



KodeKloud

© Copyright KodeKloud

Follow us on <https://kodekloud.com/> to learn more about us.



Administer Network Traffic

© Copyright KodeKloud

These Learn modules are part of the AZ-104: Configure and manage virtual networks for Azure administrators (<https://docs.microsoft.com/learn/paths/az-104-manage-virtual-networks/>) learning path.

Learning Objectives

- 01 Configure Azure Load Balancer
- 02 Configure Azure Application Gateways
- 03 Configure Network Watcher

© Copyright KodeKloud

Module overview



Azure Load Balancer

© Copyright KodeKloud

- A repeatable way to deliver software and infrastructure code to its destination
- Build and test code
- Deploy to on-prem or cloud resources
- CI/CD isn't just for software developers. It's also for infrastructure pros

Azure Load Balancer



Azure Load Balancer is a Layer-4 load balancer, which supports Azure Virtual Machines and Azure Virtual Machine Scale Sets as backend



Load Balancer is offered in two SKUs: Standard and Basic



It supports all TCP/UDP protocols



Security is managed with the help of Network Security Groups



Load Balancer SKU

Basic Load Balancer

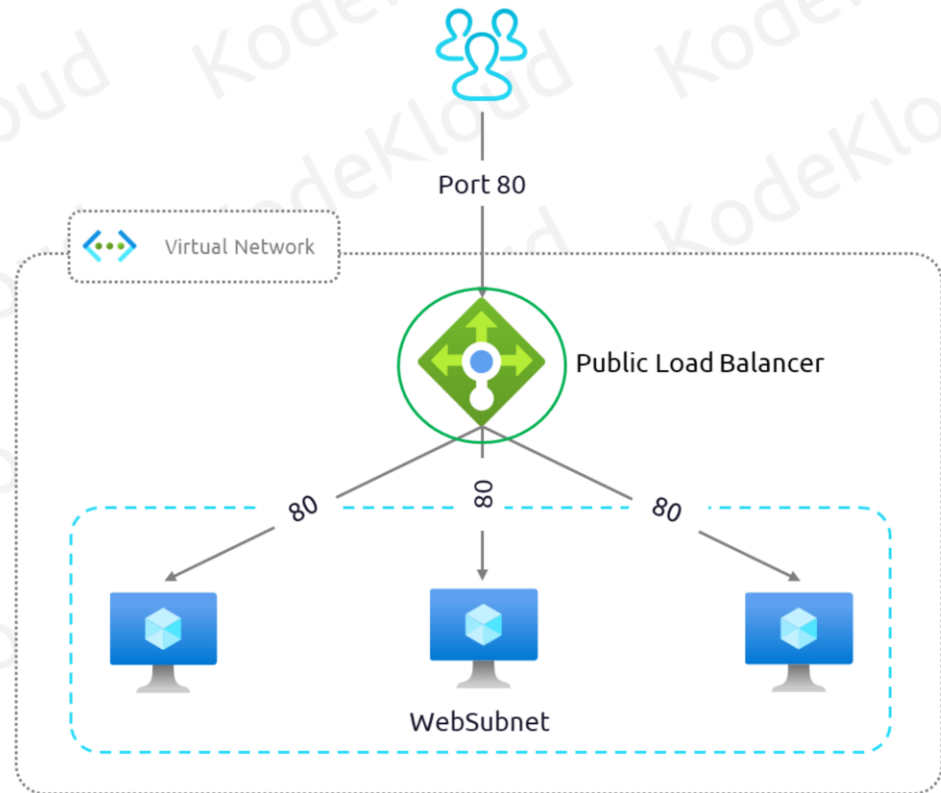


Standard Load Balancer



Feature	Basic	Standard
Backend pool size	Up to 300 instances	Up to 1000 instances
Health probes	TCP, HTTP	TCP, HTTP, HTTPS
Redundancy	Not available	Zone redundant and zonal redundant
Multiple frontend	Inbound only	Inbound and outbound
Security	Open by default. NSG is optional	Closed, unless traffic is allowed by NSG
SLA	Not applicable	99.99%

Public Load Balancer



© Copyright KodeKloud

Ideal for public facing workloads

- Public load balancer will have public IP address
- Incoming traffic's public IP address and port number will be mapped to the private IP address and port number of the

