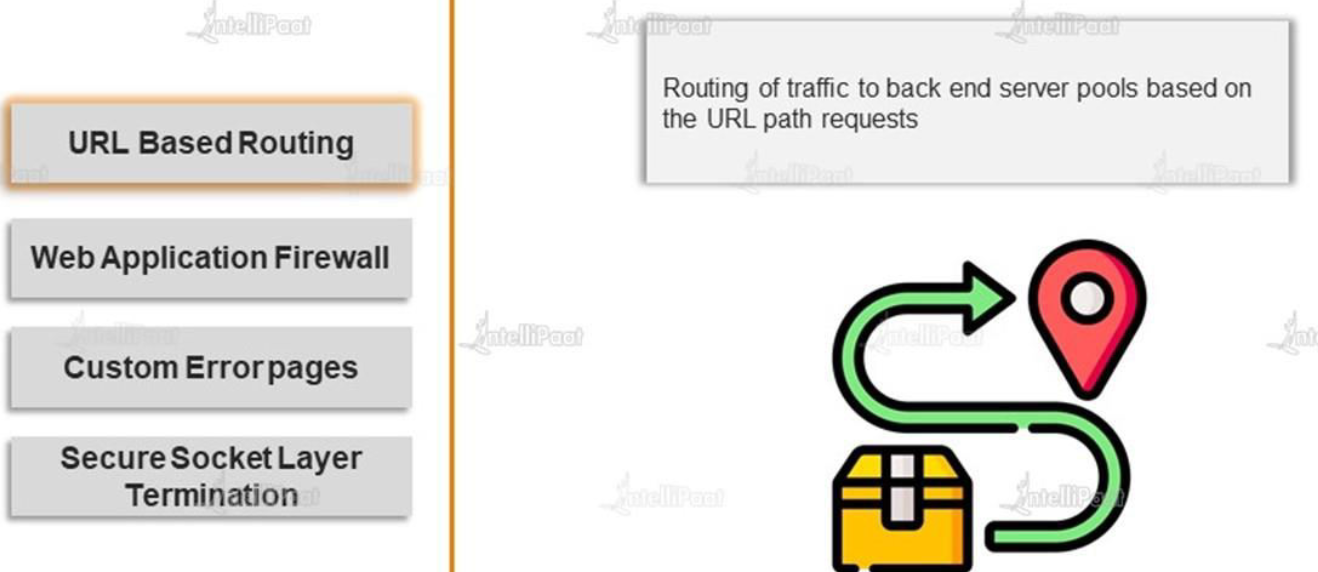
* Let's say that we have a user that has made a request via the load balancer on its frontend public IP address and the user has been directed on to load VM-1.
* If we **enable session persistence**, the load balancer will kind of create an affinity to the session between the load balancer and the client. Hence, this particular user for that particular session will always be directed onto load vm-1
* **ADVANTAGE**
  + Helps in better performance for the sessions itself. - if we don't want in a particular session the request to be distributed across the VMs
* **DISADVANTAGE**
  + But the disadvantage is if we have long sessions in those sessions – all the requests are directed towards loadvm-1 causing more load in loadvm-1) but load Vm2 may not be having that much load

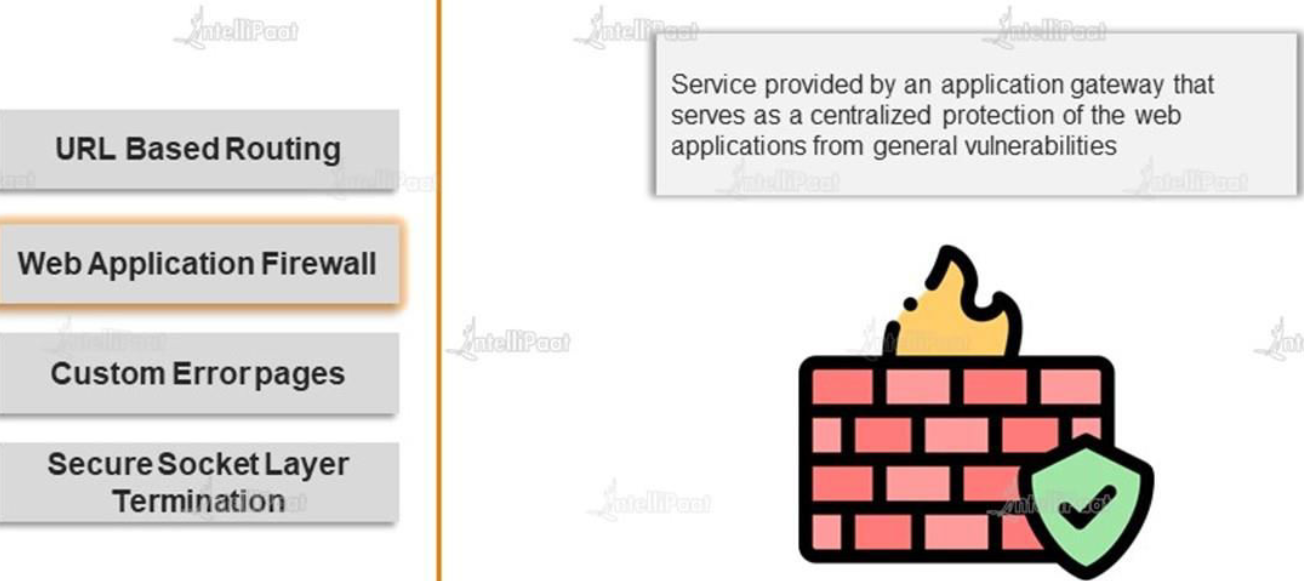
## AZURE APPLICATION GATEWAY

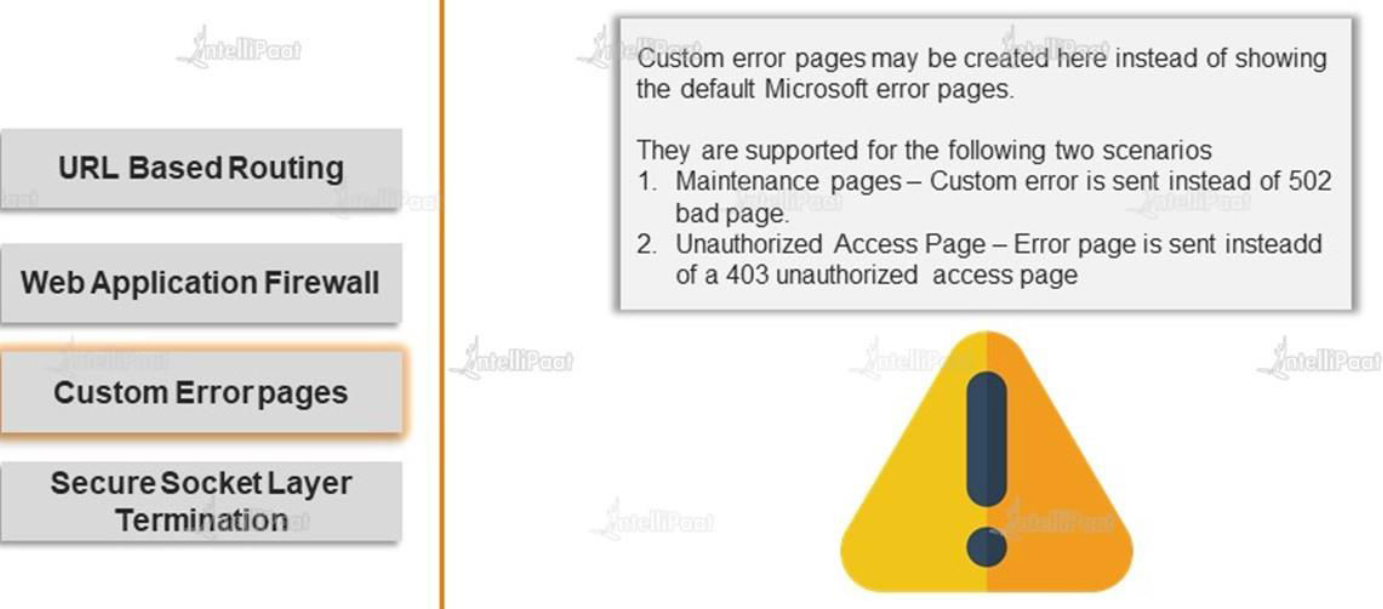


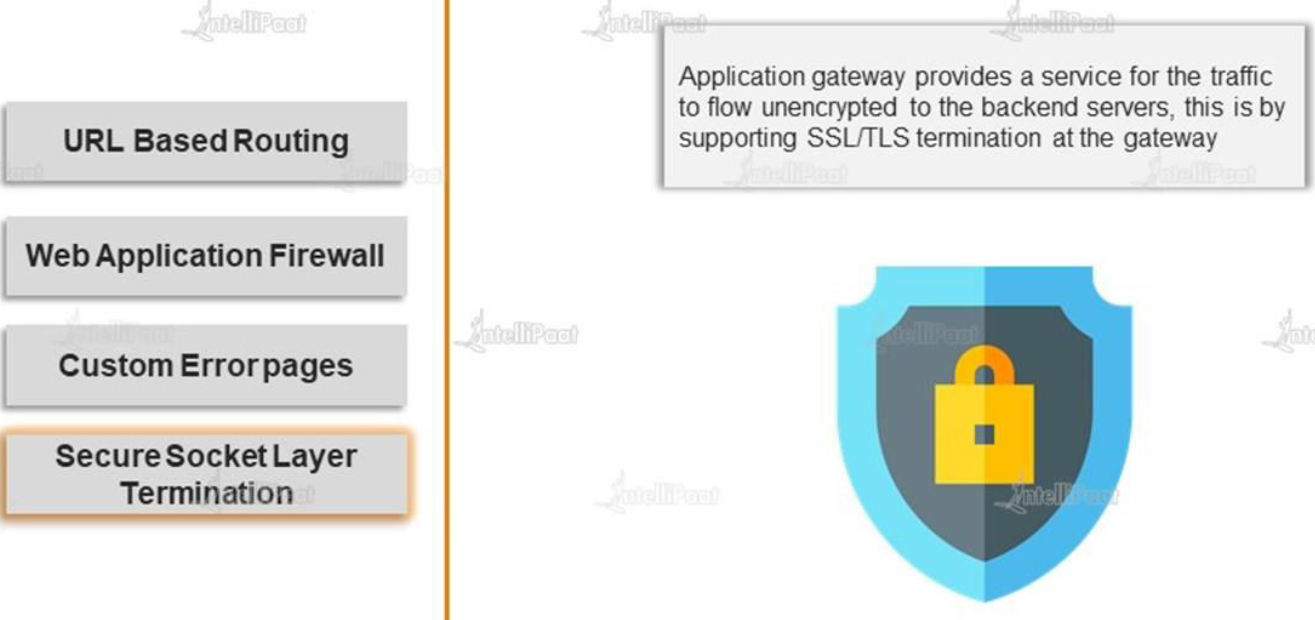
* Unlike other load balancer - Application Gateway not just simply routes the request on to backend pools- but it routes based on the URL.
* Azure Application Gateway is also enabled with Web Application firewall (WAF). It protects the applications against attacks which can be implemented on top of the Azure Application Gateway.

