Table of Contents

[AZURE ADVANCED NETWORKING 2](#_Toc130550860)

[AZURE LOAD BALANCER 2](#_Toc130550861)

[AZURE LOAD BALANCER CONCEPTS 2](#_Toc130550862)

[LOAD BALANCER COMPONENTS 2](#_Toc130550863)

[LOAD BALANCER SKUs 2](#_Toc130550864)

[TYPES OF LOAD BALANCERS 3](#_Toc130550865)

[SETTING UP BASIC LOAD BALANCER 3](#_Toc130550866)

[NAT RULES (NETWORK ADDRESS TRANSLATION) LOAD BALANCER 8](#_Toc130550867)

[AZURE APPLICATION GATEWAY 8](#_Toc130550868)

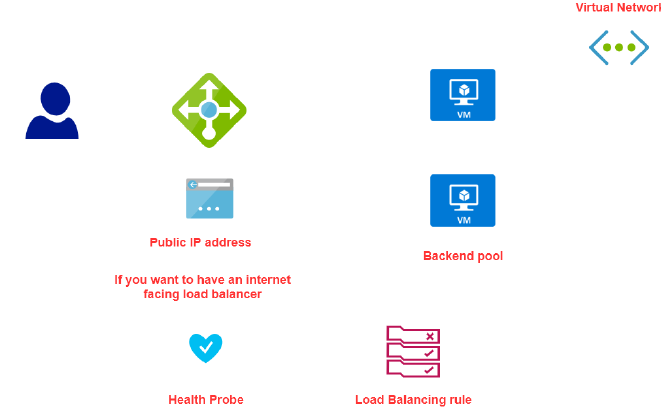
[FEATURES OF APPLICATION GATEWAY 9](#_Toc130550869)

# AZURE ADVANCED NETWORKING

## AZURE LOAD BALANCER

|  |  |
| --- | --- |
|  | * Let's say that we have an application that is being hosted on a set of virtual machines. If the application is being accessed by a lot of users- the load balancer service ensures that the traffic from the users get equally distributed across all virtual machines. * The azure load balancer works on Layer 4(Transport Layer) and Application Gateway (Application Layer) of the OSO Model * The Azure load balancer comes in 2 pricing model (SKU)   + BASIC LOAD BALANCER   + STANDARD LOAD BALANCER |

### AZURE LOAD BALANCER CONCEPTS



### LOAD BALANCER COMPONENTS

|  |  |
| --- | --- |
| BACKEND POOL | A backend is the pool(group) of resources that is being managed by load balancer |
| FRONTEND IP | A frontend IP address is the IP address that is assigned to load balancer and is used to access the resources being managed by load balancer. |
| HEALTH PROBE | Health Probe is a special signal sent to each resource in the backend pool to check if it’s healthy and available |
| LOAD BALANCING RULES | A load balancing rule is used to associate the frontend IP , backend pool and health probe together.   * The redirect of request from LB to VM are done via private IP of VM * This helps the LB monitor the health of VMs in the backend pool * These rules drive how request can be distributed across the VM (which are part of backend pool) |

### LOAD BALANCER SKUs

|  |  |
| --- | --- |
| BASIC LOAD BALANCER | STANDARD LOAD BALANCER |
| Free | Charges per hour |
| The machine in the backend pool need to be part of an availability set or scale set | Here VM can be an independent machine that are part of a VNET |
| Health probes – TCP, HTTP | Health probes – TCP, HTTP, HTTPs |
| No Support for Availability Zone | Availability Zone Support |
| No SLA | SLA of 99.99% |