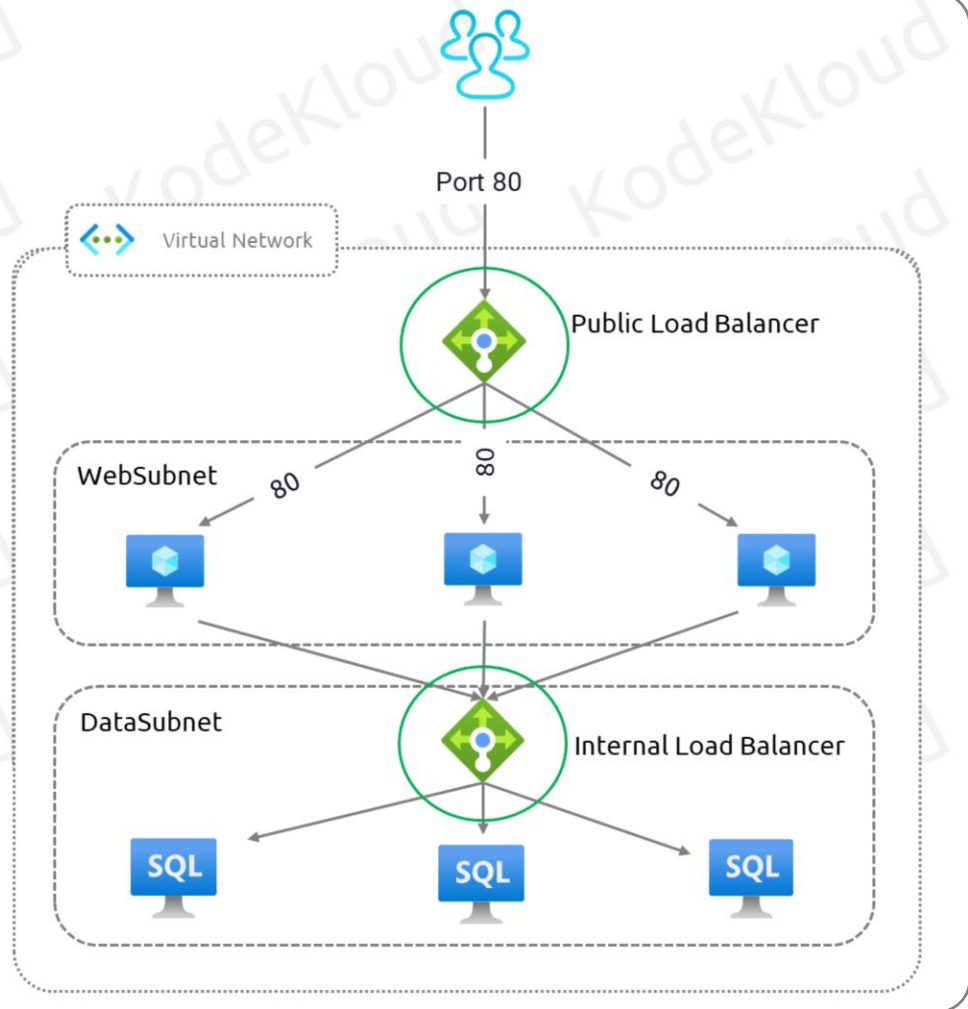
backend servers.

- With the help of load balancing rules, we can distribute the traffic across backend servers.
- Used in all public facing workloads which require load balancing.

Internal Load Balancer



Ideal for internal workloads



© Copyright KodeKloud

Ideal for internal workloads

- Internal load balancer doesn't have public IP address as frontend
- Incoming traffic inside the virtual network or from a VPN can be distributed across the backend servers

- This load balancer is never exposed to the internet, so the IP addresses and port numbers are not visible to the internet.
- Used in internal resources that needs to be accessed from Azure or on-premises via VPN connection.