### APPLICATION GATEWAY FEATURES

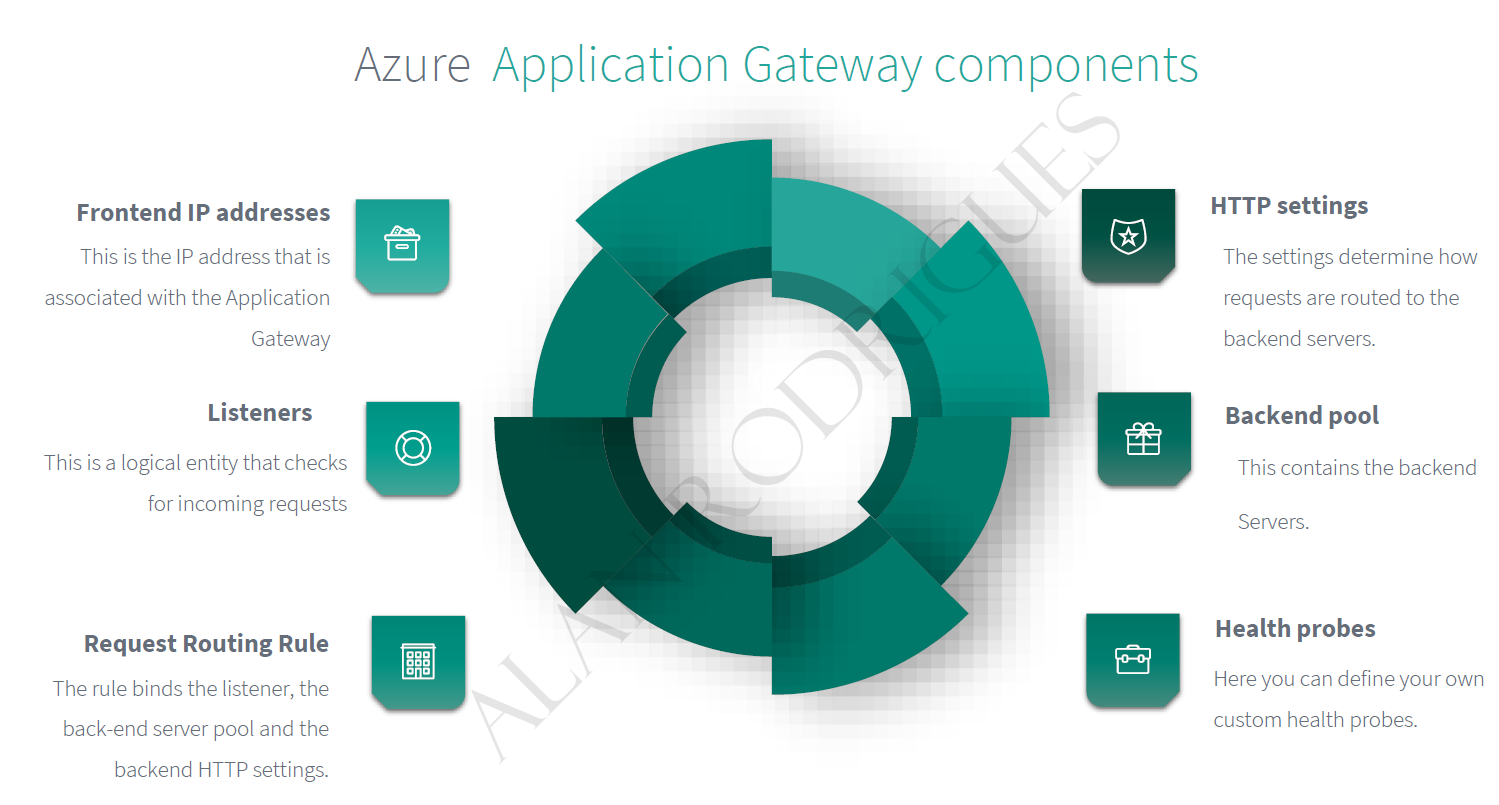




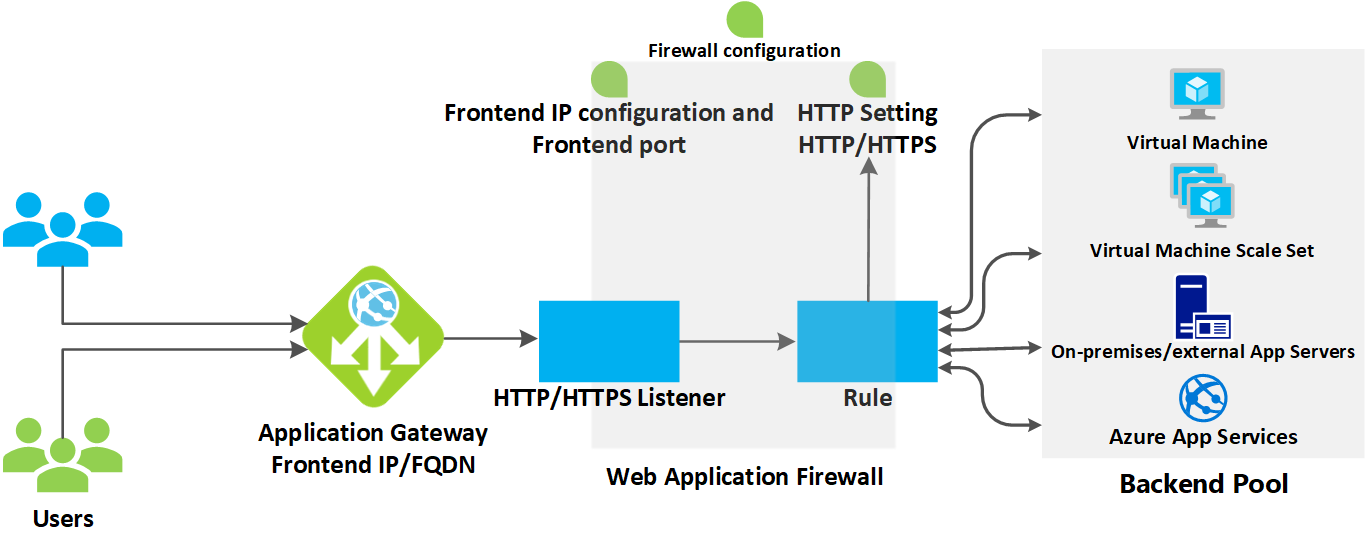




### APPLICATION GATEWAY COMPONENTS



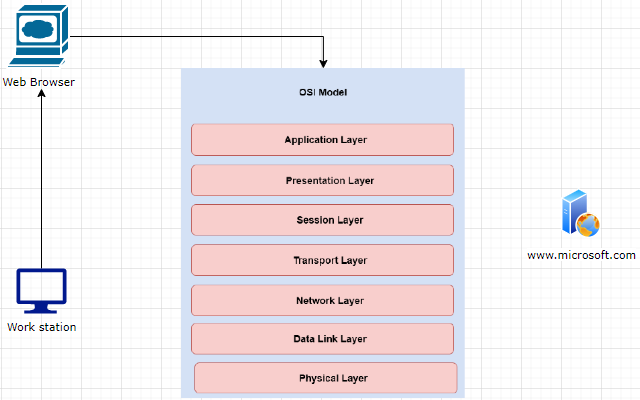
1. As the application Gateway a routing service so instead of users directly going on to the applications hosted in the backend pool (like VM, VMSS, Web app or On Premises), they make request to the frontend public IP address of Azure Application Gateway.
2. In App gateways – VM in the backend can be VM in availability set, VMSS - But here we have the added advantage of adding other endpoints as well on to the backend pool.
3. We can have one or more listeners -so that it can listens for user requests configured on App Gateway
4. The rules in the App gateway defines how the traffic is routed onto the backend pool.
5. The settings define the configuration of the backend pool. For example - if we want secure requests on services in the backend pool, we can define as part of HTTP settings.

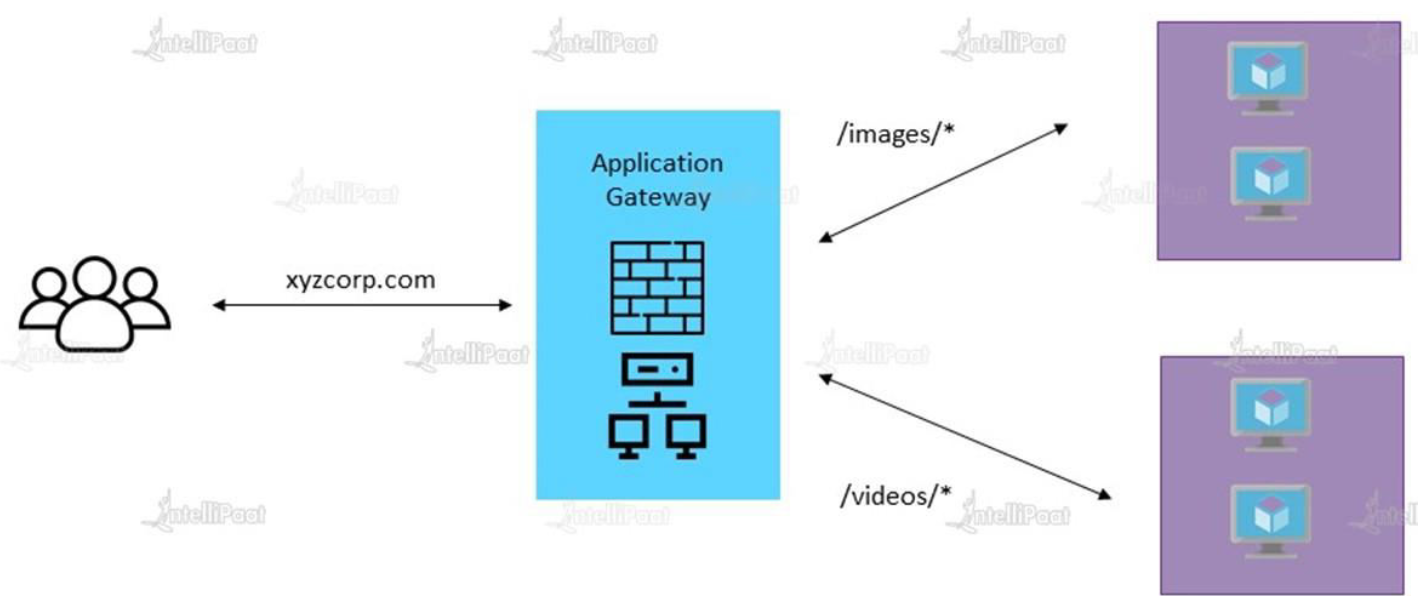


|  |  |
| --- | --- |
| **BACKEND POOL** | In the backend pool we can have   1. **VM & VM SCALE SETS** 2. **WEB APP** 3. **ON PREM SERVERS** |
| **FRONTEND-IP** | * Public IP of load balancer |
| **HTTP/HTTPS LISTENER** | * The application gateway is going to listen for requests on the front end IP address |
| **RULES** | * These rules decide how the traffic is routed to backend pool. |
| **HTTP/HTTPS SETTINGS** | This setting determines how the traffic will be routed to backend pools |

### APPLICATION GATEWAY – PATH BASED ROUTING

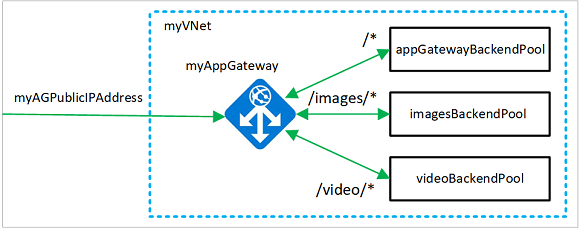
* As App gateway is a layer 7 load-balancer. It will all different HTTP request attributes. Hence this information helps in routing the traffic based on path





* **In the Azure Application Gateway – we have another feature which we can enable known as the Web Application firewall to protect the web applications from Internet based attacks.**

### SETTING UP APPLICATION GATEWAY – URL ROUTING



#### STEP 1: SET THE VMS

* Create 2 VMs. Let’s call it as imagesVm and videosVm
* Install IIS in both VMs .
* Create a images folder in imagevm and place Default.html
* Create a videos folder in videovm and place Default.html

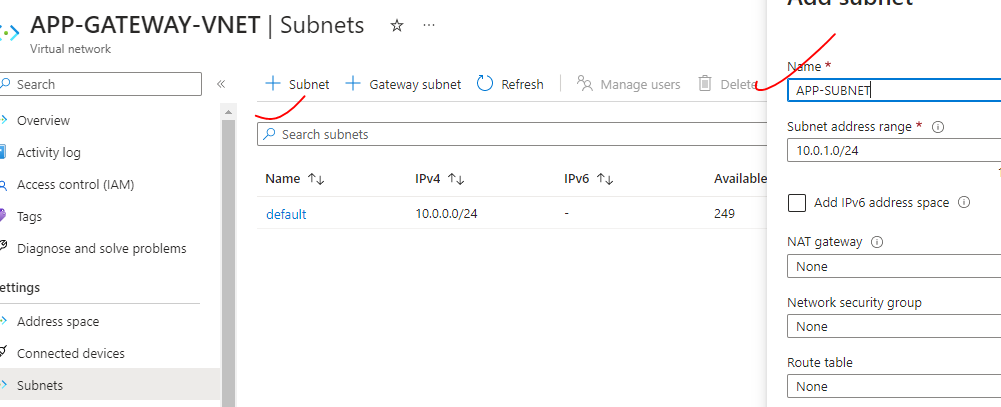
***With this set up – request via Application gateway frontend ip to the path “/images” will be routed to “imagevm” and “/videos” will be routes to videovm***

#### STEP 2: CREATE EMPTY SUBNET FOR APPLICATION GATEWAY

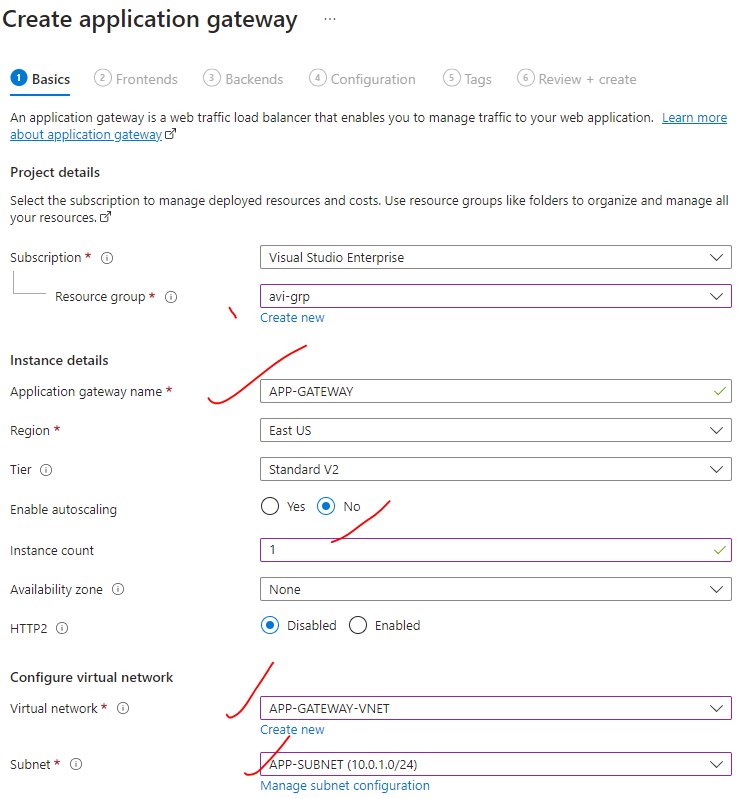
* Before deploying Application Gateway - we have to add a new subnet (empty subnet) In the VNET, (Note - VMS are deployed in default subnet)

NOTE:

* The Application Gateway is going to deploy its own compute machines, its own resources on to this empty subnet. These resources are required for the routing of traffic to the back-pool.
* Since App gateway is layer -7 load balancer - that means it needs to process the request, and then do the routing accordingly. That’s why it need an infrastructure (managed by Azure itself)

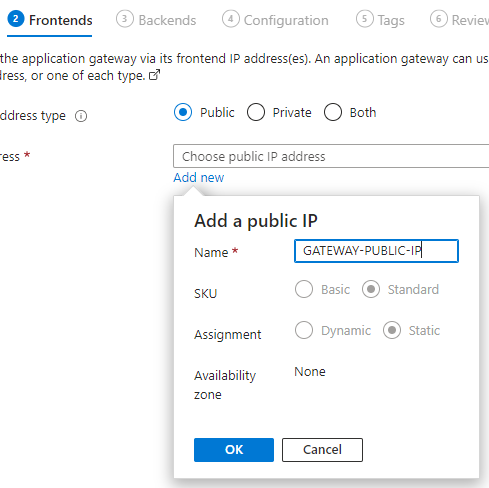


#### STEP 3: DEPLOY APPLICATION GATEWAY

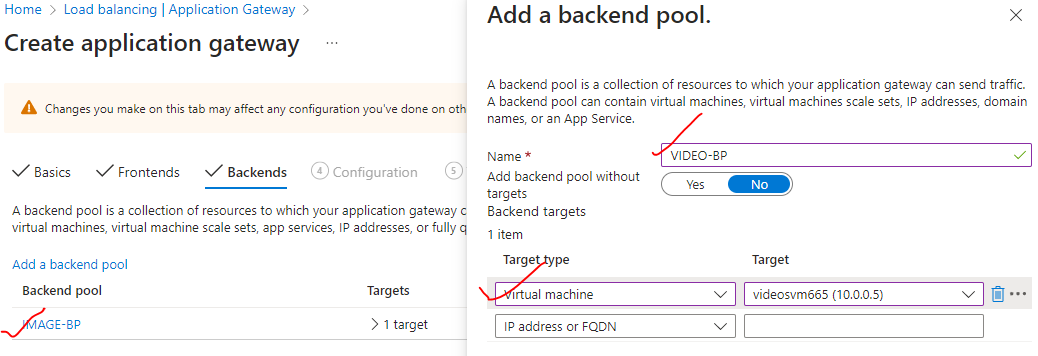


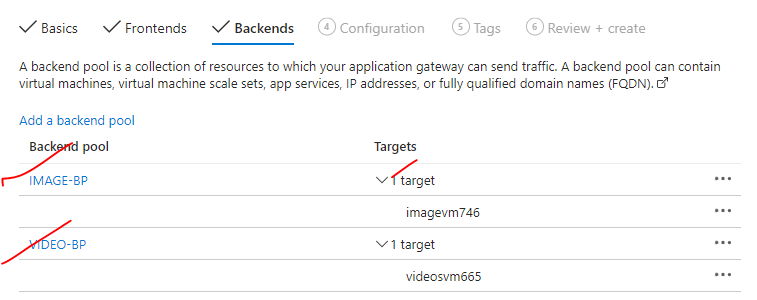
|  |  |
| --- | --- |
| AUTOSCALING | * The Application Gateway is going to deploy its own compute machine in the subnet where it is deployed. Hence – when demand increases it automatically scale up the amount of compute resources.(VMS) in the same subnet |

