Microsoft Azure Load Balancer Training Course Content

Course Outline

In this course you will explore different types of load balancing solutions in Azure and their features. The demonstration video gives a walkthrough of creating the Azure Load Balancer.

After completing this course, you will be able to create and configure Load Balancers in Azure.

1. Module 1: Introduction to Load Balancing
    - Introduction
        - What is Load Balancing?
        - Different types of Load Balancers in Azure
    - Types of Load Balancers in Azure
        - Azure Load Balancer
        - Application Gateway
        - Azure Traffic Manager

2. Module 2: Load Balancers in Azure
    - Azure Load Balancer
        - Azure Load Balancer
    - Application Gateway
        - Application Gateway
        - Application Gateway features
    - Azure Traffic Manager
        - Azure Traffic Manager
        - Azure Traffic Manager features

3. Module 3: Hands On Labs
    - Azure Load Balancer
        - Creating Standard Azure Load Balancer

Module 1: Introduction to Load Balancing

What is Load Balancing?

Modern high-traffic websites serve hundreds of thousands of concurrent requests from users or clients and return the application data in fast and reliable manner. Multiple servers are added to the backend to meet this high volume of requests. These group servers are referred to as a Server Pools and the traffic is distributed between these servers using load balancers.

A load balancer routes the client requests across all servers capable of fulfilling the requests ensuring the maximum speed and utilization. It prevents any one server getting overloaded and affecting the performance. It keeps track of the health of the servers using health probes and redirects the traffic to healthy servers if any server goes down. When a new server is added to the server pool, the load balancer automatically starts sending requests to it.

Different types of Load Balancers in Azure

Azure has different load balancing services available as follows.

1. Azure Load Balancer:

   Load distribution, health probe and automatic traffic distribution on Scale Sets. Works for end points within the same region.
2. Application Gateway:

   SSL offloading, Web Application Firewall, HTTP/HTTPS based routing. Works for multiple region endpoints.
3. Azure Traffic Manager

   DNS based routing and routed to Global Azure region endpoints.

Module 2: Load Balancers in Azure

Azure Load Balancer:

The Azure Load balancer effectively distributes the web traffic to the backend server pool. The backend pool is used to route requests to the backend servers that serve the request. Load Balancer distributes inbound traffic that arrive at the load balancer's front end to backend pool instances. The backend pool instances can be Azure Virtual Machines or instances in a virtual machine scale set, Public IPs, Private Ips or Azure

Back end services. The balancing rules are configured, and health probe is set to route the flow.

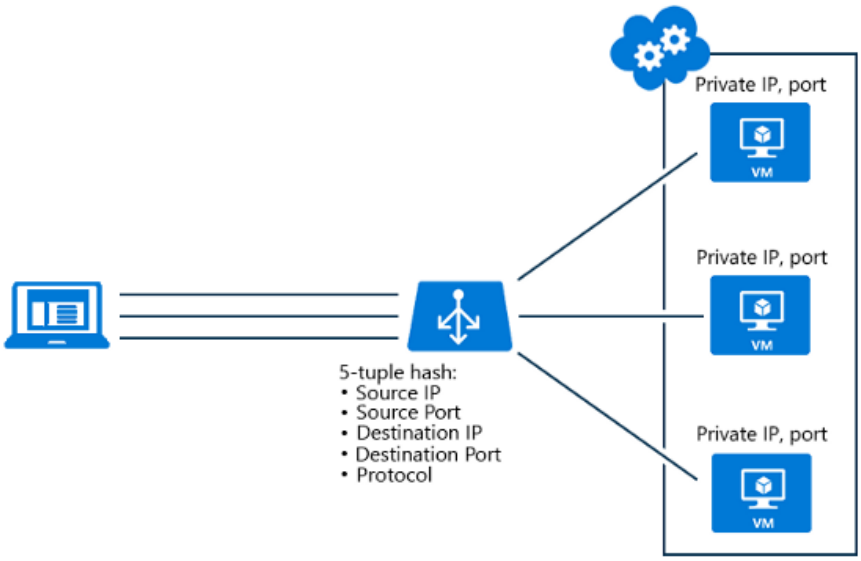

Image Source – Microsoft Docs

Azure load balancers operate at the transport layer (OSI layer 4 - TCP and UDP) and route traffic based on source IP address and port, to a destination IP address and port. Azure load balancer can distribute network traffic to endpoints in the same Azure region. It can be used to distribute internet traffic as well as internal traffic.