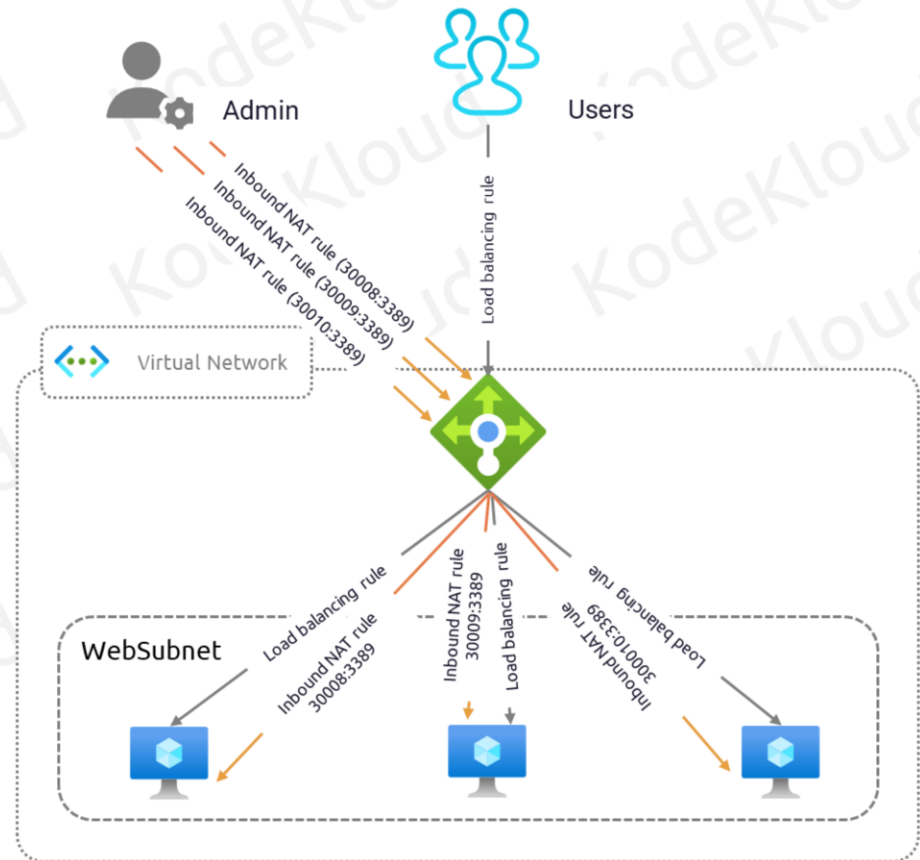
Azure Load Balancer Rules

© Copyright KodeKloud

- A repeatable way to deliver software and infrastructure code to its destination
- Build and test code
- Deploy to on-prem or cloud resources
- CI/CD isn't just for software developers. It's also for infrastructure pros

Load Balancer Rules

- Load balancing rules
- Inbound NAT rules
- Outbound rule



© Copyright KodeKloud

Load balancing rules

The incoming traffic to backend pools is distributed with the help of load balancing rules. We can create frontend IP to backend IP port mapping and the traffic is distributed accordingly.

Inbound NAT rules

Instead of backend pool, we can target a specific virtual machine and create a NAT rule. Frontend IP and port combination

is used to send traffic to IP and port of the designated VM.

Outbound rule

Allows instances in the backend pool to communicate to the Internet and other endpoint.

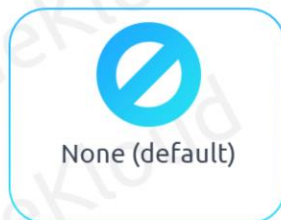


Session Persistence

© Copyright KodeKloud

- A repeatable way to deliver software and infrastructure code to its destination
- Build and test code
- Deploy to on-prem or cloud resources
- CI/CD isn't just for software developers. It's also for infrastructure pros

Session Persistence



Session persistence ⓘ
None
None
Client IP
Client IP and protocol

None (default)

Request will be routed based on a 5-tuple hash. Five tuple comprises of Source IP, Source Port, Destination IP, Destination port, and Protocol. Requests can be handled by any VM and the chances of getting a new VM for every session is very high.

Client IP

Client IP is called two-tuple where the hash of source IP and destination IP is used to route the traffic. Requests will be

handled by the same VM if the source IP or destination IP doesn't change.

Client IP and protocol

This is also called as three-tuple hash, where the hash of source IP, destination IP and protocol is used to route the traffic to the VM. Requests coming from same IP and protocol will be handled by the same VM.