### TYPES OF LOAD BALANCERS

### SETTING UP BASIC LOAD BALANCER

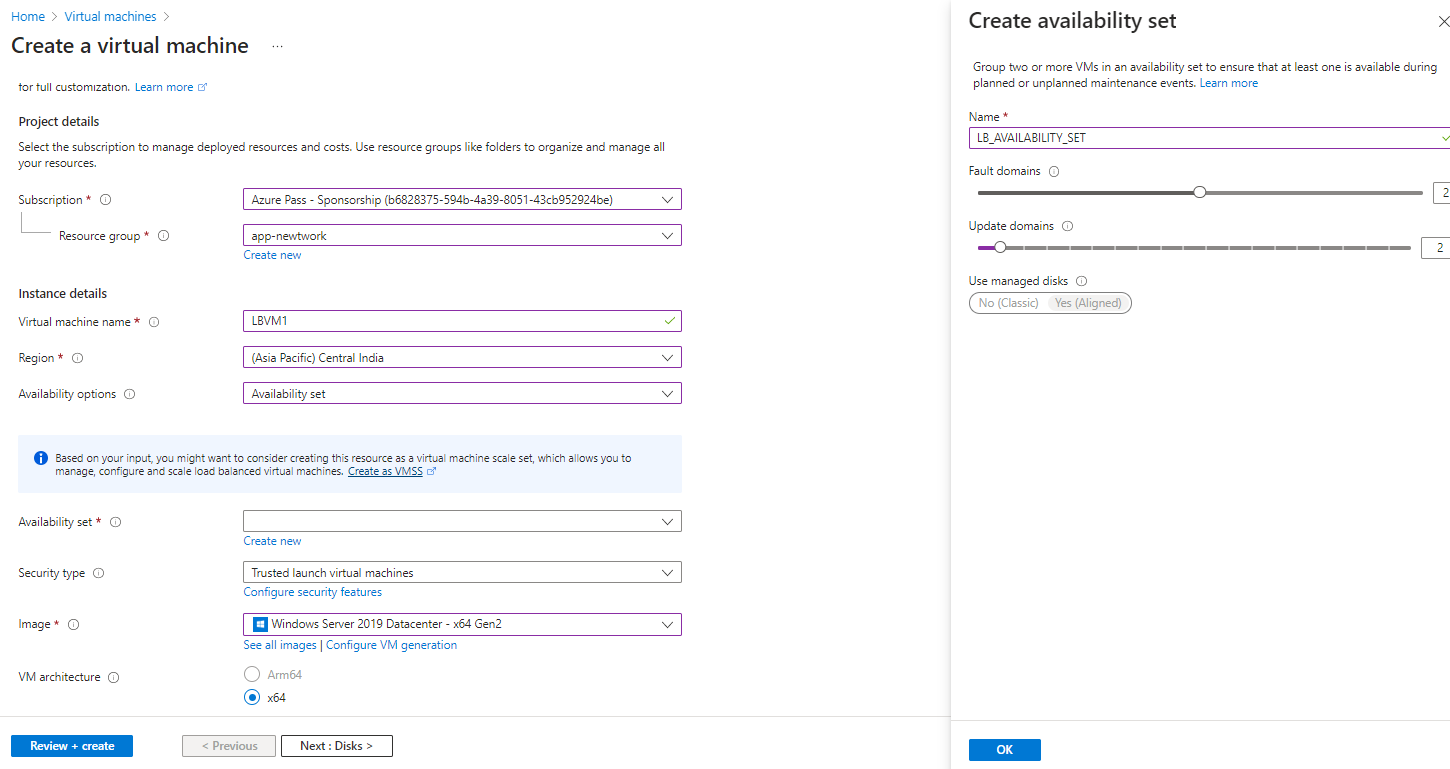
To illustrate the basic load balancer services set up. Let’s follow the following steps

* **STEP 1:** We will create 2 - VMs, which will be a part of an Availability Set (Make sure the VMs are part of same VNET)
* **STEP 2**:
  + Install IIS with a Default.html page. [Path of HTML- C:\inetpub\wwwroot]
  + PowerShell command to install IIS - **Install-WindowsFeature -Name Web-Server -IncludeManagementTools**
* **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**
* **STEP 4**: 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 5**: Configure the health probe to check the health of VM in the backend pool
* **STEP 6**: Create Load balancing Rules – which will give the routing of request to the VM in backend pool
* **STEP 7**: 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.