##### SET UP PUBLIC IP ADDRESS

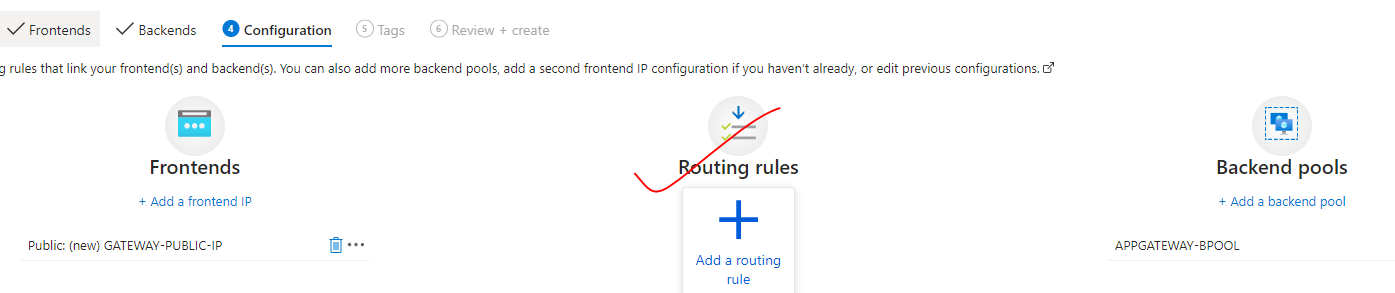


##### BACKEND POOL





##### SET UP THE ROUTING RULES



|  |  |
| --- | --- |
|  | * So here we have two types of listeners.   + BASIC LISTENER: Listens to just one domain name.   + MULTISITE: Listens on multiple domain names.   PATH CONFIGURATION |
|  | |

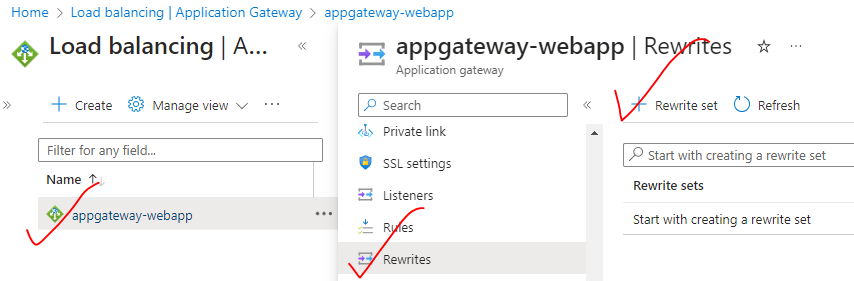
## APPLICATION GATEWAY – REWRITE

* The rewrite feature in an Application Gateway refers to
* the ability to modify or rewrite the URLs or HTTP headers of incoming requests before they are forwarded to the backend servers. It allows for URL manipulation and header modification to ensure proper routing and handling of requests.

KEY ASPECTS OF THE REWRITE FEATURE IN AN APPLICATION GATEWAY:

* URL REWRITING: The rewrite feature allows you to modify the URL path or query string of incoming requests. This can be useful in scenarios where you need to redirect or route requests to different backend servers based on specific URL patterns.
* HOST HEADER REWRITE: You can rewrite the host header of incoming requests to ensure that the backend servers receive the requests with the appropriate host information. This is particularly useful when you have multiple websites hosted on the same backend servers.
* HEADER MODIFICATION: The rewrite feature enables you to modify or add HTTP headers in the incoming requests. This can be helpful in scenarios where you need to add custom headers, manipulate existing headers, or remove certain headers before the requests reach the backend servers.
* PATH-BASED ROUTING: Application Gateway can rewrite the URL path of incoming requests to enable path-based routing. This allows you to route requests to different backend pools or servers based on specific path patterns.
* REDIRECTS AND REWRITES: You can configure the rewrite feature to perform URL redirects or rewrites. This allows you to redirect requests from one URL to another or rewrite the URL to a different format while preserving the user experience and ensuring proper routing.
* REGULAR EXPRESSIONS: Application Gateway supports regular expressions, allowing you to define complex matching patterns and rewrite rules based on regular expression patterns. This provides more flexibility in handling different URL or header scenarios.
* HTTP TO HTTPS REDIRECT: Application Gateway can be configured to automatically redirect HTTP requests to HTTPS. This ensures that all incoming requests are securely redirected to the appropriate HTTPS URL.

### SETTING UP RERWRITE FOR APP GATEWAY

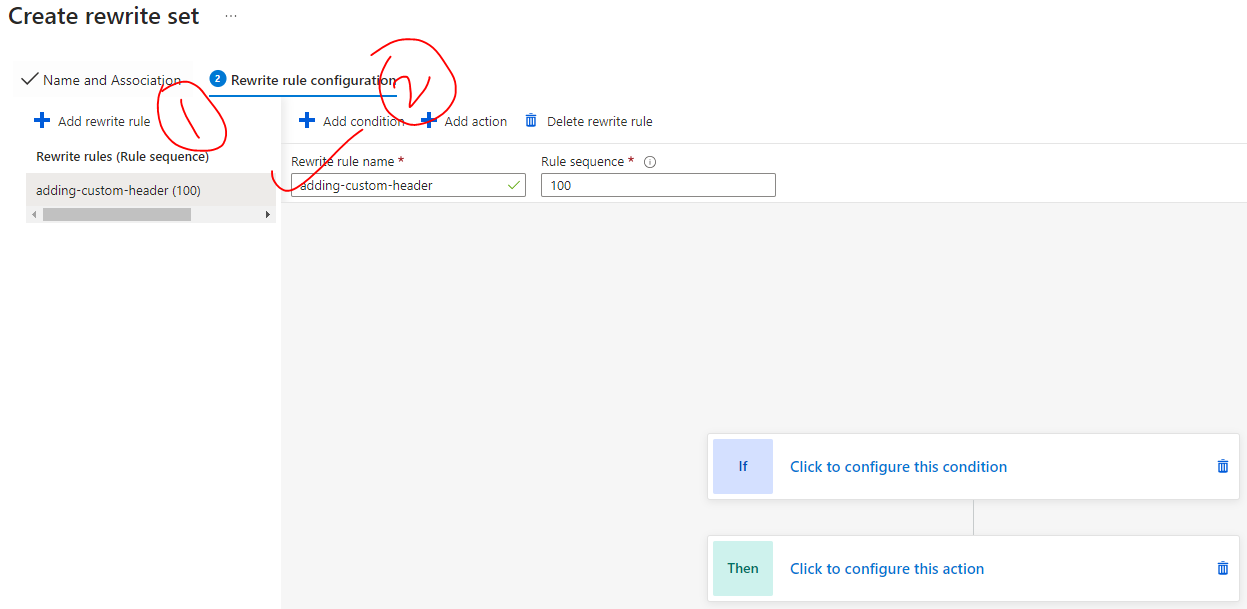


SELECT THE BACKEND TARGETS WHERE WE WANT TO SET UP THE REWRITE FOR

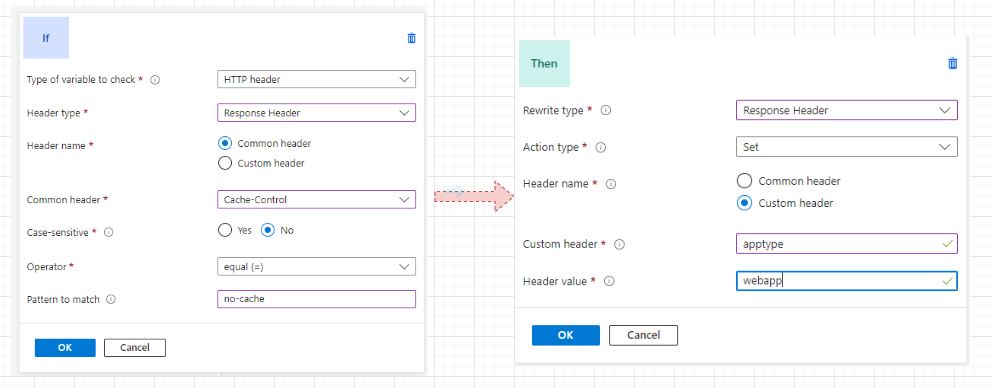
# 

Click on Add Rewrite Rule🡪 Give a name to the rewrite

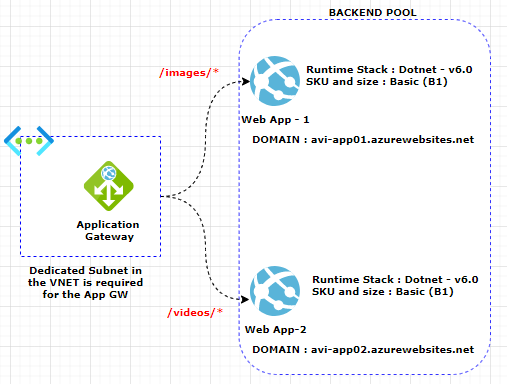
USE CASE: WE WANT TO SET A CUSTOM HEADER IF THE RESPONSE HEADER HAS CACHE-CONTROL: NO-CACHE



IF (CONDITION) AND THEN (ACTION)

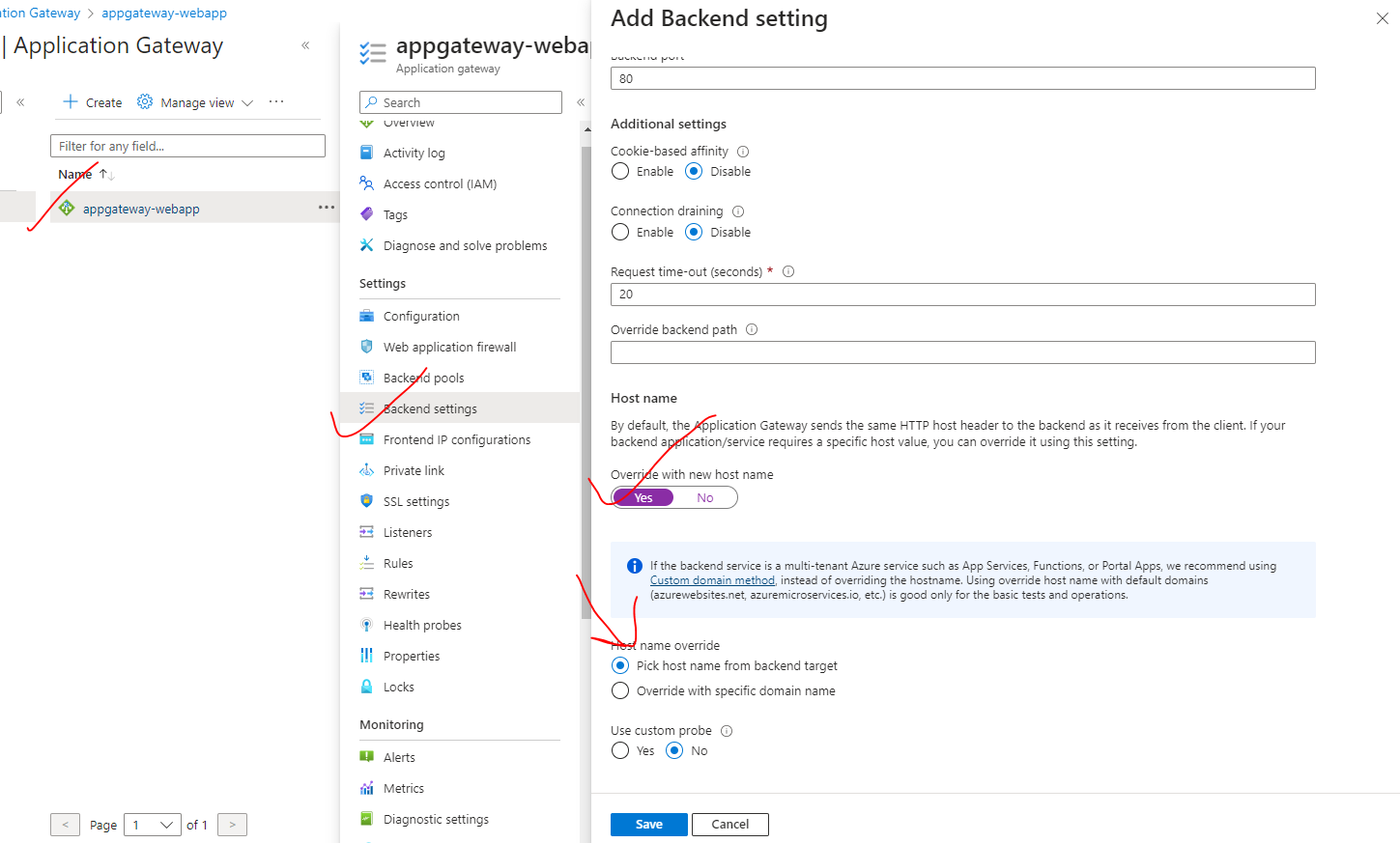


## APPLICATION GATEWAY WITH WEBAPP (URL ROUTING)



|  |  |  |  |
| --- | --- | --- | --- |
| 1. Step 1: SET UP 2 WEBAPP   *Create images and videos folder in respective app with a default .html* | |  |  | | --- | --- | |  |  | |

1. **UPDATE THE BACKEND SETTING**



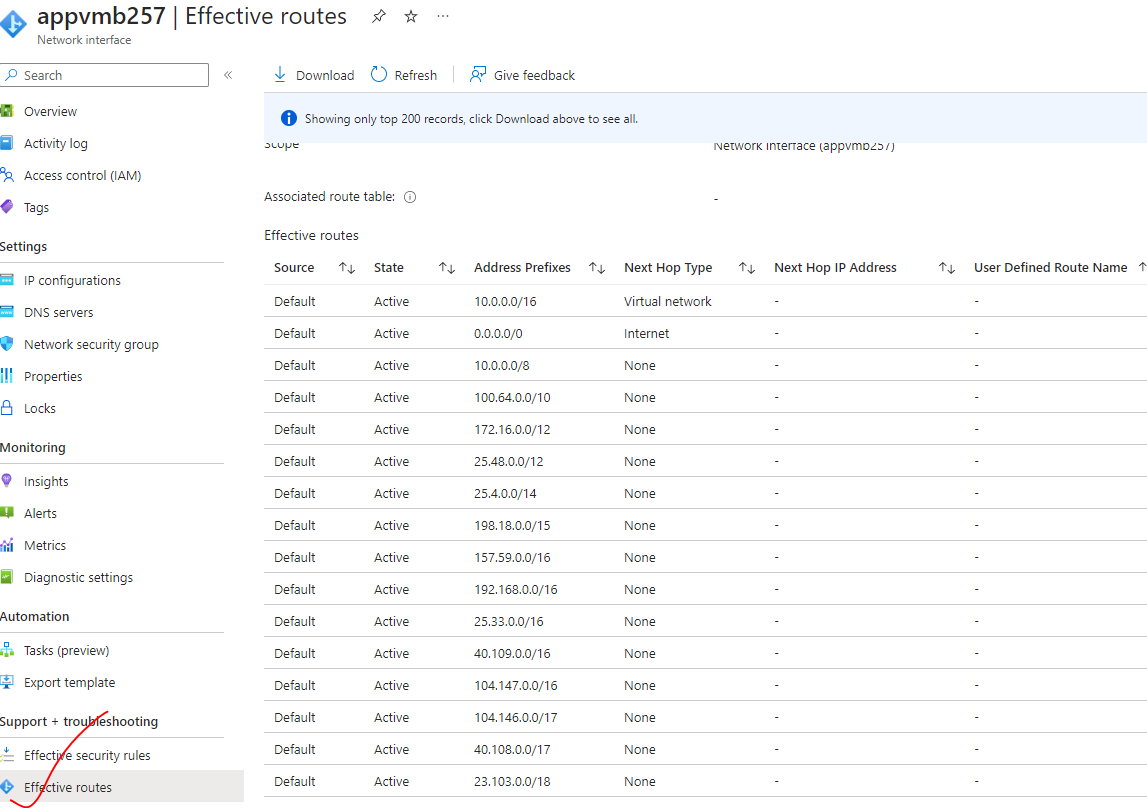
## APPLICATION GATEWAY WITH APIM

## USER DEFINED ROUTES

* In a virtual network- which has multiple subnets – we can have VMs located in each subnet. By default, they can communicate with each other(using private IP).
* In the VNET - this is a default system route that tells the packets of information how to be routed onto or how

to be routed from the source on to the destination virtual machine within the same virtual network itself.