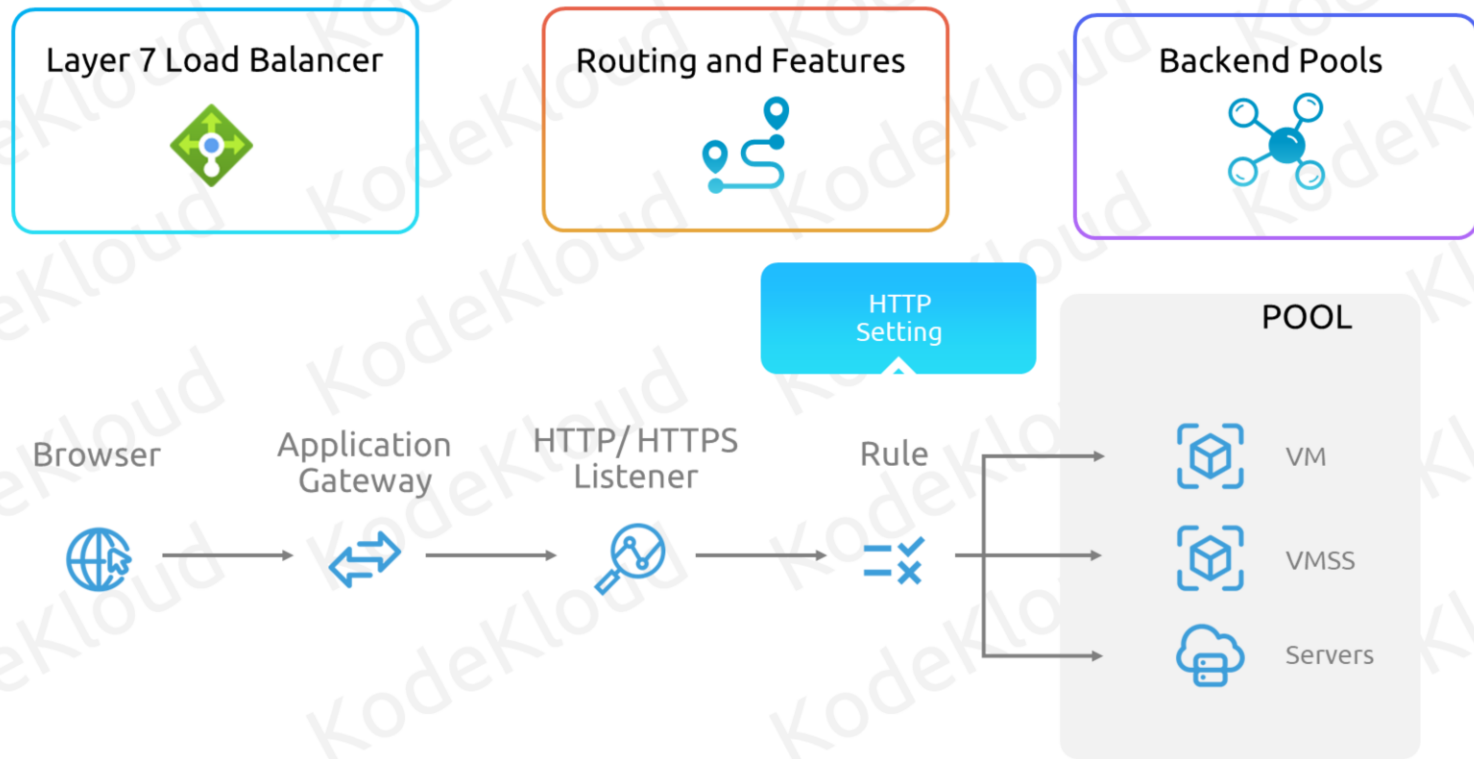


Azure Application Gateway

© Copyright KodeKloud

- A repeatable way to deliver software and infrastructure code to its destination
- Build and test code
- Deploy to on-prem or cloud resources
- CI/CD isn't just for software developers. It's also for infrastructure pros

Application Gateway



© Copyright KodeKloud

Layer 7 Load Balancer : Manages HTTP, HTTPS, HTTP/2, and WebSocket requests. Requests will be routed to the backend pool. Web Application Firewall can be added to Application Gateway as an option component.

Routing and features : Requests can be routed to the backend pool based on URL also known as path-based routing. Also, we can host multiple sites behind an application gateway. Features includes URL Redirect, SSL termination, Rewrite HTTP headers and Custom error pages.

Backend pools The web servers can be hosted in Azure Virtual Machines, Azure Virtual Machine Scale Sets, Azure App Services, and even on-premises servers.