#### VM SET UP

**STEP 1**: CREATION OF VMs. 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



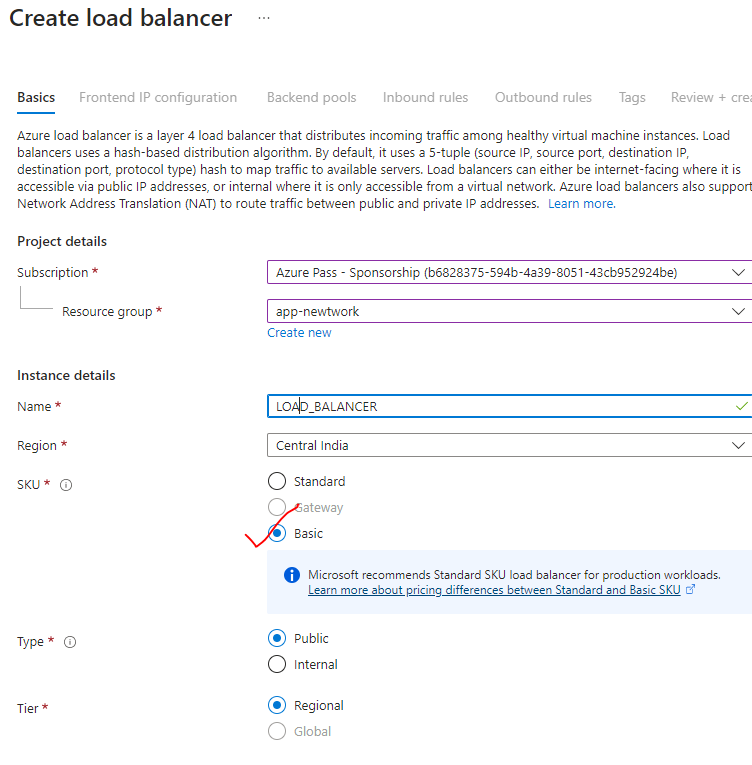
|  |  |
| --- | --- |
| VM1 | VM2 |
|  |  |

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

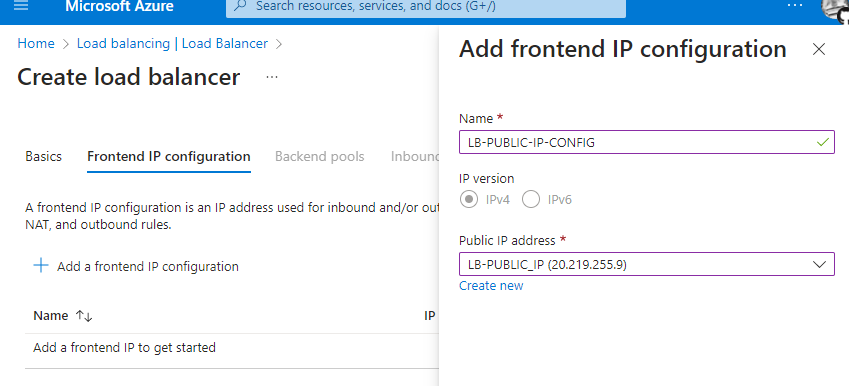
#### CREATE A PUBLIC ADDRESS FOR LOAD BALANCER

|  |  |
| --- | --- |
|  | * We need to create a public IP address that is going to be assigned onto the load balancer. When users want to reach the virtual machines, they can reach it by the public IP address of the load balancer. * Note –   + Public IP address is a separate resource in Azure   + For public IP SKU- use “Basic SKU” of Basic Load balancer and “Standard” SKU for standard load balancer |