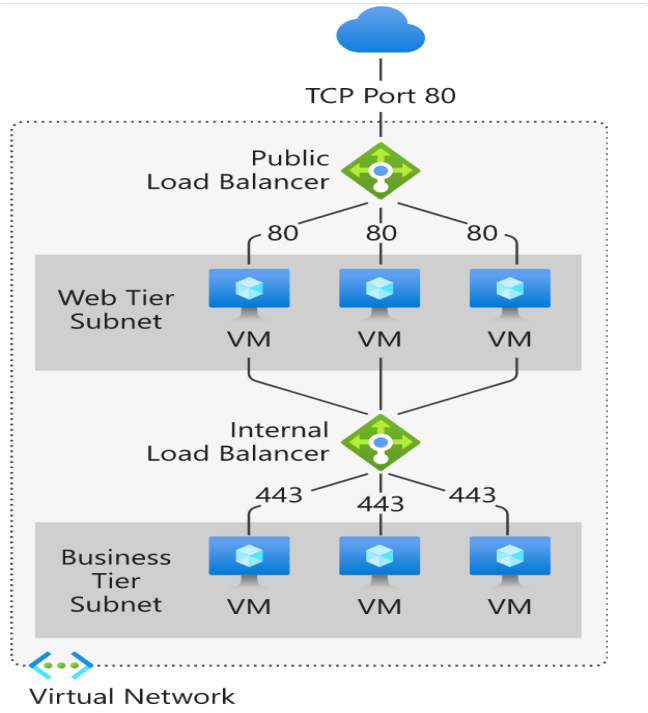

Image Source – Microsoft Docs

A *Public load balancer* 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.

An *Internal (or private)* load balancer 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.

Azure offers a Basic SKU and Standard SKU that have different functional, performance, security and health tracking capabilities.

Basic Load Balancer is open to the internet by default. The Load Balancing is limited to the same virtual network and resources in the same availability sets.

Standard Load Balancer is secure by default and is part of the virtual network. The virtual network is a private and isolated network. This means Standard Load Balancers and Standard Public IP addresses are closed to inbound flows unless opened by Network Security Groups. NSGs are used to explicitly permit allowed traffic. If you do not have an NSG on a subnet or NIC of your virtual machine resource, traffic is not allowed to reach this resource.

Key scenarios that you can accomplish using Standard Load Balancer include:

- Increase availability by distributing resources within and across zones.
- Configure outbound connectivity for Azure virtual machines.
- Use health probes to monitor load-balanced resources.
- Load balance services on multiple ports, multiple IP addresses, or both.
- Move internal and external load balancer resources across Azure regions.
- Load balance TCP and UDP flow on all ports simultaneously using HA ports.

Azure Application Gateway

Azure Application Gateway is a web traffic load balancer that enables you to manage traffic to your web applications.

Application Gateway gives you more control and rules how the web traffic is routed. We can make routing decisions based on additional HTTP/HTTPS headers, for example

URI path or host headers. The traffic can be routed based on the incoming URL. This type of routing is known as application layer (OSI layer 7) load balancing. Application Gateway also supports SSL offloading and Reverse Proxy. The WAF or the web application firewall integrated into the Azure Application Gateway secures web-based applications from session hijacks, cross-site scripting breaches, SQL injection, and common web attacks.

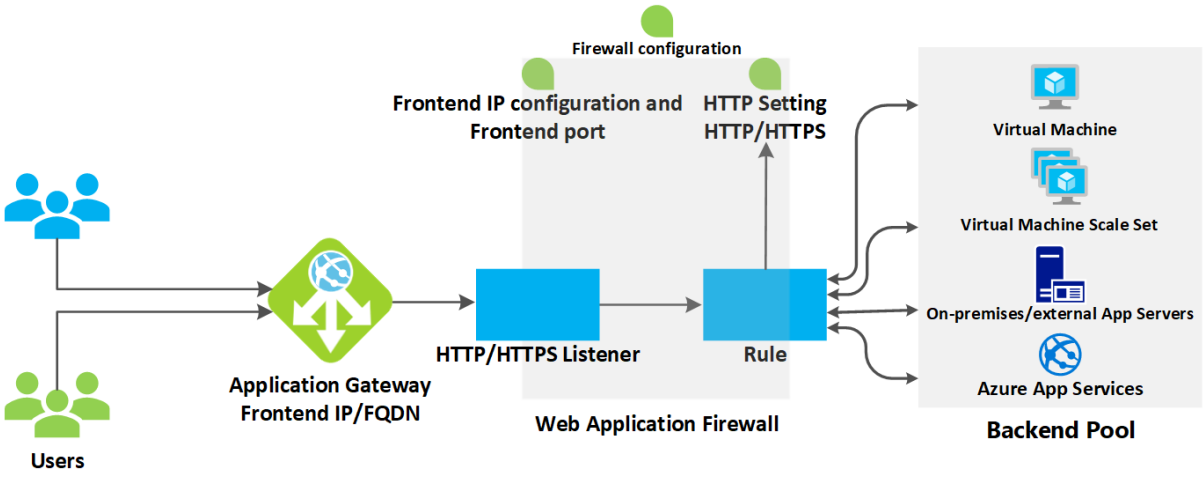

Image Source – Microsoft Docs

- Azure application gateway has the ability to automatically scale up and down the resources based on the traffic and load patterns.
- A single application gateway can be utilized for one or more applications.
- Application Gateway provides native support for the WebSocket and HTTP/2 protocols.