* These default system routes are configured at the Network interface of the VMs. Similar to below we can create our own routes.



### USECASE - SETTING UP USER DEFINED ROUTE

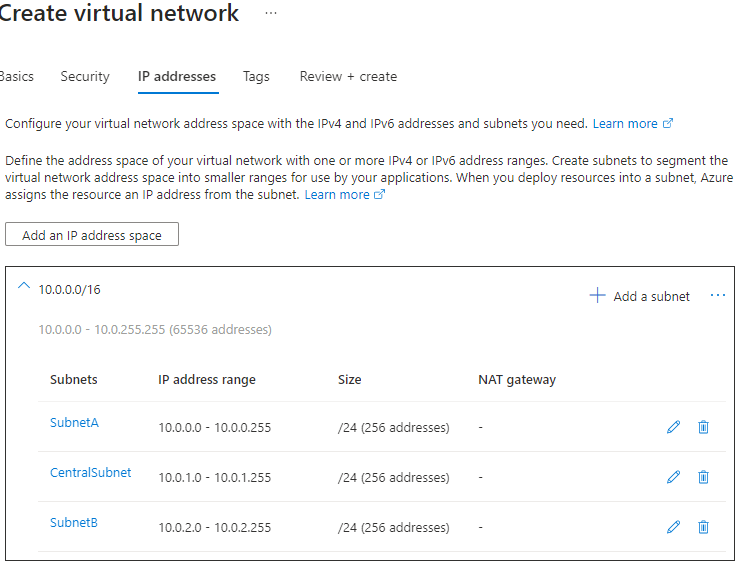
|  |  |
| --- | --- |
|  | * **The objective of setting up the user defined route is that traffic from appvmA to appVmB has to go via centralVm** * The can be accomplished using User defined route * **Note – All the VM within a VNET can communicate with each other via their private IP address** * We don’t have to enable the NSG for PORT “80” as within the the VNET . This VNET rule is need when the VM are getting accessed from internet. |
| * The “AllowVnetBound” is the default NSG rule which allow the communication with VNET (even with private IP address) | |

#### STEP TO SETTING UP USER DEFINED ROUTE

1. CREATE A VNET (APP-VNET)
2. CREATE SUBNET AND ATACH A VM TO EACH SUBNET

|  |  |  |
| --- | --- | --- |
| VMs | SUBNETs | PUBLIC IP ON VM? |
| appVmA | SubnetA | No (private ip - 10.0.0.4) |
| appVMB | SubnetB | No( private ip - 10.0.2.4) |
| CentralVM | CentralSubnet | Yes + INSTALL IIS(private ip - 10.0.1.4) |

#### STEP 2: CREATE THE VNET



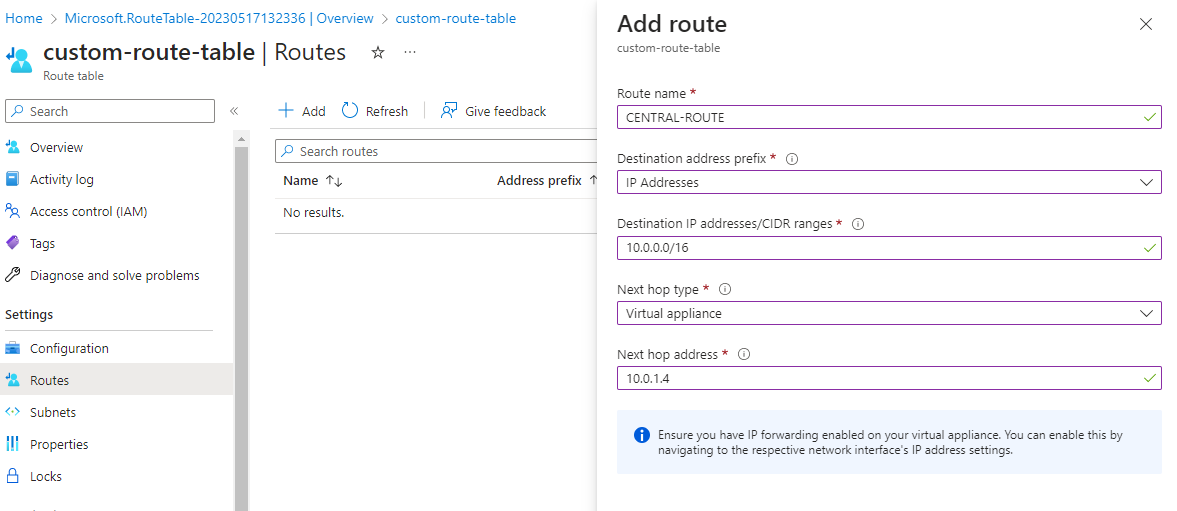
#### STEP 3: CREATE THE ROUTE TABLE

* Create a “Route table” resource.
* Defined the route in the route table
* Associate the rout with the subnet

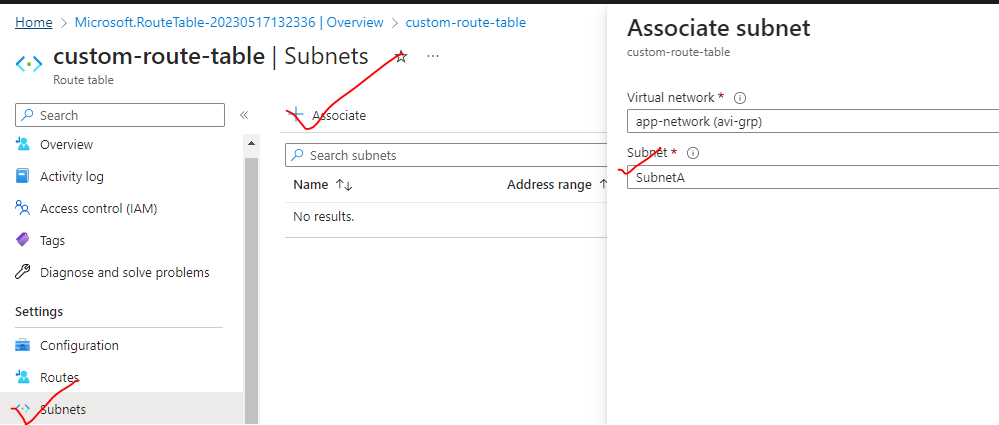
CREATE A ROUTE TABLE



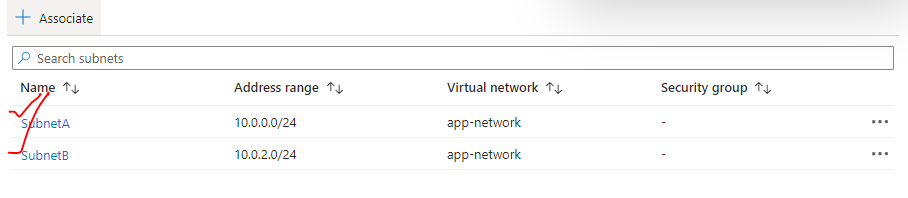
ADDING A ROUTE



ASSOCIATE A SUBNET WITH THE ROUTE



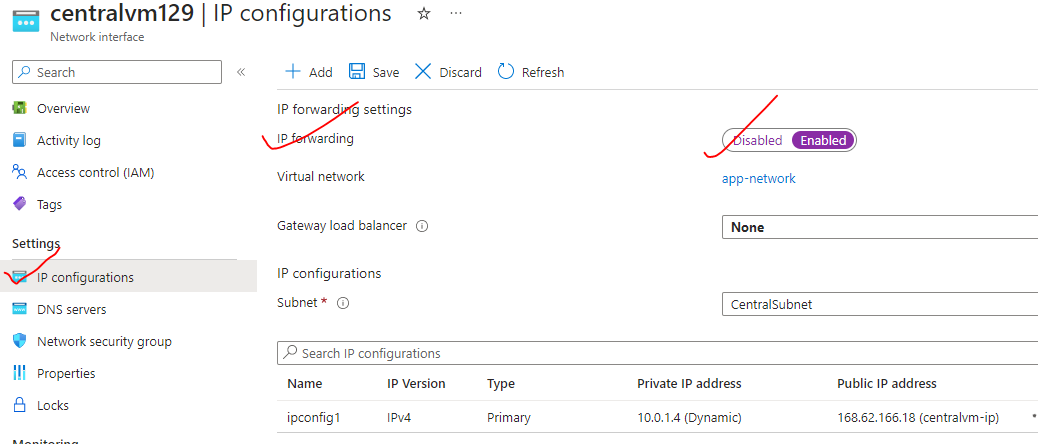
* Associate both SubnetA and SubnetB with the route



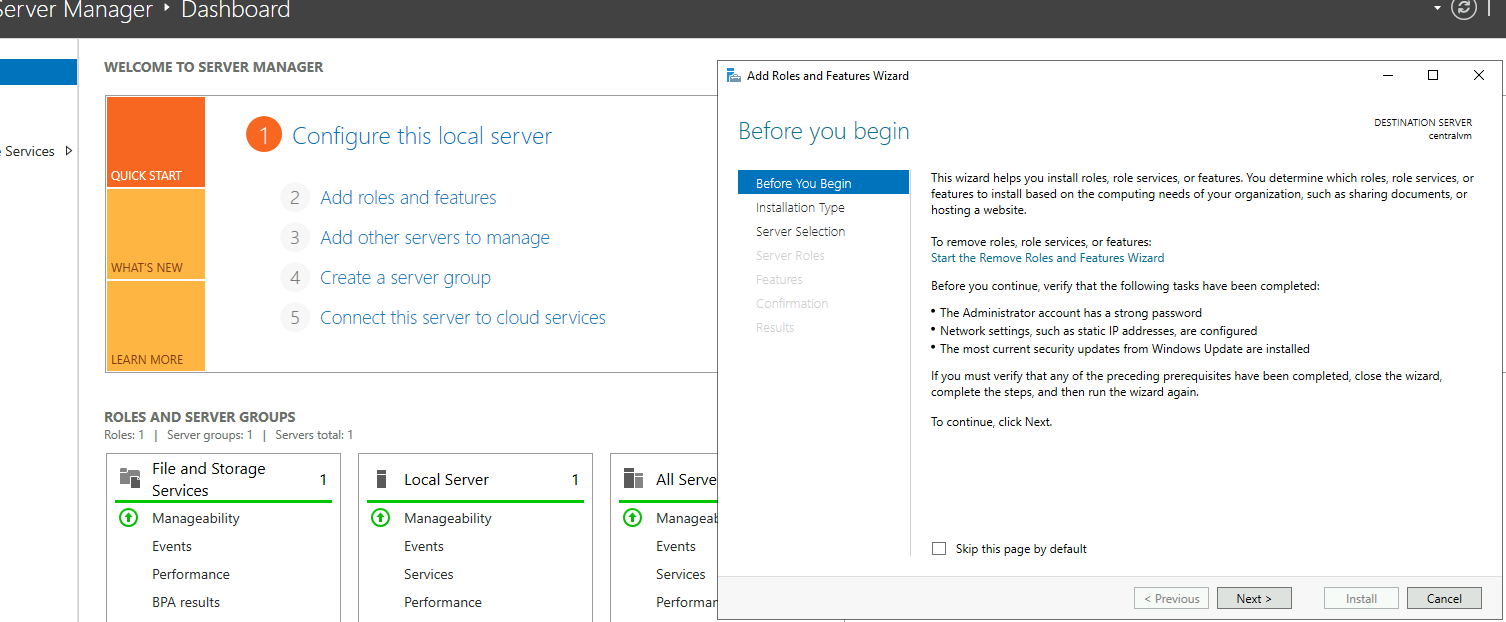
#### STEP 4: ENABLE FORWARDING

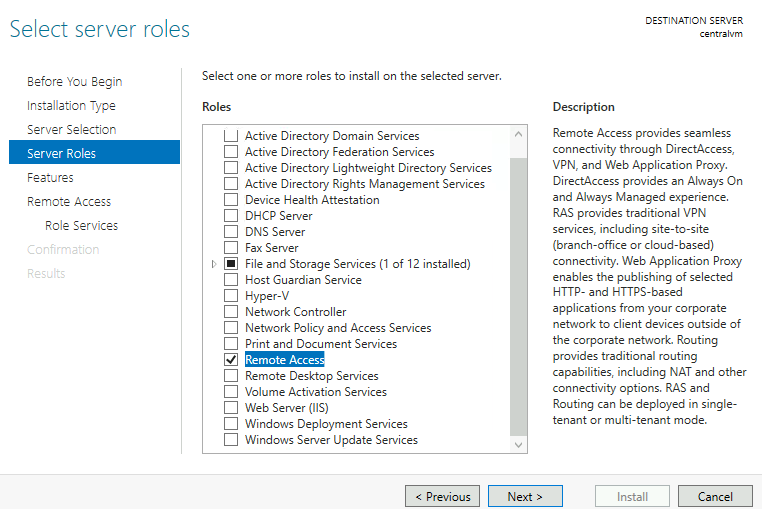
* In this step – we need to forward the request from central VM to appvmB(destination)