#### SETTING UP A LOAD BALANCER SERVICE

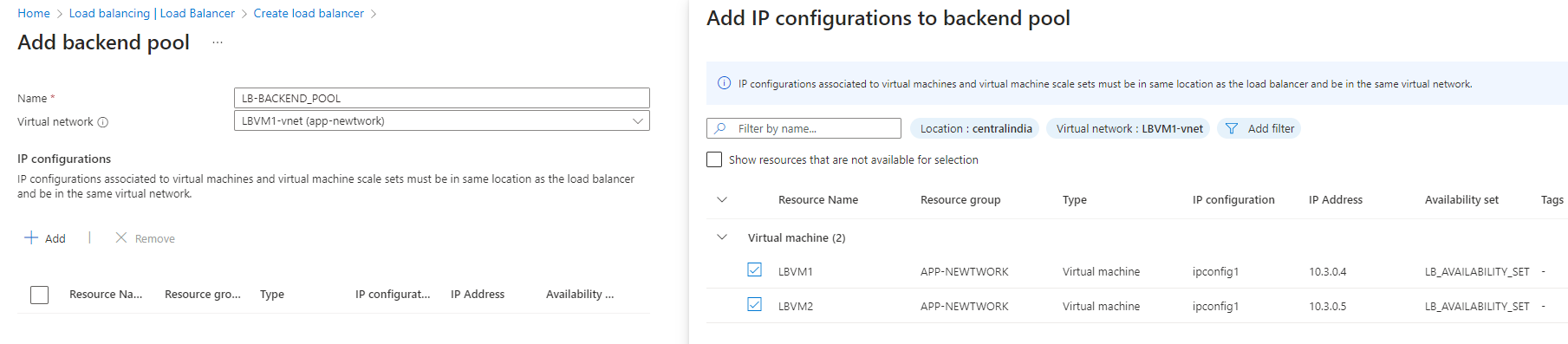


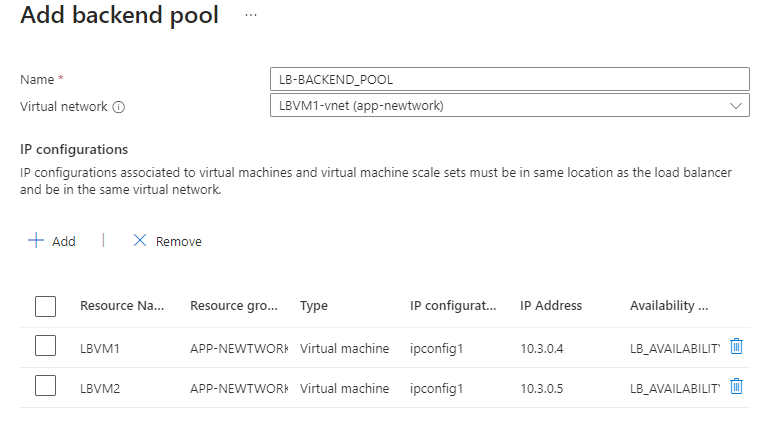
##### ASSOCIATE PUBLIC IP WITH LOAD BALANCER



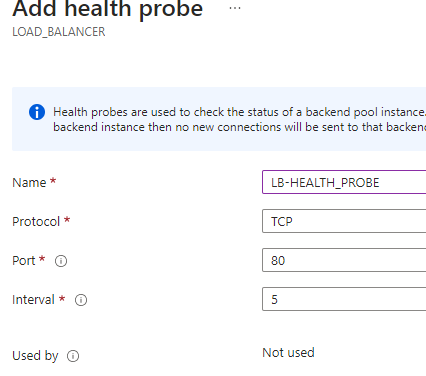
##### CONFIGURE THE BACKEND POOL

* VMs are associated with the Load balancer

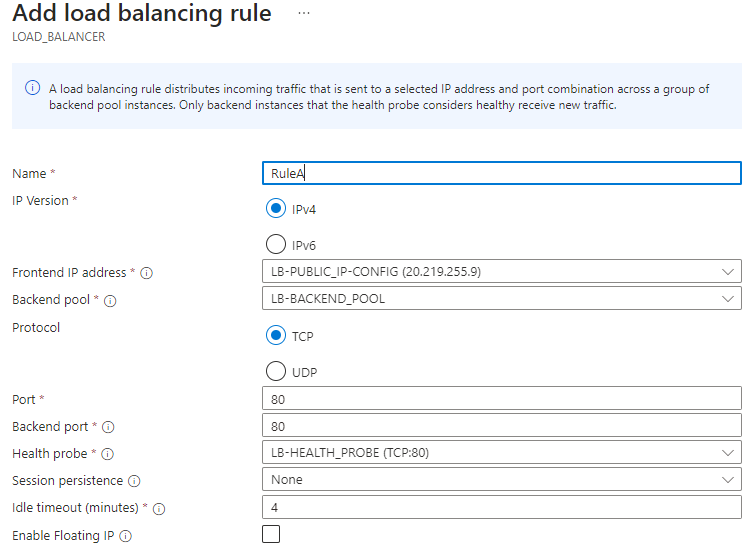




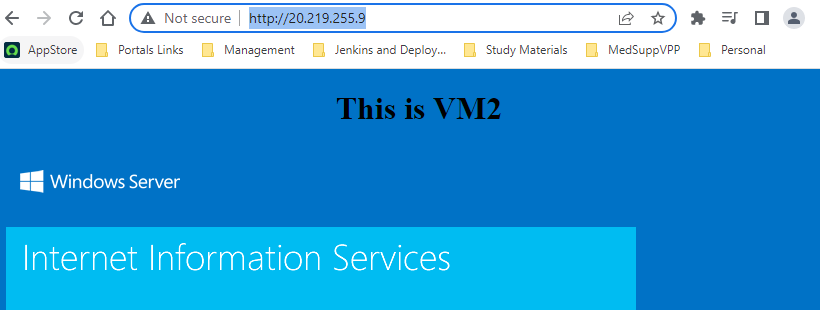
##### CONFIGURE THE HEALTH PROBE



##### LOAD BALANCING RULES

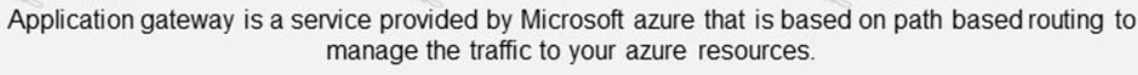


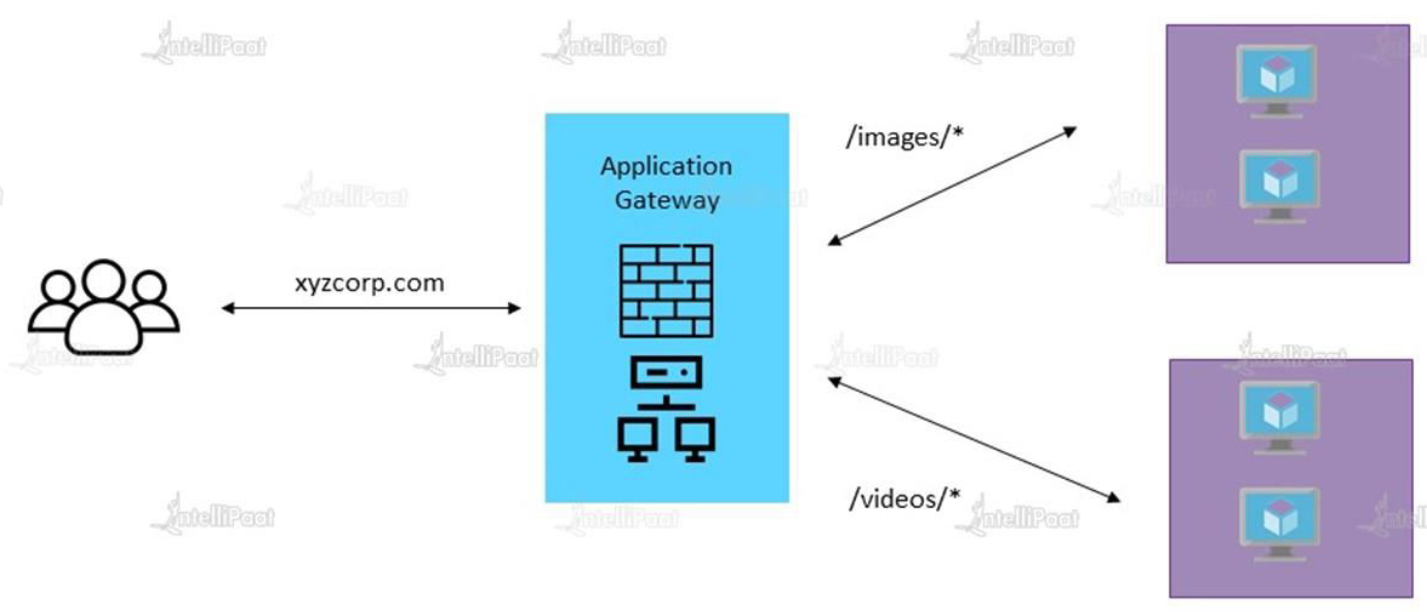
##### ACCESSING THE APPLICATION USING LB PUBLIC IP

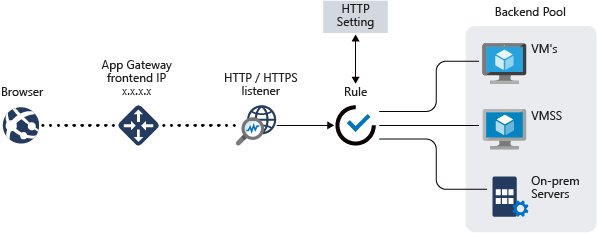


### NAT RULES (NETWORK ADDRESS TRANSLATION) LOAD BALANCER

## AZURE APPLICATION GATEWAY







### FEATURES OF APPLICATION GATEWAY

|  |  |
| --- | --- |
| URL BASED ROUTING | Routing of traffic to backend server pools based on URL path requests |
| WEB APPLICATION FIREWALL | Service provided by application gateway that serves as centralized protection of the web application from general vunerabilities |
| CUSTOM ERROR PAGE | Custom Error page may be created here instead of showing the default Microsoft Error Page  They are supported for following scenarios   1. Maintenance Page – Custom error is sent instead of 502 bad page 2. Unauthorized Access Page – Error page is sent instead of a 403 unauthorized access page |
| SECURE SOCKET LAYER TERMINATION | Application gateway provides a service for a traffic to flow encrypted to the backend servers, this is by supporting SSL / TLS termination at the gatway |