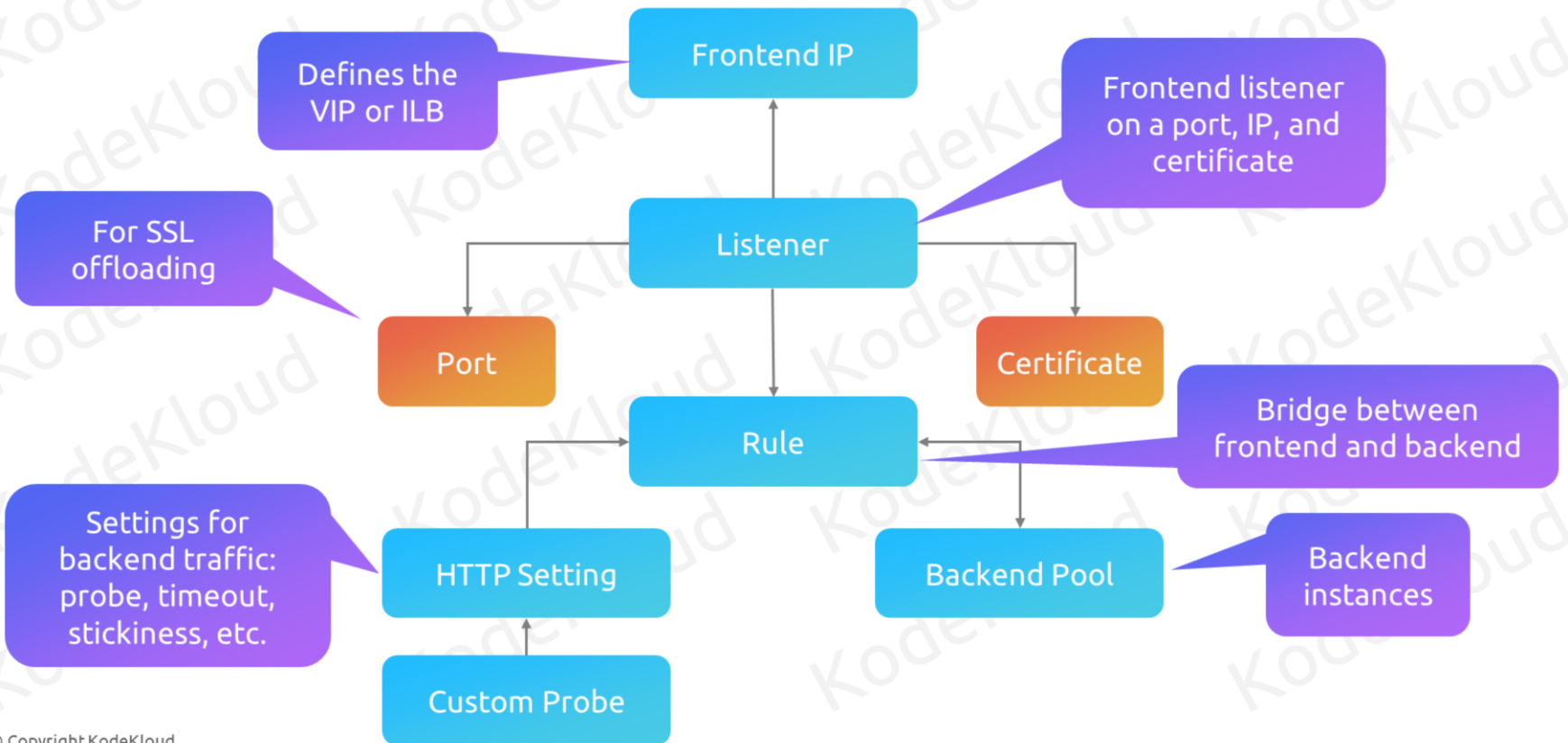


Azure Application Gateway Components

© Copyright KodeKloud

- A repeatable way to deliver software and infrastructure code to its destination
- Build and test code
- Deploy to on-prem or cloud resources
- CI/CD isn't just for software developers. It's also for infrastructure pros