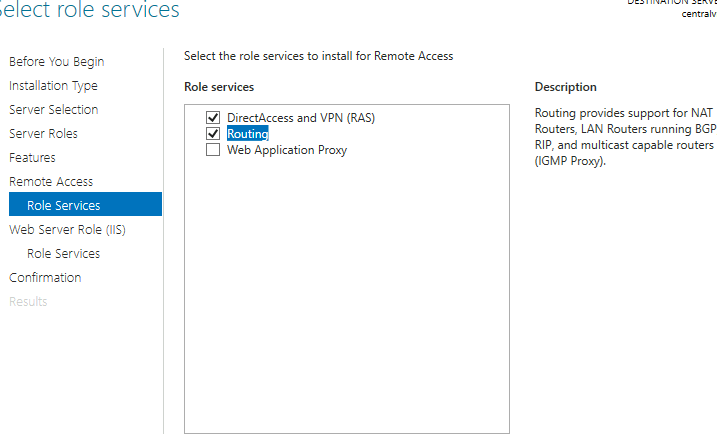
ENABLE EVENT FORWARDING ON CENTRAL VM

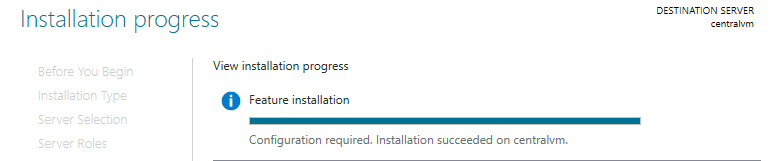


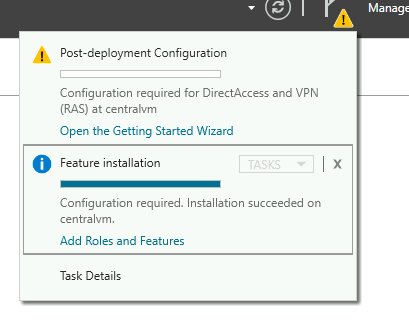
ENABLE EVENT FORWARDING ON CENTRAL VM

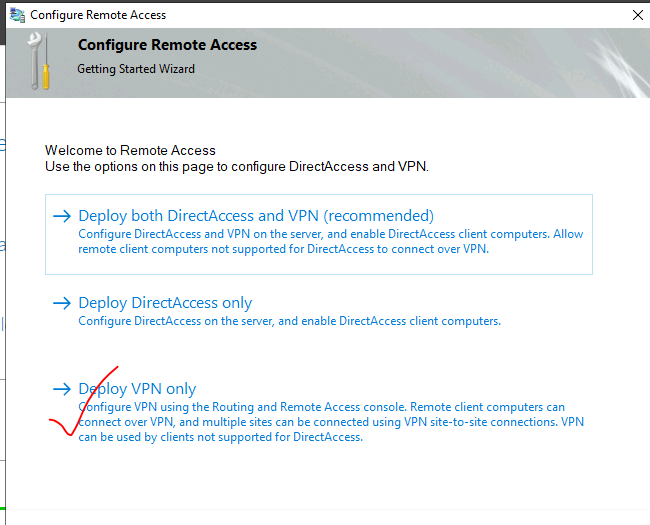


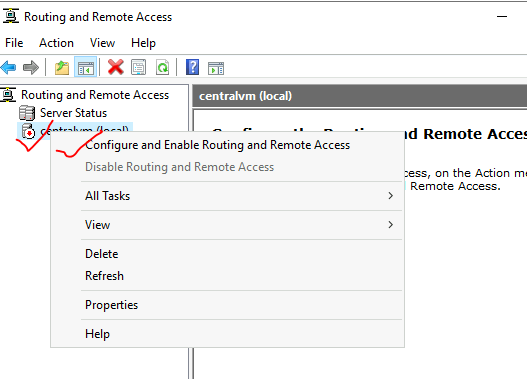


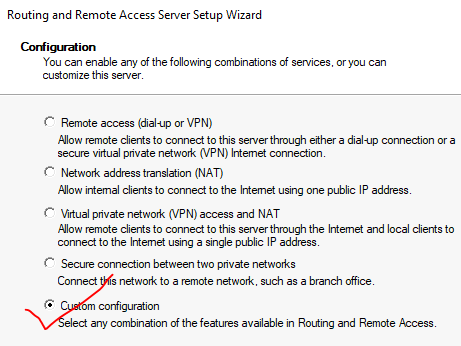


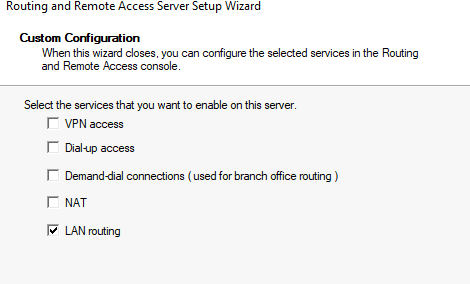


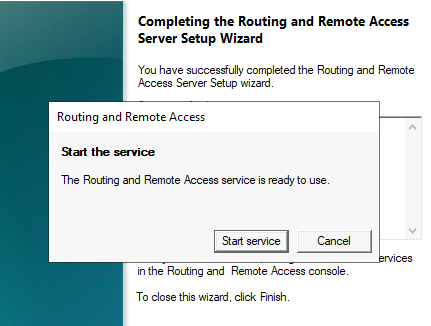


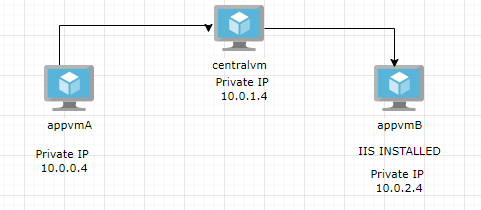


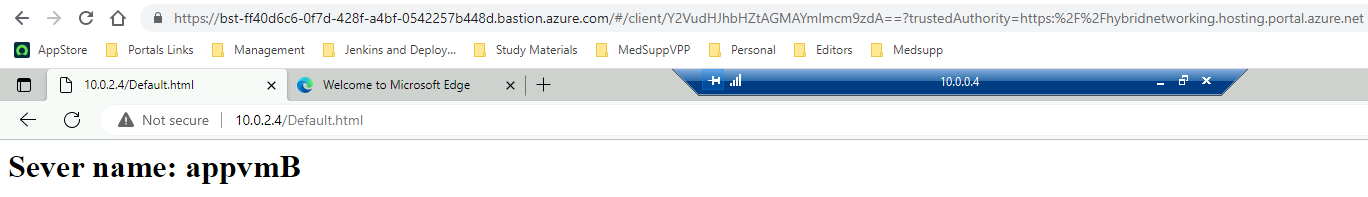






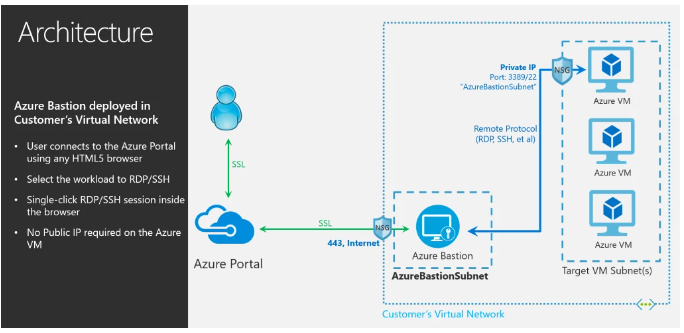






## NETWORK WATCHER

## AZURE BASTION SERVICE



* Azure Bastion is a fully managed platform as a service (PaaS) offering provided by Microsoft Azure.
* **It provides secure and seamless RDP (Remote Desktop Protocol) and SSH (Secure Shell) connectivity to virtual machines (VMs) within Azure without the need for a public IP address or a VPN connection.**
* Azure Bastion acts as a jump server or a bastion host, allowing users to securely access their VMs through the Azure portal using a web browser. It eliminates the need to expose VMs directly to the public internet or manage complex network configurations.

KEY FEATURES AND BENEFITS OF AZURE BASTION INCLUDE:

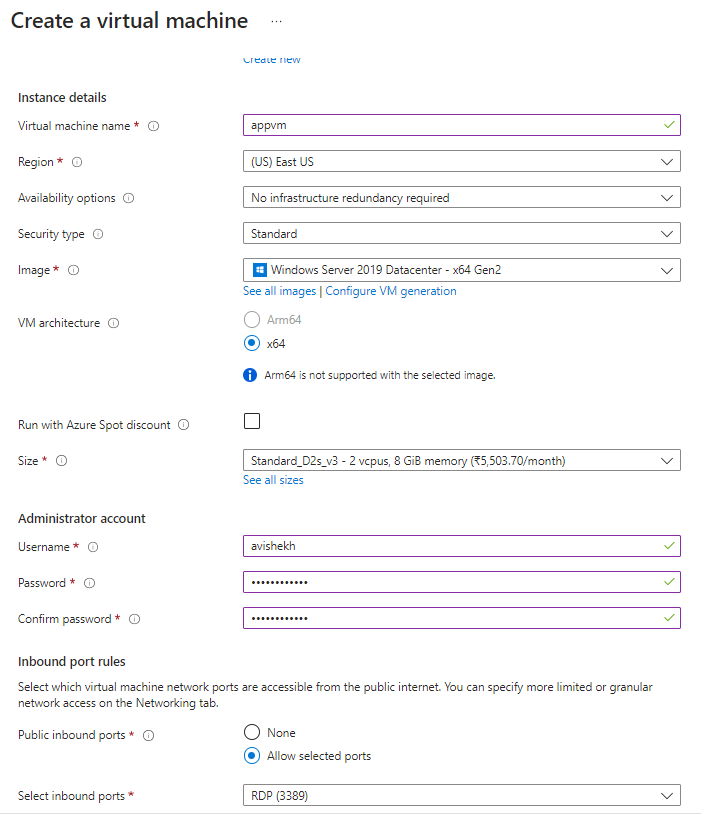
* SECURE REMOTE ACCESS:
  + **Azure Bastion provides secure and encrypted RDP/SSH connectivity to VMs over the public internet**, reducing the attack surface area compared to traditional methods.
* NO PUBLIC IP REQUIRED:
  + With Azure Bastion, VMs do not require a public IP address.
  + Access to VMs is done through the Azure portal, which simplifies network security by reducing the exposure of VMs to the internet.
* SIMPLIFIED CONNECTIVITY:
  + Users can connect to VMs from the Azure portal without the need for additional client software or VPN configurations. It provides a seamless and user-friendly experience.
* BUILT-IN PROTECTION:
  + Azure Bastion is fully integrated with Azure Active Directory (Azure AD) and supports multi-factor authentication (MFA), providing an additional layer of security for remote access.
* AUDITING AND LOGGING:
  + Azure Bastion provides audit logs, which can be used for monitoring and tracking access to VMs. These logs can be integrated with Azure Monitor and other security monitoring tools.

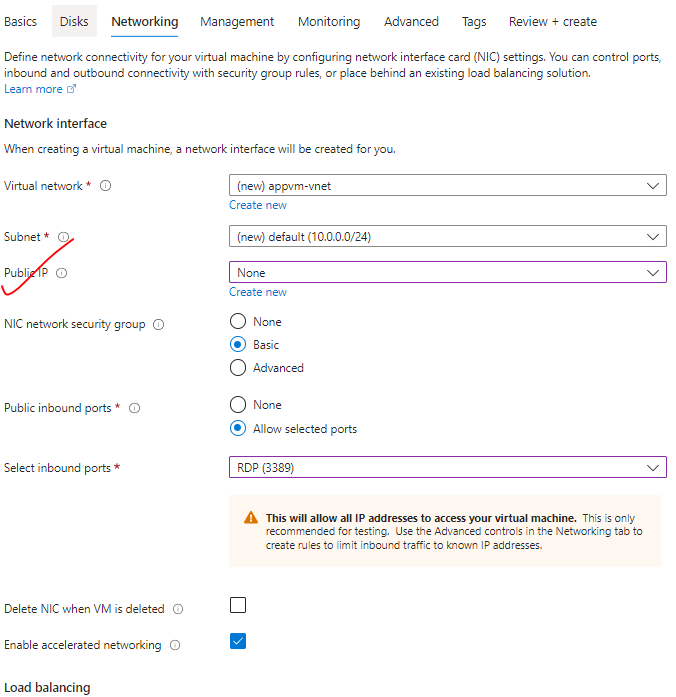
**NOTE**:

* Azure Bastion is deployed within a virtual network (VNet) as a dedicated subnet(named as “***AzureBastionSubnet***”.). This subnet acts as a secure gateway for accessing VMs within that VNet.