Azure Traffic Manager

Azure Traffic Manager is used when the endpoints are distributed over multiple regions in Azure. The traffic is distributed to services across global Azure regions, while providing high availability and responsiveness. The traffic can be routed to any endpoint that is any Internet-facing service hosted inside or outside of Azure. Traffic Manager uses DNS to direct clients to specific service endpoints based on the rules of the traffic-routing method. Clients connect to the selected endpoint directly. Traffic Manager is not a proxy or a gateway. Azure Traffic Manager doesn't work like Load Balancer or Application Gateway but routes the traffic just like DNS or performs policy-based routing as per the configured rules.

There are three types of endpoint supported by Traffic Manager:

- Azure endpoints are used for services hosted in Azure.
- External endpoints are used for IPv4/IPv6 addresses, FQDNs, or for services hosted outside Azure that can either be on-premises or with a different hosting provider.

- Nested endpoints are used to combine Traffic Manager profiles to create more flexible traffic-routing schemes to support the needs of larger, more complex deployments.

Azure Traffic Manager and Application Gateway can be deployed together for better availability and load balancing. Azure Traffic Manager can be used for redirection and the availability of incoming traffic to varied Application gateway resources at various regions, while the Application gateway deploys the layer 7 load balancing.

Azure Traffic Manager is used when the endpoints are distributed over multiple regions in Azure. The traffic is distributed to services across global Azure regions, while providing high availability and responsiveness.

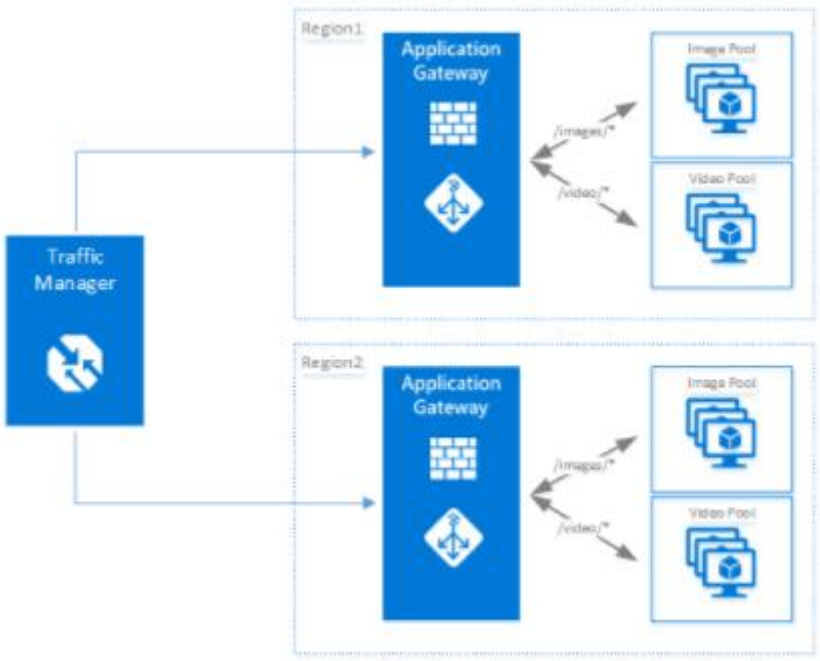

Image Source – Microsoft Docs

Module 3: Hands On Lab

The lab demonstrates the steps by step creation of Azure Load Balancer.
Azure Load Balancer includes a few key components. These components can be configured in your subscription via:

- Azure portal
- Azure CLI
- Azure PowerShell
- Resource Manager Templates

Frontend/Virtual IP address – This is the load balancer IP address that works as a front door to clients. After clients initiate connections to a frontend IP address, the traffic will be distributed to the back-end servers.

Server pool – The back-end application servers will be grouped together as a pool to serve an incoming request from a load balancer.

Rules – The incoming traffic will be distributed to the backend servers according to the rules defined in the load balancer.

Probes – The load balancer uses probes to detect the health of the back-end servers. If a back-end server is down, load balancer stops distributing traffic to the faulty server.

Inbound NAT rules – Inbound NAT rules define how the traffic is forwarded from the load balancer to the back-end server.

The Lab module can be downloaded from the Github location:
https://github.com/studioanomaa/Azure-Learning.git

https://github.com/studioanomaa/Azure-Learning/blob/Documents/Hands%20on%20Lab%20Module.pdf

The demo video is available in the following location:
https://drive.google.com/drive/folders/1uRMadRrWDg8hq6l--7NriBcrfCeh_sAZ?usp=sharing

Reference Links:

https://docs.microsoft.com/en-us/azure/load-balancer/

https://docs.microsoft.com/en-us/azure/virtual-network/quick-create-portal