Application Gateway – Components



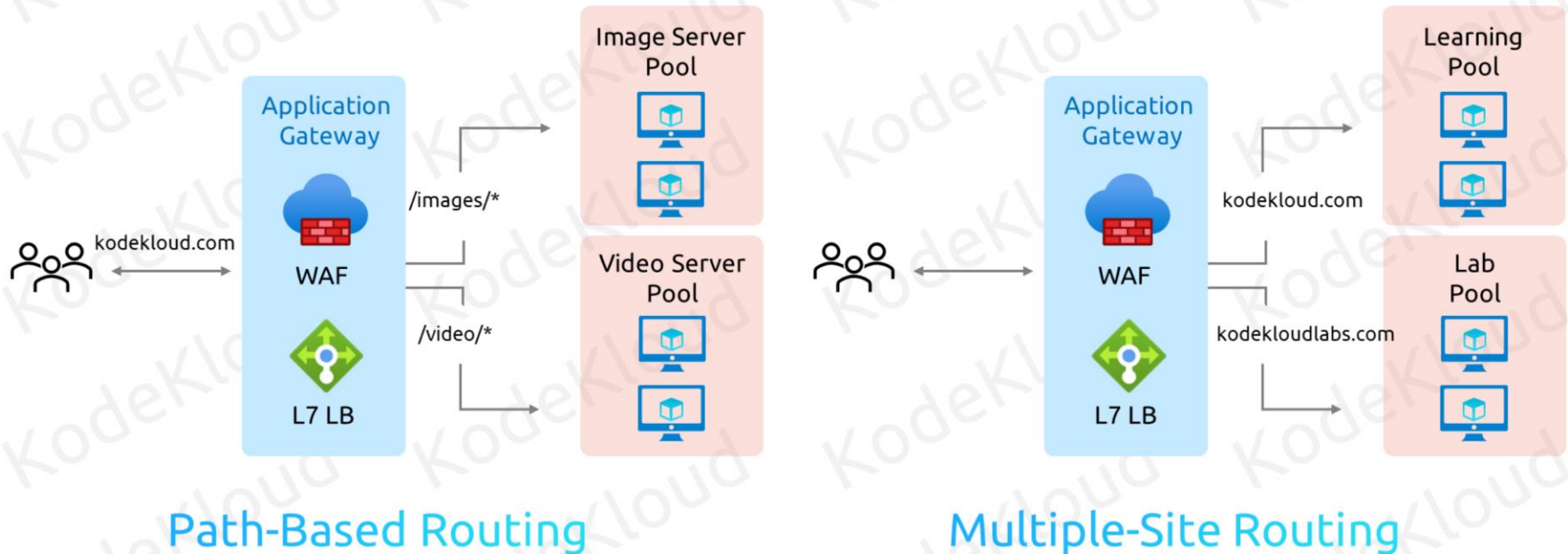


Azure Application Gateway Routing Rules

© Copyright KodeKloud

- A repeatable way to deliver software and infrastructure code to its destination
- Build and test code
- Deploy to on-prem or cloud resources
- CI/CD isn't just for software developers. It's also for infrastructure pros

Application Gateway – Routing Rules



© Copyright KodeKloud

Path based routing: Based on the path in the URL, we can route the request to different backend pools. Ideal for routing requests to different backend pools optimized for different paths.

Multiple-site routing: Multiple sites can be hosted behind a single application gateway. Based on the domain, the request can be routed to the backend pool hosting the requested domain.



Other Load Balancing Solutions

© Copyright KodeKloud

- A repeatable way to deliver software and infrastructure code to its destination
- Build and test code
- Deploy to on-prem or cloud resources
- CI/CD isn't just for software developers. It's also for infrastructure pros

Other Load Balancing Solutions

Azure Front Door



Azure Traffic Manager



© Copyright KodeKloud

Azure Front Door

Modern CDN solution that provides reliable, fast content delivery . Azure Front Door is a global solution which leverages the Microsoft's global edge network with hundreds of global and local point-of-presence locations. These endpoints are distributed across the globe and closer to your customers.

We can deploy our solutions in multiple regions and load balance using the Azure Front Door. Path based routing and

multiple-site routing is available.

Web Application Firewall can be added as an optional component.

Azure Traffic Manager

ATM or Azure Traffic Manager is a DNS based load balancer. Traffic coming to your public facing applications can be distributed across the globe with the help of ATM.

As this is a DNS load balancer, it uses DNS to direct the client request to an endpoint based on the routing rule we configure. Traffic Manager finds the best endpoint for you based on the routing and returns a DNS response with the endpoint name. Client then directly reaches out to the endpoint.

ATM can be used with the public facing services deployed in Azure or non-Azure environments. Routing methods includes Priority, Weighted, Geography, Performance and Nested Profile.