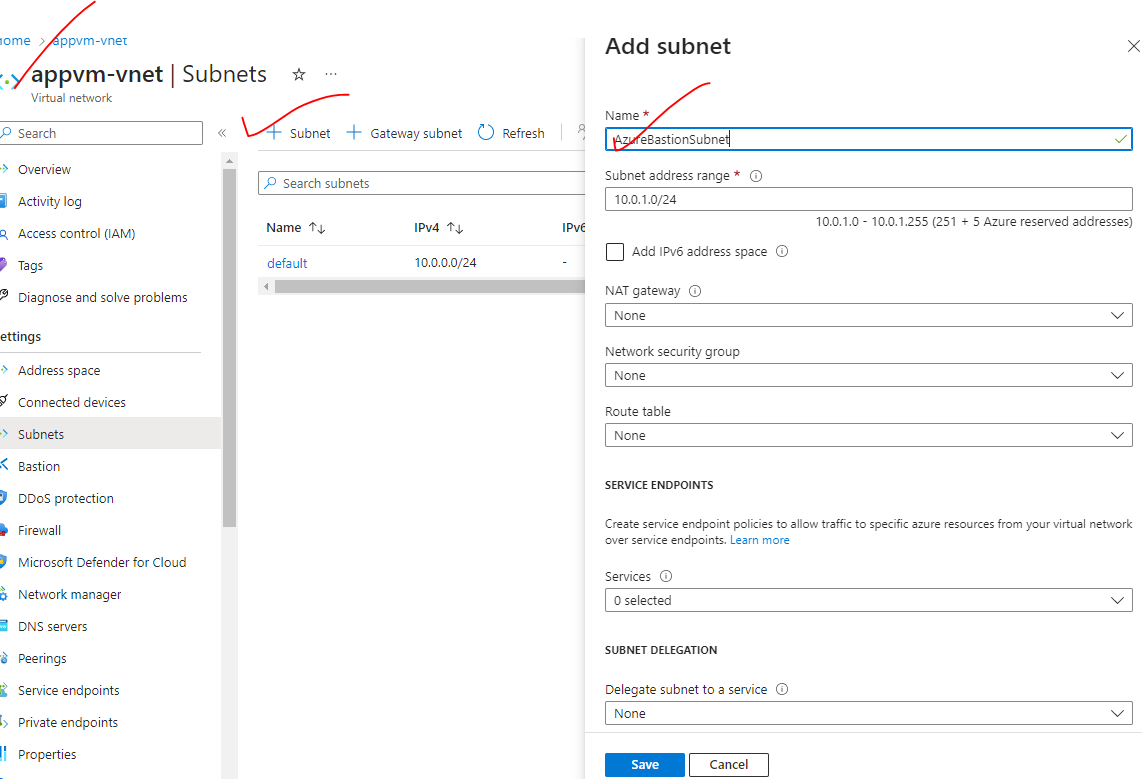
### SETTING UP BASTION SERVICE

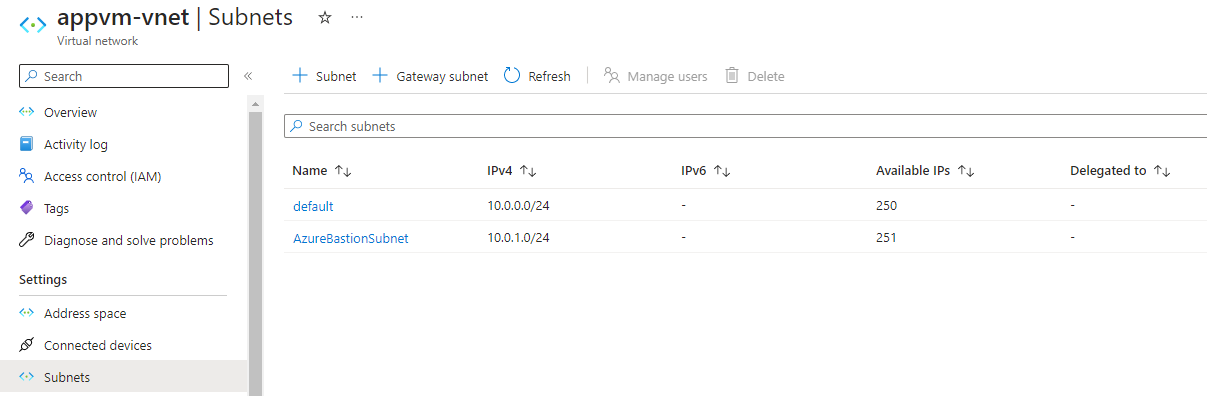
**CREATING A VM WITHOUT PUBLIC IP**



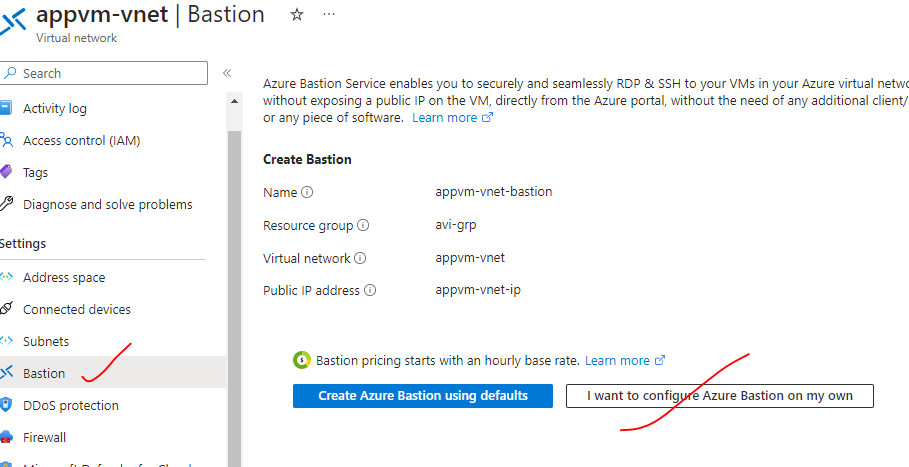


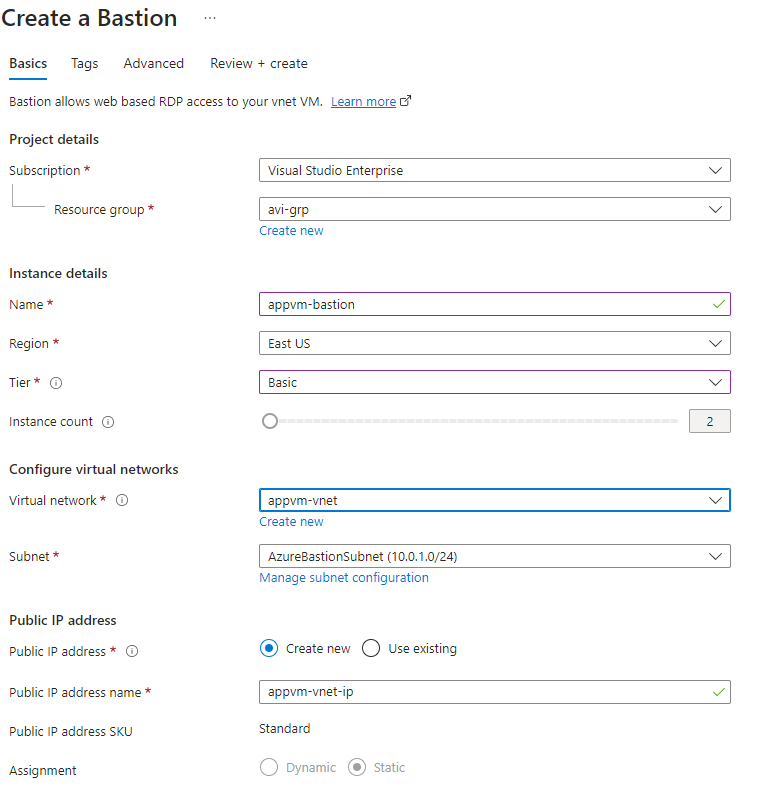
**CREATING SUBNET WITH NAME “AzureBastionSubnet”**



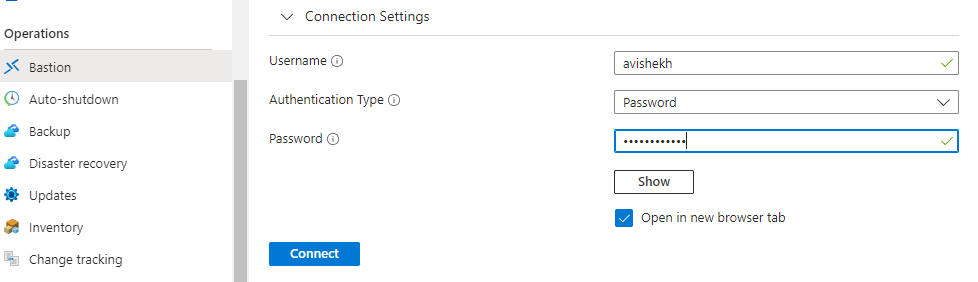


**CONFIGURE THE BASTION SERVICE**



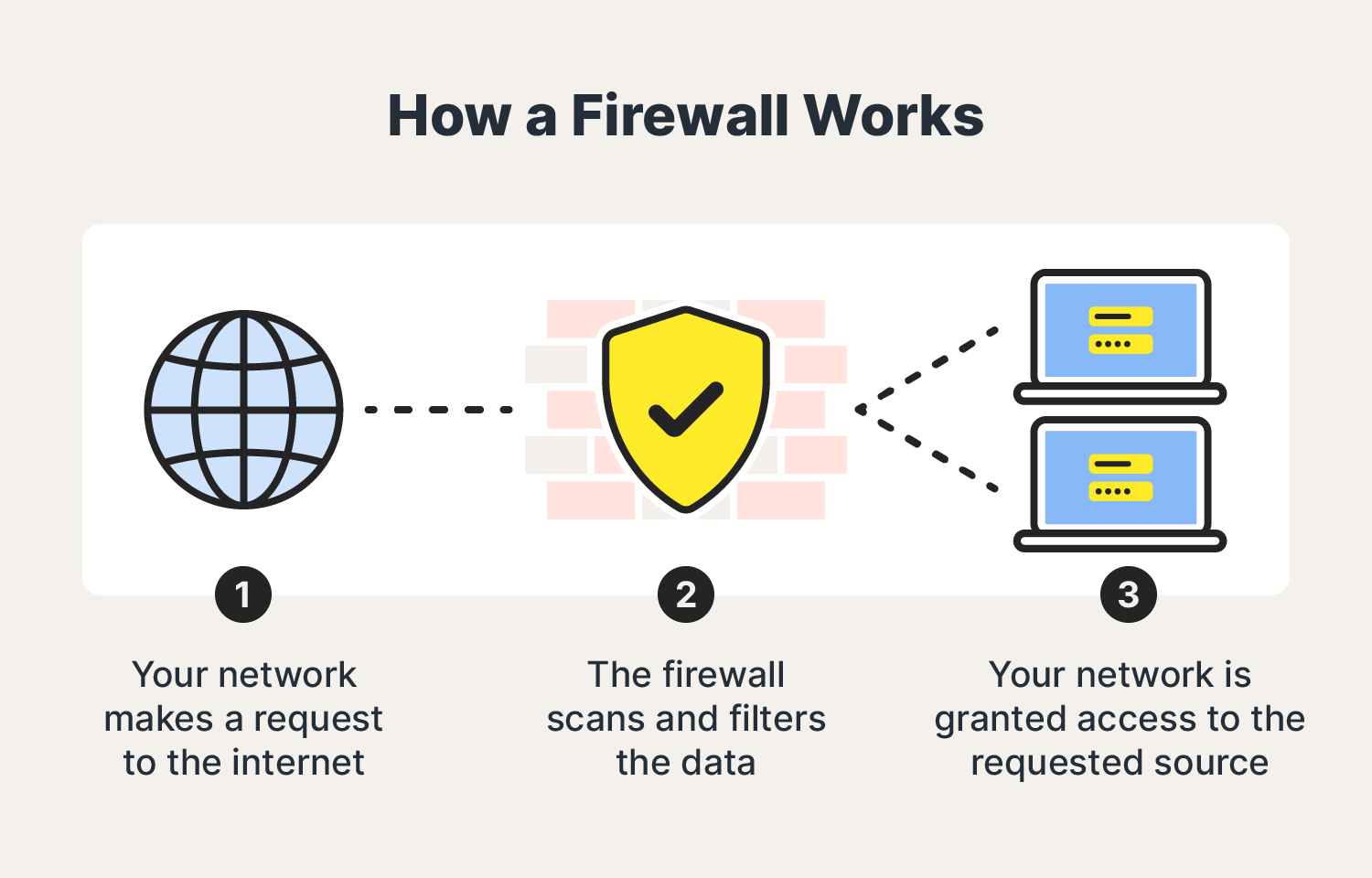


LOGIN INTO VM USING BASTION



## AZURE FIREWALL

### WHAT IS A FIREWALL



* **A firewall is a network security device or software that acts as a barrier between a trusted internal network and an untrusted external network, such as the internet.**
* Its primary function is to monitor and control incoming and outgoing network traffic based on predetermined security rules. It helps protect a network by inspecting each packet of data that enters or leaves the network and making decisions on whether to allow or block the traffic based on the configured rules. These rules can be defined by administrators to enforce security policies and protect against unauthorized access, threats, and malicious activities.

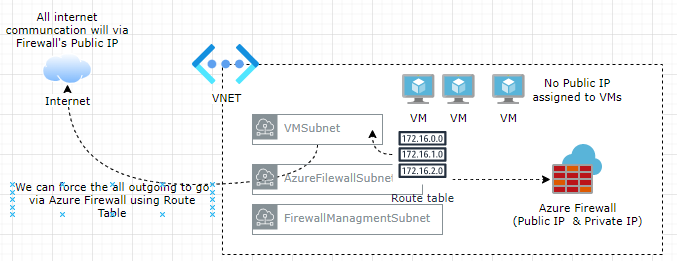
### AZURE FIREWALL SERVICE

* Azure Firewall is a cloud-based network security service offered by Microsoft Azure. It provides centralized, highly scalable, and fully stateful firewall capabilities for securing Azure Virtual Network (VNet) resources.

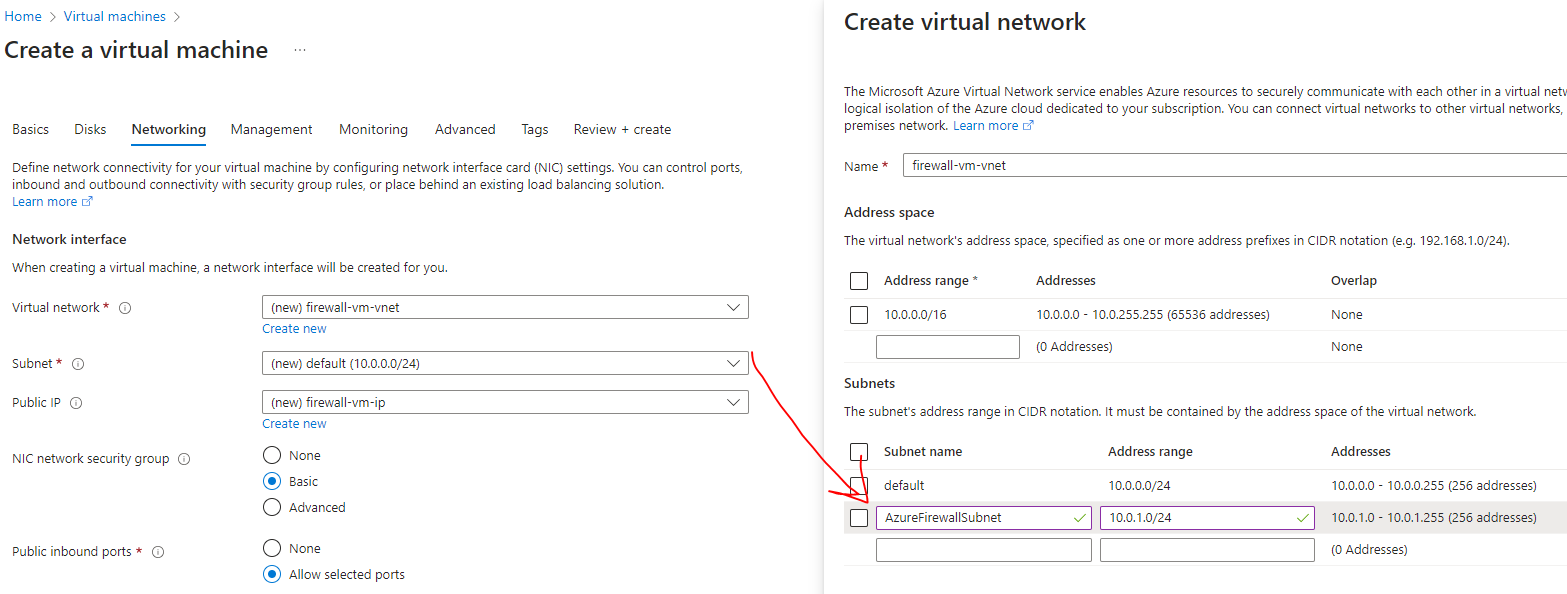
KEY FEATURES AND FUNCTIONALITIES OF AZURE FIREWALL

* NETWORK SECURITY:
  + Azure Firewall acts as a network-based, layer 3 and 4 firewall, allowing us to define and enforce network security policies for Azure VNets.
  + It provides protection against unauthorized access, threats, and malicious activities.
* APPLICATION-LEVEL FILTERING:
  + Azure Firewall supports application-level filtering, allowing us to define rules based on specific applications and protocols, such as HTTP, HTTPS, SQL, and more.
  + This allows granular control over network traffic and enhances security for applications running in Azure.
* FULLY STATEFUL FIREWALL:
  + Azure Firewall maintains the state of network connections, which means it can intelligently allow or deny traffic based on the context of the connection. This ensures that only legitimate and authorized traffic is allowed through.
* HIGH AVAILABILITY:
  + Azure Firewall is a highly available service that is automatically scaled and distributed across multiple Azure regions, providing redundancy, and ensuring continuous protection for VNets.
* INTEGRATION WITH AZURE SERVICES:
  + Azure Firewall seamlessly integrates with other Azure services, such as ***Azure Monitor, Azure Log Analytics, and Azure Sentinel****,* allowing us to monitor and gain insights into network traffic, security events, and logs.
* SECURE CONNECTIVITY:
  + Azure Firewall supports features like outbound network address translation (NAT) and integration with Azure Virtual Network Gateway, enabling secure connectivity between on-premises networks and Azure VNets.
* CENTRALIZED MANAGEMENT AND POLICY ENFORCEMENT:
  + With Azure Firewall, we can centrally manage and enforce network security policies across multiple VNets using Azure Firewall Manager.
  + This provides a unified view and simplifies management of firewall rules and configurations.