Reference : <https://learn.microsoft.com/en-us/azure/application-gateway/features>

* Application gateway do the load balancing of the traffic at the OSI Layer 7. (Application layer of OSI model)

USECASE – HOW APPLICATION GATEWAY MANAGE THE TRAFFIC

* When the end users hit the application gateway service via a front-end IP address. We can then create different listeners and different rules to route traffic on two different back and endpoints like a web application running on a virtual machine.or on an on premise server. All those endpoints are part of a back-end pool.
* When we are deploy the application gateway It's important to have an empty subnet as part of your virtual network.
* So remember that when you want to deploy an application Gateway onto Azure, the application gateway
* service will actually be deployed onto virtual network. In that virtual network you need to have at least
* one empty subnet to deploy
* the instances of the application Gateway itself.
* Now another feature of the application Gateway is that you can also enable something known as a web
* application firewall.
* So if you want to ensure that you have a firewall service in place.
* So remember if you have web applications running as part of your back end pool they can be exposed to
* attacks from the Internet.
* So let's say if someone is trying to cross site scripting attack for your web application.
* Well all of these can be denied when you enable the web application firewall has part of the application
* Gateway instance.
* Now another important feature that's actually available has part of the application.
* Gateway is the ability to road traffic based on what is the you order of the request itself.
* So remember since the application Gateway lured by this traffic based on layer 7 that's the application
* layer you can actually look at the request itself and then direct the traffic based on the request.
* So let's say a user is making a request on the card portal hop dot com and you're basically having this
* application running on your watch the machines.
* Now let's say that as part of your application you have one washing machine that may be responsible
* for processing images that are uploaded by the users and maybe you are under the watch of a machine
* that's responsible for processing the videos which are uploaded by your users.
* And let's say that depending upon whether it's an image or whether it's a video.
* So remember that your application will have different let's say you orders for processing the images
* and the videos you want those requests to go on a different works and machines.
* Well you can do that with the help of the application gateway.
* So you can actually see that if the request is going for images then make sure the request goes on to
* a washing machine in one back and pool.
* And if it's for videos it can go on to another virtual machine which is part of another back and pool.
* So because the application gave you a walk has it at the application layer it has the added advantage
* of routing requests based on the order itself.
* So going into the application gateway service.
* So this is a web traffic load balancer that can be used to separate traffic onto web applications not
* the web applications can reside.
* You don't watch on machines on what the machine skill sets or even on your on premise service.
* And the application BP is and always say yes 7 load balancer it also has support for secure sockets
* layer termination.
* So here the request of the application Gateway can be secure in nature and then the requests can then
* go on to go back and pool resources in an encrypted fashion.
* So what happens over here is that your application deeply manages the SSL for you.
* So the communication from the client to the application Gateway can be made secure with the help of
* SSL so this can lift the burden off the back and pull for decrypting requests.
* So if you have to have SSL working on your watch on machines they need extra ICP utilization just to
* ensure that it decrypt all of the communication from the client whereas all of this button can actually
* be done by the application gateway service itself so the decryption of requests can be left over onto
* the application source
* no good order enable order scaling for application Gateway resource.
* So this allows the application Gateway resource itself to be scaled up was killed out based on load
* patterns.
* So if the load increases your application gateway service or resource would increase accordingly you
* can also enable the web application firewall feature for the application gateway to source you can also
* enable session affinity which allows a user session to be directed onto the same server for processing.
* So in the state of these session is stored on the solar then this can be a useful feature know the different
* components of the application KP.
* So first you have the front end IP address so users will actually hit the application gaping via the
* front end IP address.
* You can have the listener.
* So this is a logical entity that takes for the incoming connection requests.
* Now there can be multiple listeners attached to the application gateway.
* There are two types of listener configurations you first have the basic.
* So here that listener listens to to a single domain site and then you have the mighty site you're the
* listener mapped onto multiple domain sites within app routing rules.
* So this can be use allow traffic from the listener onto the backend pool are two types of routing rules.
* So you have the basics that your all the requests are order to the backend pool directly or your part
* base here.
* The requests are louder to the backend pool based on the you are in the request you can have your back
* and pool.
* So this can be network interface guards your two machine skill sets public or Internet IP addresses
* fully qualified domain names are back in such as the apps service you didn't have your help process
* so it defines how the application Gateway men want to the head of the resources in the backend pool.
* Is all important information when it comes to the OCO application catering service.