Comparing Load Balancing Solutions

Feature	Application Gateway	Front Door	Load Balancer	Traffic Manager
Usage	Optimize delivery from application server farms while increasing application security with web application firewall.	Scalable, security-enhanced delivery point for global, micro service-based web applications.	Balance inbound and outbound connections and requests to your applications or server endpoints.	Distribute traffic optimally to services across global Azure regions, while providing high availability and responsiveness.
Protocols	HTTP, HTTPS, HTTP2	HTTP, HTTPS, HTTP2	TCP, UDP	Any
Internal support	Yes		Yes	
Cross Region	No	Yes	Preview	Yes
Environment	Azure, non-Azure cloud, on premises	Azure, non-Azure cloud, on premises	Azure	Azure, non-Azure cloud, on premises
Security	WAF	WAF, NSG	NSG	-

[Reference architecture examples](#)










Network Watcher

© Copyright KodeKloud





- A repeatable way to deliver software and infrastructure code to its destination
- Build and test code
- Deploy to on-prem or cloud resources
- CI/CD isn't just for software developers. It's also for infrastructure pros

Network Watcher




Network diagnostic tools

-  IP flow verify
-  NSG diagnostic
-  Next hop
-  Effective security rules
-  VPN troubleshoot
-  Packet capture
-  Connection troubleshoot

Monitoring

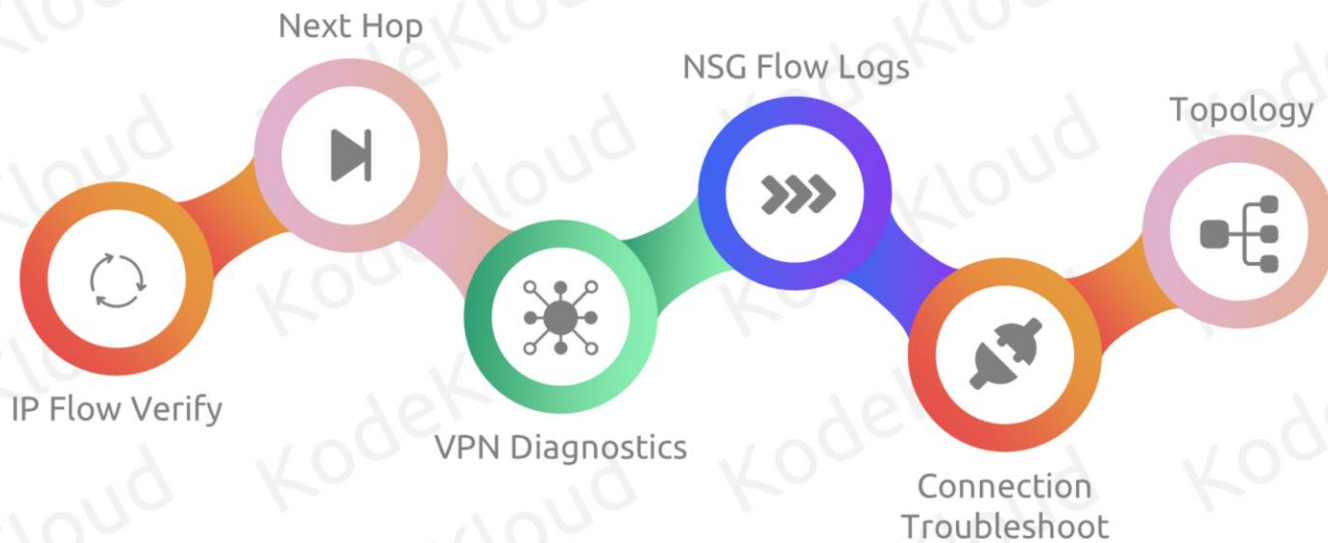
-  Topology
-  Connection monitor (classic)
-  Connection monitor
-  Network Performance Monitor

Logs

-  NSG flow logs
-  Diagnostic logs
-  Traffic Analytics

Network Watcher is a regional service that can be used to diagnose, monitor, and setup logging for resources that are deployed in Azure Virtual Network

Network Watcher



© Copyright KodeKloud

IP Flow verify is used to verify inbound and outbound connectivity from or to a VM from a remote IP address

Next hop is used to identify the next destination the traffic will be routed to.

VPN diagnostics will help you diagnose VPN connectivity issues and troubleshoot them.

NSG Flow Logs will store the details of the traffic through an NSG in a storage account.

Connectionn troubleshoot can be used to identify network performance and connectivity issues

Topology can be used to see the topology of your Azure infrastructure.



KodeKloud

© Copyright KodeKloud

Follow us on <https://kodekloud.com/> to learn more about us.