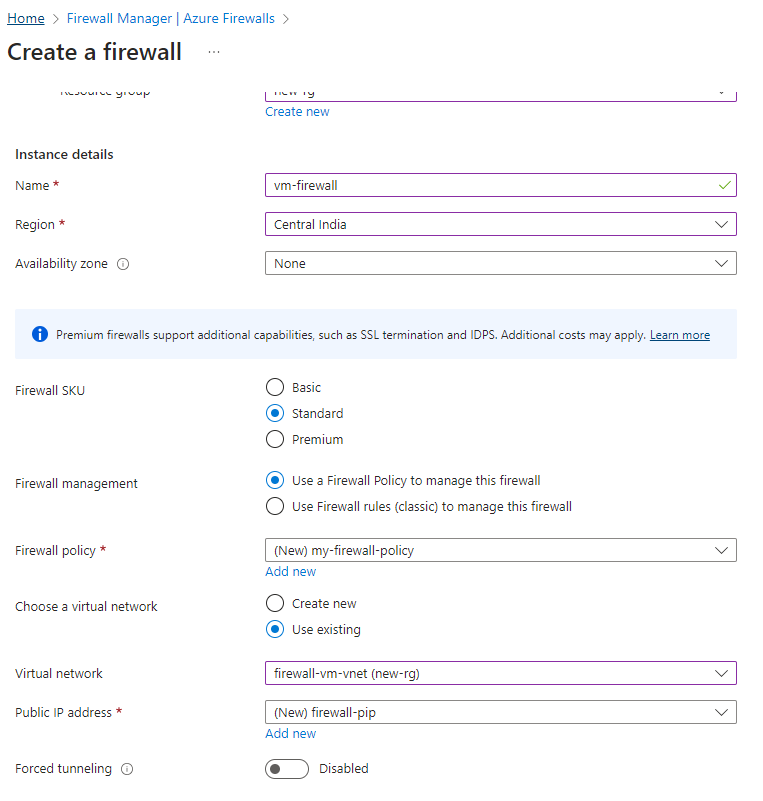
#### DEPLOYING AZURE FIREWALL SERVICE



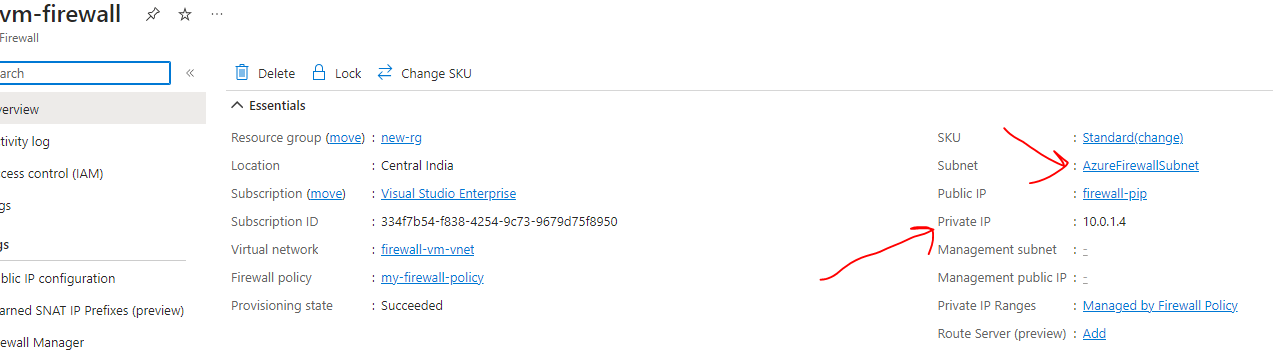
1. Create a VNET
2. Provision a VM in the VNET without a public IP address.
3. Note: The Azure Firewall service requires its own dedicated subnet names as “***AzureFirewallSubnet***”

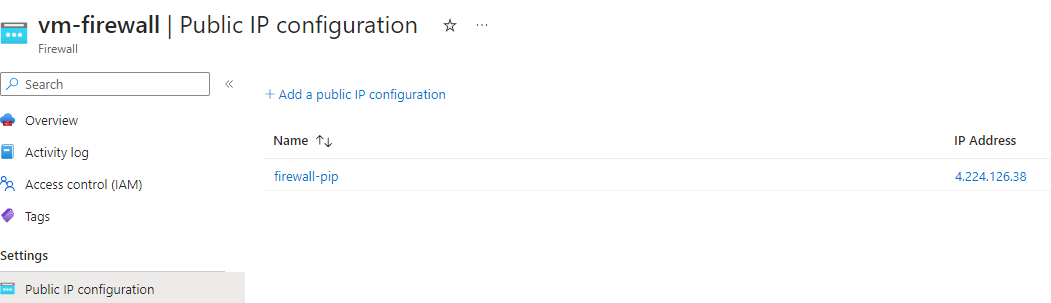


##### CREATING A FIREWALL SERVICE



* **Azure Firewall will have its own private IP address which will be used for internal communication between the Azure VMs and the firewall itself.**
* Since the firewall look at traffic that is flowing from internal network onto the internet and vice versa – hence it has been assigned a public IP address. This exposes its interface onto the internet itself.

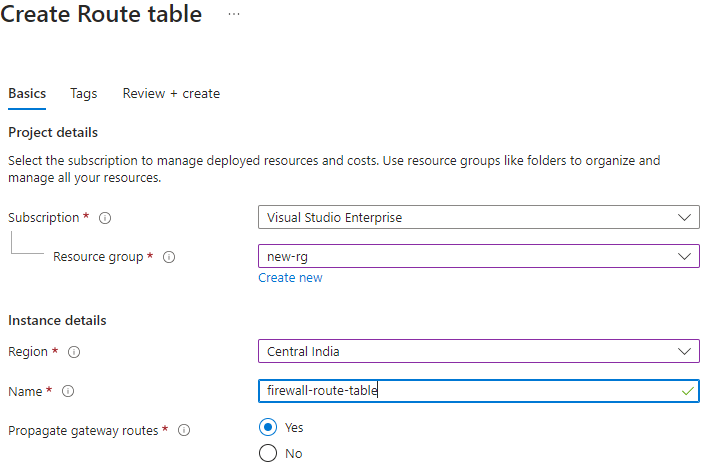




##### CONFIGURING ROUTE TABLE (SUBNET LEVEL)

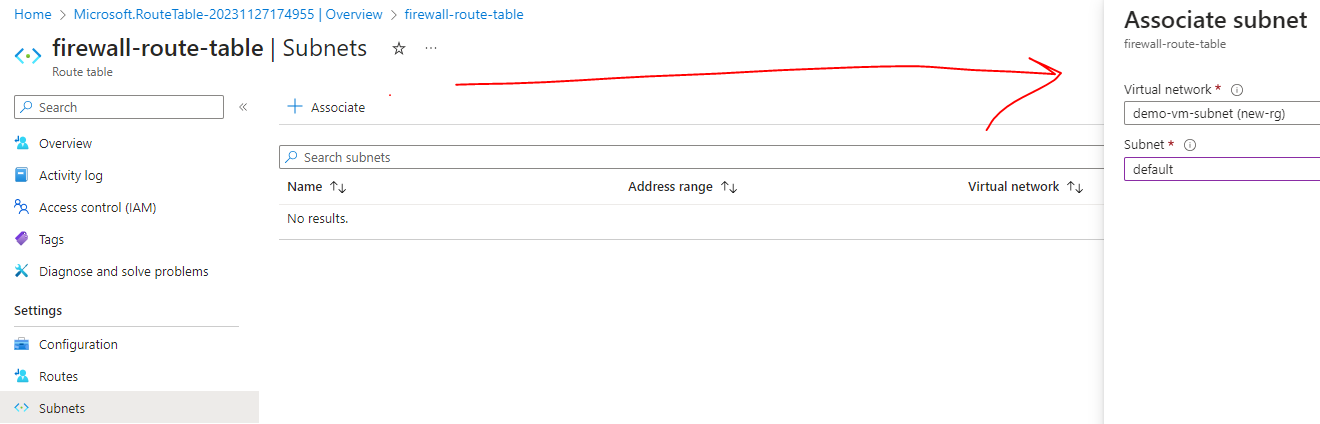
* The purpose of a firewall is to ensure that it restricts the outbound and inbound traffic to VM in the VNET.
* To enforce such restrictions, we need to create a route table and attach that table onto the subnet.

CREATING A ROUTE TABLE

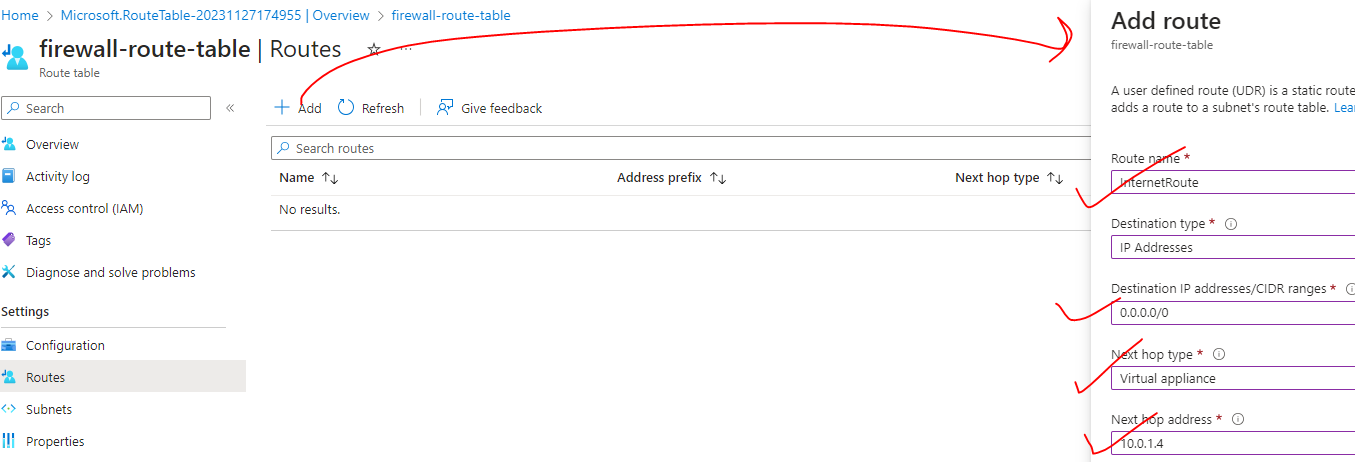


ASSOCIATE THE ROUTE TABLE WITH THE SUBNET

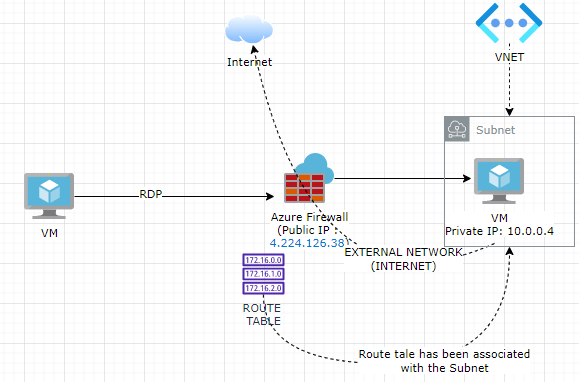
* The route table are configured on VM Subnet level



ADD ROUTES TO THE ROUTE TABLE



* **The route table will say that for any traffic that is destined for the internet needs to flow via the Azure Firewall resource**. In the above configuration we are saying that if there is any traffic that is destined for the internet, then the next hop type needs to be a virtual appliance. The next hop address is it needs to be the **private IP address** of the Azure Firewall.
* *Note:* 
  + *While adding routes- for the internet, the address prefix is normally 0.0.0.0/0.*
  + *Next hop address – This is the private IP address of the Azure Firewall*
* ***This route says - any outbound traffic(internet) needs to be routed onto the Azure Firewall on its private IP address.***



#### SETTING UP FILEWALL POLICIES

* After configuring the route table on subnet level – we can define rules/ policies on Firewall level

AZURE FIREWALL SUPPORTS MULTIPLE POLICY TYPES TO DEFINE AND ENFORCE NETWORK SECURITY RULES.

1. NETWORK RULE COLLECTION
   1. Network rule collections allow us to define rules based on source and destination IP addresses, ports, and protocols.
   2. We can create rules to allow or deny traffic between specific IP addresses or ranges.
   3. Network rule collections operate at the transport layer (Layer 4) of the network stack.
2. APPLICATION RULE COLLECTION
   1. Application rule collections enable us to control traffic based on specific applications and protocols.
   2. We can define rules to allow or deny traffic for applications like HTTP, HTTPS, SQL, FTP, and more.
   3. Application rule collections operate at the application layer (Layer 7) of the network stack.
3. NAT RULE COLLECTION
   1. NAT (Network Address Translation) rule collections **allow us to perform network address translation for outbound traffic**.
   2. We can define rules to translate the source IP address or port of outbound traffic to a different IP address or port (usually the port and public IP address of Azure Firewall).
   3. NAT rule collections are useful for hiding the internal IP addresses of the resources.
4. DNS RULE COLLECTION
   1. DNS rule collections allow us to control DNS resolution for the virtual networks.
   2. We can define rules to allow or deny DNS queries based on DNS domain suffixes or specific DNS servers. DNS rule collections operate at the DNS layer.

##### CONFIGURING NAT RULES

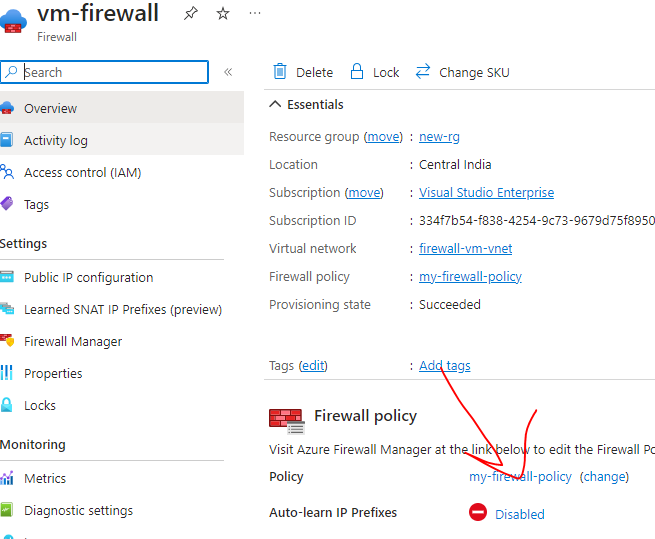
* Click on the *Firewall Policy 🡪 DNAT Rules 🡪 Add Rule Collection*. DNAT rules are used for Network Address Translation.

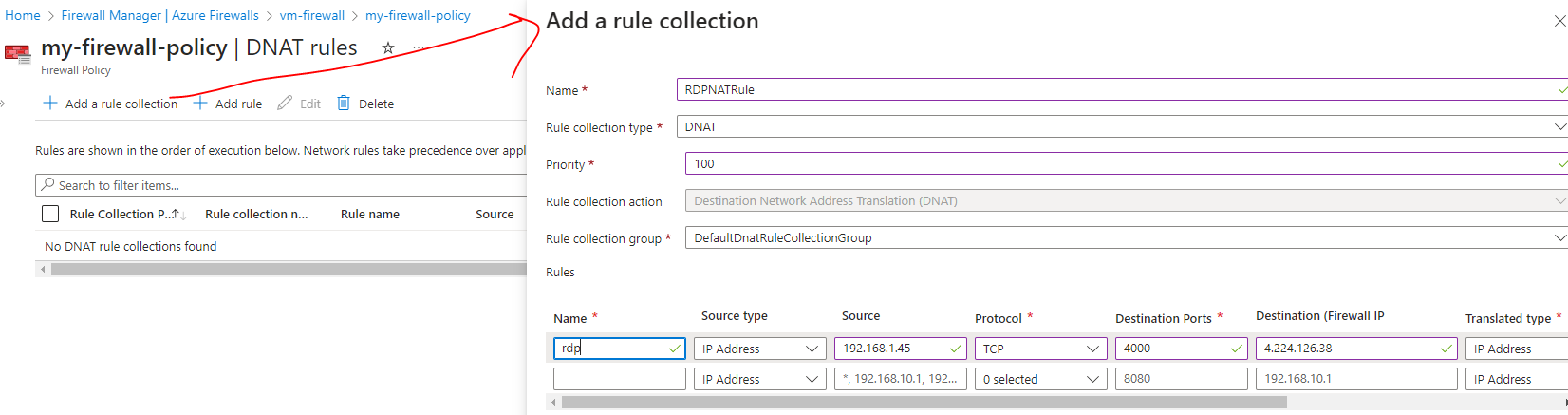
EXAMPLES - 1

1. *Let’s say we have a web application deployed in the VM- which has only private IP. We can access the web application using the Public IP address of the Azure Firewall.*
2. ***The NAT Rules translates the public IP of firewall to the private IP of the VM***

EXAMPLES - 2

1. *On the similar note – we can RDP to the Azure VMs that are part of the Azure virtual network via the Azure Firewall public IP. Here also the NAT Rules translates the public IP of firewall to the private IP of the VM*





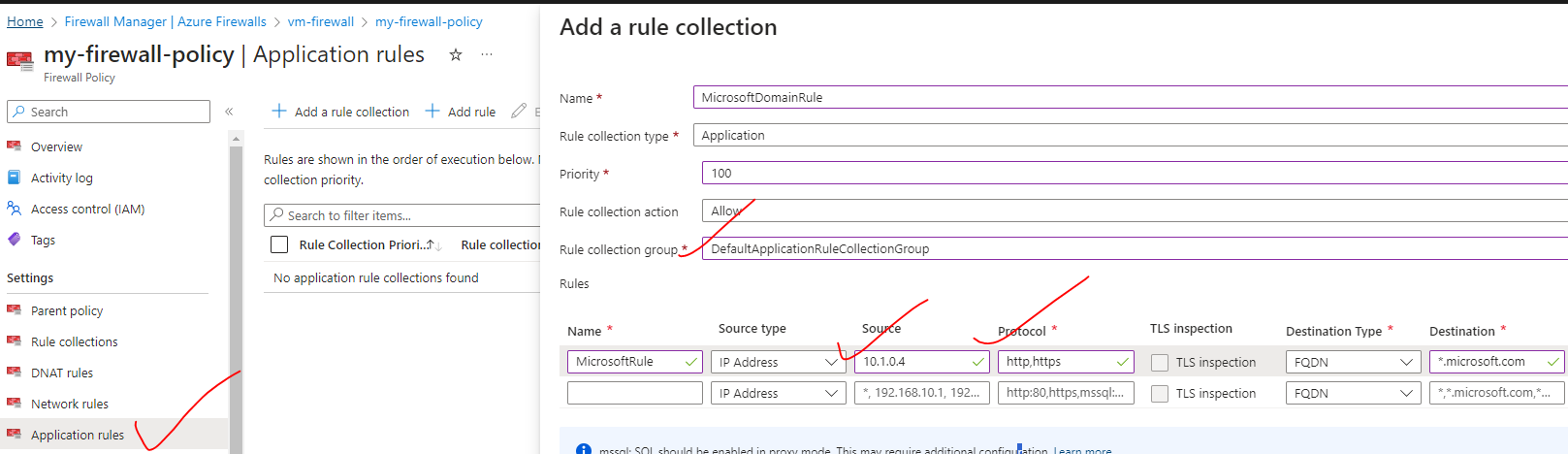
NAT RULE CONFIGURATION

1. For **Name**, enter *rdp*.
2. For **Priority**, enter *200*.
3. For **Rule collection group**, select **DefaultDnatRuleCollectionGroup**.
4. Under **Rules**, for **Name**, enter *rdp-nat*.
5. For **Source type**, select **IP address**.(it can be public IP address of another VM from where we want to do RDP)
6. For **Source**, enter *\**.
7. For **Protocol**, select **TCP**.
8. For **Destination Ports**, enter ***4000***.
9. For **Destination Type**, select **IP Address**.
10. For **Destination**, enter the **firewall public IP address**.
11. For **Translated address**, enter **the private IP address of the VM**.
12. For **Translated port**, enter ***3389***.
13. Select **Add**.

|  |  |
| --- | --- |
|  |  |

##### CONFIGURING APPLICATION RULES

* Application rules are organized into application rule collections. An application rule collection consists of one or more rules that define the traffic allowed or denied based on specific applications or protocols.
* **For example, let's say that we want to allow outgoing traffic- to a fully qualified domain name (e.g., microsoft.com) - we can do that with the help of application-based rules.**



|  |  |
| --- | --- |
| **Source** | *This is the private IP of the VM where we want to allow the FQDN (*[*https://www.microsoft.com/*](https://www.microsoft.com/)*)* |
| **Protocol** | Allowed Protocol (http and https) – Comma Separated |
| **Destination Type** | FQDN – Fully Qualified Domain Name |
| **Destination** | Allowed Domain (Comma Separated) |

## AZURE TRAFFIC MANAGER

* **Traffic Manager a DNS based traffic load balancer.**
* The Azure load balancer and Application gateways are regional (i.e.it can manage the resources in a given region) , but a traffic manager is a global service. Hence when we deploy a traffic manager profile- we don’t to specify a region for the deployment of the resource.
* The traffic manager allows us to direct the client requests to an appropriate service endpoint (end point can be VMs , Web App or application hosted on-premise datacenter) based on routing method. The endpoint needs to be public endpoint that can be hosted inside or outside Azure
* The Traffic manager monitors the health monitoring of the endpoints.

### GEOGRAPIC ROUTING METHOD

1. ***In Geographic routing method the end point depending upon the location the DNS query originates from (it depends upon user’s location).***
2. This is different from the performance routing method. In the performance routing method, the traffic manager looks for a resource which takes less time in terms of latency. That is the endpoint that will be returned to the user.

#### SETTING GEOGRAPIC ROUTING METHOD

Step 1: Create 2 VMs in two different Region

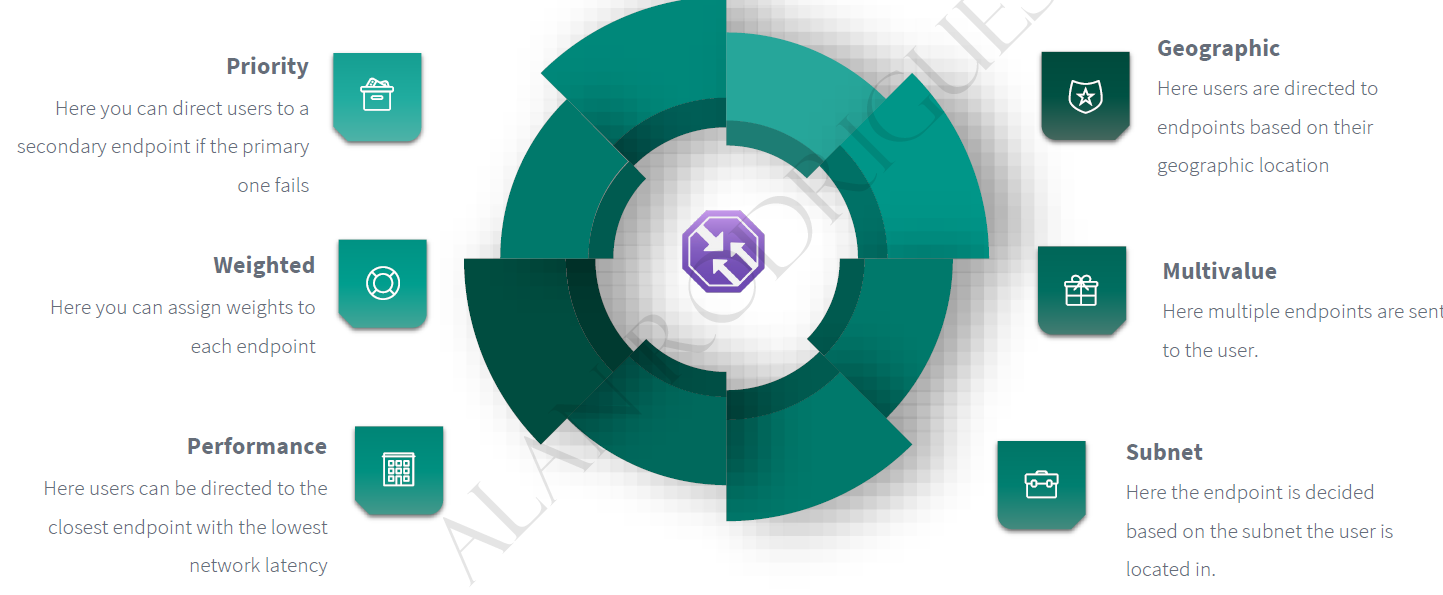
Step 2: Configure the traffic manager endpoint 🡪 Select the region which will serve the request which is coming from the same region

|  |  |
| --- | --- |
|  |  |

### AZURE TRAFFIC MANAGER SET UP

### AZURE TRAFFIC MANAGER ROUTING METHODS

Azure Traffic Manager supports **six traffic-routing methods to determine how to route network traffic to the various service endpoints.** For any profile, Traffic Manager applies the traffic-routing method associated to it to each DNS query it receives. The traffic-routing method determines which endpoint is returned in the DNS response.



### PRIORITY ROUTING METHOD

|  |  |
| --- | --- |
|  | * This routing method help in direct traffic to secondary endpoint of primary endpoint is not available. |

#### SETTING UP PRIORITY ROUTING METHOD

STEP 1*: SET UP VMs IN DIFFRENT REGION (it can be in same region too. Since TM is a global service, it can manage resources in any region)*

STEP 2:

* + INSTALL IIS on both the VM – These are the VM where the traffic will be directed
  + Add a DNS names to the VMs – as traffic manager does DNS based routing.

|  |  |
| --- | --- |
|  | * STEP 3: Search for **Traffic Manager Profile 🡪 Create** * *As it is a global service, hence we don’t need to mention the region of the Traffic Manager Profile (unlike Load Balancer and App Gateway).* |
|  | * Add a DNS names to the VMs * Go to VM Overview 🡪 Click on Public IP address🡪 DNS name label |

STEP 4: Add the VMs to the traffic Manager endpoint

|  |  |  |
| --- | --- | --- |
|  | **The priority will define – which public IP(VM public IP) will be a Primary End point** | |
| * When the priority is higher means when users access the traffic manager end point, all of the users will be directed to this VM. Only when the primary VM goes down that user will be directed the secondary VM the IBM or the endpoint, this is like a fallback mechanism. * After adding the endpoint – make sure Monitor Status is “Online” | |

STEP 4: Now the VMs can be accessed via Traffic Manager DNS name.



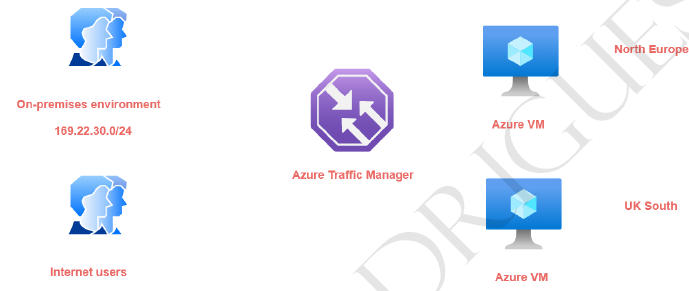
|  |  |
| --- | --- |
|  | * Note – In the above example – if we stop the primary VM – the request will be then route to secondary endpoint * PROBING INTERVAL (In sec.) – The time interval in which probing will happen * TOLERATED NUMBER OF FAILURES – After this TM will consider it as unhealthy resource * PROBE TIMEOUT - |
|  | |

|  |  |
| --- | --- |
|  | **TO UPDATE THE EXISTING ROUTING METHOD**   1. Delete the existing endpoints 2. Go to configuration of TM 🡪 Routing Method 🡪 Save 3. Add the endpoints again |

### PERFORMANCE ROUTING METHOD

1. In performance routing method – it routes the traffic to the location which is closest to use location

### SUBNET ROUTING METHOD



|  |  |
| --- | --- |
|  | * In this routing method – we map a specific set of end-user IP address range to specific endpoint. For example, if we want to direct the traffic from on premises environment- having a particular IP address range to an endpoint and all other internet users onto another endpoint. * The subnet routing methods - looks at the IP address range of the clients that are connecting to the traffic manager and then they be directed onto the end point. * If we want to create a default endpoint that is created- so that if the other end points don't * match the subnet range then the default end point will serve the request. **For default endpoint the subnet routing settings is kept empty.** * Hence – let’s say if the user hit the TM DNS and if the user’s IP does not fall in the range of Subnet routing setting – it will fallback to the default route |

### MULTIVALUED ROUTING METHOD

### WEIGHTED ROUTING METHOD

|  |  |
| --- | --- |
|  | * In weighted routing method we weight each endpoint in the traffic manager profile * Lets say if we 2 VM (endpoints)- which are weighted **50.**  The traffic to TM will be distibuted across endoint independently evenly. |

#### USE CASE OF WEIGHTED ROUTING METHOD

* So in our case, we have two AC vents in place
* Now we can assign leads on to the end points that are mapped on to our traffic margin profile.
* So, for example, I can't assign a bit of go on to the end point for the as the IBM in the North,
* their application.
* And then I can assign a weight of 50 here by the end point that is marked onto the UK South location.
* So this is like actually load balancing now request across these virtual machines.
* So when half of the users are connecting onto the air traffic manager profile, half of them will be
* directed onto the beam in the Noctua application and the other half will be directed onto the VM in
* the UK South location.
* So here the requests are actually distribute based on the bits.
* Now, one of the most useful scenarios of using the reedit routing method is when it comes onto something
* known as blue green deployments.
* So normally what happens is that initially all your users.
* So you could be having an endpoint with a bit of full 100 percent when an after users are being directed
* onto one end point.
* Now let's say you are deploying a newer version of the application on new end point, so it could be
* an A-Z IBM.
* It could be a ACR bebop.
* It could be another endpoint.
* So now you want us to form some of the users to be detected on to the newer version of your application.
* So you might maybe change the reteach from 80 percent here and 20 here.
* So 20 percent of the users are now directed onto the newer version of the application.
* Once you know you know that there are no issues with the newer version of your application, then you
* can slowly switch up.
* You know, you could make this 80 percent and you can make this 20 percent.
* And in the end, you could do a full cut over that, and this could be 100 percent and you can just
* go and disable this endpoint.
* So this is good for actually distributing the traffic across multiple endpoints.
* Again, this is very easy to achieve.
* Let's see how we can implement this.
* So again, first of all, I'll go onto my traffic manager profile.
* I'll go on to my end points and let's delete and points.
* And I'll go back to my profile.
* Let's change the configuration.
* So from the multi value onto the Beated.
* Let me click on Save.
* Go on to the profile.
* Let me go on to and points out and then point.
* You can put an end point one there, I can choose the cloud service, the public IP address, you can
* put traffic via one.
* And here in the weeds, you can put 50 and you can go out and click on Add.
* Take a look at the other end point.
* Give it a name.
* Yeah, public IP address to the public IP does a stop at the M2 and put the webpage has again 15.
* And click on Add.
* You have no unequal distribution when it comes onto the beach on two end points.
* And if I go ahead and just take the the innocent point.
* In a new type, if I go on to be followed, Estima, so I'm being directed onto the Not Europe location.
* So with the help of the state, you can actually go in and disrupt traffic across the end points when
* it comes as air traffic manager.

## AZURE FRONTDOOR